■「政府情報システムのためのセキュリティ評価制度(ISMAP)における各種基準(案)」に対する意見公募　御意見に対する考え方

整理番号	関連文書	御意見の概要	御意見に対する考え方
1	制度全般	そもそも、セキュリティ関連の下請けや製品が中国共産党政府のスパイが入り込んでおり、スパイ防止法などアメリカ政府を見習い運用していかなければならない。	様々なクラウドサービスが存在する中で、各政府機関においては、その利用目的や業務の性質に照らして、リスクに応じてサービスの性質を見極めながら利用する必要があります。係る観点から、サービスの利用に当たって海外の法令が適用される場合のリスク等について、クラウド事業者から情報開示を求めることで、個別の情報システムの調達の際に、当該システムの性質に応じて、調達者が適切にサービスの利用を判断することに資するようにしたいと考えております。 その上で、各府省庁におけるリスク評価等の結果、必要に応じて、本制度の管理基準に加えて追加的対策の確認を行って頂くことは妨げられるものではありません。 また、本制度においては、申請者に対して、「IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」（平成30年12月10日関係省庁申合せ）の運用への協力を求めており、当該申合せにおいては、サプライチェーン・リスクの観点から必要な場合において、各省庁等は、情報通信技術（IT）総合戦略室及び内閣サイバーセキュリティセンターに対して、講ずべき必要な措置について、原則、助言を求めることとしております。
2	制度全般	「サイバーセキュリティー対策」が重要な構造と、私し個人は思います。例えばですが、「センサー技術、 ネットワーク技術、デバイス技術」から成る「CPS（サイバーフィジカルシステム）」の導入により、「ゼネコン（土木及び建築）、 船舶、鉄道、航空機、自動車、産業機器、家電」等が融合される構造と、私は考えます。具体的には、「電波規格（エレクトロリカルウェーブスペック）」及び「通信規格（トランスミッションスペック）」での「回線（サーキット）」の事例が有ります。（ア）「通信衛星回線（サテライトシステム）」における「トランスポンダー（中継器）」から成る「ファンクションオード（チャンネルコード及びソースコード）」のポート通信での「DFS（ダイナミックフレカンシーセレクション）」の構造。（イ）「電話回線（テレコミュニケーション）」における基地局制御サーバーから成る「SIP サーバー（セッションイニテーションプロトコル）」の構造。（ウ）「インターネット回線（ブロードバンド）」におけるISPサーバーから成る「DNSサーバー（ドメインネイムシステム）」の構造。（エ）「テレビ回線（ブロードキャスト）」における「通信衛星回線、電話回線、インターネット回線」の構造。具体的には、「方式（システムスペック）」での「回線（サーキット）」の事例が有ります。（ア）「3G（第3世代）」における「GPS（グローバルポジショニングシステム）」から成る「3GPP方式（GSM方式及びW-CDMA方式）」の構造。（イ）「4G（第4世代）」における「LTE方式（ロングタームエボリューション）」から成る「Wi-Fi（ワイアーレスローカルエリアネットワーキング）」の構造。（ウ）「5G（第5世代）」での「NR（New Radio）」における「MCA方式（マルチチャンネルアクセス）」から成る「DFS（ダイナミックフレカンシーセレクション）」の構造。具体的には、「情報技術（IT）」及び「人工知能（AI）」での「回線（サーキット）」の事例が有ります。（ア）クラウドコンピューティングでは、「ビッグデータ（BD）」から成る「データーベース（DB）」の導入により、ITネットワークの構造。例えばですが、ファイアーウォールにおける強化では、ルーターとスイッチを挟み込む様に導入する事で、「クラウド側（プロバイダー側）←ルーター⇔ファイアーウォール⇔スイッチ→エッジ側（ユーザー側）」を融合する事で、ハードウェアーの強化の構造。（イ）エッジコンピューティングでは、Web上における「URL（ユ ニフォームリソースロケーター）」での「HTML（ハイパーテキストマークアップラングエッジ）」から成る「API（アプリケーションプログラミングインタフェース）」に導入により、「HTTP 通信（ハイパーテキストトランスファープロトコル）」における暗号化によるソフトウェアーでの「HTTPS（HTTP over SSL/TLS）」の融合により、AIネットワークの構造。具体的には、「サイバー空間（情報空間）」及び「フィジカル空間（物理空間）」での「回線（サーキット）」の事例が有ります。（ア）「サイバー空間（情報空間）」では、「SDN/NFV」における「仮想化サーバー（メールサーバー、Web サーバー、FTP サーバー、ファイルサーバー）」から成る「リレーポイント（中継点）」での「VPN（バーチャルプライベートネットワーク）」が主流な構造。（イ）「フィジカル空間（物理空間）」では、「AP（アクセスポイント）」が主流な構造。要約すると、「ボット（機械における自動的に実行する状態）」による「DoS攻撃」及び「DDoS攻撃」でのマルウェアーにおける「C＆Cサーバー（コマンド及びコントロール）」では、「LG-WAN（ローカルガーブメントワイドエリアネットワーク）」を導入した「EC（電子商取引）」の場合では、クラウドコンピューティング及びエッジコンピーティングにおける「NTP（ネットワークタイムプロトコル）」の場合では、「検知（ディテクション）⇒分析（アナライズ）⇒対処（リアクションメソッド）」での「サイバーセキュリティー対策」が重要と、私は考えます。	本制度における各種基準等の案への御意見ではないと認識しておりますが、御意見は拝聴いたしました。
3	制度全般	政府のシステムには、中国製の製品を使わないでください。 バックドアが仕掛けられていて、政府の情報が中国政府に取られてしまうかもしれないからです。	様々なクラウドサービスが存在する中で、各政府機関においては、その利用目的や業務の性質に照らして、リスクに応じてサービスの性質を見極めながら利用する必要があります。係る観点から、サービスの利用に当たって海外の法令が適用される場合のリスク等について、クラウド事業者から情報開示を求めることで、個別の情報システムの調達の際に、当該システムの性質に応じて、調達者が適切にサービスの利用を判断することに資するようにしたいと考えております。 その上で、各府省庁におけるリスク評価等の結果、必要に応じて、本制度の管理基準に加えて追加的対策の確認を行って頂くことは妨げられるものではありません。 また、本制度においては、申請者に対して、「IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」（平成30年12月10日関係省庁申合せ）の運用への協力を求めており、当該申合せにおいては、サプライチェーン・リスクの観点から必要な場合において、各省庁等は、情報通信技術（IT）総合戦略室及び内閣サイバーセキュリティセンターに対して、講ずべき必要な措置について、原則、助言を求めることとしております。
4	ISMAP管理基準	１　クラウドサービスの安全性評価に関する検討会とりまとめ案のパブリックコメント【案件番号：595219056】で、「可用性にかかわる、ＳＬＡや、通知等の内容について、稼働率やその条件等の指標（メトリクス）レベルの事項を、ISO/IEC 19086シリーズを活用して共通化し、管理策として追加が必要と考える。」とコメントを行った(整理番号８２)。ご回答には「管理基準においては、可用性や復旧についての要件を設定することを要件とする予定です。」とあった。しかしながら、ISMAP管理基準（案）を拝見したが、該当の記載を確認できなかったので、どの条項がご回答いただいた内容に該当するか教えていただきたい。記載がないのであれば、記載の追加を検討いただきたい。	御指摘の可用性や復旧に関する要件については、管理基準において、例えば、以下のとおり統制目標としての三桁管理策をクラウドサービス事業者に要求しています。 16.1.1 情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立する。 17.2.1 情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。 上記を踏まえつつ、個々のサービスの具体的なSLA等についてははサービスごとにそれぞれ設定され、調達府省庁等が確認をするものと想定しています。

5	ISMAPクラウドサービス登録規則	2　ISMAPクラウドサービス登録規則（案）についてのコメント 　第９章　情報セキュリティインシデント発生時の報告では、９．１項で、「登録者は、登録されている自身のクラウドサービスについて情報セキュリティインシデントが生じた場合、遅滞なく報告すること。」とされている。２０１９年８月のAWSのAZ障害や、１２月の日本電子計算のIaaS障害のような情報セキュリティインシデントは報告すべきと考えるが、報告すべきインシデントの基準の記載がないので、登録規則に追加を検討いただきたい。記載がないと、クラウドサービス事業者とクラウドサービス利用者の認識の齟齬が出ると考える。	いただいた御意見も踏まえて、インシデント報告を求めるのはどのような場合かが明らかとなるよう、FAQ等において例示を行うものとします。
6	ISMAP管理基準	「ISMAP 管理基準（案）」別紙3 1.3.14　消去(もしくは抹消)について 論理的消去の手法が、暗号化とその暗号鍵の管理（消去）に限定されていますが、上書消去も対象とすべきと考えます。 理由としては、「ISO/IEC 27040 ストレージのセキュリティ要件」において、暗号化を実装されたメディアであったとしても、利用終了時においては、データの完全消去が推奨されるためです。	御指摘の点については、利用者によるクラウドサービスの利用が終了される時点において、当該サービスを利用していた利用者のデータが消去されることを求めることから、論理的消去については、暗号化消去を対象としています。
7	ISMAP情報セキュリティ監査ガイドライン	１．Ｐ８　行番２３　"監査基準等に準拠している旨"⇒準拠した基準も明示するように求めた方がよいのでは。	御指摘の点につきましては、1.1 本ガイドラインの目的において、「情報セキュリティ監査基準、 本ガイドライン及び標準監査手続（以下、「監査基準等」という。）」と記載しており、原案のままとさせていただきます。
8	ISMAP情報セキュリティ監査ガイドライン	２．同頁　行番３８－３９　"ISMAP運用支援機関のみにみに配布"⇒単純な誤字です。訂正をお願いします。	御指摘を踏まえ、修正致しました。
9	制度全般	GAFAなどの特定メガクラウド事業者のデータロックインによる国民および日本企業の不利益を防ぐ為に、該当クラウドサービスのプラットフォームからメタデータ含めマスタデータの切り離し、暗号キーの切り離しを可能とするハイブリッド型クラウド構成の準拠を求めます。 AWSなど一部SaaSやPaaSなどサービスプラットフォームと顧客データの切り離しを認めていないサービスに関しては、厳しく規制して欲しい。 顧客データの他クラウドプラットフォームへの実質移動制限となっている多額の課金モデルへの規制も行って欲しい。	御指摘の点については、ISMAP管理基準の10.1.1.9及び10.1.2.20において、クラウドサービス事業者に対し、利用者が暗号技術を利用する機能又は利用する環境についての情報を提供することや、暗号鍵を利用者が管理する機能や暗号鍵を管理する方法についての情報を提供することを基本言明要件として求めており、暗号技術を活用して利用者がデータを保護し、かつ消去することを可能たらしめることをクラウドサービス事業者に要求しております。 また、他のプラットフォームへの移動制限となる課金モデルの規制の是非については、クラウドサービスの安全性の評価を行う本制度のスコープ外と考えます。
10	ISMAP基本規程	■「基本規定1.4.1 クラウドサービス」はサービスの範囲がCSPの任意で決められる定義となっており、最悪全てのサービスを一つのサービスとして審査を受けることも考えられる。例えば米国FedRAMPではAmazonは、連邦政府向けAWSとして218の認証をパスしている（民間向けAWSでは195のサービス）。最長でも数ヶ月以内に監査可能な範囲にサービスが定義されるようクラウドサービスの定義をもっと厳密にする必要がある。例えばCSPが料金を顧客へ請求する単位とするなどが考えられる。	御指摘の点について、ISMAP基本規程の定義は、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」及び「政府機関等の情報セキュリティ対策のための統一基準」において使用されている定義を活用したものです。他方、管理基準については、本制度において、クラウドサービスのセキュリティの要件を設定するにあたり、既存の基準との整合性を踏まえ、クラウド情報セキュリティ管理基準の定義を活用したものです。 その上で、SaaS/IaaS/PaaSそれぞれにおいて、本制度において提示しているクラウドサービスの定義に該当するものについては、政府機関等への納入を目指す限りにおいて、原則として共通の管理基準に適合したセキュリティ対策を実装し、登録や登録の更新をしていただく必要がございますが、サービスの特性上、原理的に特定の管理策についての具備が不可能と解される場合には、一定の例外措置を設けることとします。ただし、その場合においても、利用者による当該サービスの採否の判断に資するよう、当該管理策の具備が不可能である理由など関連する情報については、適切に利用者に対して開示を行うことが必要です。 なお本制度の登録の単位はクラウドサービス事業者による言明の範囲によることを前提としており、追加のサービスがすでに登録されているサービスと言明の対象範囲が異なる場合や、同様の統制の下に服していない場合には、別個のサービスとして監査や登録審査を受ける必要があります。
11	制度全般	■「セキュリティ評価制度基本規定7.4監査機関」もしくは「クラウドサービス登録規則６審査」のいずれかに監査法人に対して運営委員会もしくは運用支援機関が必要と認めた場合には監査調書の提出を求めることができるようにすべきである。監査報告書だけで審査の合否を決定することは実質的に不可能と思われる。また、監査報酬との兼ね合いで杜撰な監査が行われることを防ぐ意味でも監査調書を監査法人に求めることは監査法人への牽制となる。	御指摘を踏まえ、修正致しました。
12	制度全般	■制度全般について 民間監査会社に監査を委ねるスキームになっているが国が採用ずるクラウドサービス等には厳密なセキュリティが求められる。暗号化したとしても暗号鍵が一度中国のデータセンターを経由するなど（zoomに前科あり）暗号化自体が無意味にされるケースもあり、クラウドサービスで扱われる暗号鍵を含む全データがセキュアに扱われる必要がある。また、監査報酬がクラウド使用者に転嫁されることは自明であることから、IPAなどの政府系団体が、独法などと同じように将来的には無償で監査を行得るよう技術研鑽すべきである。	御指摘の点について、現在既に数多くのクラウドサービスが提供されている中で、制度発足後の監査のキャパシティを考えると、独立行政法人などの政府系団体のみで本制度の監査を行うのではなく、一定の基準をクリアした専門的な知見のある監査法人に監査を実施していただくスキームの方が機動的に監査のニーズに対応できると考えます。 その上で、監査法人については、ISMAP監査機関登録規則及びISMAP情報セキュリティ監査ガイドラインによって、登録及び監査の実施に関して適切なガバナンスをかけるほか、監査報酬についても、各クラウドサービス事業者によって採用する管理策を精査することで、低廉化が可能と考えます。 なお、御参考までに、米国の類似の制度であるFedRAMPも第三者による監査を活用したスキームになっています。

13	制度全般	政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することは、ユーザーが安心してクラウドを利用することを促進するものであり、大賛成です。 逆に言えば、その信頼性が重要になるため、クラウドサービス事業社の監査は定期的なモニタリングは必須とすべきです。そして、プライバシーマークと同じような認証マークの付与をすべきと考えます。 ※既に検討中であれば単なる老婆心としてご容赦を！ 制度としては、必要だし、是非前に進めてください。	本制度に登録されたクラウドサービスは、公表することとしておりますが、御意見につきましては、今後の制度運営の参考とさせていただきます。
14	制度全般	＜意見＞ サービスを利用する場合、データは、派生データを含め所有者の管理下に置くべきである。 ＜理由＞ 様々な情報がデータ化される現在においてデータは非常に重要な国家資源であることは明白であり、「データの消失」、「外部流出」、「第3者からの攻撃」を含めて様々なリスクから何かあっても守に抜く必要があるクラウドサービスでは、サービス業者が提供するデータ保護、暗号化を利用できるが下記リスクを払拭することができないためコンピューティングリソースはクラウドを利用してもストレージリソースはデータ所有者の管理下におくべきと考える ・データが存在する場所を含めて正しい状況の把握が困難 ・データ保護、暗号化といった各種技術をサービス業者がデータ所有者の了解なく変更できるリスク ・データに対して新たな管理要件が発生した時に対応できないリスク ・日本の法律が無効となる可能性（海外データセンタに知らない間にデータが移動するなどのリスク） ・ データおよび派生データを特定のサービス業者の管理下に保管すると、大容量データの移動がネックとなり他サービス業者での利用が困難になるリスク	クラウドサービスの利用にあたっては、調達側がその利用目的や業務の性質に照らして、リスクに応じてサービスの性質を見極めながら利用することが大前提であり、一律に派生データやストレージリソースを直接の管理下に置くことを位置づける必要はないと考えております。御指摘の点については、ISMAP管理基準の10.1.1.9及び10.1.2.20において、クラウドサービス事業者に対し、利用者が暗号技術を利用する機能又は利用する環境についての情報を提供することや、暗号鍵を利用者が管理する機能や暗号鍵を管理する方法についての情報を提供することを基本言明要件として求めており、暗号技術を活用して利用者がデータを保護し、かつ消去することを可能たらしめることをクラウドサービス事業者に要求しております。 また、ISMAPクラウドサービス登録規則の3.4(2)において、申請者はクラウドサービスで取り扱われる情報に対して国内法以外の法令が適用され、調達府省庁等が意図しないまま調達府省庁等の管理する情報にアクセスされ又は処理されるリスクに関する評価を行うために必要な情報を開示しなければならないこととされています。
15	ISMAP基本規程	意見1 ・該当箇所 政府情報システムのためのセキュリティ評価制度（ISMAP）基本規定（案）中、P1 23行目から28行目 1.4.1 クラウドサービス 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（平成30年6月7日各府省情報化統括責任者（CIO）連絡会議決定）の定義された、「事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの」をいう。の記述について。 ・意見 本記述が定義されている「政府情報システムにおけるクラウドサービスの利用に係る基本方針」において、SaaS及びIaaS/PaaSのクラウドサービスに関しては検討方針や利用方針、選定に関する基本方針が示されております。 しかしながら、このいずれにも属さないセキュリティ系のクラウドサービスが多く市場では提供されておりますが、その性質上SaaS及びIaaS/PaaSのクラウドサービスの基本方針に全てを当て嵌めて検討することは適切ではないと考えます。 この類のクラウドサービスについても本制度への登録が可能になるよう、管理基準項目からの例外等ご検討頂き、より明確に記載頂くか、あるいは、そういったセキュリティ系のクラウドサービスは本規定の対象外として、別指針を作成頂くことを意見として提出致します。 ・意見理由 クラウドサービスの一つの形態として、セキュリティ系のサービスをクラウド化する動きが顕著であり、EDR(Endpoint Detection and Response)、CASB(Cloud Access Security Broker)、SIG(Secure Internet Gateway)、SASE (Secure Access Service Edge)等がセキュリティ系のクラウドサービスが該当するかと存じます。 これらのセキュリティ系のクラウドサービスではその性質上、セキュリティ分析の必要性や検体情報等の扱い、暗号鍵の管理方法等でSaaS及びIaaS/PaaSのクラウドサービスとは大きく異なる点がございます。 セキュリティ系のクラウドサービスにおいても、優れたサービスが競争力のある費用で政府機関で活用出来るよう、検討頂く必要があると考えます。	御指摘の点について、ISMAP基本規程の定義は、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」及び「政府機関等の情報セキュリティ対策のための統一基準」において使用されている定義を活用したものです。他方、管理基準については、本制度において、クラウドサービスのセキュリティの要件を設定するにあたり、既存の基準との整合性を踏まえ、クラウド情報セキュリティ管理基準の定義を活用したものです。 その上で、SaaS/IaaS/PaaSそれぞれにおいて、本制度において提示しているクラウドサービスの定義に該当するものについては、政府機関等への納入を目指す限りにおいて、原則として共通の管理基準に適合したセキュリティ対策を実装し、登録や登録の更新をしていただく必要がございますが、サービスの特性上、原理的に特定の管理策についての具備が不可能と解される場合には、一定の例外措置を設けることとします。ただし、その場合においても、利用者による当該サービスの採否の判断に資するよう、当該管理策の具備が不可能である理由など関連する情報については、適切に利用者に対して開示を行うことが必要です。

16	ISMAP管理基準	意見2 ・該当箇所 ISMAP管理基準（案）中、P28 41及び42行目 「8.1.5.Pクラウドサービス事業者の領域上にあるクラウドサービス利用者の資産は、41 クラウドサービス利用の合意の終了時に、時期を失せずに返却または除去する。」の記述について。 ・意見内容 返却または除去するクラウドサービス利用者の資産の定義について確認させて下さい。 ・理由 クラウドサービス事業者が提供するサービスのうち、セキュリティ分析等を実施するサービスにおいては、クラウドサービス利用者より分析の為に送られた疑わしい検体やURL情報等が含まれます。 この類の情報に関しては資産という定義から外れ、当該利用者に限らず以後の対策の為に広く必要なものであり、返却または除去の対象ではない認識でおりますが、相違御座いませんでしょうか。	御指摘の点について、原則ユーザにとって情報資産に該当するものは返却または除去する必要がある情報資産となります。 サービスの特性上、原理的に特定の管理策についての具備が不可能と解される場合には、一定の例外措置を設けることとします。ただし、その場合においても、利用者による当該サービスの採否の判断に資するよう、当該管理策の具備が不可能である理由など関連する情報については、適切に利用者に対して開示を行うことが必要です。例えば、対象となるクラウドサービスが、そもそも情報資産をユーザ側から提供しそれに基づいて分析するようなサービスである場合、返却や除去にの扱いについてはユーザとプロバイダの契約に基づいてその扱いが決定されるべきものであり、上記の対象として解される可能性があると考えております。
17	ISMAP管理基準	意見3 ・該当箇所 ISMAP管理基準（案）中、P28 29行から36行に掛けての管理策8.1.2.7.PBについて ・意見内容 上記該当箇所に、下記の文章を追記されることを意見として提出致します。 (c)当該利用者が、情報の解析等を行うために資産をクラウドサービス事業者に提供する場合は、クラウドサービス事業者が記録媒体に記録する前に暗号化し、暗号鍵を管理し消去する機能 ・理由 一般的にセキュリティの解析等を行うサービスにおいては、当該利用者は解析に必要な情報をクラウドサービス事業者に提供し、その情報に基づいて、クラウドサービス事業者がリスク分析やアノマリ検知等の解析サービスを実施致します。その際に提供される情報は、解析に使用できるようクラウドサービス事業者がその内容を確認できる必要があります。よって、当該利用者が暗号鍵を管理し、当該利用者のみが内容を確認できる方式ではなく、クラウドサービス事象者において、当該利用者から提供された情報を管理し暗号鍵によって管理することが必要だと考えます。	御指摘の点について、本管理策においては、利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理する機能を提供し、または、当該利用者が暗号鍵を管理する方法についての情報を提供することを求めていますが、一方で、クラウドサービス事業者において鍵を管理できることを否定しておらず、10.1.1において事業者側による暗号化の取組を求めているため、原案のままとします。
18	ISMAP管理基準	意見4 ・該当箇所 ISMAP管理基準（案）中、P30 8行から11行に掛けての管理策9.4.1.8.PBについて ・意見内容 上記該当箇所において下記の通り、文章を修正されることを意見として提出致します。 9.4.1.8.PB クラウドサービス事業者は、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス、及びサービスにて保持されるクラウドサービス利用者のデータへのアクセスを、クラウドサービス利用者が制限できるよう、アクセス制御を提供する。また、このアクセス制御についてはユーザ認証等による制御も可とする。 ・理由 当該管理策の「アクセス制御」に求められる具体的な機能が解釈次第で異なることが懸念されますので、具体的な例を記載することにより、要件の内容が明確になるものと考えます。	御意見の件について、ユーザ認証等による制御も本管理策の対象に含まれると考えます。 御意見を踏まえ、今後予定をしておりますガイドライン等の作成時の参考とさせて頂きます。
19	ISMAP管理基準	意見5 ・該当箇所 ISMAP管理基準（案）中、P30 42行から45行に掛けての管理策10.1.2.20.PBについて ・意見内容 上記該当箇所において下記の通り、文章を修正されることを意見として提出致します。 10.1.2.20.PB クラウドサービス事業者は、クラウドサービス利用者に、当該利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理する機能を提供し、または、当該利用者が暗号鍵を管理する方法についての情報を提供する。ただし、当該利用者が、情報の解析等を行うために資産をクラウドサービス事業者に提供する場合は、暗号鍵をクラウドサービス事業者が管理する機能を提供する。 ・理由 一般的にセキュリティの解析等を行うサービスにおいては、当該利用者は解析に必要な情報をクラウドサービス事業者に提供し、その情報に基づいて、クラウドサービス事業者がリスク分析やアノマリ検知等の解析サービスを実施致します。その際に提供される情報は、解析に使用できるようクラウドサービス事業者がその内容を確認できる必要があります。よって、当該利用者が暗号鍵を管理し、当該利用者のみが内容を確認できる方式ではなく、クラウドサービス事象者において、当該利用者から提供された情報を管理し暗号鍵によって管理することが必要だと考えます。	御指摘の点について、本管理策においては、利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理する機能を提供し、または、当該利用者が暗号鍵を管理する方法についての情報を提供することを求めていますが、一方で、クラウドサービス事業者において鍵を管理できることを否定しておらず、10.1.1において事業者側による暗号化の取組を求めているため、原案のままとします。

20	ISMAP管理基準	意見6 ・該当箇所 ISMAP管理基準（案）中、P57 別表3管理策基準10.1.1.10.Pについて ・意見内容 下記の通り、文章を修正されることを意見として提出致します。 10.1.1.10.PB クラウドサービス事業者は、クラウドサービス利用者が独自の暗号による保護の適用を希望した場合、実装の可否について回答し、また実装が可能な場合はそれを支援するために必要な情報をクラウドサービス利用者に提供する。 ・理由 原文ではクラウドサービスにおいて、独自の暗号が適用可能な実装が必須かが不明瞭なため、明確に記述すべきと考えます。また、クラウドサービスが電子政府推奨暗号リスト記載の暗号を標準で実装している場合は、独自の暗号の利用は必須ではなく任意の実装とすることが妥当と考えます。 以上	御指摘の点については、管理策10.1.1.10.Pについては、基本言明要件でない管理策のため、実施については各クラウドサービス事業者の判断に委ねられることとなります。そのため、独自の暗号が適用可能な実装は、制度上の登録の観点からは必須項目ではありません。したがって原案のとおりとします。
21	ISMAP管理基準	ISMAP管理基準1.3.14の『消去』において、論理的消去が含まれている事は、素晴らしいと思います。実際に記載されている方法である、暗号化後に暗号鍵を消去し、元のデータの復号を不可能にする方法は、セキュリティを担保した消去の方法として有効だと考えますが、現時点では既に広く普及しているSSDやNVMe等の媒体での対応は限定的になるかと存じます。 そこで、選択肢の幅を広めるため、世界的にも広まっている基準：NIST SP800-88 rev.1に準拠した消去方法も追加頂く事をご検討ください。NIST SP800-88 rev.1にはSSD等のデータ消去方法に関する言及もございますが、技術の進歩を反映させたセキュアな消去方法の取り入れは、ISMAP管理基準においても必要かと存じます。 なお、NIST SP800-88 rev.1では、媒体のサニタイズについて機密性に応じてデータ消去レベルを3段階に分類しています。そのうちの最高レベルはDestroy(破壊)のため消去については2段階に分類されていることとなりますが、この分類を活用して機密性の高いデータについては高レベルのPurge(除去)以上を求めるが機密性の低いデータはErase(消去)で可とするなど、機密性とコストのバランスが確保可能なものとすることが望ましいと考えます。	御指摘の点について、ISMAP管理基準は、政府機関等の情報セキュリティ対策のための統一基準に規定されているデータの消去の方法を可能化するために、クラウドサービス事業者に対して求める要件を規定しております。 御指摘の点については、今後作成するガイドライン等や本制度のレベル１やレベル３の基準を検討する際の参考とさせていただきます。
22	ISMAP管理基準	ISMAP管理基準9.4.2.2.Bにおいて、生体認証が含まれている事は、素晴らしいと思います。なお、生体情報はセンシティブな情報であり、ユーザー側の懸念が想定されます。特に情報漏洩リスクに対し、生体認証情報を管理するシステムに対して、適切な情報管理が必要になるかと存じます。 そこで、生体情報がネットワークに流れない方式であるFIDO2も追加頂くことをご検討ください。FIDO2は、国際連合のICT専門機関であるITUの標準化機関の１つである国際電気通信連合の電気通信標準化部門（ITU-T）によって、国際標準と承認された規格になります。 また、FIDO2では、安全性と利便性の両立だけではなく、コスト面においても優れており、Windows HelloやAndroid 7+等主要デバイスのソフトウェアバージョンアップにより利用が可能になります。	御指摘の点について、FIDO2対応の認証デバイスを活用した認証も9.4.2.2の要件の範囲内と考えます。 御指摘の点については、今後作成するガイドライン等においてお示しすることも検討致します。
23	ISMAPクラウドサービス登録規則	(ISMAP クラウドサービス登録規則) ・政府情報システムを扱うのですから、当然外資が少しでも入っていれば排除されるべきで、また、役員も含めて全ての職員は日本国籍所有者に限定すべき。さもなくば、情報漏洩や情報操作のリスクが抑えられなくなります。(3.5に追加で明記すべき)	御指摘の点については、様々なクラウドサービスが存在する中で、各政府機関においては、その利用目的や業務の性質に照らして、リスクに応じてサービスの性質を見極めながら利用する必要があります。係る観点から、サービスの利用に当たって海外の法令が適用される場合のリスク等について、CSPから情報開示を求めることで、個別の情報システムの調達の際に、当該システムの性質に応じて、調達者が適切にサービスの利用を判断することに資するようにしたいと考えており、一律でいただいた御意見のような内容を基準として位置付けることは考えておりません。 その上で、各調達府省庁におけるリスク評価等の結果、必要に応じて、本制度の管理基準に加えて追加的対策の確認を行って頂くことは妨げられるものではありません。
24	ISMAP監査機関登録規則	(ISMAP 監査機関登録規則) ・3.1にて、外資が入った企業を排除する旨明記してください。 ・3.6および3.7において、日本国籍を有することを要件としていることは評価できますが、これはチームメンバー全てに適用すべき(3.8)です。さもなくば国益に反する活動阻止が徹底できなくなります。	御指摘の点については、クラウドサービスの監査には高度で専門的なスキルやノウハウが要求されます。一方で、我が国政府の情報システムに係るクラウドサービスの監査には安全保障上留意すべき点もあるのも事実であり、係る観点から、適格な監査主体の要件に関し、わが国において情報セキュリティ監査を業務として行っている法人とした上で、業務執行責任者と、業務実施者のうち現場責任者（チームマネジャー）の国籍要件として日本国籍を要求しておりますが、技術的知見などからやむを得ない場合には制度の実効性の観点から例外を認めることがあることとしています。なお、当面の間、監査実務の安定性等の観点から、監査法人を優先した審査を進める方針です。

25	ISMAP監査機関登録規則	「ISMAP監査機関登録規則」の「3.6.2 実務経験等」に「通算10年以上の外部監査の実務経験を有すること」との記載がありますが、この「通算10年」の考え方には、例えば (1)申請年月日を基準日として10年遡った同一日以前に1回でも監査実績があればよい (2)上記(1)の範囲内には、何らかの規定する間隔、回数以上の監査実績が必要 (3)上記(1)の範囲内で、途中の数年間は監査業務から離れていた期間があってもよい（離れても、監査の品質管理者等、関わりのある多くのパターンが考えられる）など、いろいろなパターンが考えられますし、(3)で言う「監査業務から離れていた」の解釈も、 (4)同一の会社に継続して所属していること (5)他社へ転職、転籍等、異動した場合で直接、監査業務をしていない場合は除外、もしくは、それも算入するなど (6)上記(4)や(5)があったものの元の監査業務に復帰した場合であっても、途中の空白期間は算入されない など多岐に渡ります。 これらのことより、ISMAP運営委員会にて都度、申請時に適切に資格要件の充足判断がなされ、通知されるものと考えてよろしいでしょうか。	「通算」と記載しているとおり、業務執行責任者の業務経験全体を通じて、情報セキュリティ監査基準に基づく監査、システム監査基準に基づく監査、あるいは、これらと同等と見なせる監査制度における外部監査の実務経験を要求するものとなります。また、登録審査においては、これらに関する過去の実績等をお示し頂き、要件を満たしていることを確認した上で登録を行うこととなります。
26	ISMAP基本規程	質問1 ●該当ページ：P.3　8行目 2.1 本制度に関する規程等 本制度に関する規程等は次のとおりとする。 ●意見内容/確認内容 2.1に本制度に関する規程が纏められておりますが、提示された規程類にISMAP運用支援機関が遵守しなければならない文書が提示されておりません。存在するのであればご教示下さい。	御指摘の点については、ISMAP運用支援機関はISMAP運営委員会からの委任を受けて業務を実施するものであり、ISMAP運営委員会や制度所管省庁と同様、2.1の規程類を遵守する義務を負います。
27	ISMAP基本規程	質問2 ●該当ページ：P.8　6行目 5.4 登録の一時停止又は削除 ISMAP 運営委員会は、モニタリング、再審査又は再監査の結果、ISMAP クラウドサービス登録規則又は ISMAP 監査機関登録規則に定めるところにより、ISMAP クラウドサービスリストへ登録されたクラウドサービス又は ISMAP 監査機関リストへ登録されたクラウドサービス又は監査機関の登録の一時停止又は削除を行うことができる。また、本制度に基づくISMAP運営委員会の要請に正当な理由なく当該クラウドサービス事業者又は監査機関が応じなかった場合にも、同様の措置を講ずることができる。 ●意見内容/確認内容 5.4に「再審査又は再監査」と記載されていますが、「再審査」に関して定義されておりませんので、「再監査」との違いは何かご教示ください。	御指摘の点について、再審査は5.3で求めた登録の再申請を受理した後、ISMAP運営委員会において実施する審査のことで、再審査に当たっては、3.3及び4.2の規定を準用することを想定しています。 それに対し、再監査は5.2において定義されているとおり、3.8の届出や5.1のモニタリングの結果を踏まえ、ISMAP運営委員会がクラウドサービス事業者に対し、当該クラウドサービスの整備状況評価の再監査を要求するものです。 なお、「再審査」の定義がございませんので、以下のとおり、修正いたします。 ＜修正後＞ 5.3 再申請 ISMAP運営委員会は、登録されているクラウドサービス又は監査機関について、ISMAPクラウドサービス登録規則又はISMAP監査機関登録規則に定めるところにより、必要に応じて、クラウドサービス事業者又は監査機関に対し、登録の再申請を求めることができる。なお、再申請後の登録の再審査や再登録については、それぞれ4.2、4.3の規定を準用する。
28	ISMAPクラウドサービス登録規則	＜クラウドサービス登録申請者に対する要求事項（案）＞ 質問1 ●該当ページ：P.1　15行目 3.1 申請者は「ISMAP 管理基準」(以下、「管理基準」という)の規定に従い「様式 1 言明書」及び「様式 2 経営者確認書」を作成し、自身のセキュリティ対策について言明要件に沿った言明を行い、言明した事項について監査機関の監査を受けなければならない。 ●意見内容/確認内容 3.1記載の「言明要件」と3.7及び6.1記載の「基本言明要件」は同一のものを指しているのでしょうか？異なる意味で使っているのであれば、その違いをご教示ください。	3.1の「言明要件」と3.7及び6.1の「基本言明要件」は同一のものを指しております。御指摘を踏まえて、「基本言明要件」に表記を統一致します。
29	ISMAP基本規程	以下4点の要望を意見として提出いたしますので、ご検討くださいますようお願いします。 (別添1)政府情報システムのためのセキュリティ評価制度(ISMAP)基本規程(案) 2.3　制度の基本的枠組み 「（中略）調達府省庁等はISMAPクラウドサービスリストに掲載されているクラウドサービスの中から調達を行うことを原則とする」とありますが、調達対象であるIaaS/PaaSを提供する主要なクラウドサービス事業者の定める基本契約では、損害賠償は契約額が上限となる場合が一般的であり、それらのクラウドサービス上で構築されるサービスについても同様に、損害賠償は契約額が上限となることが一般的です。 一方、従前の政府機関と受託業者との契約では損害賠償の上限が明記されていないことが多いため、本制度にて調達されるクラウドサービスの契約条件についてもご検討いただけますよう、要望します。	本制度はあくまで政府が調達するクラウドサービスの安全性の評価のための制度であり、IaaS/PaaSを政府機関が調達する際の、SIerと政府の間の契約については検討の対象外です。

30	ISMAP基本規程	3.7　報告 「クラウドサービス事業者は、登録されている自身のサービスについて、利用者に重大な影響を及ぼしうる情報セキュリティインシデントが生じた場合には、速やかにISMAP運営委員会にその概要を報告しなければならない。」とありますが、具体的に利用者に重大な影響を及ぼし得る、という点の影響のレベル感を定義していただけますよう、要望します。	いただいた御意見も踏まえて、インシデント報告を求めるのはどのような場合かが明らかとなるよう、FAQ等において例示を行うものとします。
31	ISMAP基本規程	5.2 再監査 「ISMAP運営委員会は、登録されているクラウドサービスについて、3.8に規定する届出の内容、5.1に規定するモニタリングの結果に応じて（中略）再監査を求めることができる」との記載がありますが、届出から再監査が要求されるまでの期間、および届出てから再監査が要求され監査により再認定されるまでの期間は、本制度上のステータスは登録として維持されるのか、又は別のステータスとなるのかを明確にしていただくよう、要望します。	御指摘のケースでは、再監査の段階では登録は維持されています。他方、再申請を求められる場合には再申請の要求と合わせて登録が削除されることとなります。
32	ISMAPクラウドサービス登録規則	(別添2)ISMAPクラウドサービス登録規則(案) 3.5(6) 「申請者は、ISMAP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について登録の一時停止又は削除を受けた場合には、当該サービスを利用している調達府省庁等に、その旨を速やかに通知又は登録者のWebサイトにて公開しなければならない。」とありますが、以下のような形態での扱いを明確化していただけますよう、要望します。 例）Aクラウドサービス（IaaS）上で別のBクラウドサービス（SaaS）を展開し、Bクラウドサービスを登録しているケースにおいて、Aクラウドサービスが登録の一時停止又は削除を受けた場合、Bクラウドサービスとしても登録の一時停止又は削除を受けるのか、またその場合において、Bクラウドサービス事業者から調達府省庁等への通知、又はWebサイトでの公開を実施する必要があるか否か。 （複数のクラウドサービスを組み合わせて新たなクラウドサービスを提供し、登録を受けた場合も同様）	御指摘の点については、今後作成するガイドライン等においてお示しすることも検討致します。
33	ISMAP情報セキュリティ監査ガイドライン	監査ガイドラインについて ・1.1の「監査基準等」について、本ガイドラインが参照する情報セキュリティ監査基準は、保証業務と助言業務の両方を対象とした基準である。監査ガイドラインにおいて、本業務は保証業務でないとしているが、上位基準に保証業務の概念も含まれているため、本業務の建付けがあいまいになる可能性が否定できない。 従って、監査ガイドラインは上位監査基準を一般基準としつつも、その一部、すなわち助言業務に関する部分に準拠するものであり、監査基準と監査ガイドラインの解釈に相違が発生した場合は、監査ガイドラインが優先して適用される旨を明記する必要があると考える。	御指摘のとおり、情報セキュリティ監査基準は保証業務と助言業務を対象とした基準であること、本業務は保証業務ではないことから、1.1 本ガイドラインの目的において、本制度における監査業務は情報セキュリティ監査基準の助言業務に関する部分のみに準拠するものであることが明確になるよう、下記のとおり修正致します。 ＜修正後＞ なお、本ガイドラインの適用にあたっては、情報セキュリティ監査基準（平成15年経済産業省告示第114号）に準拠することを前提とするが、準拠する範囲は当該基準の助言型監査に関する部分のみとする。
34	ISMAP情報セキュリティ監査ガイドライン	・第2章の独立性要件について、監査基準を参照しているが、監査基準における独立性の記述は抽象的な表現であり実際の判断ができないと思われる。資本関係を見るという考え方もあるが、例えば監査4大ファームにおいても資本関係は様々なので、不明確であると思われる。また本業務は保証業務ではないため、そもそも独立性の問題ではなく、利益相反（コンフリクト）の問題であると考えるべきである。監査基準にはこの概念が監査の目的によって要求される事項となっていることから、監査ガイドラインにおいて、利益相反の解消を条件にするよう、明記する必要があると考える。	いただいた御意見も参考に、ISMAP情報セキュリティ監査ガイドラインの独立性に関する記載を修正致します。
35	ISMAP情報セキュリティ監査ガイドライン	・4.1において、解釈の相違等を発生させないためにも、業務依頼者と業務実施者の責任が1対１で対応するように記載すべきであると考える。	記載内容としてはほぼ対応関係にあると考えており、また、正確には三者間の関係であることから、原案のとおりとします。
36	ISMAP情報セキュリティ監査ガイドライン	・ガイドライン1.4．1に「業務依頼者は、言明の対象となるクラウドサービス、すなわち、ISMAPクラウドサービスリストへの登録申請を行うクラウドサービスに関して、当該サービスの内容及びセキュリティリスク分析の結果を踏まえて、管理基準に準拠して統制目標及び詳細管理策を選択して必要な統制を整備するとともに、対象期間にわたりそれらを有効に運用していることを言明する責任を有している。」及びガイドライン4.1.1(1)に業務依頼者は言明対象となるサービスの範囲及び手続の対象期間を決定する責任負う旨が明記されているが手続の選定についての記載はない。また、業務実施者もガイドライン1.2では、「また、業務実施者の報告に基づき実施結果報告書の利用者が不適切な結論を導くリスクの評価は行わず、実施した手続や入手した証拠の十分性についても評価しない。」とあるが、本制度において、手続の十分性に責任を負う者を明確に記載すべきではないか。	手続の十分性はISMAP標準監査手続により確保されており、業務依頼者及び業務実施者を本ガイドラインに記載された責任を果たすとともに、最終的にはISMAP運営委員会が標準監査手続の実施状況の妥当性も踏まえて登録することとなるため、手続の十分性の確認に責任を負うのは運営委員会であることになりますが、現在の記載で十分読み取れると思料するため文案のとおりとします。
37	ISMAP基本規程	ISMAP基本規程について ・5.1のISMAP運営委員会のモニタリング活動の一環として想定されている監査機関への立入検査は、現実問題として会計監査法人では許容できない旨、ご了解頂きたい。（フロア内には、クライアント企業数千社の未発表財務情報等があるため、強制捜査以外での立入は一切認めていない）	モニタリング方法については、ISMAP監査機関登録規則9.3においてその手順を記載しておりますが、本項において、文書による回答と聞き取り調査によってモニタリングを実施することを規定しているとおりであり、フロア内に立ち入る立入検査は想定しておりません。

38	ISMAPクラウドサービス登録規則	1) ISMAPクラウドサービス登録規則(案) 第3章 申請者に対する要求事項 3.4 申請者は、言明書に記載の内容に加えて以下の情報をISMAP運営委員会に提供しなければならない。 (4) 第三者による検査（ペネトレーションテストを含む）の実施に関する情報 【コメント】 本来、本制度自体が監査主体による監査を行い、報告書を添付して申請する仕組みとなっており、これに加えて「第三者による検査」の情報提供を求める目的が不明確です。目的が不明確な場合、申請者によっては提供する情報が大きく乖離し、制度主旨の実現、および申請者の負担への悪影響が考えられます。要求事項の目的を明示することが必要だと思われます。 具体的には、以下2点を明示する必要があると思われます。 a)「含む」と書かれているが、ペネトレーションテスト以外には「第三者による検査」として具体的に何を期待するのか。例えば、ISMSやSOC2などが該当するのであれば、それらを例示するなどの対応が必要。 b) 第三者による検査の実施に関する情報とは、検査の実施有だけで十分か、それとも実施結果の内容(レポート等)の提供まで必要か。	本項における「第三者による検査（ペネトレーションテストを含む）」とは、脆弱性対策としての脆弱性検査ツールを用いた手法やペネトレーションテスト等を想定しております。また、「実施に関する情報」とは、その実施状況や受入に関する情報を指しており、実施結果内容の提供は想定しておりません。 いただいた御意見も踏まえて、上記の趣旨が明確になるよう、記載を修正致しました。 ＜修正後＞ （４）ペネトレーションテストや脆弱性診断等の第三者による検査の実施状況と受入に関する情報
39	ISMAPクラウドサービス登録規則	2) ISMAPクラウドサービス登録規則(案) 第9章 情報セキュリティインシデント発生時の報告 9.1登録者は、登録されている自身のクラウドサービスについて情報セキュリティインシデントが生じた場合、遅滞なく「様式7 情報セキュリティインシデントに関する報告書」に必要事項を記載し、ISMAP運用支援機関を通じてISMAP運営委員会に報告すること。 【コメント】 「情報セキュリティインシデントが生じた場合」として想定している条件等をガイドライン等で示すことが必要だと思われます。条件等が不明確な場合、申請者によっては報告内容および発生頻度が想定と大きく乖離し、ISMAP運用支援機関および申請者の双方の負担に悪影響が考えられます。 例えば、下記のような例示が考えられます。 例）調達府省等の管理する情報に侵害が生じた場合 例）申請者が記載した言明書からの逸脱が明らかとなった場合 例）申請者が定めるリスク管理手順に基づいて、インシデントが重大に該当した場合 例）調達府省等へのサービス影響が 6 時間以上生じた場合 また、事業者自身がインシデントレベルを定め、例示を基に報告が必要なレベルのインシデントについては、報告が上がる運用を行うことも考えられます。この時には、関連する要求事項について監査時に確認を行うことになります。	いただいた御意見も踏まえて、インシデント報告を求めるのはどのような場合かが明らかとなるよう、FAQ等において例示を行うものとします。
40	ISMAPクラウドサービス登録規則	3) ISMAPクラウドサービス登録規則(案) 第11章 モニタリング 11.2(2)　登録者は、(1)の通知を受けた場合、文書により回答を行う。 11.2(3)　ISMAP運用支援機関は、回答を確認し必要と認めた場合、当該登録者に対する聞き取り調査を行う。 【コメント】 モニタリングとして期待する調査内容を明示することが必要だと思われます。調査内容が不十分な場合、制度主旨の実現に悪影響が考えられます。情報セキュリティインシデント発生時の調達府省等への影響の有無を把握できるために、特に、以下の調査内容は含まれるべきだと考えられます。 a) 第三者による立入検査 b) 情報セキュリティインシデントの原因追跡が可能な証跡(ログ等) これらは、様式を具体化する際に要否を見極め、様式の提示と合わせて、調査で求めることがあることを事前に条件を提示しておかないと必要性が生じた時点で対応が難しくなることが想定されます。立ち入りの契約や制限事項の調整などが生じる、原因追跡に必要な証跡が取れていない、などが考えられます。	モニタリング方法については、ISMAPクラウドサービス登録規則11.2においてその手順を記載しておりますが、本項において、文書による回答と聞き取り調査によってモニタリングを実施することを規定しているとおりであり、フロア内に立ち入る立入検査は想定しておりません。

41	ISMAP監査機関登録規則	該当箇所 「ISMAP監査機関登録規則（案）」第3章 3.6 業務執行責任者の要件 業務執行責任者は、以下の全ての要件を満たすこと。 3.6.1 資格要件 以下に掲げる資格のうち、いずれかを保有すること。 公認情報セキュリティ監査人又は公認情報セキュリティ主任監査人 公認システム監査人 公認情報システム監査人 システム監査技術者 3.7 業務実施責任者の要件 業務実施責任者は、以下の全ての要件を満たすこと。 3.7.1 資格要件 以下に掲げる資格のうち、いずれかを保有すること。 公認情報セキュリティ監査人又は公認情報セキュリティ主任監査人 公認システム監査人 公認情報システム監査人 システム監査技術者 意見内容 資格要件として「情報セキュリティマネジメント審査員　又は　情報セキュリティマネジメント主任審査員　又　ISMSクラウドセキュリティ審査員」を追加する。 理由 ISMAPの管理基準のベースには、JISQ27001、JISQ27002、JISQ27017に加え、ISO27014とNISTSO800-53がある。 情報セキュリティマネジメント審査員（ISMS審査員）は、ISO27006の認証基準に従ってJISQ27001シリーズに適合していることを審査する力量を保有している。 この力量を保有していることは、ISO17024の認定を受けた要員認証機関に登録されていることで確認することができる。 また、ISMSクラウドセキュリティ審査員（ISMS-CLS審査員）は、上記に加えJISQ27017に適合していることを審査する力量を保有している。ここでJIS27017への適合審査は、JIP-ISMS517-1.0に従っている。この力量を保有していることは、上記と同様に要員認証機関に登録されていることで確認することができる。 これらの資格を持つものは、3.6.2のISMAP情報セキュリティ監査ガイドラインにおいて定める研修を受講することにより、ISMAP対応の監査において業務執行責任者又は業務執行責任者としての力量を保有できることが期待される。 ISMS審査員補、審査員、主任審査員の合計は、約2500名おり、ISMS-CLS審査員は、300名いる。 3.7項にリストアップされている資格に提案の資格を追加することにより、ISMAPの監査に対応できる要員をより多く確保することが期待できる。 ISMS審査員は、日本国内の一般企業で組織のISMS制度運営にキーマンとして携わっていることも多い。これらのキーマンにISMAPに含まれるNIST SP800-53のサイバーセキュリティに関する管理策を強化する概念を意識づけさせることにより、日本国内の企業のサイバーセキュリティに対する取り組みを強化することが期待できる。	御指摘の点について、監査主体の資格要件としては、「情報セキュリティサービス基準」における「情報セキュリティ監査サービス」の資格要件と同一のものとすることを想定しておりますので、原案のとおりとさせていただきます。
42	ISMAP管理基準	ISMAP管理基準に関して 9ページ37行目「どのように説明責任を果たしているかについて、独立した客観的な意見を委託する。」は日本語としておかしい。「独立した客観的意見を監査人に求める。」などの変更が必要。	御指摘を踏まえ、以下のとおり修正致します。 「独立した客観的な意見を委託する。」⇒「独立した客観的な意見を監査人等に求める。」
43	ISMAP管理基準	21ページ23行目「範囲の一部のみを対象とする場合もあり、」とあるがこの記述は一般論であり、制度の主旨からすると毎回全ての適用範囲について監査されるものではないか。	御指摘の点について、マネジメント基準の4.6.2.3で規定している監査とは、クラウドサービス事業者が自身の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評価するために実施する取り組みを指しており、監査機関が実施する本制度における監査業務に関する要件を定めるものではありません。その上で、マネジメント基準の4.6.2.3において要求されるCSP自ら実施する監査の範囲については、対象となるクラウドサービスに関する設備や体制等の規模によっては毎年度の実施が現実的に難しいことも想定されるため、監査の目的の明確化や適切な監査計画の立案を担保することで実効性を確保することを想定しています。
44	ISMAP管理基準	27ページ9行目「レビューする。」とあるが主語が不明。「管理層は」というような主語を記載すべきである。	プロバイダはマネジメント基準に基づく体制に応じてレビューするものであり、原案のとおりとします。
45	ISMAP管理基準	27ページ31行目「テレワーキングの場所でアクセス」は「テレワーキングの場所でのアクセス」ではないか。	御指摘の点については「テレワーキングの場所でアクセス」で相違ありません。
46	ISMAP管理基準	28ページ44行目「情報分類」は、クラウドサービス事業者の情報分類の何が機密性２に該当するのか明言すべきである。	御指摘の点について、クラウドサービス事業者が管理する情報の情報分類については、政府統一基準の機密性区分のルールに従う必要があるものではないことから、原案のとおりとします。
47	ISMAP管理基準	30ページ44行目「暗号鍵を当該利用者が管理する機能を提供し、」は日本語としておかしい「暗号鍵のついて当該利用者が管理する機能を提供し、」ではないか。	御指摘の点については、「暗号鍵を当該利用者が管理する機能を提供し、」で問題ないと考えます。
48	ISMAP管理基準	32ページ19行目「検査する」とは何を行えば検査したことになるのか明示すべきである。	御指摘の点については、今後作成するガイドライン等においてお示しすることも検討致します。
49	ISMAP管理基準	32ページ25行目「ログ取得機能を提供する」とあるがクラウドサービス利用者はログを自由に使用できるという意味か。	本管理策は、クラウドサービス利用者が自らの情報セキュリティ対策としてイベントログを取得し、レビューを行うことを可能とするために要求するのものです。
50	ISMAP管理基準	33ページ25行目「合意ではー取り扱う」は日本語として意味が取りづらい。わかりやすい表現にすべきだ。	御指摘の点については、ISOやクラウド情報セキュリティ管理基準においても同様の表現のため、原案どおりとさせていただきます。
51	ISMAP基本規程	政府情報システムのためのセキュリティ評価制度 (ISMAP)基本規程(案) P5(3行目） 調達府省庁等は ISMAP クラウドサービスリストに掲載されているクラウドサービスの中から調達を行うことを原則とする →　原則に該当しない場合を明記もしくは例示して頂きたい。クラウドベンダが登録を判断する際に重要な指標となると考えているため。 ISMAP管理基準(案）　（対象：第３照、管理基準） 管理策基準（8.1.2.7.PB）及び管理策基準（10.1.2.20.PB） → SaaSの場合は、当該機能を提供することが技術的、運用的な観点から合理的でないと考えている（仕組みが複雑になるため、コストが相当上昇する） SaaSを利用した場合は、サービス提供者が適性な方法で鍵を管理すること、又はCASB等を利用してサービス利用者側で仕組みを用意する基準が合理的と考えています。	御指摘の点について、制度利用の原則に該当しない場合については、「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」（令和2年1月30日サイバーセキュリティ戦略本部決定）において、「各政府機関等は、クラウドサービスを調達する際には、本制度において登録されたサービスから調達することを原則とし、本制度における登録がないクラウドサービスの調達については、本制度で要求する事項を満たしていると、当該調達を行う政府機関等の最高情報セキュリティ責任者の責任において、それぞれの政府機関等で確認するものとし、詳細は、サイバーセキュリティ対策推進会議、各府省情報化統括責任者（CIO）連絡会議において定めるものとする。」としており、今後同会議において定めることとしています。

52	ISMAP管理基準	ISMAP管理基準（案）の1.3.15 暗号の定義に関して、 電子政府推奨暗号が、現実の課題解決に必要な暗号であって安全性を満たしているものを全て列挙している訳ではないため、例外規定は必要とは考えられますが、「又はそれと同等以上の安全性を有す暗号を指す」という文言は、「同等以上」を判断する権限をもつ組織が指定されておらず、適切ではありません。 個々の組織がCRYPTREC以上に暗号の安全性を分析でき判断できるとも読めますが、ほとんど非現実的と思われ、事業者を審査するに際して問題となると考えられます。 次に、ISMAP管理基準（案）の18.1.5 において、「暗号化機能」に限定していますが、「政府機関等の情報セキュリティ対策のための統一基準」においては、「暗号・電子署名」としており、「暗号化」機能のみを対象とするのは適切では無いと考えられます。電子署名や、復号機能などのも同様に確認の対象とすべきものと考えます。	御指摘の点について、現行の政府統一基準の考え方では、暗号化又は電子署名を導入する場合においては、「電子政府推奨暗号リスト」に記載されたアルゴリズムを採用することが原則 とされているため、ISMAP管理基準においても本原則を踏まえて電子政府推奨暗号リスト又はそれと同等以上の安全性を有す暗号を対象としているものです。 以上を踏まえ、本制度においては基本的には電子政府推奨暗号リストの利用が想定されておりますが、仮に電子政府推奨暗号リスト以外の暗号の利用が発生したとしても、現時点では管理基準に示したとおり、電子政府推奨暗号のアルゴリズムを活用しつつ、電子政府推奨暗号以上の鍵長を有している暗号などを想定しています。その上で、個々のケースについては、ISMAP運営委員会が個別に判断をする形となります。 また、御指摘の電子署名や復号機能に関しては、管理策10.1.1及び10.1.2において暗号の利用に関する方針に関する要件を定めております。
53	ISMAP監査機関登録規則	【総論】 情報処理安全確保支援士会として、政府情報システムの導入に際して、投資対効果が高く、最新技術の活用が容易なクラウド技術を活用する方向性は極めて高く評価するものである。あわせて、国民の安心安全を考えた時ときに、セキュリティ評価制度を明確にする今回の取り組みは非常に意義があると考えている。 一方で、本会としては、情報セキュリティの確保に関し、定期的な講習の受講による最新技術の習得が義務付けられている情報処理安全確保支援士を活用することにより、今回の各種基準に関する安全性をより高めることに貢献したいと考え、意見を提出するものである。 意見の対象：(別添4)ISMAP監査機関登録規則(案) 【概論】 申請者の業務執行における監査体制を定めることは有意義であると考える。 しかし、その資格要件について、「情報セキュリティ」に係る知識経験が資格制度において十分に担保されていないものや、クラウドの情報セキュリティという最新の知見を求められる分野においては、継続的な講習（CLE）等が十分に確保されていないと思われる。 そこで、業務執行責任者の資格要件を強化又は業務執行体制の充実による情報セキュリティ確保を実現するために有効だと考えられる以下２案を提言したい。 （意見１：業務執行責任者の資格要件の強化） 3.6.1 資格要件 ・公認システム監査人 ・公認情報システム監査人 ・システム監査技術者 資格要件として定められた上記3資格について、情報セキュリティの観点から情報処理安全確保支援士会として、いくつかの懸念がある。 これらの資格は、情報システム監査を主とする資格であり、情報セキュリティに関する知識経験については、それぞれの資格制度における位置づけや比重が監査分野に比して相当に低くなっているからである。 例えば、システム監査技術者においては、情報セキュリティの分野は、他の高度試験と同程度に午前試験の多肢選択式試験で問われる程度であり、そもそも資格の更新制度が存在していないといった問題がある。 これらの資格については、有効な資格を有することに加えて、以下のとおり、情報セキュリティ分野における十分な知見を有することを要件とすべきである。 ・公認システム監査人（ただし、情報セキュリティ分野で十分な知見を有する者に限る。） ・公認情報システム監査人（ただし、情報セキュリティ分野で十分な知見を有する者に限る。） ・システム監査技術者（ただし、情報セキュリティ分野で十分な知見を有する者に限る。） また、情報処理安全確保支援士は、情報セキュリティに関する専門的な知見が資格試験制度及び継続研修・更新制度により担保されている。 したがって、政府で導入するクラウドコンピューティングという国民の安心・安全に直結する分野においては、「サイバーセキュリティの確保を支援することを業とする」情報処理安全確保支援士も、業務執行責任者の資格要件として採用すべきであると考える。	御指摘の点について、監査主体の資格要件としては、「情報セキュリティサービス基準」における「情報セキュリティ監査サービス」の資格要件と同一のものとすることを想定しておりますので、原案のとおりとさせていただきます。
54	ISMAP監査機関登録規則	（意見２：業務執行体制の強化） 3.6.1で指摘したとおり、業務執行責任者においては、情報処理安全確保支援士等の情報セキュリティ分野で十分な知見を有する者を充てることを基本とされたい。 しかしながら、セキュリティ分野の十分な知見を同時に有する人材の確保が困難な事業者もあると考えられることから、当面の対策として以下の方法で実施することを提言したい。具体的には、以下の内容に修正することを提言する。 3.7.1 資格要件 以下に掲げる資格のうち、いずれかを保有すること。 (1)公認情報セキュリティ監査人又は公認情報セキュリティ主任監査人 (2)公認システム監査人 (3)公認情報システム監査人 (4)システム監査技術者 ただし、業務チームが上記資格のうち(2)～(4)で構成される場合、メンバーに情報処理安全確保支援士等情報セキュリティ分野において十分な知見を有する者を含めること。	御指摘の点について、監査主体の資格要件としては、「情報セキュリティサービス基準」における「情報セキュリティ監査サービス」の資格要件と同一のものとすることを想定しておりますので、原案どおりとさせていただきます。
55	ISMAP監査機関登録規則	（他の項目に関する意見） 3.6.2 実務経験等 「クラウドコンピューティングに関する知見を有すること」とあるが、それをどのような客観的事実をもって検証できるのかが明らかではない。例えば、「クラウドコンピューティングサービスを提供する事業者が認定する資格その他の当業者における十分な専門的知見を担保する仕組みを有する資格試験又は認定制度によりクラウドコンピューティングに関する知見を証明できること」と変更することが望ましい。 3.7.2 研修等の受講等 3.6.2に対する意見と同内容	審査においては、クラウド技術に関する資格の取得状況や、クラウドサービスに対する監査の実務経験、クラウドサービスの技術に係る実務経験等を確認することを想定しておりますが、詳細についてはいただいた御意見も参考に今後検討して参ります。

56	ISMAP基本規程	今回のISMAPにおける各種規程に関して、クラウドサービスプロバイダー（以下、CSP）として以下のコメントを提出いたします。 基本規定（案） Page 1 Line 23-28: 1.4.1. クラウドコンピューティングの定義 この定義は、最後の部分である「情報セキュリティに関する十分な条件設定の余地かがあるもの」の追加を除いて、NISTとISO/ISEの定義を1つに組み合わせたものと認識しています。すべてのCSPがこの機能をユーザーに提供していると仮定しているように見えますが、多くのSaaSではそうではないと考えます。優れたCSPであれば、暗号化を有効にしたり、データの保存を選択したりするなど、ユーザーが情報セキュリティ条件を設定できるようにすべきですが、最後の文ではクラウドの定義を不必要に制限しているため、一部のCSPが除外されている可能性があると考えます。そのため、「情報セキュリティに関する十分な条件設定の余地があるもの」という文を削除することをご提案します。	御指摘の点について、ISMAP基本規程の定義は、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」及び「政府機関等の情報セキュリティ対策のための統一基準」において使用されている定義を活用したものです。他方、管理基準については、本制度において、クラウドサービスのセキュリティの要件を設定するにあたり、既存の基準との整合性を踏まえ、クラウド情報セキュリティ管理基準の定義を活用したものです。 その上で、SaaS/IaaS/PaaSそれぞれにおいて、本制度において提示しているクラウドサービスの定義に該当するものについては、政府機関等への納入を目指す限りにおいて、原則として共通の管理基準に適合したセキュリティ対策を実装し、登録や登録の更新をしていただく必要がございますが、サービスの特性上、原理的に特定の管理策についての具備が不可能と解される場合には、一定の例外措置を設けることとします。ただし、その場合においても、利用者による当該サービスの採否の判断に資するよう、当該管理策の具備が不可能である理由など関連する情報については、適切に利用者に対して開示を行うことが必要です。
57	ISMAP基本規程	また、基本規定の1.4.1の定義が、管理基準の文書の1.3.2.のクラウドサービスの定義と異なることについてご確認願います。	御指摘の点について、ISMAP基本規程の定義は、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」及び「政府機関等の情報セキュリティ対策のための統一基準」において使用されている定義を活用したものです。他方、管理基準については、本制度において、クラウドサービスのセキュリティの要件を設定するにあたり、既存の基準との整合性を踏まえ、クラウド情報セキュリティ管理基準の定義を活用したものです。 その上で、SaaS/IaaS/PaaSそれぞれにおいて、本制度において提示しているクラウドサービスの定義に該当するものについては、政府機関等への納入を目指す限りにおいて、原則として共通の管理基準に適合したセキュリティ対策を実装し、登録や登録の更新をしていただく必要がございますが、サービスの特性上、原理的に特定の管理策についての具備が不可能と解される場合には、一定の例外措置を設けることとします。ただし、その場合においても、利用者による当該サービスの採否の判断に資するよう、当該管理策の具備が不可能である理由など関連する情報については、適切に利用者に対して開示を行うことが必要です。
58	ISMAP基本規程	Page 5 Line 33-37: 3.5 登録の更新 ISMAPの認定は、IaaS、PaaS、SaaSのカテゴリーを含むあらゆるタイプのサービスをカバーすることが期待されています。必要なコントロールがサービスの特性に合わせて行われることが重要ですが、サービスタイプ毎に調達の頻度や規模が異なります。SaaSの提供と調達は、IaaSおよびPaaSとは異なりサービス調達規模は必ずしも大きくないと想定するため、登録期間は2年間とし、他国での実施の状況を踏まえた上での導入をご提案いたします。	御提案の件ですが、SaaSのサービスにおいても、IaaSやPaaSと同様に、管理基準への適合状況について適切に運用状況評価を行う必要があると考えられることから、クラウドサービスについては同様の登録の有効期間とすることが適当と考えます。その上で制度の効率化については今後の運用状況等も踏まえて検討していくこととしています。
59	ISMAPクラウドサービス登録規則	ISMAP クラウドサービス登録規則(案) Page 1 3.4(1). 法律で財政を開示する必要がある上場企業は、情報が既に公開されているとして、追加の詳細を提供することを必要としないことをお勧めします。 また、政府が提供する資金調達の情報を開示する必要があることを推奨します。	サービス登録規則3.4では、申請者が登録申請の際にISMAP運営委員会に提供しなければならない情報を規定するものであり、既に公開されている情報か否かに関わらず、本項の要求事項を満たす情報を提供いただくこととなります。そのため、既に公開されている情報で本項の要求事項を満たすことが可能な情報が存在する場合には、当該情報を含めて申請いただくことを否定するものではありません。
60	ISMAPクラウドサービス登録規則	Page 1 3.4(2). この項目の範囲は非常に広く、日本以外の国の法律を「国内法外」と言う可能性があります。本規定の意図が、開示について日本政府に通知することなく、他の政府が開示を求める可能性のある適用法の提示を求める場合は、この点を明確にするために、この項目での開示項目を絞り込んで行うことを推奨します。また、この項目に必要な情報の粒度と説明を示す例について、早期にガイダンスを提供することをお勧めします。	クラウドサービスの利用にあたっては、調達側がその利用目的や業務の性質に照らして、リスクに応じてサービスの性質を見極めながら利用することが大前提となりますので、調達側がリスク評価を行うにあたって必要な情報提供がなされるよう、次のとおり修正致します。 ・クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用され、調達府省庁等が意図しないまま当該調達府省庁等の管理する情報にアクセスされ又は処理されるリスクについて、ISMAP運営委員会及び当該省庁等がリスク評価を行うために必要な情報 なお、具体的にどのような情報を求めるのかについてはFAQ等で例示したいと思います。

61	ISMAP管理基準	ISMAP 管理基準(案) 我々は、このプロセスに適用される統一基準を形成するために、そのISOおよびNIST規格を利用して基礎を形成した政府を称賛します。 すでに認識され、グローバルに使用される標準に依存することは、世界中のセキュリティ標準の一貫した適用をサポートし、より多くのクラウドサービスを利用可能とすることを可能にします。 提案された管理基準案は、監査役コミュニティによって異なる解釈をうける可能性が高いと考えています。 監査人が一貫してこれらの基準を適用し、CSPが同様の方法でこの規制に準拠できるように、監査基準に対して統一的なアプローチを作成することが非常に重要です。 この期待の明確さは、基準の開発の成功にとって非常に重要な要素です。 したがって、CSPに対しては「標準監査手順書」が開示されていないため、ISMAP運営委員会としてCSP向けのガイダンスを早期に発行し、あわせて個別監査の際に発生する可能性のある疑問点をQ&A集などで開示することで、情報共有を促進していただきたいと考えます。 また併せて、今後、海外に本社を置くCSPの登録の実施も多く予想されることから、英語での管理基準の発行を要望いたします。 以上	頂いた御意見も踏まえて各種文書の英訳版の整備についても今後検討してまいります。
62	ISMAPクラウドサービス登録規則	ISMAPクラウドサービス登録規則（案）についての意見 （P1、14行目からP2、28行目）第3章で用いられている「申請者」及び「登録者」 ・意見内容 当該「申請者」及び「登録者」に関し、外国法人が提供しているクラウドサービスであって、その日本法人が日本において登記されている場合の申請及び登録の手続きについて、クラウドサービスの提供の実際を踏まえてその詳細をご検討頂くとともに、できるだけ早期にその申請及び登録手続きの詳細を公開して頂きたいと考えます。 ・理由 クラウドサービスは、一般に、外国法人がサービスの一部を提供し、その日本法人が日本の国内法に準拠し自ら責任を負って日本国内におけるサービスを提供していることが多いと考えます。そのため、そのようなサービス提供の主体が申請及び登録を受ける場合の一連の手続きについて、上記クラウドサービス提供の実際を踏まえてその詳細を検討して頂くとともに、登録制度が円滑かつ公平に運営されるように、できるだけ早期に手続きの詳細を明らかにして頂きたいと考えます。	いただいた御意見も踏まえて、申請及び登録手続の詳細も速やかに検討して参ります。
63	ISMAPクラウドサービス登録規則	（P1、32行目）「申請するクラウドサービス従事者」 ・意見内容 当該部分について「申請するクラウドサービスの提供に従事する者」あるいは「申請するクラウドサービスの提供に直接従事する者」との変更を提案します。 ・理由 クラウドサービスの提供にあたって、そのサービス提供に関係する者の数は、恒常的なメンテナンス等を担当する者まで含めると膨大な数に上り、その中にはクラウドサービスの提供そのものには実質的に関与せず、クラウドサービス提供自体に影響を与えない者も多く含まれます。「クラウドサービス従事者」との表現では、申請にあたって申請者が調達機関に提供すべき情報の範囲について、申請者と調達機関との間で認識の齟齬が生じる恐れがあることから、これをより明確な文言とし「申請するクラウドサービスの提供に従事する者」あるいは「申請するクラウドサービスの提供に直接従事する者」との変更を提案します。	御指摘を踏まえ、次のとおり修正致します 。 (1)申請者は、調達府省庁等との調達交渉時に、調達機関の求めに応じて、言明書の詳細、申請するクラウドサービスの従事者のうち、利用者の情報又は利用環境に影響を及ぼす可能性のある者の所属、専門性、実績、国籍に関する情報を調達機関に対して提出すること。国籍については、個々人に紐付かない形で該当する国名を提出すること。
64	ISMAP管理基準	ISMAP管理基準(案)についての意見 （P28、35行目から36行目）「暗号鍵を管理し消去する機能を実装するための情報」 ・意見内容 当該部分について「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」との変更を提案します。 ・理由 クラウドサービス事業者がクラウドサービス利用者に対して提供すべき情報の範囲を、より明確にするため「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」との変更を提案します。	御指摘のとおり、修正いたします。 ＜修正後＞ 8.1.2.7.PB クラウドサービス事業者は、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。 (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
65	ISMAP管理基準	（P30、44行目から45行目）「当該利用者が暗号鍵を管理する方法についての情報を提供する。」 ・意見内容 当該部分について「当該利用者が暗号鍵を管理する機能を実装するために必要となる情報を提供する。」との変更を提案します。 ・理由 クラウドサービス事業者がクラウドサービス利用者に対して提供すべき情報の範囲を、より明確にするため「暗号鍵を管理する機能を実装するために必要となる情報を提供する。」との変更を提案します。	御指摘を踏まえ、以下のとおり修正致します。 「暗号鍵を管理する方法についての情報を」⇒「暗号鍵を管理する機能を実装するために必要となる情報」

66	制度全般	○　「情報セキュリティクラウド」の言葉の適用について全般（お題目） （私がご意見を申し上げたい各種基準(案)の記載箇所） 下記の資料に「情報セキュリティインシデント」についての記載がございます。 ○　「(別添1)政府情報システムのためのセキュリティ評価制度(ISMAP)基本規程(案)」の「3.7 報告」 ○　「(別添2)ISMAPクラウドサービス登録規則(案)」の「第9章 情報セキュリティインシデント発生時の報告」 ○　「(別添3)ISMAP管理基準(案)」の「16 情報セキュリティインシデント管理」 （ご意見） 　これまでの情報セキュリティに関する知識及び経験から申し上げます。「政府情報システムのためのセキュリティ評価制度(ISMAP)」においても共通する問題も憂慮されます。国として、国益、国民等のプライバシー、個人情報等を守るため、下記の問題についてしっかりと対策を講じていただけますよう、よろしくお願い申し上げます。 ○　問題１：業務の委託先、その再委託先等がＩＳＭＳ認証、ＰＭＳ認証等を取得しているといっても、委託先、その再委託先等で情報セキュリティ、個人情報等の問題（「情報セキュリティインシデント」、情報事故等のもみ消し、障害管理の裏帳簿等）を巧妙にもみ消すおそれがあること （１）業務の委託先、その再委託先等がＩＳＭＳ認証、ＰＭＳ認証等を取得しているといっても、内部で情報セキュリティ、個人情報等の問題（「情報セキュリティインシデント」、情報事故等のもみ消し等）をもみ消していた場合、外部のＩＳＭＳ認証機関（審査機関）に通報しなければ、その情報セキュリティ、個人情報等の問題（「情報セキュリティインシデント」、情報事故等のもみ消し等）が放置されてしまう場合があること （２）業務の委託先、その再委託先等がＩＳＭＳ認証、ＰＭＳ認証等を取得しているといっても、内部で情報セキュリティ、個人情報等の問題（「情報セキュリティインシデント」、情報事故等のもみ消し等）をもみ消していた場合、外部のＩＳＭＳ認証機関（審査機関）が毎年の審査時にもその情報セキュリティ、個人情報等の問題（「情報セキュリティインシデント」、情報事故等のもみ消し等）に気付かないおそれがあること （３）業務の委託先、その再委託先等がＩＳＭＳ認証、ＰＭＳ認証等を取得しているといっても、組織内部の情報セキュリティに関する規程が曖昧である場合（情報セキュリティの喪失、情報セキュリティ事象、情報セキュリティインシデント等の曖昧な定義等）、情報セキュリティ、個人情報等の問題（「情報セキュリティインシデント」、情報事故等のもみ消し、報告の不実施、怠慢等）をもみ消せること 　曖昧さがなく、誰もが理解できる、分かりやすい定義、条文、多くの例等を明示する必要があると存じます。問題発生前の事象も「情報セキュリティインシデント」として報告するべきかも明記し、関係者全員に理解させるべきであると存じます。定義が曖昧であると、定義が理解されていないと、「情報セキュリティインシデント」に相当する事象を発見しても、発見者、責任者、管理職、経営者等が曖昧さ等を理由に報告を怠るおそれもございます。 （４）情報セキュリティに関する不正を通報又は報告した通報者が保護されない場合があること 　通報に対する報復（解雇、雇止め、左遷、仲間はずれ、いじめ、人権侵害等）のおそれがあり、現状、現場の労働者（委託元、業務の委託先、その再委託先等）は、法規及び社内規程上、情報保護のための正しい行動もしにくいこともございます。公益通報者保護法、社内の公益通報者保護規程等で通報者を適切に保護するべきであると存じます。現場で情報セキュリティを維持する現場の労働者及び通報者を悪質な経営者、責任者、管理職、外部協力会社等から適切に保護するよう、「政府情報システムのためのセキュリティ評価制度(ISMAP)における各種基準(案)」を含め、個人情報保護法、公益通報者保護法等の関連法令等、様々な情報セキュリティに関するガイドラインに明記し、保護していただきたく存じます。	御指摘の点については、ISMAP管理基準の6以下の情報セキュリティのための組織及び15以下の供給者関係において担保できていると考えます。
67	制度全般	（ご意見） 　これまでの情報セキュリティに関する知識及び経験から申し上げます。「政府情報システムのためのセキュリティ評価制度(ISMAP)」においても共通する問題も憂慮されます。国として、国益、国民等のプライバシー、個人情報等を守るため、下記の問題についてしっかりと対策を講じていただけますよう、よろしくお願い申し上げます。 ○　問題１の続き：業務の委託先、その再委託先等がＩＳＭＳ認証、ＰＭＳ認証等を取得しているといっても、委託先、その再委託先等で情報セキュリティ、個人情報等の問題（「情報セキュリティインシデント」、情報事故等のもみ消し、障害管理の裏帳簿による報告の不実施等）を巧妙にもみ消すおそれがあること （５）業務の委託先、その再委託先等がＩＳＭＳ認証、ＰＭＳ認証等を取得しているといっても、業務の委託先、その再委託先等の内部、そして、ＩＳＭＳ認証機関（審査機関）等に通報しても、問題がもみ消されるおそれがあること 　「ISMAP情報セキュリティ監査」の監査は、本当に全て信頼できるのでしょうか。監査機関による、ごまかし、空疎な権威主義、専門用語、レトリック等に騙されてはいないでしょうか。ところで、ISMS適合性評価制度においては、基本的に、認証機関（審査機関）がISMS適合性評価制度等の審査料等でキャッシュを得て、経営を成り立たせていることが悪く作用しているおそれを憂慮しております。そのため、認証機関（審査機関）が顧客をつなぎとめること等のために、甘い審査をすること、認証機関（審査機関）による苦情のもみ消し、収賄等が発生することを危惧しております。ISMS適合性評価制度においては、実際に、現状のある認証機関（審査機関）は、審査時のサンプリングの仕方も不透明であり、緻密な確認、厳密な確認、効果のある確認等を行っていない場合があります。一般的に、製品に欠陥、瑕疵等がある場合、リコールがあります。監査機関、組織内部等で「ISMAP情報セキュリティ監査」の形骸化、空洞化、不正、怠慢、不実施等があった場合、国民、労働者等のステークホルダーは、いつでも「ISMAP情報セキュリティ監査」のリコール（監査責任者、監査担当者等の罷免、監査による評価の取り消し、監査のやり直し、説明を受けること等）を請求できる制度、警察等の捜査機関へ通報できる制度等があると、個人情報、プライバシー等の保護の観点から、国民、労働者等が安全で安心できるのではないかと存じました。お手数をおかけしますが、ご検討とご対応のほど、よろしくお願いいたします。	御指摘の点については、ISMAP管理基準の6以下の情報セキュリティのための組織及び15以下の供給者関係において担保できていると考えます。

68	ISMAP情報セキュリティ監査ガイドライン	（６）内部統制と同様の「政府情報システムのためのセキュリティ評価制度(ISMAP)」の限界 下記の資料にも「内部統制」についての記載がございます。 ○　(別添5)ISMAP情報セキュリティ監査ガイドライン(案) 　下記引用文献の「内部統制の限界」についても、対策の実施をよろしくお願いいたします。「政府情報システムのためのセキュリティ評価制度(ISMAP)」の限界もあると存じます。この限界について、国、委託先、再委託先、その他の関係機関は、理解する必要があると存じます。日本国民等へも周知し、情報セキュリティに関する問題について情報開示によるチェックができるようにした方がよいと存じます。 引用文献 「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂について」 金融庁企業会計審議会（会長 徳賀 芳弘 京都大学副学長・教授）（令和元年１２月６日現在） 「財務報告に係る内部統制の評価及び監査の基準」 ＵＲＬ　https://www.fsa.go.jp/news/r1/sonota/20191213.html 「３．内部統制の限界 内部統制は、次のような固有の限界を有するため、その目的の達成にとって絶対的なものではないが、各基本的要素が有機的に結びつき、一体となって機能することで、その目的を合理的な範囲で達成しようとするものである。 （１）内部統制は、判断の誤り、不注意、複数の担当者による共謀によって有効に機能しなくなる場合がある。 （２）内部統制は、当初想定していなかった組織内外の環境の変化や非定型的な取引等には、必ずしも対応しない場合がある。 （３）内部統制の整備及び運用に際しては、費用と便益との比較衡量が求められる。 （４）経営者が不当な目的の為に内部統制を無視ないし無効ならしめることがある。」（PDFファイル　１５ページ）	御指摘の点については、本制度の運用に当たって留意してまいります。
69	ISMAP情報セキュリティ監査ガイドライン	（ご意見） 　これまでの情報セキュリティに関する知識及び経験から申し上げます。「政府情報システムのためのセキュリティ評価制度(ISMAP)」においても共通する問題も憂慮されます。国として、国益、国民等のプライバシー、個人情報等を守るため、下記の問題についてしっかりと対策を講じていただけますよう、よろしくお願い申し上げます。 ○　問題１の続き：業務の委託先、その再委託先等がＩＳＭＳ認証、ＰＭＳ認証等を取得しているといっても、委託先、その再委託先等で情報セキュリティ、個人情報等の問題（「情報セキュリティインシデント」、情報事故等のもみ消し、障害管理の裏帳簿による報告の不実施等）を巧妙にもみ消すおそれがあること （７）組織の情報セキュリティの運用状態の経年劣化 　業務の委託元、委託先、その再委託先等が組織的には、最初は、良い状態でも、年数が経過するにつれ、巧妙なもみ消し方を覚え、状態が悪くなっていくおそれもございますので、ご検討とご留意のほど、よろしくお願いいたします。 （８）組織の情報セキュリティの教育の怠慢 　各種基準(案)にも、教育についての記載がありましたが、組織内の情報セキュリティについてのeラーニング等でも、読まず、読み飛ばし、修了することができ、テストのカンニングも可能であるおそれもあるため、現状、教育も不十分であることを憂慮しております。なお、経験上、私は、組織内の定期の情報セキュリティについてのeラーニングをきちんと受講し、満点合格しておりました。	御指摘の点については、ISMAP管理基準の15以下の供給者関係の要件において担保できていると考えます。
70	制度全般	○　問題２　今般の新型コロナウイルスの場合のような非常事態等の場合への対応 　今般の新型コロナウイルスのように、委託先、その再委託先等の多くの従業員（有期雇用の社員、派遣労働者を含む。）が出勤できない場合、サービスレベルを保証できないおそれ、サービス自体も提供できないおそれもあります。非常事態における対策を検討し、事前に委託先と協議し、契約書における非常事態時についての行動、対応策、サービスレベル等の共通認識を得て、定めておくことも必要ではないかと存じました。感染症流行、地震災害、豪雨災害、津波災害、浸水被害、火山噴火、戦争等も考えられます。非常事態時の行動方針、管理策、コミュニケーションの方法、ＳＬＡ、監査の方法等の明記についてもご検討とご対応のほど、よろしくお願いいたします。	クラウドサービス事業者に対しては、「管理策基準」の「17 事業継続マネジメントにおける情報セキュリティの側面」において、危機や災害等の困難な状況においても情報セキュリティ及び情報セキュリティマネジメントの継続を可能とするためのプロセス、手順及び管理策を実施し、有効に機能することを検討することを要求しております。
71	制度全般	○　問題３　業務の委託元、委託先、その再委託先、監査機関等のステークホルダーの働き方改革やワークライフバランスへの配慮 　情報セキュリティを確保しつつ、業務の委託元、委託先、その再委託先、監査機関等のステークホルダーの長時間労働の防止、労働時間の管理、テレワーク活用等がしやすくなるよう、ご検討のほど、よろしくお願いいたします。	本制度における各種基準等の案への御意見ではないと認識しておりますが、御意見は拝聴いたしました。

72	ISMAPクラウドサービス登録規則	エストニアが旧連邦国ロシアからサイバー攻撃を受け、国家の存亡をかけて防衛したのは記憶に新しい。また中国軍と深い関係のあるファーウェイが、情報コントロールをするとして米国から排除されたのも近年のことである。数年前には、米国のインフラが上海のあるビルからアクセスされていたが、それは人民解放軍のオフィスであり、活動時間が現地時間9：00～17：00であったことが話題になった。 ＜ISMAPクラウドサービス登録規則＞ このような例から、政府情報システム関連システムは、純国産、関わる人間すべてが日本国籍者でありことが当然と理解している。ところが、今年2月に「政府共通プラットフォーム」にAmazon Web Services（AWS）を採用するニュースが流れ、驚愕した。 今回は政府情報システムの「セキュリティ評価」なので、せめて次の項目だけでも徹底して頂きたい。 -3.5　に以下を明記願いたい。－＞システムは純国産。人は、会社、トップ、スタッフ、下請け・子会社などに至るまで、すべて日本国籍保有者であること。外国資本が直接間接とも入っていないこと。当該会社の身体身辺チェックを義務付けること。これによって情報漏洩、情報操作のリスクを最低限にとどめるよう願いたい。	御指摘の点については、様々なクラウドサービスが存在する中で、各政府機関においては、その利用目的や業務の性質に照らして、リスクに応じてサービスの性質を見極めながら利用する必要があります。係る観点から、サービスの利用に当たって海外の法令が適用される場合のリスク等について、CSPから情報開示を求めることで、個別の情報システムの調達の際に、当該システムの性質に応じて、調達者が適切にサービスの利用を判断することに資するようにしたいと考えており、一律でいただいた御意見のような内容を基準として位置付けることは考えておりません。 その上で、各調達府省庁におけるリスク評価等の結果、必要に応じて、本制度の管理基準に加えて追加的対策の確認を行って頂くことは妨げられるものではありません。
73	ISMAP監査機関登録規則	＜ISMAP監査機関登録規則＞ -3.1　外資が入った企業を排除する旨を明記する。 -3.6、3.7　日本国籍の保有はチームメンバーすべてに適応すべき。 それでなくとも我が国はスパイの規制が無いに等しく、情報は筒抜けであり、世界から「スパイ天国」と揶揄されているほどである。それは、かつての「真珠湾攻撃」を連想させる。すべての暗号が解読されており、真珠湾に侵攻する空母は追跡されていたにも関わらず、奇襲攻撃であると2002.3.11の際まで、いや現在もいまだに非難されている始末である。 また、今回の武漢コロナで明らかなように、政府、与党、野党には数多くの親中派がおり、国民の生命よりも他国の国益を優先し、著しく国民の生命・財産を危険に晒している状況である。また、国境の管理が甘く、武漢出身者が規制の網を軽々とくぐり抜け、得意げにSNSで発信している。	御指摘の点については、クラウドサービスの監査には高度で専門的なスキルやノウハウが要求されます。一方で、我が国政府の情報システムに係るクラウドサービスの監査には安全保障上留意すべき点があることも事実であり、係る観点から、適格な監査主体の要件に関し、わが国において情報セキュリティ監査を業務として行っている法人とした上で、業務執行責任者と、業務実施者のうち現場責任者（チームマネジャー）の国籍要件として日本国籍を要求しております。
74	ISMAP情報セキュリティ監査ガイドライン	1．「監査」という用語について 「ISMAP情報セキュリティ監査ガイドライン」 1.2 本制度における監査業務の特質 　本制度における監査業務は、ISMAP運営委員会が行うISMAPクラウドサービスリストの登録審査において、登録審査の対象となるクラウドサービスに関して、管理基準に基づいた情報セキュリティに係る内部統制の整備及び運用の状況を確認するために、クラウドサービス事業者の依頼に基づいて、業務実施者たる監査機関が監査基準等に準拠して手続を実施し、その結果を事実に即して報告することを目的としている。業務実施者が作成した実施結果報告書は、サービス登録申請書の添付資料としてクラウドサービス事業者によってISMAP運営委員会に提出され、ISMAPクラウドサービスリストへの登録審査を行う際に参照する資料として利用される。 このため、本制度の監査業務において、業務実施者の報告は、手続実施結果を事実に即して報告するのみにとどまり、手続実施結果から導かれる結論の報告も、保証も提供しない。また、本制度における監査業務は、結論の基礎となる十分かつ適切な証拠を入手することを目的とはしておらず、保証業務とはその性質を異にするものである。さらに、業務実施者は、本制度における監査業務において、重要性の概念の適用やリスク評価に基づく手続の決定は行わず、また、業務実施者の報告に基づき実施結果報告書の利用者が不適切な結論を導くリスクの評価は行わず、実施した手続や入手した証拠の十分性についても評価しない。 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ とあり、 「手続実施結果を事実に即して報告するのみにとどまり、手続実施結果から導かれる結論の報告も、保証も提供しない。」や、 「実施した手続や入手した証拠の十分性についても評価しない。」 とありますので、これが「監査」と呼べるのか疑問です。 「レビュー」や「確認」と呼ぶ方が相応しいと考えます。	情報セキュリティ監査には保証型監査と助言型監査が存在しますが、本制度は保証型監査ではないことから、1.2において、保証業務の要素である「手続実施結果から導かれる結論の報告も、保証も提供」することや、「実施した手続や入手した証拠の十分性についても評価」することはしない旨を明らかにしております。 加えて、「監査」という用語は多義的な意味を有する用語であることから、本ガイドラインにおいて、本制度における「監査」を「本制度における監査業務」と定義し、「1.2 本制度における監査業務の特質」においてその特質を明記しております。
75	ISMAP管理基準	2．管理基準　第２章　言明書に記載すべき内容の小さな違和感 管理基準　第３章　ガバナンス基準 　3.1.6 保証 保証は、経営陣が独立した客観的な監査、レビュー又は認証を委託するガバナンスプロセスである。これは、レベルの情報セキュリティを達成するためのガバナンス活動の実行及び運営の遂行に関連した目的及び処置を特定し、妥当性を検証する。 「レベルの情報セキュリティ」の意味が理解し難いです。	御指摘を踏まえ、以下のとおり、修正をいたします。 ＜修正後＞ 3.1.6 保証は、経営陣が独立した客観的な監査、レビュー又は認証を委託するガバナンスプロセスである。これは、望ましいレベルの情報セキュリティを達成するためのガバナンス活動の実行及び運営の遂行に関連した目的及び処置を特定し、妥当性を検証する。
76	制度全般	政策の提案	本制度における各種基準等の案への御意見ではないと認識しておりますが、御意見は拝聴いたしました。

77	ISMAP基本規程	該当箇所3.2 監査 意見内容 「監査機関の選択」というタイトルの新しいセクションを 3.1 の後に次のテキストとともに追加するよう提案します。 クラウドサービスプロバイダーは、登録された監査機関を選択し、監査を要求する。 理由 案文の 3.2 では、クラウドサービスプロバイダーが適切な監査人を選択するのか、プロセスがクラウドサービスプロバイダーに対して監査人を指定するのかが明確ではありません。 クラウドサービスプロバイダーが、登録済み監査人リストから優先的に監査人を選択できる柔軟性を付与することをお勧めします。 これにより、監査人が会社すなわち当該クラウドサービスプロバイダーのプロセスに精通している場合は、コンプライアンスコストを削減することができ、監査の効率性とスピードを向上させることができます。	いただいた御意見を踏まえて、クラウドサービス事業者はISMAP監査機関リストに登録されている監査機関の中から選択しなければならない旨が明らかとなるよう、記載を修正致します。 ※「第 4 章の規定に基づき登録された監査機関による監査を受けなければならい。」→「第 4 章の規定に基づき登録された監査機関の中から選択し、監査を受けなければならい。」
78	ISMAP基本規程	該当箇所9.2 禁止事項 意見内容 AWSJ は、「制度運営に関わる者」の義務の範囲を明確にするため、以下のとおり脚注を追加し、9.2 を変更することを提案します。 ISMAP クラウドサービス登録の範囲外でアドバイザリサービスを提供する監査人またはクラウドサービスプロバイダーは、 9.2 の「ISMAP システムの管理に関与する者」の範囲内ではない。 理由 案文では、禁止事項の対象となる監査人およびクラウドサービスプロバイダーが広範囲であり9.2 では、「ISMAP 運営委員会及び制度運営に携わる者」の定義が明確ではありません。 9.13で定義されている秘密保持義務は、監査人および登録済みクラウドサービスプロバイダーに課せられる場合があります。 一方、監査人およびクラウドサービスプロバイダーは、9.1 の義務に含まれない勧告サービスを他の企業に提供することがあります。 9.2 は、ISMAP 規則に基づき、「ISMAP システムの管理に関与する者」に対する義務が、ISMAP システムと無関係な活動には適用されないことを明確にすべきと考えます。	御質問の件について、例えば、クラウドサービス事業者が登録や登録の更新等を行うために制度運営側に提供した自社のサービスのセキュリティ等に関する機微な情報は全て「秘密情報」に該当します。その上で、当該「秘密情報」については、本制度の運用にあたって、ISMAP運営委員会、制度所管省庁、ISMAP運用支援機関がアクセスする可能性がございますが、これらの職員については、国家公務員法第100条第 1 項及び情報処理の促進に関する法律第41条の秘密保持義務の規定が適用されます。 その上で、いただいた御意見を踏まえて、制度運営に関わる者の範囲が明確となるよう、記載を修正致します。 「ISMAP 運営委員会及び制度運営に携わる者」⇒「ISMAP運営委員会、制度所管省庁、ISMAP運用支援機関及びその委託を受けた者」
79	ISMAPクラウドサービス登録規則	「ISMAP クラウドサービス登録規則(案)」第3 章部分)(別添2) 該当箇所 3.4(2)申請者に対する要求事項 意見内容 AWSJ は、案文の3.4(2)を次のとおり改訂することを提案します。 クラウドサービスを調達する府省庁等が提供する情報にアクセスまたは制御するための申請者の権利に関連する情報また、3.4(2)の義務は、いわゆる共有セキュリティモデルに基づき、クラウドサービスプロバイダーと、その顧客との間で共有される責任あることを明確にする必要があります。 理由 案文の3.4 は過度に広く、クラウドサービスプロバイダーが容易に識別できるような法規制の範を定義するものではなく、クラウドサービスプロバイダーがこの要件に対応できないリスクを増大させるものです。 また、共有セキュリティモデルのもとにおいては、クラウドサービスプロバイダは、顧客の情報にアクセスしたり処理したりしないため、クラウドサービスを利用する顧客の側にクラウド内の情報のアクセスやコントロールの責任があります。 この項で、法律や地域の見直しに必要な範囲が不必要に広く定義されますと、クラウドサービスプロバイダのリスク評価と検証に過度の負担がかかります。 また、調達府省庁が自発的なアクセスや開示を必要とする外国の法律のリスクを評価する義務として一般的且つ広範囲に過ぎる可能性があります。 クラウドサービスに関する顧客情報の管理権の帰属に関する役割の分担を明確化することは、ユーザーが採るべき必要な管理措置を明らかにし、またクラウドプロバイダのサービスの利用の範囲の判断に資することになります。	クラウドサービスの利用にあたっては、調達側がその利用目的や業務の性質に照らして、リスクに応じてサービスの性質を見極めながら利用することが大前提となりますので、調達側がリスク評価を行うにあたって必要な情報提供がなされるよう、次のとおり修正致します 。 ・クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用され、調達府省庁等が意図しないまま当該調達府省庁等の管理する情報にアクセスされ又は処理されるリスクについて、ISMAP運営委員会及び当該省庁等がリスク評価を行うために必要な情報 なお、具体的にどのような情報を求めるのかについてはFAQ等で例示したいと思います。
80	ISMAPクラウドサービス登録規則	該当箇所 3.5(1)申請者の要求事項 意見内容 AWSJ は、案文の3.5(1)から「クラウドサービス従業員の国籍」の削除を次のように要求します。 申請者は、調達府省庁等との調達交渉時に、調達機関の求めに応じて、申請する, クラウドサービス従業者の所属、専門性、実績、国籍に関する情報を調達機関に対して提出すること。 理由 ベンダーが単一の調達に固有のリソースを供給する従来の調達とは異なり、クラウドサービスは一般的に共有サービスとして提供されます。 クラウドサービスの場合、「申請者クラウドサービス従業員」は不必要に非常に広く解釈される恐れがあります。 クラウドサービスシステムの監査は、クラウドサービスプロバイダによる制御とユーザーによる制御とを個別に評価することを意図しており、クラウドサービスエンティティのビジネスの性質に注目されるべきであり、個人の特性、専門知識、国籍に焦点を当てるのではないようにすべきです。 そうでなければ、クラウドサービスプロバイダに過度の負担を課すこととなり、サービス利用にも限界が生じてしまいます。	御指摘を踏まえ、次のとおり修正致します 。 (1)申請者は、調達府省庁等との調達交渉時に、調達機関の求めに応じて、言明書の詳細、申請するクラウドサービスの従事者のうち、利用者の情報又は利用環境に影響を及ぼす可能性のある者の所属、専門性、実績、国籍に関する情報を調達機関に対して提出すること。国籍については、個々人に紐付かない形で該当する国名を提出すること

81	ISMAPクラウドサービス登録規則	該当箇所 3.5(2)応募者の要求事項 意見内容 AWSJ は案文の3.5(2)を削除するよう要求します。 理由 2018 年のコメントで提起されているように、ISMAP の強みは、提案されたサービスの監査において、クラウドサービスプロバイダとユーザーの管理を個別に評価することアプローチをとっていることにあります。 クラウドサービスプロバイダーは、サービスを構成する機器やその他の機能を継続的に管理する責任があります。 特定の調達の履行過程におけるシステムの要素は、省庁による調達発生時と異なる場合があるため、システムの設計項目事項を特定の調達の要件としないことを提案します。	ご指摘を踏まえ、本項は、宣誓事項ではない形で要求事項に記載します。 ＜修正後＞ 3.6 申請者は、調達府省庁等との調達交渉時に、調達機関の求めに応じて、「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」(平成30年12月10日関係省庁申合せ)(以下、「申合せ」という)の運用に協力すること。
82	ISMAP管理基準	「ISMAP 管理基準(案)」(別添3) 該当箇所 4.9 情報セキュリティリスクコミュニケーション 意見内容 AWSJ は、このセキュリティコントロールと、詳細な実装ガイダンスを含むその他のセキュリティコントロールの削除を提案いたします。 代わりに、コントロールの実装に関連する詳細を記載する場合には、クラウドサービスの特性に配慮することを求めます。 理由 本要求事項は過度に事前規制的であり、クラウドサービスの顧客の多様なニーズを捉えるものではありません。 クラウドサービスプロバイダーは、クラウド環境のお客様に利用可能な共有サービスを使用して、クラウドサービスの使用状況の詳細を開示し、コミュニケーションします。 過度の規制は、クラウドサービスプロバイダーが顧客と情報を共有する方法を改善し続けることを制限する恐れがあります。	「4.9情報セキュリティコミュニケーション」では、利用者や委託先を含む利害関係者との間でリスク管理の方法に関して継続的にコミュニケーションを行うことを要求しておりますが、クラウドサービス事業者が実施すべきリスクアセスメントの方法を詳細に規定したり、あるいは、当該利害関係者との間で詳細なリスク分析結果についてまで合意することを要求するものではありません。
83	ISMAP情報セキュリティ監査ガイドライン	「ISMAP 情報セキュリティ監査ガイドライン（案）」第4 章部分)(別添５) 該当箇所 4.5 他の認証・監査制度等の証拠の利用 意見内容 AWSJ は、案文の4.5 を次のように変更するよう提案します。 業務実施者は、標準監査手続に準拠して自ら手続を実施する。そのため、他の認証・監査制度や内部監査等の実施結果あるいはその報告書をそのまま利用することは原則認められない。ただし、業務実施者が標準監査手続を実施する際に適切とみなす場合には、他の認証・監査制度や内部監査等において、また他の場所で収集された証拠を利用することは可能である。 理由 セキュリティ評価制度の対象となる AWS クラウドサービスは、世界中で同じ技術メカニズムを使用して実装されるため、日本でホストされているサービスだけに限定される証拠を得ることによるセキュリティ上の利点はありません。 AWS は 4.5 の文言が他の認定/監査システムから収集または参照された証拠の使用を許可していることをサポート致します。 適切と判断される場合に、前述の理由により、監査プロセスで他のリージョンから引き出された証拠の価値も認識されるのが妥当であるため、上記のとおり提案いたします。	「クラウドサービスの安全性評価に関する検討会とりまとめ」の「2.3 監査関連基準等の検討 (4) リージョンとサンプリングの考え方」に記載のとおり、監査証拠として用いられる資料は言明書に明記したリージョンの中から収集する必要がありますが、言明書に明記したリージョンの範囲内であって、かつ、統制が同質である場合には、複数のリージョンをまたいでいる場合でも監査対象となる母集団を単一と見なしてサンプル抽出を行うことを認めることとしています。
84	ISMAP基本規程	【該当箇所】 別添１ 政府情報システムのためのセキュリティ評価制度(ISMAP)基本規定(案) P1 1.2　本制度の目的 【意見内容・理由】 　本制度により一定のセキュリティ水準は確保されると考えますが、一方で、米国においてもFedRAMPを取得しているIaaS、SaaS上のシステムでサイバー攻撃の被害に遭う事案が発生しているのも事実です。これは安全なクラウドサービスを調達・採用したうえで、さらに調達府省庁等においても、クラウド上のセキュリティ対策をしないと危険にさらされるということを示しています。本制度が単純な免罪符とならないためにも、本制度でクラウドサービスのセキュリティ水準を確保したうえで、調達府省庁等の責任範疇でのセキュリティ対策が必要であることを、基本規定で示した方がよろしいのではないかと考えます。	御指摘の件について、「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」（令和２年１月30日サイバーセキュリティ戦略本部決定）において、「本制度に登録されているサービスを利用するに当たっては、当該サービスが組み込まれる情報システムの情報セキュリティに係るリスクを適切に把握した上で、当該サービスの機能の範囲や当該サービスが行っている情報セキュリティ対策を踏まえ、情報システム全体の情報セキュリティ対策を実施するとともに、情報セキュリティ確保についての最終的な責任を負わなければならないことに十分留意する必要がある」とされているところであり、御指摘の趣旨は既に関係各府省庁等において周知済みです。

85	ISMAP基本規程	【該当箇所】 別添１ 政府情報システムのためのセキュリティ評価制度(ISMAP)基本規定(案) P1 1.4用語の定義 　1.4.1クラウドサービス 【意見内容・理由】 　現在、クラウドリソースを活用したSaaS形式のサービスが多数存在しており、基本規定（案）に示されているクラウドサービスの定義だけでは本評価制度の対象か否かの判断がつきかねるサービスが存在すると考えます。つきましては、本評価制度の対象となるクラウドサービスが明確となるように類例等で示すべきと考えます。 （例） ・クラウド上で提供されるCRM(Customer Relationship Management）やERP(Enterprise Resources Planning)のサービス ・クラウド上で提供されるWeb会議・テレビ会議システム ・クラウド上で提供される仮想デスクトップサービス ・クラウドにログ等の情報を転送し、AI等を用いた解析を行い、その結果を返答するサービス ・クラウド上に設置された管理サーバからオンプレミス環境のハードウェアもしくは ソフトウェアを制御するサービス ・クラウドサービスとAPI等のインターフェースを用いて連携し、クラウドサービスの利用状況 等についてリアルタイムで可視化や制御を行うサービス	御指摘の点について、ISMAP基本規程の定義は、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」及び「政府機関等の情報セキュリティ対策のための統一基準」において使用されている定義を活用したものです。他方、管理基準については、本制度において、クラウドサービスのセキュリティの要件を設定するにあたり、既存の基準との整合性を踏まえ、クラウド情報セキュリティ管理基準の定義を活用したものです。 その上で、SaaS/IaaS/PaaSそれぞれにおいて、本制度において提示しているクラウドサービスの定義に該当するものについては、政府機関等への納入を目指す限りにおいて、原則として共通の管理基準に適合したセキュリティ対策を実装し、登録や登録の更新をしていただく必要がございますが、サービスの特性上、原理的に特定の管理策についての具備が不可能と解される場合には、一定の例外措置を設けることとします。ただし、その場合においても、利用者による当該サービスの採否の判断に資するよう、当該管理策の具備が不可能である理由など関連する情報については、適切に利用者に対して開示を行うことが必要です。
86	ISMAP基本規程	【該当箇所】 別添１ 政府情報システムのためのセキュリティ評価制度(ISMAP)基本規定(案) P1 1.4用語の定義 　1.4.1クラウドサービス 【意見内容・理由】 　上記の意見に関連して、明確に本評価制度の対象とならないSaaS形式のサービスがある場合、その種のサービスについても、調達府省庁等が採用するにあたっての判断基準となる規定や基準が別途示されるべきと考えております。 　また、特に「クラウドサービスとAPI等のインターフェースを用いて連携し、クラウドサービスの利用状況等についてリアルタイムで可視化や制御を行う」サービスなど、本評価基準の対象となるクラウドサービスを安全に利用することを目的としたサービスについては、本評価制度と同時、もしくは、速やかに、調達府省庁等が採用するにあたっての規定や基準等が示されるべきと考えます。	御指摘の点について、ISMAP基本規程の定義は、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」及び「政府機関等の情報セキュリティ対策のための統一基準」において使用されている定義を活用したものです。他方、管理基準については、本制度において、クラウドサービスのセキュリティの要件を設定するにあたり、既存の基準との整合性を踏まえ、クラウド情報セキュリティ管理基準の定義を活用したものです。 その上で、SaaS/IaaS/PaaSそれぞれにおいて、本制度において提示しているクラウドサービスの定義に該当するものについては、政府機関等への納入を目指す限りにおいて、原則として共通の管理基準に適合したセキュリティ対策を実装し、登録や登録の更新をしていただく必要がございますが、サービスの特性上、原理的に特定の管理策についての具備が不可能と解される場合には、一定の例外措置を設けることとします。ただし、その場合においても、利用者による当該サービスの採否の判断に資するよう、当該管理策の具備が不可能である理由など関連する情報については、適切に利用者に対して開示を行うことが必要です。
87	ISMAPクラウドサービス登録規則	【該当箇所】 別添2　ISMAPクラウドサービス登録規則(案) P1 3.4(2) クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用され、 調達府省庁等が意図しないまま当該府省庁等の管理に関する情報にアクセスされ 又は処理されるリスクの評価結果とその具体的内容に関する情報 【意見内容・理由】 　ISMAPクラウドサービスリストにおいて、上記は一般公開することを前提とされていると思われるため、「調達府省庁等が意図しないまま当該調達府省庁等の管理する情報にアクセスされ又は処理されるリスクの評価」について、各クラウドサービスが公平に横並びで評価されるよう、リスクの評価項目等を具体的に示すべきと考えます。	クラウドサービスの利用にあたっては、調達側がその利用目的や業務の性質に照らして、リスクに応じてサービスの性質を見極めながら利用することが大前提となりますので、調達側がリスク評価を行うにあたって必要な情報提供がなされるよう、次のとおり修正致します。 ・クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用され、調達府省庁等が意図しないまま当該調達府省庁等の管理する情報にアクセスされ又は処理されるリスクについて、ISMAP運営委員会及び当該省庁等がリスク評価を行うために必要な情報 なお、具体的にどのような情報を求めるのかについてはFAQ等で例示したいと思います。
88	ISMAPクラウドサービス登録規則	【該当箇所】 別添2　ISMAPクラウドサービス登録規則(案) P1 3.5(1) 【意見内容・理由】 　「申請するクラウドサービス従事者の所属、専門性、実績、国籍に関する情報を調達機関に対して提出すること。」とありますが、クラウドサービスに従事する全員の情報を調達機関に対して提示することは現実的ではないと考えます。具体的にどのような粒度の情報が必要かを具体的に示すべきと考えます。	御指摘を踏まえ、次のとおり修正致します。 (1)申請者は、調達府省庁等との調達交渉時に、調達機関の求めに応じて、言明書の詳細、申請するクラウドサービスの従事者のうち、利用者の情報又は利用環境に影響を及ぼす可能性のある者の所属、専門性、実績、国籍に関する情報を調達機関に対して提出すること。国籍については、個々人に紐付かない形で該当する国名を提出すること。

89	制度全般	・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。） [ISMAP 管理基準（案）] 第2章/2.2.言明書に記載すべき内容/2.2.5監査の対象となる期間 [ISMAP 情報セキュリティ監査　ガイドライン（案）] 第4章/4.5 他の認証・監査制度等の証拠の利用 ・意見内容 下記を推奨します。 ・監査期間を3年ごとに変更し、一般競争入札の参加登録要件と合わせること ・管理基準を異なるクラウドコンピューティングのモデルに合わせていくこと ・不可欠な管理策をさらに識別し狭めること ・日本のクラウドサービスのためのIT監査人材を訓練し、技能上達の手法を政府が策定すること。 ・運用開始前に管理基準に関する追加ガイドラインやQ&Aを策定すること。 ・理由 ISMAP管理基準（案）の2.2.5では、クラウドサービスリストに登録されるクラウドサービスの全ての管理基準について、毎年、監査が必要であると記されています。ISMAP情報セキュリティ監査ガイドラインにおいて、標準監査手続の実施に他の認証・監査制度や内部監査等において収集された証拠を再利用することを認める旨が記されているものの、関連する先行投資は技術革新的であるクラウドサービスプロバイダー（CSP）にとっては障壁となります。監査手続は高額であるだけでなく、監査要求を満たすために、セキュリティ人員から本来の責務を果たす時間を奪うことにもなります。その点からも、多くの国際認証の手続においては、2年もしくは3年ごとの監査要件となっており、それによってセキュリティが損なわれることもありません。このことからも、監査手続を簡略化し、CSP側の不要な負担を最小限におさえる方法を引き続き模索して頂きたく思います。 ISMAPにおいては、頻度を減らした監査スケジュールを設定されることを我々は推奨します。クラウドサービスの複雑性によっては、ISO-27000のような監査手続は長期に亘る活動となり、大がかりなシステム変更においては短くなることもありますが、通常は3年の期間を設けています。毎年監査が実施されることになれば、CSPは連続して監査プロセスを実施しなくてはならず、常時、監査対応に追われることとなります。また、調達省庁側にとっても、年度ごとの監査により関連する契約更新の負荷が増すことになります。官公庁の一般競争入札参加資格の登録制度における有効期間が3年ごとであることからも、監査に係る全てのISMAP関係者の作業を減らす上でも、監査期間を3年ごとに変更し、一般競争入札の要件と合わせることを奨めます。 我々はまた、IaaS（Infrastructure-as-a-Service）、PaaS（Platform-as-a-Service）、SaaS（Software-as-a-Service）といった、異なるクラウドコンピューティングのモデルに管理基準を合わせていくことを奨めます。これらのモデルは、CSPとクラウドサービスカスタマ（CSC）間の関係性や、責任共有における分配等、様々な点で異なります。 前述したように、BSAはISMAPが日本の限られたクラウド監査人材に過剰な負荷をかけることになるのではないかと懸念しております。クラウドサービスのIT監査や認証には高度な専門的技能が必要であり、国際的にもこれを効果的に実施できる有能な人材は限られています。世界における同様の制度においては、これが課題となりました。特に運用開始から最初の2年間においては、新たな要件で多数のクラウドサービス初めて認証を受けることになります。世界的に監査人が限られているということは、有能な職員が高額になることを意味します。これは、ISMAPを実施する省庁とCSPの間で妥当な範囲の期待と金額を協議すること、また、同時に、最も重要なシステムを防御するためには、高い技能をもった人員を世界的に育成する必要があることを意味します。ISMAPに係わるCSP、監査人、政府にとっての限られた人材をより有効に活用するためにも、これらを考慮した上で、不可欠な管理策をさらに識別し、狭めることを奨めます。監査人とCSPにとっての手続を能率的にするために有効なのは、ISMAP管理基準に関する追加ガイドラインもしくはQ&Aを数カ月内に策定して頂くことです。これにより、運用開始前にCSPは管理基準要件を正確に理解することができ、初期の評価活動を効率化することができます。また、ISMAPの策定手続と並行して、日本のクラウドサービスのためのIT監査と認証人材を訓練し、技能を磨く手法を日本政府が策定することを推奨します。	監査期間に関して、クラウドサービスに関する技術革新のスピード等も考慮して、情報セキュリティ対策が適切に実施・運用されていることを評価する観点から１年間を対象としております。なお、SOC2等の他のセキュリティ監査の仕組みにおいても、1年を超える期間で監査の有効性を認めているものは、主要なものとしては存在しないと考えております。加えて、通常、継続的な監査を行う過程で、工程については一定の効率化が図られるものと考えておりますが、制度全体としてのコストのさらなる効率化については運用状況も踏まえ適切に検討していきたいと考えています。 　管理基準の関係に関しては、ISMAP管理基準2.2.4基本言明要件に規定しているとおり、クラウドサービス事業者は基本言明要件を満たすように管理策を選択しなければならないものの、対象サービスに照らして合理的な適用が不可能な統制目標については、その理由を示すことで対象外とすることを認めており、提供するサービスの形態に応じて対応頂くことが可能であると考えます。その上で、サービスの特性上、原理的に特定の管理策についての具備が不可能と解される場合には、一定の例外措置を設けることとします。。 　IT監査人材の訓練、技能上達の手法の策定に関して、本制度の監査品質の維持・向上を図る上でも監査人に対する研修等は必要であると考えており、ISMAP情報セキュリティ監査ガイドラインにおいて継続的な研修の受講を要求しております。また、このような研修等を含む本制度の取り組み全体を通じて、国内のクラウドセキュリティ監査の裾野を広げることに寄与するものと考えます。 　追加ガイドラインやQ&Aの策定は、本制度の理解を深める施策を検討する中で、今後も継続的に検討してまいります。
90	ISMAPクラウドサービス登録規則	・該当箇所 [ISMAP クラウドサービス登録規則] 8章サービス登録の有効期間 ・意見内容 ISMAPのクラウドサービス登録期間を3年とすることを求めます。 ・理由 上記と同様の懸念となりますが、8.1では、登録者は登録の対象となった監査の対象期間の末日の翌日から1年4カ月後までに、更新の申請をしなければならない、と記してあります。上記で述べておりますように、ISMAPのクラウドサービス登録期間を3年とすることを求めます。	監査の有効期間については、SOC2等の監査においても、1年を超える期間で監査の有効性を認めているものは、主要なものとしては存在しないと考えております。 他方で、サービス登録の有効期間の考え方については、制度運用を行う中で効率化した方法について引き続き検討して参りたいと考えております。
91	ISMAPクラウドサービス登録規則	・該当箇所 [ISMAP クラウドサービス登録規則] 第4章　サービス登録に関する申請/4.2、第5章　申請の受理/5.4 (1)、第6章　審査/6.1 (4) ・意見内容 登録申請、申請受理、審査時の発見事項の統制改善に関する期間を３ヶ月とすることを奨めます。 ・理由 上記においては、申請者によるサービス登録申請、問い合わせへの回答、また審査時の発見事項に係る統制の改善に関する期間が設定されていますが、現在の１ヶ月か２ヶ月という期間は、申請者が要件を完了するために十分な準備期間となっておりません。従って、期間は３ヶ月とすることを奨めます。	全ての準備期間を3か月とした場合、実際の審査・登録が行われるのが監査期間末日から1年以上経過するようなケースが生じることが考えられ監査結果を適切なものとして扱うことが難しくなることから、原案のとおりの期間としています。
92	ISMAP管理基準	・該当箇所 [ISMAP管理基準（案）] 第4章　マネジメント基準/4.2. 記載内容について ・意見内容 政府ネットワークへの情報セキュリティリスクに関する情報交換をCSPとするための正式な仕組みの策定を奨めます。 ・理由 4.2では、CSCとCSP間において、クラウドサービスにおける情報セキュリティリスクについて情報交換することが非常に重要である、と記しています。CSPとリスクに関して情報交換することは、サイバーセキュリティの成果をあげるためには不可欠である、ということに我々は同意します。これに適合する国際規格はISO27005:2018となります。 また、日本政府が民間と公共部門から集めた政府ネットワークへの情報セキュリティリスクに関するあらゆる情報や機密情報をCSPとやりとりするために、日本政府が正式な仕組みを策定することを奨めます。政府のデータやサービスの保護のために適用すべき管理基準をCSPが適切に判断するためには、これが不可欠となります。	御指摘のとおり、クラウドサービスプロバイダと各政府機関等との情報交換は重要な取組と考えますので、本制度の運用を実施しつつ、その在り方についても継続的に検討を行ってまいります。

93	ISMAP管理基準	・該当箇所 [ISMAP管理基準（案）] 第6章　情報セキュリティのための組織 6.3.P クラウドサービス利用者及びクラウドサービス事業者の関係 ・意見内容 基本的な管理策以外の管理策、また、CSPと調達省庁間の共同責任の詳細は個別のクラウドサービス契約において合意されるということをISMAP関係者に対して明確化することを奨めます。 ・理由 ISMAPにおいては、政府のクラウドサービス調達において、適切なセキュリティ・レベルを確保するために一律的なアプローチをとっておりますが、政府期間のサービスは多様で、サービスの管理策は個別のクラウドサービス契約（クラウドSLA）で網羅されていることをISMAP関係者が理解することも重要です。ISMAPにおいては中核となる、基本的な管理策をまとめており、その他の管理策については、CSPと調達省庁間で、両者の共同責任の詳細も含め、ISMAP制度での調達時に、クラウドSLAにおいて合意されるという理解でおります。この点についてISMAP関係者に対して明確化することを奨めます。	御指摘の件について、「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」（令和２年１月30日サイバーセキュリティ戦略本部決定）において、「本制度に登録されているサービスを利用するに当たっては、当該サービスが組み込まれる情報システムの情報セキュリティに係るリスクを適切に把握した上で、当該サービスの機能の範囲や当該サービスが行っている情報セキュリティ対策を踏まえ、情報システム全体の情報セキュリティ対策を実施するとともに、情報セキュリティ確保についての最終的な責任を負わなければならないことに十分留意する必要がある」とされているところであり、御指摘の趣旨は既に関係各府省庁等において周知済みです。
94	ISMAPクラウドサービス登録規則	・該当箇所 [ISMAPクラウドサービス登録規則] 第9章　情報セキュリティインシデント発生時の報告 ・意見内容 情報セキュリティインシデント発生時の報告は、未解決であり、緊急で、データ損失や重大な影響を及ぼす結果となったセキュリティインシデントのみとすることを奨めます。 ・理由 9.1 においては、登録されているサービスについて情報セキュリティインシデントが生じた場合にCSPが報告することが記載されています。どのようなセキュリティインシデントがISMAP運営委員会に報告されるべきかが明確になっていると、報告実施において大変有効です。政府のサービスやデータがリスクに晒されるような大規模のセキュリティインシデントの際の連絡手段として、この規則が重要となってくることは理解しておりますが、報告における敷居が低すぎると、政府に影響を及ぼさない、解決済みの、さして深刻でないセキュリティ事象にISMAP運営委員会が忙殺されることとなります。従って、未解決、又、緊急で、データ損失や重大な影響を及ぼす結果となったセキュリティインシデントのみを報告とすることを奨めます。また、個人情報に関連するインシデントに関しては、個人情報保護法における漏えい報告要件と合致させることを求めます。 最後に、本案には報告に使う様式が添付されていないため、報告においてどのような情報が求められるのかを本登録規則において明確化して頂きたく考えます。	いただいた御意見も踏まえて、インシデント報告を求めるのはどのような場合かが明らかとなるよう、FAQ等において例示を行うものとします。
95	ISMAPクラウドサービス登録規則	・該当箇所 [ISMAPクラウドサービス登録規則] 第15章　登録に係る異議申立て ・意見内容 ISMAP運営委員会の決断への申し立ての際に求められる情報については、本規則に明確な記載をすることを求めます。 ・理由 ISMAPクラウドサービス登録規則の15章においては、申請者が指定の様式によってサービス登録に関する処置への異議申し立てをISMAP運営委員会あてにすることができるとしています。そのような意義申し立てにはISMAP運営委員会による特定のクラウドサービスの登録拒否も含まれるかもしれませんが、本規則案には指定の様式が含まれていないため、どのような情報が提供されるべきかが明確でありません。決断に関する申し立ての際に求められる情報について、本規則に明確な記載をすることを求めます。	異議申し立て時にご提出いただく「様式13　異議申立書」を含む様式類については、制度立ち上げに合わせて速やかに整備し、公開することとしています。
96	ISMAPクラウドサービス登録規則	・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。） [ISMAPクラウドサービス登録規則] 別表１．申請書の提出方法、様式1-14 ・意見内容 申請書提出は郵送ではなくオンライン申請を推奨します。 ・理由 別表１には申請書は郵送とすることが記載されておりますが、日本政府がデジタルファーストを原則としていることからも、オンラインでの申請書提出を推奨します。また、様式1から14が本案に添付されていないため、登録に際して求められる項目や情報を確認する上においても、実際の様式がISMAP関係者に公開されると助かります。	今後、本制度ホームページの構築を予定しており、その中でご要望のオンライン申請につきましても、対応を検討して参ります。

97	ISMAP基本規程	・該当箇所 [政府情報システムのためのセキュリティ評価制度（ISMAP）基本規程（案）] 第9章　その他 ・意見内容 ISMAP運営委員会による秘密保持がどのように担保されるのかを明確化することを奨めます。 ・理由 9.1ではISMAP運営委員会及び制度運営に携わる者は、秘密情報が無権限の者に伝わり、情報の機密性が損なわれることがないようにしなければならない、としています。しかし、この秘密保持がどのように実施されるのか、また、ISMAPの実施プロセスの中で、別途詳細な秘密保持契約（NDA）によって担保されるのかが、明確ではありません。ISMAP関係者が意見できるように、この点に関して提示頂けると助かります。	御質問の件について、例えば、クラウドサービス事業者が登録や登録の更新等を行うために制度運営側に提供した自社のサービスのセキュリティ等に関する機微な情報は全て「秘密情報」に該当します。その上で、当該「秘密情報」については、本制度の運用にあたって、ISMAP運営委員会、制度所管省庁、ISMAP運用支援機関がアクセスする可能性がございますが、これらの職員については、国家公務員法第100条第１項及び情報処理の促進に関する法律第41条の秘密保持義務の規定が適用されます。 その上で、いただいた御意見を踏まえて、制度運営に関わる者の範囲が明確となるよう、記載を修正致します。 「ISMAP 運営委員会及び制度運営に携わる者」⇒「ISMAP運営委員会、制度所管省庁、ISMAP運用支援機関及びその委託を受けた者」
98	ISMAP基本規程	・該当箇所 [政府情報システムのためのセキュリティ評価制度（ISMAP）基本規程（案）] 第1章　総則/1.4.5　ISMAP運営委員会 ・意見内容 ISMAPの今後の手続きの透明化を奨めます。 ・理由 今後の手続きに透明性をもたらすためにも、ISMAP運営委員会の構成員、又、議事録の公開も含めISMAP運営委員会における協議内容がISMAPの利害関係者とどのように共有されるのかも明確にして頂けるようお願い致します。	御質問の件について、ISMAP運営委員会の構成員については、有識者及び制度所管省庁を想定しています。なお、有識者の選定については、利益相反のおそれがあるため、構成員の名前・所属等については非公表とさせていただきますが、クラウドサービス又は監査において知見があり、かつ中立的な立場での検討・判断が可能な方に参加していただくことを想定しています。 また、ISMAP運営委員会の議事についても、内容が個々のサービスのセキュリティに関する機微な情報を扱うため、公表することは予定しておりません、
99	ISMAPクラウドサービス登録規則	■コメント対象箇所 3.2 申請者は、言明書に記載の監査対象期間の末日から原則として最大3ヶ月以内を報告書日とする監査報告書を監査機関から入手しなければならない。 ■コメント 監査報告書と実施結果報告書 は同じか。実施結果報告書という用語がこの規則ふくめ他の資料にて使われているようなのでそうであれば統一してほしい。	監査報告書と実施結果報告書は同一のものとなります。実施結果報告書に用語を統一致します。
100	ISMAPクラウドサービス登録規則	■コメント対象箇所 3.3 監査報告書において発見事項が発見された場合には、当該発見事項について改善計画書を作成しなければならない。 ■コメント 監査報告書と実施結果報告書 は同じか。実施結果報告書という用語がこの規則ふくめ他の資料にて使われているようなのでそうであれば統一してほしい。	監査報告書と実施結果報告書は同一のものとなります。実施結果報告書に用語を統一致します。
101	ISMAPクラウドサービス登録規則	■コメント対象箇所 (3) 契約に定める準拠法・裁判管轄に関する情報 ■コメント 監査報告書と実施結果報告書 は同じか。実施結果報告書という用語がこの規則ふくめ他の資料にて使われているようなのでそうであれば統一してほしい。	監査報告書と実施結果報告書は同一のものとなります。実施結果報告書に用語を統一致します。
102	ISMAPクラウドサービス登録規則	■コメント対象箇所 (4) 第三者による検査（ペネトレーションテストを含む）の実施に関する情報 ■コメント テストの結果まで必要なのか、それともペンテストを実行していることを記せばいいのか明確にしていただきたい。	本項における「第三者による検査（ペネトレーションテストを含む）」とは、脆弱性対策としての脆弱性検査ツールを用いた手法やペネトレーションテスト等を想定しております。また、「実施に関する情報」とは、その実施状況や受入に関する情報を指しており、実施結果内容の提供は想定しておりません。 いただいた御意見も踏まえて、上記の趣旨が明確になるよう、記載を修正致しました。 ＜修正後＞ （４）ペネトレーションテストや脆弱性診断等の第三者による検査の実施状況と受入に関する情報
103	ISMAPクラウドサービス登録規則	■コメント対象箇所 2) 申請者は、調達府省庁等との調達交渉時に、調達機関の求めに応じて、「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」(平成30年12月 10日関係省庁申合せ)(以下、「申合せ」という)の運用に協力すること。 ■コメント 前提として、この申し合わせが当該規則と齟齬がないようになっていないといけないが、そのようなすり合わせは事前に行われていることが確保されているのでしょうか。	ご指摘を踏まえ、本項は、宣誓事項ではない形で要求事項に記載します。 ＜修正後＞ 3.6 申請者は、調達府省庁等との調達交渉時に、調達機関の求めに応じて、「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」(平成30年12月10日関係省庁申合せ)(以下、「申合せ」という)の運用に協力すること。

104	ISMAPクラウドサービス登録規則	■コメント対象箇所 申請者は、ISMAP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について、登録期間中に利用者に重大な影響を及ぼしうる情報セキュリティインシデントが発生した場合には、 ■コメント 重大、の例示等をしていただきたい。 CSP側が「重大」とする定義とISMAP運営委員会側が「重大」とする定義が違った場合、（特にISMAP運営委員会側がより広くの案件を「重大」とした場合）CSP側では「重大」とみなされなかったインシデントを報告しなかった場合、何らかの理由でISMAP運営位委員会側がそのインシデントに気づき、彼ら側で「重大」と定義したために、CSPの報告がなかったことによって登録を抹消されてしまう（つまり、CSPとしては報告義務なしと思っていたために報告しなかったが、ISMAP運営委員会側で報告義務あり、と思っているためにCSP側が責任を果たさなかったとみなされてしまう）ようなことが起こりうるため。 例えば、CSPがその管理するCSIRTプロセスにおいて定義している重大レベル同等の場合でよし、など。	いただいた御意見も踏まえて、インシデント報告を求めるのはどのような場合かが明らかとなるよう、FAQ等において例示を行うものとします。
105	ISMAPクラウドサービス登録規則	■コメント対象箇所 本規則第 9 章の規定に従い、遅滞なくISMAP運営委員会に報告すること。 ■コメント 遅滞なく、の例示等をしていただきたい。 CSP側が「遅滞なく」とする定義とISMAP運営委員会側が「遅滞なく」とする定義が違った場合、（特にISMAP運営委員会側がより短い期間を「遅滞なく」とした場合）CSP側では「遅滞なく」報告したと考えた場合でも、ISMAP運営位委員会側がそのインシデントの報告された日時が「遅滞なく」報告したものではないと定義したために、CSPの報告が「遅滞なく」なかったことによって登録を抹消されてしまう（つまり、CSPとしては遅滞なく報告できたと思っていたが、ISMAP運営委員会側遅滞あり、と思ったためにCSP側が責任を果たさなかったとみなされてしまう）ようなことが起こりうるため。 例えば、CSPがその管理するCSIRTプロセスにおいて定義している外部に報告が必要な案件の対応計画と同等のレベルであればよし、など。	報告対象のセキュリティインシデントが生じた場合速やかにということを想定しています。
106	ISMAPクラウドサービス登録規則	■コメント対象箇所 申請者は、ISMAP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について登録期間中に重大な統制の変更及び当該変更につながりうる事象が生じた場合 ■コメント 重大、の例示等をしていただきたい。 CSP側が「重大」とする定義とISMAP運営委員会側が「重大」とする定義が違った場合、（特にISMAP運営委員会側がより広くの案件を「重大」とした場合）CSP側では「重大」とみなされなかったインシデントを報告しなかった場合、何らかの理由でISMAP運営位委員会側がそのインシデントに気づき、彼ら側で「重大」と定義したために、CSPの報告がなかったことによって登録を抹消されてしまう（つまり、CSPとしては報告義務なしと思っていたために報告しなかったが、ISMAP運営委員会側で報告義務あり、と思っているためにCSP側が責任を果たさなかったとみなされてしまう）ようなことが起こりうるため。 例えば、CSPがその管理するCSIRTプロセスにおいて定義している重大レベル同等の場合でよし、など。	いただいた御意見も踏まえて、インシデント報告を求めるのはどのような場合かが明らかとなるよう、FAQ等において例示を行うものとします。
107	ISMAPクラウドサービス登録規則	■コメント対象箇所 又はISMAPクラウドサービスリストに掲載されている情報に変更が生じた場合には、本規則第10章の規定に従い、遅滞なくISMAP運営委員会に届け出ること。 ■コメント 具体的になんの情報か明確にしていただきたい。	ISMAPクラウドサービスリストに掲載する情報については、ISMAPクラウドサービス登録規則 3.8に規定しております。その上で、3.5(3)では、当該項目に変更が生じた場合に、本規則第10章の規定に従い、遅滞なくISMAP運営委員会に届け出ることを要求しております。
108	ISMAPクラウドサービス登録規則	■コメント対象箇所 本規則第10章の規定に従い、遅滞なくISMAP運営委員会に届け出ること。 ■コメント 遅滞なく、の例示等をしていただきたい。 CSP側が「遅滞なく」とする定義とISMAP運営委員会側が「遅滞なく」とする定義が違った場合、（特にISMAP運営委員会側がより短い期間を「遅滞なく」とした場合）CSP側では「遅滞なく」報告したと考えた場合でも、ISMAP運営位委員会側がそのインシデントの報告された日時が「遅滞なく」報告したものではないと定義したために、CSPの報告が「遅滞なく」なかったことによって登録を抹消されてしまう（つまり、CSPとしては遅滞なく報告できたと思っていたが、ISMAP運営委員会側遅滞あり、と思ったためにCSP側が責任を果たさなかったとみなされてしまう）ようなことが起こりうるため。 例えば、CSPがその管理するCSIRTプロセスにおいて定義している外部に報告が必要な案件の対応計画と同等のレベルであればよし、など。	ISMAPクラウドサービスリストに掲載されている情報について変更が生じたことを認知し次第速やかにということを想定しています。

109	ISMAPクラウドサービス登録規則	■コメント対象箇所 (6) 申請者は、ISMAP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について登録の一時停止又は削除を受けた場合には、当該サービスを利用している調達府省庁等に、その旨を速やかに通知又は登録者のWebサイトにて公開しなければならない。 ■コメント 7.2によるとウェブサイトの更新は運営支援機関が実施すると読み取れる。 ここの書き方だとクラウドサービスの申請者がWebサイトに公開できるように読み取れるので、Webサイトで公開する権限を申請者に付与しないのであれば、明確に、登録者のWebサイトでの公開をISMAP運営支援機関に申請する、などとしていただきたい。	御指摘の3.5(6)における「登録者のWebサイト」とは、クラウドサービス事業者のHP等を想定しており、サービスの登録の一時停止又は削除を受けた場合には、当該クラウドサービスを提供する事業者は、当該サービスを利用している調達府省庁等に対してその旨を速やかに通知を行うか、自社のHP等において公開することを要求しております。 そのため、原案のとおりとします。 なお、7.2は、サービスの登録更新に関する規定であり、これについてはISMAP運用支援機関がISMAPクラウドサービスリストを更新し、制度のWebサイトを通じて公開するものとします。
110	ISMAPクラウドサービス登録規則	■コメント対象箇所 (7) 申請者は、他の事業者（以下、「委託先」という）の利用の有無にかかわらず、自社のクラウドサービスにおける契約及び情報セキュリティ上の問題が生じた場合は、自社の責任において当該クラウドサービスの利用者との間で解決を図ること。 ■コメント この対応の対象となる委託先を絞らなければ、全てのクラウドサービスの運用に関わらない委託先（例えばクラウドサービス事業者の給与支払いサービスの委託先など）も含められるように解釈されてもおかしくない。明確に、申請するクラウドサービスの運用に関わる委託先、とすべき。	クラウドサービスの利用者との間で解決が必要なケースの場合、必然的に委託先の範囲もサービス提供に限定されると考えられるため、原案のままとします。
111	ISMAPクラウドサービス登録規則	■コメント対象箇所 3.8 申請者が提出書類、申請手続き及びISMAP運用支援機関との連絡に使用する言語は、日本語でなければならない。 ■コメント 提出書類のうち、別添するような資料には日本語以外も含まれる可能性があるため、別添以外の、としていただく必要がある。	いただいた御意見も踏まえて、提出書類のうち別添資料に関しては、日本語もしくは英語で記載いただくものとし、英語の場合には参考訳をつけることを求める場合がある旨を補足するものとします。
112	ISMAPクラウドサービス登録規則	■コメント対象箇所 3.12 サービス登録を更新に際しても本章の内容を準用する。なお、前回申請時の監査対象期27 間と更新の申請時の監査対象期間が連続するようにしなければならない。 ■コメント を ではなく の ではないでしょうか	いただいた御意見を踏まえて修正致します。
113	ISMAPクラウドサービス登録規則	■コメント対象箇所 (1) 4.1に規定する申請文書が日本語で作成されており、不足がないこと。 ■コメント 申請文書（特に別添）については、管理策に関する説明等が含まれると思うが、その場合、管理コントロールのオーナーがAttestしなければならない。 コントロールオーナーがほぼグローバルであることから、基本的に英語でしかAttestできない。（日本語訳はコントロールオーナーが理解できないため、訳文をAttestはできない）したがって、こういう情報は英語で作成せざるを得なくなるため、「別添」については日本語でなくてよし、としていただかなければ、コントロールオーナーからの宣誓がとれない。	いただいた御意見も踏まえて、提出書類のうち別添資料に関しては、日本語もしくは英語で記載いただくものとし、英語の場合には参考訳をつけることを求める場合がある旨を補足するものとします。
114	ISMAPクラウドサービス登録規則	■コメント対象箇所 (4) 実施結果報告書が有効であること ■コメント 監査報告書と実施結果報告書 は同じか。実施結果報告書という用語がこの規則ふくめ他の資料にて使われているようなのでそうであれば統一してほしい。	監査報告書と実施結果報告書は同一のものとなります。実施結果報告書に用語を統一致します。
115	ISMAPクラウドサービス登録規則	■コメント対象箇所 5.2 ISMAP運用支援機関は、申請文書の確認の結果、内容に不明点がある場合、申請者に問い合わせ又は追加の資料提出要請を行う。 ■コメント 意図不明確な資料まで要求されないよう、追加資料提出要請時には、その理由を記すなどの対応をお願いしたい。	5.2の「不明点がある場合」とは、5.1(1)から(4)の確認が取れない場合等を想定しております。 その上で、実際の運用を行う上では、いただいた御意見も参考に、追加資料提出要請時にその理由もあわせて通知する等の対応を検討して参りたいと思います。
116	ISMAPクラウドサービス登録規則	■コメント対象箇所 (7) その他、本制度の規程類に照らして違反がない、もしくは違反歴がないこと。 ■コメント 違反歴があった場合は例えば是正したとしても何度申請しなおしても認められないとなるのでしょうか。そうでないならば、違反歴については削除すべき。	ここでの違反歴とは、ISMAPクラウドサービス登録規則14.2の規定によって削除された場合を指しており、その旨が明らかとなるよう、ご指摘も踏まえて下記のとおり修正致しました。 ＜修正後＞ (7) その他、本制度の規程類に照らして違反がない、もしくは過去に14.2(4)による登録の削除を受けていないこと。
117	ISMAPクラウドサービス登録規則	■コメント対象箇所 6.2 ISMAP運用支援機関は、前項の審査を行うにあたり、必要に応じて、制度所管省庁の監督の下、申請者に追加の情報提供を求めることができる。 ■コメント 意図不明確な資料まで要求されないよう、追加資料提出要請時には、その理由を記すなどの対応をお願いしたい。	「前項の審査を行うにあたり」と記載のとおり、6.2において追加の情報提供を要請するケースとしては、6.1の(1)から(7)の確認が取れない場合等を想定しております。 その上で、実際の運用を行う上では、いただいた御意見も参考に、追加資料提出要請時にその理由もあわせて通知する等の対応を検討して参ります。

118	ISMAPクラウドサービス登録規則	■コメント対象箇所 (3) 申請を受理した日から6カ月以内に開催するISMAP運営委員会において、登録の審査を行う。 ■コメント 基盤となるIaaSに依存するサービスの場合は年に２度しか審査がないと、監査のタイミングによっては、最悪１年以上待たなければ自社サービスが登録されないということになる。 この審査のいかんによってはサービスを使える・使えないが明確に別れビジネスへの影響が大きいことから、もう少し審査頻度をあげていただきたい。 また、監査の実施時期をあらかじめ予定立てするためにも、審査のタイミングを事前に公表していただきたい。	6.4(3)は、申請を受理してから登録の審査を行うまでの期限を定めるものであり、審査頻度を定めるものではありません。 また、審査の実施時期については、いただいた御意見も参考に、目安となる時期を公表する等、具体的な運用方法を検討して参ります。
119	ISMAPクラウドサービス登録規則	■コメント対象箇所 7.1 ISMAP運用支援機関は、ISMAP運営委員会が登録の決定を行ったクラウドサービスについて、ISMAPクラウドサービスリストに登録し、Webサイトを通じて公開する。また、申請者に「様式5 登録通知書」により通知する。 ■コメント 公開する情報の範囲を明確にしていただきたい。その内容によっては、必要な社内承認プロセスが追加されるため。	ISMAPクラウドサービスリストに掲載する情報については、ISMAPクラウドサービス登録規則3.7に規定しております。
120	ISMAPクラウドサービス登録規則	■コメント対象箇所 7.1 ISMAP運用支援機関は、ISMAP運営委員会が登録の決定を行ったクラウドサービスについて、ISMAPクラウドサービスリストに登録し、Webサイトを通じて公開する。また、申請者に「様式5 登録通知書」により通知する。 ■コメント 現状のCOVID-19関連でも浮き彫りになっている問題として、紙のやりとりがあります。例えば、ビルやオフィスが閉鎖されたために紙のやりとりに対応ができず、そのために契約等のやりとりが滞るなど。 この時代においては、他国でも電子的な署名を用いるなどの対応でデジタルな書類を正とするやりとりが行われていますので、この取り組みでも是非、紙ではなく電子的書類でのやりとりをしていただきたい。	今後、本制度ホームページの構築を予定しており、その中でご要望のオンライン申請につきましても、対応を検討して参ります。
121	ISMAPクラウドサービス登録規則	■コメント対象箇所 7.4 ISMAP運用支援機関は、本規則の6.3に規定するISMAP運営委員会の判断を受けて、登録要求事項を満たしていないとしたクラウドサービスについて、ISMAPクラウドサービスリストに登録できない旨を申請者に「様式6 結果通知書」により通知し、審査登録手続を終了する。 ■コメント 結果通知書には、明確にどこが登録できないと判断した理由なのかを記載いただくことを明記してほしい。（でないと、改善対応が難しい）	登録審査において要求事項を満たしていないと判断された場合において、その理由を通知することは検討しておりません。
122	ISMAPクラウドサービス登録規則	■コメント対象箇所 9.1 登録者は、登録されている自身のクラウドサービスについて情報セキュリティインシデントが生じた場合、遅滞なく「様式7 情報セキュリティインシデントに関する報告書」に必要事項を記載し、ISMAP運用支援機関を通じてISMAP運営委員会に報告すること。 ■コメント 遅滞なく、の例示等をしていただきたい。 CSP側が「遅滞なく」とする定義とISMAP運営委員会側が「遅滞なく」とする定義が違った場合、（特にISMAP運営委員会側がより短い期間を「遅滞なく」とした場合）CSP側では「遅滞なく」報告したと考えた場合でも、ISMAP運営位委員会側がそのインシデントの報告された日時が「遅滞なく」報告したものではないと定義したために、CSPの報告が「遅滞なく」なかったことによって登録を抹消されてしまう（つまり、CSPとしては遅滞なく報告できたと思っていたが、ISMAP運営委員会側遅滞あり、と思ったためにCSP側が責任を果たさなかったとみなされてしまう）ようなことが起こりうるため。 例えば、CSPがその管理するCSIRTプロセスにおいて定義している外部に報告が必要な案件の対応計画と同等のレベルであればよし、など。	報告対象のセキュリティインシデントが生じた場合速やかにということを想定しています。
123	ISMAPクラウドサービス登録規則	■コメント対象箇所 9.2 ISMAP運用支援機関は、登録者が9.1の報告を行っていないにも関わらず、情報セキュリティインシデントの発生を認知した場合、当該サービス登録の一時停止を行うとともに、前項に規定する報告を求めることができる。 ■コメント いきなりサービスを停止するのではなく、登録者と事実関係確認後、などの文言をいれていただきたい。	運用において適切にコミュニケーションはとりますが、規定上は原案のとおりといたします。
124	ISMAPクラウドサービス登録規則	■コメント対象箇所 9.3 ISMAP運用支援機関は、前二項の報告の内容を受けて、必要に応じて追加の報告を求めることができる。 ■コメント 報告内容の定義や制限をしていただきたい。ISMAP運用支援機関が必要以上に社内情報や機密情報を取得しないコントロールも必要である。	本規定の趣旨は、審査に必要な限度で追加的な情報を要求するというものであり、「必要に応じて」と記載している原案のとおりで御指摘は踏まえられているものと考えています。

125	ISMAPクラウドサービス登録規則	■コメント対象箇所 9.4 ISMAP運用支援機関は、本章に規定する報告の内容を受けて、必要に応じて本規則第11章に規定するモニタリングを実施することができる。 ■コメント こちらも、何が必要となる定義なのかを制限していただかないと、ISMAP運用支援機関が細かく必要以上にモニタリングをしてしまう可能性を否定できない。 もし定義が難しい場合は、登録者と協議の上、などの条件をつけてほしい。（クラウド運営に影響がないためにも）	本規定の趣旨は、審査に必要な限度で追加的な情報を要求するというものであり、「必要に応じて」と記載している原案のとおりで御指摘は踏まえられているものと考えています。
126	ISMAPクラウドサービス登録規則	■コメント対象箇所 10.1 登録者は、登録されている自身のクラウドサービスについて重大な統制変更又は重大な統制変更につながり得る事象が発生した場合、 ■コメント 重大、の例示等をしていただきたい。 CSP側が「重大」とする定義とISMAP運営委員会側が「重大」とする定義が違った場合、（特にISMAP運営委員会側がより広くの案件を「重大」とした場合）CSP側では「重大」とみなされなかったインシデントを報告しなかった場合、何らかの理由でISMAP運営位委員会側がそのインシデントに気づき、彼ら側で「重大」と定義したために、CSPの報告がなかったことによって登録を抹消されてしまう（つまり、CSPとしては報告義務なしと思っていたために報告しなかったが、ISMAP運営委員会側で報告義務あり、と思っているためにCSP側が責任を果たさなかったとみなされてしまう）ようなことが起こりうるため。 例えば、CSPがその管理するCSIRTプロセスにおいて定義している重大レベル同等の場合でよし、など。 また、「重大な統制変更」が重複して記載されているので、削除が必要。	いただいた御意見も踏まえて、インシデント報告を求めるのはどのような場合かが明らかとなるよう、FAQ等において例示を行うものとします。
127	ISMAPクラウドサービス登録規則	■コメント対象箇所 遅滞なくISMAP運用支援機関を通じてISMAP運営委員会に「様式8 重大な統制変更届出書」により変更内容を届け出ること。 ■コメント 遅滞なく、の例示等をしていただきたい。 CSP側が「遅滞なく」とする定義とISMAP運営委員会側が「遅滞なく」とする定義が違った場合、（特にISMAP運営委員会側がより短い期間を「遅滞なく」とした場合）CSP側では「遅滞なく」報告したと考えた場合でも、ISMAP運営位委員会側がそのインシデントの報告された日時が「遅滞なく」報告したものではないと定義したために、CSPの報告が「遅滞なく」なかったことによって登録を抹消されてしまう（つまり、CSPとしては遅滞なく報告できたと思っていたが、ISMAP運営委員会側遅滞あり、と思ったためにCSP側が責任を果たさなかったとみなされてしまう）ようなことが起こりうるため。 例えば、CSPがその管理するCSIRTプロセスにおいて定義している外部に報告が必要な案件の対応計画と同等のレベルであればよし、など。	報告対象の重大な統制変更につながる事象が生じた場合速やかにということを想定しています。
128	ISMAPクラウドサービス登録規則	■コメント対象箇所 10.3 ISMAP運用支援機関は、登録者が前二項の届出を行っていないにも関わらず、当該規定に位置づける事象を認知した場合、当該サービス登録の一時停止を行うとともに、当該届出を求めることができる。 ■コメント いきなりサービスを停止するのではなく、登録者と事実関係確認後、などの文言をいれていただきたい。	運用において適切にコミュニケーションはとりますが、規定上は原案のとおりといたします。
129	ISMAPクラウドサービス登録規則	■コメント対象箇所 10.4 ISMAP運用支援機関は、本章に規定する届出の内容を受けて、必要に応じて本規則第11章に規定するモニタリングを実施することができる。 ■コメント こちらも、何が必要となる定義なのかを制限していただかないと、ISMAP運用支援機関が細かく必要以上にモニタリングをしてしまう可能性をひていできない。 もし定義が難しい場合は、登録者と協議の上、などの条件をつけてほしい。（クラウド運営に影響がないためにも）	本規定の趣旨は、審査に必要な限度で追加的な情報を要求するというものであり、「必要に応じて」と記載している原案のとおりで御指摘は踏まえられているものと考えています。
130	ISMAPクラウドサービス登録規則	■コメント対象箇所 11.1 ISMAP運用支援機関は、登録者が本規則第3章に規定する要求事項を登録期間中にわたって継続的に満たしていることを確認するために、以下の各号に該当する場合にモニタリングを実施することができる。 ■コメント モニタリングをする場合であっても、その実行期間に制限を設けていただきたい。 本業であるサービス運営に影響が出ないようにするためにも、ある程度の期間の縛りは必要と考える。（最長xx週間など）	モニタリングに要する期間は、発生した事象等の性質に応じて異なるため、一律に規定することは困難であると考えますが、11.1に規定する範囲において、サービス運営に支障をきたさない範囲で実施を行うことが適切であると考えます。
131	ISMAPクラウドサービス登録規則	■コメント対象箇所 2) 本制度を構成する者その他外部からの苦情又は情報提供等により、要求事項への適合性に疑義が生じた場合。 ■コメント 苦情内容の精査もなしに受けてしまうと、営業妨害や誹謗中傷など本来正しい苦情ではない場合に問題が生じるため、登録者と事実関係を確認の上、などの文言を入れていただきたい。	運用において適切にコミュニケーションはとりますが、規定上は原案のとおりといたします。

132	ISMAPクラウドサービス登録規則	■コメント対象箇所 14.1 登録者は、次のいずれかに該当する場合、遅滞なく「様式12 登録取下届出書」を制度所管官庁に届け出ること。 ■コメント 遅滞なく、の例示等をしていただきたい。CSP側が「遅滞なく」とする定義とISMAP運営委員会側が「遅滞なく」とする定義が違った場合、（特にISMAP運営委員会側がより短い期間を「遅滞なく」とした場合）CSP側では「遅滞なく」報告したと考えた場合でも、ISMAP運営位委員会側がそのインシデントの報告された日時が「遅滞なく」報告したものではないと定義したために、CSPの報告が「遅滞なく」なかったことによって登録を抹消されてしまう（つまり、CSPとしては遅滞なく報告できたと思っていたが、ISMAP運営委員会側遅滞あり、と思ったためにCSP側が責任を果たさなかったとみなされてしまう）ようなことが起こりうるため。例えば、CSPがその管理するCSIRTプロセスにおいて定義している外部に報告が必要な案件の対応計画と同等のレベルであればよし、など。	コメントの趣旨が御指摘の箇所と一致しておらず、回答が困難です。
133	ISMAPクラウドサービス登録規則	■コメント対象箇所 (1) 登録の有効期間が終了したとき ■コメント 有効期間が終了し、かつ、更新申請がでていないとき、ではないでしょうか。	いただいた御意見も踏まえて、下記のとおり修正致します。 ＜修正後＞ (1) 登録の有効期間までに更新の申請が行われなかったとき
134	ISMAPクラウドサービス登録規則	■コメント対象箇所 差し出した記録が確認できる郵送方法とすること ■コメント 現状のCOVID-19関連でも浮き彫りになっている問題として、紙のやりとりがあります。 例えば、ビルやオフィスが閉鎖されたために紙のやりとりに対応ができず、そのために契約等のやりとりが滞るなど。 この時代においては、他国でも電子的な署名を用いるなどの対応でデジタルな書類を正とするやりとりが行われていますので、この取り組みでも是非、紙ではなく電子的書類でのやりとりをしていただきたい。	今後、本制度ホームページの構築を予定しており、その中でご要望のオンライン申請につきましても、対応を検討して参ります。
135	ISMAP管理基準	■コメント対象箇所 1.3 用語及び定義 ■コメント 「経営陣」の定義をしていただきたい。 いわゆるボードメンバーとなると、全部の管理策をかれらが直接運営することはないが、ボードが適切な実行責任、権限を付与した組織体であれば実行可能。 そういったものが認められるかどうかが重要。	1.3 用語及び定義に記載のとおり、本項に示す用語及び定義以外に関しては、P.1 28行目から34行目に示す規程等の用語の定義に準ずるものとしております。その上で、「経営陣」についてはJIS Q 27014の定義に準ずるものとします。
136	ISMAP管理基準	■コメント対象箇所 2.2.2言明の対象範囲 一つのクラウドサービス名称であっても、その傘下に複数のサービスがある場合等、どのサービスを対象にしているのか具体的に記載する。 また、この言明の対象外となるサービスを利用してここに記載するサービスを提供している場合その範囲及び利用しているサービスを明示し、言明書の対象外になる旨記載をする。ただし、サービスの基盤に言明の対象外となるクラウドサービスを利用している場合には、当該対象外のサービスがISMAPクラウドサービスリストに登録されていることが求められる。また、対象となるリージョンを記載する。 ■コメント リージョンの意味を明確にしていただきたい。データセンターのことなのか ?それとも運営部隊か ?運営チームはグローバルであるため明記が困難だが、データセンターの場所であるならば記載が可能。	「クラウドサービスの安全性評価に関する検討会とりまとめ」の「2.3 監査関連基準等の検討（４）リージョンとサンプリングの考え方」に記載のとおり、リージョンとは、クラウドサービスを提供する情報処理設備を収容するデータセンターが設置されている独立した地域を指すと考えています。この考えについてはFAQ等において示したいと考えています。
137	ISMAP管理基準	■コメント対象箇所 4.4.1.1 ■コメント 本文の4.4.1.1には、以下のポイントも含まれているが、この別表にはない。あるべきなのか、ないはずなのか。 ・内部監査報告書やそれらに基づ□是正処置、マネジメントレビュ□ 議事録等に、トップマネジメントの□□意思、判断、指示等が□含まれていること。	「内部監査報告書やそれらに基づ□是正処置、マネジメントレビュ□□議事録等に、トップマネジメントの□□意思、判断、指示等が□含まれていること。」は4.4.1.1に含まれております。ファイル形式の問題により別表では非表示となっているため、修正致しました。
138	ISMAP管理基準	■コメント対象箇所 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。 (ア)経営陣は、管理者に、情報セキュリティが事業目的を十分にサポートし、支えることを確実にさせる。 ■コメント 「情報セキュリティ」がサポートする、というのは曖昧なので、「情報セキュリティ管理システム」がサポートし、と変更すべきではないか。	ここでいう「情報セキュリティ」とは、JIS Q 27000の定義も踏まえると、情報の機密性、完全性及び可用性を維持する組織の取り組みを指し、本管理策においては、この取り組みが事業目的と整合した形で実施されるよう要求しております。既存の規程において必要な定義が行われていることから、原案のとおりとします。

139	ISMAP管理基準	■コメント対象箇所 経営陣は、管理者に、情報セキュリティに積極的な文化を推進させる。 ■コメント ここでいう「文化」を監査するのは難しい（主観的すぎる）。 したがって、例えば情報セキュリティマネジメントの実施が確実にされていることや、従業者への情報セキュリティの教育の実施などによって判断すべきである。 これらについては、実際に管理策を見ればわかるので、この項目については、削除するべきではないか。（監査できない）	組織内で情報セキュリティ対策を維持・向上する上では、組織としてルールを遵守する文化を醸成することも重要であり、これを実現するための手段として、例えば、継続的な情報セキュリティ教育やマネジメントによる周知活動等が実施されることが想定されます。このため、監査においても、例えばこれらの取り組みを規程した文書類及びその実施結果等を確認することで、本管理策の実施状況を確認することが可能であると考えられます。そのため、原案のとおりとします。
140	ISMAP管理基準	■コメント対象箇所 経営陣は、外部の利害関係者に、組織がその事業特性に見合った情報セキュリティのレベルを実践していることを報告する。 ■コメント この「報告」について、何を具体的に要求しているのか。例えば、ISO27001などを取得していることを公表することでOKと見なされるのか。どこまでのレベルの「報告」を指しているのか明確にしていただきたい。 たとえば要求される都度、何らかの個別報告書を書かなければならないというのであれば、対応が難しい。	3.1.5に規定しているとおり、ここでの報告とは、経営陣が利害関係者との間で、双方のニーズを踏まえて情報セキュリティの活動及び課題に関する情報を伝達することを目的として実施することを要求されるものであり、具体的な報告の内容、対象、頻度等については、クラウドサービス事業者において実施するリスクアセスメントの結果を踏まえて決定されるものとなります。そのため原案のとおりとします。
141	ISMAP管理基準	■コメント対象箇所 経営陣は、情報セキュリティに関する規制上の義務、利害関係者の期待及び事業ニーズを認識する。 ■コメント 「利害関係者の期待および事業ニーズ」は主観的である。例えば全ての顧客にアンケートをとって期待やニーズを都度理解しなければならないとなると対応できない。 したがって、「利害関係者の期待および事業ニーズ」についてはどこまで対応すべきなのかを明確に示されていないと、監査できない。 過度に必要以上の要求をしてくるお客様もいるため、3.1.4.2に加えて「規制上の義務」があれば充分ではないか ？	3.1.5に規定しているとおり、ここでの報告とは、経営陣が利害関係者との間で、双方のニーズを踏まえて情報セキュリティの活動及び課題に関する情報を伝達することを目的として実施することを要求されるものであり、具体的な報告の内容、対象、頻度等については、クラウドサービス事業者において実施するリスクアセスメントの結果を踏まえて決定されるものとなります。 また、実際の監査においては、例えば、リスクアセスメント等の結果において関係する利害関係者を特定した上でアセスメントが実施されていること等を確認することで本管理策の実施状況を確認する方法等が想定されます。
142	ISMAP管理基準	■コメント対象箇所 トップマネジメントは、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。［27001-5.1b) / 5.1e) / 5.1f)］ ・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する。 ・情報セキュリティマネジメントがその意図した成果を達成することを確実にする。 ・情報セキュリティマネジメントの有効性に寄与するよう人々を指揮し、支援する。 また、トップマネジメントがリーダーシップ及びコミットメントを発揮していることを以下により確認する。 ・経営会議等の議事録に、トップマネジメントの情報セキュリティマネジメントに関する意思、判断、指示等が記録されていること。 ・情報セキュリティ方針、情報セキュリティ目的及びそれを達成する計画を策定する際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・達成すべきセキュリティの水準として、リスクレベルをトップマネジメントが決定していること。 ・リスクレベルに応じて選択したセキュリティ管理策を実施させる際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・内部監査において確認すべき事項に、トップマネジ ■コメント ここでいう「トップマネジメント」にでは、何を指しているのか。ガバナンス基準の「経営陣」と同じように、トップマネジメントが、単なるボードメンバーだけではなく、ボードメンバーに指名されたISMS運営の組織体をさすようであれば細かい項目へ対応ができる。 一概に「経営陣」＝ボードメンバーのみをさす、としないよう、定義を明確にすべきである。（文字通りの経営陣、が全ての各項目における細かい役割を実行しているかという観点で監査されてしまうと、問題が生じる可能性がある）「さらに、保証プロセスによって、情報セキュリティガバナンス及び達成したレベルについての独立した客観的な意見が得られる。」 この文章の「保証プロセス」とは具体的には何を求めているのか。独立した内部監査の実行等をさすのか、それとも外部監査の実行を求めているのか。具体的な要求事項を記載していただきたい。	JIS Q 27000に定義されているとおり、トップマネジメントとは、最高位で組織を指揮し、管理する個人又は人々の集まりを指します。また、マネジメントシステムの適用範囲が組織の一部だけの場合には、トップマネジメントとは、組織内のその一部を指揮し、管理する人をいい、また、トップマネジメントとは、ときに業務執行幹部と呼ばれることもあり、最高経営責任者、最高財務責任者、最高情報責任者及び類似の役職が含まれることがあります。本項における用語についても、上述の定義に準ずるものとなります。

143	ISMAP管理基準	■コメント対象箇所 トップマネジメントは、組織の役割について、以下の責任及び権限を割り当て、伝達する。［27001-5.3］ ・情報セキュリティマネジメントを、本管理基準の要求事項として適合させる。 ・情報セキュリティマネジメントのパフォーマンス評価をトップマネジメントに報告する。 また、情報セキュリティマネジメントを本管理基準の要求事項に適合させるために、以下のような責任・権限を割り当てていることを確認する。 ・セキュリティ要求事項を盛り込んだ情報セキュリティ方針等の文書を策定する責任・権限 ・リスクアセスメントにおいて、リスクを運用管理する責任･権限を持つリスク所有者 ・セキュリティ要求事項を満たす管理策を教育、普及させる責任・権限 ・セキュリティ要求事項を満たしているか監査する責任・権限 ・各プロセスの結果及び効果をトップマネジメントに報告する責任・権限 ・各プロセスの結果及び効果を組織内に周知する責任・権限 ■コメント 「各プロセスの結果および効果を組織内に周知する責任・権限」とあるが、具体的には何を要求しているのか。 例えばセキュリティ対応が不十分である時にその是正のために関係部門に通知し是正を求めることが当然あるが、全社員に細かいところまでを周知することは難しい。関係する部門ということであれば問題ない。 また、問題のない（期待通りの効果である）プロセスにおいて、継続プロセスであれば特に、その効果を都度都度通知することはないと考えられるため、どこまでを対応すべきなのかを明確にしてほしい。 （セキュリティコントロール全てのモニタリング結果を全社員・全部門に周知することは、どの会社も対応していないのではないか）	リスクアセスメントの結果及び効果を組織内に周知する際には、言明の対象となる範囲において、各組織において想定されるリスクに十分に対応できると当該組織が判断する粒度で周知されるべきものであると考えます。
144	ISMAP管理基準	■コメント対象箇所 組織は、組織の目的に関連し、かつ、情報セキュリティマネジメントの意図した成果を達成する組織の能力に影響を与える、以下の課題を決定する。［27001-4.1］ ・外部の課題 ・内部の課題 これらの課題の決定とは、組織の外部状況及び内部状況の確定のことをいう。外部状況及び内部状況には、以下のようなものが含まれる。 a) 外部状況 ・国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 ・組織の目的に影響を与える主要な原動力及び傾向 ・外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観 b) 内部状況 ・統治、組織体制、役割及びアカウンタビリティ ・方針、目的及びこれらを達成するために策定された戦略 ・資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術） ・情報システム、情報の流れ及び意思決定プロセス （公式及び非公式の双方を含む。） ■コメント 「以下のようなものが含まれる」とあるが、a)以下の例は全て内部資料（内部ポリシー）に反映されていないといけないのか、明確にしていただきたい。 当然考慮にはいれているが「以下のようなもの」となっているので、全例示を文書に含まなくても良いと考えていいか。 また、「ステークホルダの認知および価値観」とあるが、内部・外部共に、「価値観」を定義づけるのは難しい。ここでは何を求めているのか、具体的に示してほしい。（人の価値観を定義づけ、監査できるものなのか）	「以下のような」と記載しているとおり、a)以下は例示であり、本管理策に記載の内容及びリスクアセスメントの結果を踏まえて、本管理策及び関連する統制目標を満たすために必要と考えられる事項を実施いただくものとなります。

145	ISMAP管理基準	■コメント対象箇所 組織は、利害関係者のニーズ及び期待を理解するために、以下を決定する。 [27001-4.2] ・情報セキュリティマネジメントに関連する利害関係者 ・利害関係者の、情報セキュリティに関連する要求事項 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てもよいが、利害関係者には、以下のようなものが含まれる。 ・組織内で情報セキュリティマネジメントプロセスを推進する役割・権限を持つ人又は組織。例えば、以下のようなものをいう。 -情報セキュリティに関する方針等を策定する人又は組織(トップマネジメント等) -セキュリティ管理策を全組織に徹底させる人又は組織(総務部、情報システム部等) -情報セキュリティ監査を行う人又は組織(監査室等) -組織内の情報セキュリティ専門家 ・取引先、パートナー、サプライチェーン上の関係者 ・親会社、グループ会社 ・当該組織のセキュリティを監督する省庁、政府機関 ・ ■コメント 「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てもよい」とあるが、逆に、それ以外の要求事項を広く理解するのは難しい。 ガバナンスの3.1.5.3の項目にもコメントしたが、利害関係者の要求事項を知るために、例えば全ての顧客にアンケートをとって期待やニーズを都度理解しなければならないとなると対応できない。 また、「利害関係者には以下のようなものが含まれる」とあるが、例示されている名称全てを文書に入れないと監査が通らないのか、明確にしていただきたい。	具体的な対策内容については、本管理策の内容を踏まえた上で、クラウドサービス事業者において実施するリスクアセスメントの結果を踏まえて決定されるものとなります。 また、「以下のような」と記載しているとおり、「・組織内で」以下は例示であり、本管理策に記載の内容及びリスクアセスメントの結果を踏まえて、本管理策及び関連する統制目標を満たすために必要と考えられる事項を実施いただくものとなります。
146	ISMAP管理基準	■コメント対象箇所 組) 織は、情報セキュリティマネジメントの境界及び適用可能性を明確にし、適用範囲を決定する。 [27001-4.3] a) 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。 ・自らの事業 ・体制 ・所在地 ・資産 ・技術の特徴 ・外部及び内部の課題 ・利害関係者の情報セキュリティに関連する要求事項 ・組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係 b) 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。 c) 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。 ・外部状況には、以下のようなものが含まれる。 －国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 ■コメント 「以下のようなものが含まれる」と例示があるが、全ての例示を文書に含めないといけないのか。 また、4.4.2.1でもコメントしたが、「ステークホルダの認知および価値観」とあるが、内部・外部共に、「価値観」を定義づけるのは難しい ここでは何を求めているのか、具体的に示してほしい。（人の価値観を定義づけ、監査できるものなのか）（組織文化、についても同様）	「以下のような」と記載しているとおり、それが係る範囲は例示であり、本管理策に記載の内容及びリスクアセスメントの結果を踏まえて、本管理策及び関連する統制目標を満たすために必要と考えられる事項を実施いただくものとなります。 また、具体的な対策内については、本管理策の内容を踏まえた上で、クラウドサービス事業者において実施するリスクアセスメントの結果を踏まえて決定されるものとなります。
147	ISMAP管理基準	■コメント対象箇所 トップマネジメントは、以下を満たす組織の情報セキュリティ方針を確立する。 [27001-5.2] ・組織の目的に対して適切であること。 ・情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組 ・情報セキュリティに関連して適用する要求事項を満たすことへのコミットメントを含むこと。 ・情報セキュリティマネジメントの継続的改善へのコミットメントを含むこと。 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。 ■コメント 「情報セキュリティ目的を設定するための枠組」ではどういったものを要求しているか、明示いただけますか ？	具体的な対策内容については、本管理策の内容を踏まえた上で、クラウドサービス事業者において実施するリスクアセスメントの結果を踏まえて決定されるものとなります。

148	ISMAP管理基準	■コメント対象箇所 組織は、以下によって、情報セキュリティリスクアセスメントのプロセスを定め、適用する。［27001-6.1.2a) / 6.1.2b)］ a) 以下を含む情報セキュリティのリスク基準を確立し、維持する。 ・リスク受容基準 ・情報セキュリティリスクアセスメントを実施するための基準 b) リスク受容基準に、以下を反映するよう、考慮する。 ・組織の価値観 ・目的 ・資源 c) リスク受容基準を策定する際には、以下の点を考慮する。 ・原因及び発生し得る結果の特質及び種類、並びにこれらの測定方法 ・発生頻度 ・発生頻度、結果を考える時間枠 ・リスクレベルの決定方法 ・利害関係者の見解 ・リスク基準は、法律及び規制の要求事項、並びに組織が合意するその他の要求事項によって、組織に課せられるもの又は策定されるものもあること。 ■コメント 「組織の価値観」に関しては何を具体的に要求されているか明確にしていただけますか ？（どうやって監査するのでしょうか）	具体的な対策内容については、本管理策の内容を踏まえた上で、クラウドサービス事業者において実施するリスクアセスメントの結果を踏まえて決定されるものとなります。
149	ISMAP管理基準	■コメント対象箇所 組織は、以下によって、情報セキュリティリスクを評価する。［27001-6.1.2e)］ ・リスク分析の結果、決定されたリスクレベルとリスク基準との比較をする。 ・リスク対応のための優先順位付けを行う。 ・リスク評価の結果は今後の改善に利用するため保管する。 なお、リスク対応の優先順位を決定する際には、より広い範囲の状況を考慮し、他者が負うリスクの受容レベルについて考慮するとともに、法律、規制、その他の要求事項についても考慮する。 ■コメント 「他者が負うリスクの需要レベルについて考慮する」とは、具体的に何を要求しているのでしょうか。	4.4.7.1c)において、リスク受容基準を策定する際には、利害関係者の見解を含む事項に考慮することが規定されていることを踏まえて、本項においては、利害関係者のリスク受容の程度を考慮した上でリスク対応の優先順位を決定することを要求するものとなります。その上で、具体的な対策内容については、本管理策の内容を踏まえた上で、クラウドサービス事業者において実施するリスクアセスメントの結果を踏まえて決定されるものとなります。
150	ISMAP管理基準	■コメント対象箇所 組織の管理下で働く人々は、情報セキュリティマネジメントの要求事項に適合しないことの意味を認識する。［27001-7.3c)］ ■コメント 「認識する」ことを監査するのはどうやるのでしょうか。監査にするのであれば、この項目を教育の内容に含めること、などという具体的に実施できる内容にしていただきたいです。	監査においては、従業員に対して本管理策を認識させるための取り組みが組織として定義されており、実際にその取り組みが実施されていることが確認できる資料等を閲覧することや従業員への質問を行うことで、本管理策の実施状況を確認することとなります。
151	ISMAP管理基準	■コメント対象箇所 組織は、情報セキュリティマネジメントに関連する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。［27001-7.4］ a) 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。 ・コミュニケーションの内容（何を伝達するか。） ・コミュニケーションの実施時期 ・コミュニケーションの対象者 ・コミュニケーションの実施者 ・コミュニケーションの実施プロセス b) 内部コミュニケーションでは、以下に示すような者と、適宜及び定期的なコミュニケーションを実施する。 ・トップマネジメント ・情報セキュリティマネジメントを本管理基準の要求事項に適合させる権限者 ・情報セキュリティマネジメントのパフォーマンスをトップマネジメント又は組織内に報告する権限者 ・情報セキュリティマネジメントを本管理基準の要求事項に適合させる権限者 ・組織内の従業員 c) 外部コミュニケーションでは、以下に示すような者と、必要に応じて、コミュニケーションを実施する。 ■コメント 「以下に示すような者」として例示があるが、この例示は全て文書等に含めなければならないのか。それとも、一部があればよいのか、明確にしていただきたいと思います。	「以下に示すような」と記載しているとおり、それが係る範囲は例示であることは明らかです。

152	ISMAP管理基準	■コメント対象箇所 組織は、あらかじめ定めた間隔で内部監査を実施する。［27001-9.2a) / 9.2b)］ a) 内部監査を実施する際は、以下を確認する。 ・以下に適合していること。 －情報セキュリティマネジメントに関して、組織自体が規定した要求事項 －本マネジメント基準の要求事項 ・情報セキュリティマネジメントが有効に実施され、維持されていること。 b) 内部監査は、管理策の有効性を総合的に確認するために定期的に実施し、計画及び結果について以下の文書で管理する。 ・内部監査基本計画 ・内部監査実施計画 ・内部監査報告書 基本計画書では対象範囲、目的、管理体制及び期間又は期日について、実施計画では実施時期や実施場所、実施担当者及びその割当て及び詳細な監査の手法についてあらかじめ決める。予定通り実施されたことを証明するためにも、実施報告書を作成する。 c) 適合性の監査においては、以下の項目を対象に含む。 ・関連する法令又は規制の要求事項 ・情報セキュリティリスクアセスメントなどによって ■コメント 「内部監査基本計画」「内部監査実施計画」を個別に分ける理由を明確にしていただきたい。 内部監査基本計画と実施計画に含めるべき内容が含まれていれば、内部監査計画書というような１つの文書でカバーできるのではないか。 むやみに形式上の理由で☒複数の文書を作成することは単純に作業を増やすだけなので、目的をカバーしていればよいのではないか。また、文書名の名称が違ったとしても、内容が目的をカバーしていれば十分である旨明確にしていただきたい。（社内文章の名前については、会社によって命名ルール等あるため）	内部監査基本計画では内部監査の全体方針について、内部監査実施計画では実務に即したより詳細な内容を記載いただくことを想定しておりますが、本管理策で要求している内容を満たす範囲において、具体的な証跡名についてまで指定するものではありません。
153	ISMAP管理基準	■コメント対象箇所 トップマネジメントは、あらかじめ定めた間隔で、マネジメントレビューする。［27001-9.3］ あらかじめ定められた間隔でマネジメントレビューを実施するために、以下の点について考慮するとともに、文書化する。 ・マネジメントレビュー基本計画 ・マネジメントレビュー実施計画 ・マネジメントレビューのための実施報告 基本計画書では目的及び実施時期について、実施計画では詳細な監査の手法についてあらかじめ決める。 ■コメント 「マネジメントレビュー基本計画」「マネジメントレビュー実施計画」を個別に分ける理由を明確にしていただきたい。マネジメントレビュー基本計画とマネジメントレビュー実施計画に含めるべき内容が含まれていれば、マネジメントレ ビュー計画書というような１つの文書でカバーできるのではないか。 むやみに形式上の理由で複数の文書を作成することは単純に作業を増やすだけなので、目的をカバーしていればよいのではないか。また、文書名の名称が違ったとしても、内容が目的をカバーしていれば十分である旨明確にしていただきたい。（社内文章の名前については、会社によって命名ルール等あるため） また、「詳細な監査の手法」をここで入れる意味とは。ISOにもこの項目についてはないので、レビューのプランならわかるがここに監査を入れる意味はないと思われる。	マネジメントレビュー基本計画ではマネジメントレビューの全体方針について、マネジメントレビュー実施計画では実務に即したより詳細な内容を記載いただくことを想定しておりますが、本管理策で要求している内容を満たす範囲において、具体的な証跡名についてまで指定するものではありません。

154	ISMAP管理基準	■コメント対象箇所 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] ・前回までのマネジメントレビューの結果とった処置の状況 ・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 ・以下に示す内容を含めた、情報セキュリティパフォーマンスに関するフィードバック -不適合及び是正処置 -監視及び測定の結果 -監査結果 -情報セキュリティ目的の達成 ・利害関係者からのフィードバック ・情報セキュリティリスクアセスメントの結果及び情報セキュリティリスク対応計画の状況 ・継続的改善の機会 また、これらの情報を構成することが予想される活動及び事象を記録し、必要に応じて報告するとともに、緊急性が高いものについてはあらかじめ定義しておき、誰もが同じ判断をできるように基準を定める。 ■コメント 「利害関係者からのフィードバック」に求められる要求事項を明確にしていただきたい。例えばアンケートを取れ、ということならば難しい（人数が多い）が、情報事故や懸念を関係者が提出できる仕組みがあればよい、ということであれば対応可能であると考える。	具体的な対策内容については、本管理策の内容を踏まえた上で、クラウドサービス事業者において実施するリスクアセスメントの結果を踏まえて決定されるものとなります。
155	ISMAP管理基準	■コメント対象箇所 組織は、是正処置の証跡として、以下の文書化した情報を保持する。 [27001-10.1f) / 10.1g)] ・不適合の性質及びとった処置 ・是正処置の結果 ■コメント 「不適合の性質」では何を要求されているのか。「不適合の内容」では問題があるのか、具体的に何を求めているのか明確にしていただきたい。	不適合の内容及びとった処置について、文書化した情報を保持することを要求しております。原案で意味が通じるため、原案のとおりとします。
156	ISMAP管理基準	■コメント対象箇所 組織は、以下を行うことによって、文書化した情報を作成及び更新する。 [27001-7.5.2] ・適切な識別情報の記述（例えば、表題、日付、作成者、参照番号） ・適切な形式（例えば、言語、ソフトウェアの版、図表）及び媒体（例えば、紙、電子媒体）の選択 ・適切性及び妥当性に関する、適切なレビュー及び承認 ・文書化した情報のライフサイクルの定義や、それに応じた処理ができるような手順の策定 ・文書を発行する前における、適正性のレビュー及び承認 ・必要に応じた、文書の更新及び再承認 ・廃止文書の誤使用の防止 ・廃止文書を何らかの目的で保持する場合における、廃止文書であることが分かる適切な識別情報の記述・法的及び規制の要求事項及び環境の変化に従い、定めた頻度での更新 　また、これらのすべての活動が文書管理に反映されているか、またその活動が業務に大きな障害を与えていないかなどを考慮し、適切な文書管理手順を策定する。 ■コメント 第一に、ここでいう「文書化した情報」が4.8.1.1で定義した文書に限定されることを明示していただきたい。でなければ、全ての社内の文書にあてはめると、到底管理できるものではない。 「適切な形式」に、ソフトウェアの版を含める理由を明確にしていただきたい。 例えば文書を作成する文書ソフトのバージョンを文書ごとに管理し、バージョンがアップデートされるたびにその管理表を変更することは、複雑であり対応できない。例えば、文書の保管場所や保管形式を指示するのはよいが、たとえばポリシー文書をWordで作ろうが、GoogleDocで作ろうが、最終的にPDFで保存されていればその元となるソフトウェアやそのバージョンを管理することに意味はないと考える。	4.8.1.1において文書化の範囲を規定しており、これに続く本項4.8.2.1の要求がその範囲において適用されることは管理策の構成から明らかであることから原案のとおりとします。

157	ISMAP管理基準	■コメント対象箇所 組織は、以下のことを確実にするために、情報セキュリティマネジメントで要求された文書化した情報を、管理する。 [27001-7.5.3] ・文書化した情報が、必要なときに、必要なところで、入手可能かつ利用に適した状態であること。 ・文書化した情報が十分に保護されていること（例えば、機密性の喪失、不適切な使用及び完全性の喪失からの保護）。 ・文書化した情報の配付、アクセス 、検索及び利用 ・文書化した情報の読みやすさが保たれることを含む、保管及び保存 ・文書化した情報の変更の管理（例えば、版の管理） ・文書化した情報の保持及び廃棄 また、情報セキュリティマネジメントの計画及び運用のために組織が必要と決定した文書は、外部から入手したものであっても、必要に応じて、特定し、管理する。 ■コメント 「外部から入手したもの」の定義を明確にしていただきたい。	組織の外部から入手した文書を指します。前後の文脈からその意味は明らかであるため、原案のとおりとします。
158	ISMAP管理基準	■コメント対象箇所 ー ■コメント 別表３の管理策に関しては、 1) 用語や定義が曖昧な箇所については、明確な定義をしていただく必要があります。 2) 主観的な項目、または曖昧な書き方のためにどう監査で対応していいか不明瞭な箇所についても、明確にしていただく必要があります。 3) 管理策のうち、会社として導入するのが難しい、と判断される項目で、かつそれ自身を全て導入することがリスクを回避できる唯一の手段であるとも読み取れない管理策については、導入できないと思われるが、会社としてはガバナンス・マネジメントにおいてリスク管理をしていればその管理策の採否については審査時に問題ないと考えてよいでしょうか。	いただいた御意見を踏まえ、今後、ガイドラインやFAQ等の検討を進めてまいります。
159	ISMAP基本規程	・ 該当箇所 基本規程 3ページ 10行目： 「ISMAP標準監査手続」については、その配布を監査機関に限る。 ・ 意見内容 「制度運営に携わる者」の定義、範囲を明記すべきである。 ・ 理由 監査ガイドラインでは、監査機関に所属する監査業務実施者は、監査業務依頼者であるクラウドサービス事業者に対して、「標準監査手続に準拠して業務依頼者の言明する統制に対して手続を実施する責任を負う」と定められているのであるから、監査業務依頼者が、監査業務実施者がこの責任を果たしていること、あるいは、監査業務実施者による標準監査手続きの解釈の妥当性を確認するために、当然として、標準監査手続きを参照することが必要になる。加えて、クラウドサービス事業者が、予め、標準監査手続を参照することは、監査業務の実施期間に制約のあるところ、その効率化などの面に於いて双方にとって一定のメリットがある。にも拘わらず、当該箇所の記述だけでは、監査機関がこの標準監査手続きをクラウドサービス事業者に開示することを禁じられているものと誤解する恐れがある。	御指摘の件については、クラウドサービス事業者に手続き全体を供することは監査の実効性確保の観点から想定しておりませんが、概要や一部の手続きについて可能な限り公表したいと考えております。
160	ISMAP基本規程	・ 該当箇所 基本規程 9ページ 18行目： 第8章 ISMAP運営委員会が行う業務及び業務の委任 ・ 意見内容 本章に「業務の委任」に関する記述がないように思われる。また、9.3節他にある「事務の委任」と、本「業務の委任」との違いが判然としない。	御指摘の点を踏まえ、以下のように修正いたします。 ＜修正後＞ 第8章 ISMAP運営委員会が行う業務
161	ISMAP基本規程	・ 該当箇所 基本規程 9ページ 34行目： ISMAP 運営委員会及び制度運営に携わる者 ・ 意見内容 ・ 理由 制度に関連するクラウドサービス事業者、監査機関、制度に関係する委員会等の活動への参加者等が本定義に含まれるのかが曖昧であると、例えば監査機関のグループ企業が準拠支援サービスを行うことの要否が不明確となり、本制度に違反する恐れがある。	御質問の件について、例えば、クラウドサービス事業者が登録や登録の更新等を行うために制度運営側に提供した自社のサービスのセキュリティ等に関する機微な情報は全て「秘密情報」に該当します。その上で、当該「秘密情報」については、本制度の運用にあたって、ISMAP運営委員会、制度所管省庁、ISMAP運用支援機関がアクセスする可能性がございますが、これらの職員については、国家公務員法第100条第１項及び情報処理の促進に関する法律第41条の秘密保持義務の規定が適用されます。 その上で、いただいた御意見を踏まえて、制度運営に関わる者の範囲が明確となるよう、記載を修正致します。 「ISMAP 運営委員会及び制度運営に携わる者」⇒「ISMAP運営委員会、制度所管省庁、ISMAP運用支援機関及びその委託を受けた者」

162	ISMAP基本規程	・ 該当箇所 基本規程 10ページ 17行目： 9.5 サイバーセキュリティ対策推進会議、各府省情報化統括責任（CIO）連絡会議決定事項への配慮 ・ 意見内容 「本制度に求められる配慮事項」が何であるのかを具体的に示すべきである。特に、これが、本制度の施行日に於いて既に決定されているもののみであるのか、あるいは、施行日以降に決定され得るものも含むのかは、齟齬や拡大解釈が生じないように明記すべきである。 ・ 理由 サービス登録規則5.4節（2）において、本基本規程9.5に規定する配慮事項との関連で、登録申請が受理されな場合があるとされているので、この配慮事項の明示、並びに、その意図の記載は重要と思われる。	現時点において、サイバーセキュリティ対策推進会議、各府省情報化統括責任者（CIO）連絡会議での決定事項はなされておりませんが、御質問の件については、例えば、本制度の立ち上げに当たり、監査のキャパシティ等を勘案しつつ、必要に応じて、 各政府機関等の利用が見込まれるクラウドサービスが速やかに審査されるよう制度運営側において調達府省庁等を支援することが考えられます。
163	ISMAPクラウドサービス登録規則	・ 該当箇所 サービス登録規則 1ページ 14行目： 「様式2 経営者確認書」を作成し、自身のセキュリティ対策について言明要件に沿った言明を行い、言明した事項について監査機関の監査を受けなければならない。 ・ 意見内容 ・ 理由 申請者が作成した「様式２経営者確認書」に沿って監査機関による監査を行う流れになっているので、監査機関への依頼時に作成し提出するものと思われるが、監査ガイドライン（案）4.6.1では「監査の実施結果報告書の発行に先立ち、業務依頼者から経営者確認書を入手するする」とあるので、経営者確認書の作成は業務実施者が作成する実施結果報告書発行の直前ともとれ、作成時期が不明瞭である。	サービス登録規則（案）3.1に記載のとおり、申請者は言明書及び経営者確認書を作成し、その上で、監査ガイドライン（案）4.4.1(2)に規定する範囲で監査機関に対して本制度における監査業務を依頼することとなります。そのため、原案のとおりとします。
164	ISMAPクラウドサービス登録規則	・ 該当箇所 サービス登録規則 1ページ 25行目： 調達府省庁等が意図しないまま当該調達府省庁等の管理する情報にアクセスされ又は処理されるリスク ・ 意見内容 "クラウドサービスで取り扱われる情報"の内容、性質は利用者が判断するものであり、リスクアセスメントの責任は第一義に利用者にあることを明確にすする意味で、本条項を削除する、もしくは"クラウドサービス事業者がサービス上で取り扱われる情報を明確にする場合において"などの条件を明記すべきである。 ・ 理由 取り扱われる情報に対するリスクアセスメントは利用者の責任であり、評価及びその対応は利用者の判断や実装にゆだねられる。そのため、本条項に対してクラウド事業者は、"責任範囲外であるためリスク等の該当情報はない"という回答しかできないと考えられる。（IaaSやPaaSであれば、実行責任や説明責任は、調達府省庁およびそのシステムの実装に携わるシステムインテグレーターなどが責任を負う）ただし、例えば医療情報や特定個人情報などを扱うことを規約上明示しているSaaSプロバイダーなどでは本条項はあてはまるため、その意味では条件明示でも対応が可能となると考えられる。	クラウドサービスの利用にあたっては、調達側がその利用目的や業務の性質に照らして、リスクに応じてサービスの性質を見極めながら利用することが大前提となりますので、調達側がリスク評価を行うにあたって必要な情報提供がなされるよう、次のとおり修正致します 。 ・クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用され、調達府省庁等が意図しないまま当該調達府省庁等の管理する情報にアクセスされ又は処理されるリスクについて、ISMAP運営委員会及び当該省庁等がリスク評価を行うために必要な情報 なお、具体的にどのような情報を求めるのかについてはFAQ等で例示したいと思います。
165	ISMAPクラウドサービス登録規則	・ 該当箇所 サービス登録規則 1ページ 32行目： 申請するクラウドサービス従事者の所属、専門性、実績、国籍に関する情報 ・ 意見内容 ・ 理由 本節の見出しには「登録期間中において以下の事項に対応すること」とあるが、（2）項では「調達府省庁等との調達交渉時に、「申合せ」の運用に協力すること」となっている。 ・ 理由 「クラウドサービス従事者」の定義を広く捉えた場合、大規模な事業者の場合、その人数が数千名に及ぶ可能性もあるので、これらの従業員の専門性、実績情報提出は膨大な量となり、この定義や範囲が曖昧だとクラウドサービス事業者と調達機関との間での調達交渉時のトラブルにもつながりかねない。また、クラウドサービス事業者の統制を本制度において評価することで責任範囲を明確にすることが本制度の趣旨であり、調達時にあらためて追加の情報を求め、かつその結果によって事業者自体の選定に影響を与えることは本制度の意義を失い、調達の効率化を損なう恐れがある。	御指摘を踏まえ、次のとおり修正致します 。 (1)申請者は、調達府省庁等との調達交渉時に、調達機関の求めに応じて、言明書の詳細、申請するクラウドサービスの従事者のうち、利用者の情報又は利用環境に影響を及ぼす可能性のある者の所属、専門性、実績、国籍に関する情報を調達機関に対して提出すること。国籍については、個々人に紐付かない形で該当する国名を提出すること。
166	ISMAPクラウドサービス登録規則	・ 該当箇所 サービス登録規則 1ページ 34行目： 「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」の運用に協力すること ・ 意見内容 協力することを宣誓する期間を、「登録期間中」なのか、それとも、「調達交渉時」なのかを誤解の無い要用に記載すべきである。 ・ 理由 本節の見出しには「登録期間中において以下の事項に対応すること」とあるが、（2）項では「調達府省庁等との調達交渉時に、「申合せ」の運用に協力すること」となっている。	ご指摘を踏まえ、本項は、宣誓事項ではない形で要求事項に記載します。 ＜修正後＞ 3.6 申請者は、調達府省庁等との調達交渉時に、調達機関の求めに応じて、「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」(平成30年12月10日関係省庁申合せ)(以下、「申合せ」という)の運用に協力すること。

167	ISMAPクラウドサービス登録規則	・ 該当箇所 サービス登録規則 2ページ 20行目： 委託先の提供するサービスを利用して、自らの名前で提供している者でなければならない ・ 意見内容 申請者になり得る者と、申請者にはなることができない者とが、具体的に判る様な記述にするべきである。 ・ 理由 本節の前半は、「『申請の対象となるクラウドサービスを自社の提供するサービスを利用して、』又は『委託先の提供するサービスを利用して、』」と読めるが、前者は基本規定の用語の定義（1.4.2）から「クラウドサービス事業者」を指している考えられ、拠って、後者はクラウドサービス事業者以外を想定しているものと思われる。これが、クラウドサービス事業者以外であっても、自らの名前でサービスを提供している者（例えば、サービス再販事業者など）が申請者となれるということを意図しているのかが分かり難い。逆に、申請者にはなれない者を指定した方が分かり易いのではないか。	自らの責任において言明を行い監査をうけることができる者が申請者たりうるものと考えています。
168	ISMAP管理基準	・ 該当箇所 管理基準 2ページ 20行目： 1.3.10 クラウドサービス事業者が扱う情報 ・ 意見内容 「クラウドサービス事業者が扱う情報」の定義として、「クラウドサービス事業者が扱う情報の内、～～～を指す。」は誤記もしくは難解ではないか。	御意見を踏まえ、以下のように修正いたします。 ＜修正後＞ 1.3.10 クラウドサービス事業者が扱う情報 クラウドサービス事業者が扱う各種の情報の内、クラウド派生データ及び契約データを指す。 1.3.11 クラウドサービス利用者が扱う情報 クラウドサービス利用者の扱う各種の情報の内、クラウドサービスに入力した又はクラウドサービスの公開インタフェースを使ってクラウドサービス利用者又はその代理人がクラウドサービスの能力を実行して生じるデータで、クラウドサービス利用者に管理責任があるもの。例えば、クラウドサービス利用者が、クラウドサービス上に作成し、保有するデータなど。
169	ISMAP管理基準	・ 該当箇所 管理基準 7ページ 3行目： 監査の対象期間の末日以降、経営者確認書の日付までの間 ・ 意見内容 「重大な変更を及ぼしうる事象の発生の有無（ある場合には、その内容）」の対象期間を、「経営者確認書の日付」ではなく、その必要性に応じて、具体的な期間を設定すべきである。 ・ 理由 「経営者確認書の日付」は作成日と思われるが、経営確認書の作成時期が不明瞭であり、業務依頼者が作成した日によっては対象期間が短かったりする場合も想定され、本来、必要とされる情報が得られないことが懸念される。	御指摘の点については、経営者確認書の作成日は監査の対象期間の末日以降、監査対象期間の末日から3ヶ月以内の日付（ISMAPクラウドサービス登録規則の3.2により、申請者は査対象期間の末日から3ヶ月以内の日付での実施経過報告書を入手する必要があるため。）となります。監査のキャパシティが流動的であるため、具体的な日時について一律に設定することは困難であるため、３ヶ月の範囲内で任意で設定していただくものです。 なお、御参考までに、重大な統制の変更や重大な統制の変更につながり得る事象の発生については、登録後においてはISMAPクラウドサービス登録規則第10章において届出等を行うことで対応していただくことになっております。
170	ISMAPクラウドサービス登録規則	・ 該当箇所 サービス登録規則 3ページ 33行目： 【意見公募の対象外】(2) ISMAP運用支援機関は、申請書を受領した日から2週間以内に申請文書の確認を実施する。 ・ 意見内容 「確認を実施する」が、「確認作業の開始」なのか、「確認作業の完了」（受理/不受理の決定）なのかが判るように記載するべき。 ・ 理由 「2週間以内に確認作業が完了する」と捉えた場合、5.4（1）によれば、確認作業が1ヵ月以上に及ぶことも想定されるため、2週間以内に確認作業が完了しないこともあることになる。「2週間以内に確認作業を開始する」と捉えた場合、申請を受領した日から確認作業が完了する（受理/不受理の決定）日までの定めが無いことになり、次項の「申請を受理した日から6カ月以内に開催する～」があっても、申請の提出から登録の審査までの期間が定まらない。	6.4(2)では、申請者への確認事項等が生じない場合には二週間以内で終了することを想定した記載としており、問い合わせが必要な場合については、その問い合わせの時点から1か月以内に処理することが定められているものです。
171	ISMAPクラウドサービス登録規則	・ 該当箇所 サービス登録規則 4ページ 36行目： 【意見公募の対象外】重大な統制変更又は重大な統制変更につながり得る事象が発生した場合 ・ 意見内容 重大な変更には該当しないがクラウドサービスのアップデートや新機能の追加等、クラウドサービス利用者の便益につながる変更が発生した場合、利用者が問題なく当該新機能の検証および利用を可能とする仕組みを明確にするべきである。 ・ 理由 クラウドサービス事業者が主体的に当該統制の変更が重大な変更にあたらない旨を通知するとともにクラウドサービス利用者に開示できる仕組み（SOCにおけるBridge letterのような仕組み)をもうけ、それをISMAP運営委員会が即時性をもって評価することで、よりクラウドサービスの便益を利用者が享受することが可能となる。	重大な統制変更又は重大な統制変更につながり得る事象に該当しない事象であっても、クラウドサービス事業者が言明している管理策に関しては毎年の監査において確認が行われることとなるため、プロバイダが適切な対応をすることの担保につながると考えております。

172	ISMAP基本規程	意見1 ・該当箇所 政府情報システムのためのセキュリティ評価制度（IS MAP ）基本規定（案）中、 P1 23 行目から 28 行目 1.4.1 クラウドサービス 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（平成3 0 年 6 月7 日各府省情報化統括責任者（ CIO ）連絡会議決定）の定義された、「事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの」をいう。 の記述について。 ・意見 本記述が定義されている「政府情報システムにおけるクラウドサービスの利用に係る基本方針」において、 SaaS 及び IaaS/PaaS のクラウドサービスに関しては検討方針や利用方針、選定 に関する 基本方針が示されております。 しかしながら、このいずれにも属さないセキュリティ系のクラウドサービスが多く市場では提供されておりますが、その性質上 SaaS 及び IaaS/PaaS のクラウドサービスの基本方針に全てを当て嵌めて検討することは適切 ではないと 考えます 。 この類のクラウドサービスについても本制度への登録が可能にな るよう、管理基準 項目からの例外等ご検討頂き、より明確に記載頂くか、あるいは、そういったセキュリティ系のクラウドサービスは本規定の対象外として、別指針を作成 頂くことを意見として提出致します。 ・意見理由 クラウドサービスの一つの形態として、セキュリティ系のサービスをクラウド化する動きが顕著であり、 EDR (Endpoint Detection and 、 CASB (Cloud Access SecurityBroker) 、 SIG(Secure Internet Gateway) 、 SASE (Secure Access Service Edge) 等がセキュリティ系のクラウドサービスが該当するかと存じます。 これらのセキュリティ系のクラウドサービスではその性質上、セキュリティ分析の必要性や検体情報等の扱い、暗号鍵の管理方法等で SaaS 及び IaaS/PaaS のクラウドサービスとは大きく異なる点がございます。 セキュリティ系のクラウドサービスにおいても、優れたサービスが競争力のある費用で政府機関で活用出来るよう、検討頂く必要があると考えます。	御指摘の点について、ISMAP基本規程の定義は、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」及び「政府機関等の情報セキュリティ対策のための統一基準」において使用されている定義を活用したものです。他方、管理基準については、本制度において、クラウドサービスのセキュリティの要件を設定するにあたり、既存の基準との整合性を踏まえ、クラウド情報セキュリティ管理基準の定義を活用したものです。 その上で、SaaS/IaaS/PaaSそれぞれにおいて、本制度において提示しているクラウドサービスの定義に該当するものについては、政府機関等への納入を目指す限りにおいて、原則として共通の管理基準に適合したセキュリティ対策を実装し、登録や登録の更新をしていただく必要がございますが、サービスの特性上、原理的に特定の管理策についての具備が不可能と解される場合には、一定の例外措置を設けることとします。ただし、その場合においても、利用者による当該サービスの採否の判断に資するよう、当該管理策の具備が不可能である理由など関連する情報については、適切に利用者に対して開示を行うことが必要です。
173	ISMAP管理基準	意見2 ・該当箇所 ISMAP 管理基準（案） 中、 P28 41 及び 42 行目 「8.1.5.P クラウドサービス事業者の領域上にあるクラウドサービス利用者の資産は、 41クラウドサービス利用の合意の終了時に、時期を失せずに返却または除去する。 」の記述について。 ・意見内容 返却または除去するクラウドサービス利用者の資産の定義について確認させて下さい 。 ・理由 クラウドサービス事業者が提供するサービスのうち、セキュリティ分析等を実施するサービスにおいては、クラウドサービス利用者より分析の為に送られた疑わしい検体やURL情報等が含まれます。 この類の情報に関しては資産という定義から外れ、当該利用者に限らず以後の対策の為に広く必要なものであり、返却または除去の対象ではない認識でおりますが、相違御座いませんでしょうか。	御指摘の点について、原則ユーザにとって情報資産に該当するものは返却または除去する必要がある情報資産となります。サービスの特性上、原理的に特定の管理策についての具備が不可能と解される場合には、一定の例外措置を設けることとします。ただし、その場合においても、利用者による当該サービスの採否の判断に資するよう、当該管理策の具備が不可能である理由など関連する情報については、適切に利用者に対して開示を行うことが必要です。 例えば、対象となるクラウドサービスが、そもそも情報資産をユーザ側から提供しそれに基づいて分析するようなサービスである場合、返却や除去にの扱いについてはユーザとプロバイダの契約に基づいてその扱いが決定されるべきものであり、上記の対象として解される可能性があると考えております。
174	ISMAP管理基準	意見3 ・該当箇所 ISMAP管理基準（案） 中、 P28 29 行から 36 行に掛けての管理策 8.1.2.7.PB について ・意見内容 上記該当箇所に、下記の文章を追記されることを意見として提出致します。 (c) 当該利用者が、情報の解析等を行うために資産をクラウドサービス事業者に提供する場合は、クラウドサービス事業者が記録媒体に記録する前に暗号化し、暗号鍵を管理し消去する機能 ・理由 一般的にセキュリティの解析等を行うサービスにおいては、当該利用者は解析に必要な情報をクラウドサービス事業者に提供し、その情報に基づいて、クラウドサービス事業者がリスク分析やアノマリ検知等の解析サービスを実施致します。その際に提供される情報は、解析に使用できるようクラウドサービス事業者がその内容を確認できる必要があります。 よって、 当該利用者が暗号鍵を管理し、当該利用者のみが内容を確認できる方式ではなく、クラウドサービス事象 者 において、当該利用者から提供された情報を管理し暗号鍵によって管理することが必要だと考えます。	御指摘の点について、本管理策においては、利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理する機能を提供し、または、当該利用者が暗号鍵を管理する方法についての情報を提供することを求めていますが、一方で、クラウドサービス事業者において鍵を管理できることを否定しておらず、10.1.1において事業者側による暗号化の取組を求めているため、原案のままとします。

175	ISMAP管理基準	意見4 ・該当箇所 ISMAP管理基準（案） 中、 P30 8 行から 11 行に掛けての管理策 9.4.1.8.PB について ・意見内容 上記該当箇所において下記の通り、文章を修正されることを意見として提出致します。 9.4.1.8.PB クラウドサービス事業者は、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス、及びサービスにて保持されるクラウドサービス利用者のデータへのアクセスを、クラウドサービス利用者が制限できるよう、アクセス制御を提供する。 また、このアクセス制御についてはユーザ認証等による制御も可とする。 ・理由 当該管理策の「アクセス制御」に求められる具体的な機能が解釈次第で異なることが懸念されますので、具体的な例を記載することにより、要件の内容が明確になるものと考えます。	御意見の件について、ユーザ認証等による制御も本管理策の対象に含まれると考えます。 御意見を踏まえ、今後予定をしておりますガイドライン等の作成時の参考とさせて頂きます。
176	ISMAP管理基準	意見5 ・該当箇所 ISMAP管理基準（案 中、 P30 42 行から 45 行に掛けての管理策 10.1.2.20.PB について ・意見内容 上記該当箇所において下記の通り、文章を修正されることを意見として提出致します。 10.1.2.20.PB クラウドサービス事業者は、クラウドサービス利用者に、当該利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理する機能を提供し、または、当該利用者が暗号鍵を管理する方法についての情報を提供する。ただし、当該利用者が、情報の解析等を行うために資産をクラウドサービス事業者に提供する場合は、暗号鍵をクラウドサービ ス事業者が管理する機能を提供する。 ・理由 一般的にセキュリティの解析等を行うサービスにおいては、当該利用者は解析に必要な情報をクラウドサービス事業者に提供し、その情報に基づいて、クラウドサービス事業者がリスク分析やアノマリ検知等の解析サービスを実施致します。その際に提供される情報は、解析に使用できるようクラウドサービス事業者がその内容を確認できる必要があります。 よって、当該利用者が暗号鍵を管理し、当該利用者のみが内容を確認できる方式ではなく、クラウドサービス事象者において、当該利用者から提供された情報を管理し暗号鍵によって管理することが必要だと考えます。	御指摘の点について、本管理策においては、利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理する機能を提供し、または、当該利用者が暗号鍵を管理する方法についての情報を提供することを求めていますが、同時にクラウドサービス事業者において鍵を管理できることを否定しておらず、10.1.1において事業者側による暗号化の取組を求めているため、原案のままとします。
177	ISMAP管理基準	意見6 ・該当箇所 ISMAP管理基準（案） 中、 P57 別表 3 管理策 基準 10.1.1.10.P について ・意見内容 下記の通り、文章を修正されることを意見として提出致します。 10.1. 1 10 .PB クラウドサービス事業者は、クラウドサービス 利用者 が 独自の暗号による保護 の 適用を 希望した場合、実装の可否について 回答し 、また実装が可能な場合はそれを支援するため に必要な情報を クラウドサービス 利用者に提供する 。 ・理由 原文ではクラウドサービスにおいて、独自の暗号が適用可能な実装が必須かが不明瞭なため、明確に記述すべきと考えます。 また、 クラウドサービスが電子政府推奨暗号リスト記載の暗号を標準で実装している場合は、独自の暗号の利用は必須ではなく任意の実装とすることが妥当と考えます。	御指摘の点については、管理策10.1.1.10.Pについては、基本言明要件でない管理策のため、実施については各クラウドサービス事業者の判断に委ねられることとなります。そのため、独自の暗号が適用可能な実装は、制度上の登録の観点からは必須項目ではありません。

178	ISMAP情報セキュリティ監査ガイドライン	・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。） ISMAP情報セキュリティ監査ガイドライン（案） 　4ページ　第2章　独立性、客観性と職業倫理 ・意見内容 実務実施者に対する独立性に関する要求は、情報セキュリティ監査基準の定めによるとある。この要求事項から参照される「情報セキュリティ監査基準」では、外観上の独立性として「目的によっては、被監査主体と身分上、密接な利害関係を有することがあってはならない」とある。「密接な利害関係」に対する本ガイドラインとしての解釈の追記を行う。 （例） ・対象となるクラウドサービス業者に対してセキュリティ関連の業務（コンサルティング、ソリューションなど）を提供している会社 ・対象となるクラウドサービス業者の関係会社 ・理由（可能であれば、根拠となる出典等を添付又は併記してください。） 情報セキュリティ監査基準は、汎用的な基準ではあるが、個別の状況に応じての具体性を欠く点がある。そのため、情報セキュリティ監査基準の参照だけでは、本制度で意図する実務実施者の独立性の要件として曖昧であり誤解を生じる可能性があるため、本ガイドラインでの具体的な事例の提示が必要と考える。	いただいた御意見も参考に、ISMAP情報セキュリティ監査ガイドラインの独立性に関する記載を修正致します。
179	ISMAP監査機関登録規則	・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。） ISMAP監査機関登録規則（案）１ページ 　第3章　申請者に対する要求事項　3.1　対象 ・意見内容 ISMAP監査機関リストの登録対象として、情報セキュリティ監査を業務として行っている法人とありますが、この対象として、ISMS認証機関、クラウドクラウドセキュリティ認証機関も登録対象として頂きたい。（対象に含まれているのならOK） ・理由（可能であれば、根拠となる出典等を添付又は併記してください。） ISMAP管理基準（案）は、ISO/IEC 27001、ISO/IEC 27017の要求事項が多く採用されており、このことから力量、実績ともに、ISMS認証機関、クラウドセキュリティ認証機関は対象として適切であると考える。	監査機関に対する要求事項については、本制度は情報セキュリティ監査制度に基づくものとして、ISMAP監査機関登録規則（案）第3章に規定しているとおりであり、ISMAP運営委員会によって本章の要求事項を満たしていると判断された者が監査機関として登録されることとなります。
180	ISMAP監査機関登録規則	・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。） ISMAP監査機関登録規則（案）1ページ 　3.4　業務品質 ・意見内容 “～「情報セキュリティ監査サービス」として登録を受けていること。”に加えて下記の事項も加えるべきである。 「又は、ISMS適合性評価制度のISMSクラウドセキュリティ認証の認証機関としての認定を受けていること」 ・理由（可能であれば、根拠となる出典等を添付又は併記してください。） ISMAP管理基準（案）は、ISO/IEC 27001、ISO/IEC 27017の要求事項が多く採用されており、ISMSクラウドセキュリティ認証の認証機関でも業務品質を確保することができることが可能と考える。	監査機関に対する要求事項については、本制度は情報セキュリティ監査制度に基づくものとして、IISMAP監査機関登録規則（案）第3章に規定しているとおりであり、ISMAP運営委員会によって本章の要求事項を満たしていると判断された者が監査機関として登録されることとなります。

181	ISMAP監査機関登録規則	・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。） ISMAP監査機関登録規則（案）2ページ 　3.5.1　倫理審査機能を有する組織への所属 ・意見内容 倫理審査機能を有する組織に所属することを要求しており、倫理審査機能を有する機関として指定されているのは、「特定非営利活動法人 日本セキュリティ監査協会」となっている。倫理審査機能を有する機関の役割は、「情報セキュリティ監査の実施状況等について審査を行い、必要に応じて倫理審査に諮り、処分を行う」ことから、その機関に所属する組織が監査機関であるような表現は、公平性の点から望ましくない。「所属する組織」ではなく「倫理審査機能を有する組織から審査を受けることに合意する組織」とするべきである。 また、倫理審査機能を有する組織としては1組織だけでなく、「情報マネジメントシステム認定センター（ISMS-AC）」等も含めるべきである。 ・理由（可能であれば、根拠となる出典等を添付又は併記してください。） 意見内容にも記載したとおり、倫理審査機能を有する機関の役割の点から、その期間に所属する組織という表現は望ましくないと考える。また、特定の団体の所属会員になることを義務付けることも公平性の点から問題と考える。 倫理審査機能を有する組織の追加に関しては、ISMAP管理基準（案）は、ISO/IEC 27001、ISO/IEC 27017の要求事項が多く採用されており、ISMS／クラウドセキュリティの認証機関の認定審査を行う認定機関である「情報マネジメントシステム認定センター（ISMS-AC）」も、その機能を有すると考える。	御指摘を踏まえて、以下のとおり修正いたします。 （修正案） 3.5.1　情報セキュリティ監査に関する倫理審査機能を有する組織への所属
182	ISMAP監査機関登録規則	・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。） ISMAP監査機関登録規則（案）2ページ 　3.6.1 及び3.7.1 業務執行責任者及び業務実施責任者の資格要件 ・意見内容 業務執行責任者及び業務実施責任者の資格要件の１つとして、JRCA日本要員認証協会が認定する「ISMS主任審査員資格保有者又はISMS審査員資格保有者」、「クラウドセキュリティ審査員資格保有者」の２つの資格を加える。 ・理由（可能であれば、根拠となる出典等を添付又は併記してください。） 本制度の趣旨から、業務執行責任者及び業務実施責任者の妥当な力量資格（監査員の力量、情報セキュリティ及びクラウドサービスセキュリティの力量）として、JRCA日本要員認証協会が認定するISMS主任審査員又はISMS審査員資格保有者、クラウドセキュリティ審査員資格保有者も適切と考える。 JRCA　情報セキュリティマネジメントシステム審査員の資格基準及び評価登録基準 https://www.jrca-jsa.or.jp/datas/media/10000/md_5115.pdf	御指摘の点について、監査主体の資格要件としては、「情報セキュリティサービス基準」における「情報セキュリティ監査サービス」の資格要件と同一のものとすることを想定しておりますので、原案どおりとさせていただきます。なお、同等性の評価については、申請時に過去の実務において準拠した基準等の確認を行った上で、個別に判断を行うものとします。
183	ISMAP監査機関登録規則	・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。） ISMAP監査機関登録規則（案）2ページ 　3.6.2　実務経験等 ・意見内容 本規則は、実務経験として、情報セキュリティ監査基準に基づく監査、システム監査基準に基づく監査、あるいは、これらと同等と見なせる監査制度を求めている。「これらと同等と見なせる監査制度」が具体的に何か不明である。例として、ISMS適合性評価制度及びISMSクラウドセキュリティ認証の認証機関での審査経験を示す。 ・理由（可能であれば、根拠となる出典等を添付又は併記してください。） ISMAP管理基準（案）は、ISO/IEC 27001、ISO/IEC 27017の要求事項が多く採用されており、このことから力量、実績ともに、ISMS認証機関、クラウドセキュリティ認証機関での審査経験は実務経験として適切であると考える。	御指摘の点について、監査主体の資格要件としては、「情報セキュリティサービス基準」における「情報セキュリティ監査サービス」の資格要件と同一のものとすることを想定しておりますので、原案どおりとさせていただきます。なお、同等性の評価については、申請時に過去の実務において準拠した基準等の確認を行った上で、個別に判断を行うものとします。

184	制度全般	1.本制度全般 １） 該当箇所： 全般 意見内容： 管理基準が完成する5～6月のタイミングで、英語版の説明資料や管理基準の英語版の提供をも併せてお願い出来れば幸いです（日本国内外からのアクセスを想定した英語版Webページの提供など）。 理由： 海外に本社があるクラウドサービス事業者（以下CSP）が言明をする際には、海外担当者と連携を図った上で資料を準備致しますが、その際に翻訳に係る時間や、各社がそれぞれ行う翻訳作業において、語句の解釈が異なることから、誤解が生じるコストなどを勘案しますと、何らかの形で政府側より英語での文章をご用意頂いた方が良いかと存じます。	頂いた御意見も踏まえて各種文書の英訳版の整備についても今後検討してまいります。
185	ISMAP基本規程	2.<別添1>政府情報システムのためのセキュリティ評価制度(ISMAP)基本規程(案) １） 該当箇所： 1.4.5ISMAP運営委員会（P2：2行目） 意見内容： ISMAP運営委員会のメンバーの選定はどの様に行われるのでしょうか。 理由： 本制度の根幹をなす運営委員会のメンバーの選定について、客観的な選定方法についてご共有頂けますと幸いです。	御質問の件について、ISMAP運営委員会の構成員については、有識者及び制度所管省庁を想定しています。なお、有識者の選定については、利益相反のおそれがあるため、構成員の名前・所属等については非公表とさせていただきますが、クラウドサービス又は監査において知見があり、かつ中立的な立場での検討・判断が可能な方に参加していただくことを想定しています。
186	ISMAP基本規程	２） 該当箇所： 3.3申請の受理及び審査（P5：25行目） 意見内容： 25行目の「特段の瑕疵」とは具体的に何を指しますでしょうか。 理由： 「瑕疵」の内容次第によっては、申請が受理されないとのことですが、その具体的な例（たとえば書類の不備など）をご教示頂けますでしょうか。	御質問の件について、「特段の瑕疵」に該当するものとしては、例えば、登録に当たって提出が求められている書類等の明らかな不足や記載の不備などの形式上の瑕疵が挙げられます。
187	ISMAP基本規程	３） 該当箇所： 3.3申請の受理及び審査（P5：26～27行目） 意見内容： 「ISMAP運営委員会は、審査にあたり、必要な情報の提供を当該クラウドサービス事業者及び当該クラウドサービスの監査を行った監査機関に求めることができる。」とありますが、提供した情報の取扱いの前提（機密保持契約締結など）や取扱いの目的、並びに想定される（ISMAP運営委員会から）第三者への提供の範囲についても、明確にして頂けますと幸いです。 理由： 特に監査に関わる情報については、通常クラウドサービス事業者とお客様との間の機密保持契約に基づいて扱われる情報が含まれるため、当該情報の機密が厳格に守られることをお願い申し上げたく存じます。また、情報の取扱いやISMAP運営委員会以外への提供が審査に最低限必要な方法･範囲でのみ行われ、目的外の流用や提供が認められないことを明確にして頂けますと幸いです。	御質問の件について、例えば、クラウドサービス事業者が登録や登録の更新等を行うために制度運営側に提供した自社のサービスのセキュリティ等に関する機微な情報は全て「秘密情報」に該当します。その上で、当該「秘密情報」については、本制度の運用にあたって、ISMAP運営委員会、制度所管省庁、ISMAP運用支援機関がアクセスする可能性がございますが、これらの職員については、国家公務員法第100条第１項及び情報処理の促進に関する法律第41条の秘密保持義務の規定が適用されます。 その上で、いただいた御意見を踏まえて、制度運営に関わる者の範囲が明確となるよう、記載を修正致します。 「ISMAP 運営委員会及び制度運営に携わる者」⇒「ISMAP運営委員会、制度所管省庁、ISMAP運用支援機関及びその委託を受けた者」
188	ISMAP基本規程	４） 該当箇所： 3.7報告（P6：10～13行目） 意見内容： 「クラウドサービス事業者は、登録されている自身のサービスについて、利用者に重大な影響を及ぼしうる情報セキュリティインシデントが生じた場合には、速やかにISMAP運営委員会にその概要を報告しなければならない」とありますが、ここでいう「重大な影響を及ぼしうるセキュリティインシデント」はどの様なものを指しますでしょうか？具体的な指針や「重大」さの定義について明確にして頂けますと幸いです（例えば、言明書や「監査」において、コミットしたSLAを違反する場合が複数回発生し、顧客ビジネスの運営に支障を来たした等）。併せて、インシデントが「重大」となる定義を決定する際のプロセスについてもご教示頂ければ幸いです。 理由： 一定のレベルを有する「重大」さの定義が、ISMAP運営委員会に報告する際に必要かと存じます（CSP側が自己判断によりインシデントの「重大」さを決定することで、正しい報告がISMAP運営委員会に上がらず、更なる深刻な影響を顧客に及ぼす可能性があるため）。	いただいた御意見も踏まえて、インシデント報告を求めるのはどのような場合かが明らかとなるよう、FAQ等において例示を行うものとします。

189	ISMAP基本規程	５） 該当箇所： 4.4登録の更新（P7：1～6行目） 意見内容： ここでは、CSPは2年毎に登録を更新する必要がある旨述べられておりますが、仮に登録期間中にCSPが提供するサービス内容を増やした場合は、現状の登録にどの様な影響を与えますでしょうか（何か特別な対応が必要でしょうか）？ 理由： 弊社を含むCSPは常に新しい製品･サービスを展開しており、これらがISMAPの枠組みに適合出来るよう、実証してゆきたいと考えているところです。	御質問の件について、本制度ではクラウドサービスををサービスごとに登録することを想定していますので、仮に新たなサービスを提供開始し、当該サービスがすでに登録されているサービスと言明の対象範囲が異なる場合や、同様の統制の下に服していない場合には、そのサービスについて政府機関等に納入を意図される場合は、原則として当該新たなサービスについても登録を目指していただく必要がございます。
190	ISMAP基本規程	６） 該当箇所： 9.1秘密保持P9：33行～35行 意見内容： 「ISMAP運営委員会及び制度運営に携わる者は、秘密情報が本制度の運用に当たって無権限の者に伝わり、情報の機密性が損なわれることがないようにしなければならない。」とありますが、秘密保持の対象となる「秘密情報」およびこれにアクセスしうる「ISMAP運営委員会及び制度運営に携わる者」・「権限」ある者の範囲を明確に定義頂きたく存じます。また、調達府省庁等の担当者が機密保持義務（例：国家公務員法100条1項の規程など）を負うことを明確にして頂きたく存じます。 理由： 特に登録及び監査に関連する情報はCSPにとって機密性の高い重要な情報であるところ、①秘密情報として扱われるための要件が定められている必要があり、②調達府省庁等の担当者を含め、情報にアクセスする者の範囲が特定されていなければ、安心して内部情報を開示することが難しい旨ご理解頂ければ幸いです。	御質問の件について、例えば、クラウドサービス事業者が登録や登録の更新等を行うために制度運営側に提供した自社のサービスのセキュリティ等に関する機微な情報は全て「秘密情報」に該当します。その上で、当該「秘密情報」については、本制度の運用にあたって、ISMAP運営委員会、制度所管省庁、ISMAP運用支援機関がアクセスする可能性がございますが、これらの職員については、国家公務員法第100条第１項及び情報処理の促進に関する法律第41条の秘密保持義務の規定が適用されます。 その上で、いただいた御意見を踏まえて、制度運営に関わる者の範囲が明確となるよう、記載を修正致します。 「ISMAP 運営委員会及び制度運営に携わる者」⇒「ISMAP運営委員会、制度所管省庁、ISMAP運用支援機関及びその委託を受けた者」
191	ISMAPクラウドサービス登録規則	3.<別添2>ISMAPクラウドサービス登録規則（案） １） 該当箇所： 第3章「申請者に対する要求事項」3.4（P1：22～29行） 意見内容： 「(2)クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用され、調達府省庁等が意図しないまま当該調達府省庁等の管理する情報にアクセスされ又は処理されるリスクの評価結果とその具体的内容に関する情報」とありますが、①この項目を削除、若しくは②「意図」ではなく「関与」に変更、の何れかに変更願います。 変更されないのであれば、どういうケースを調達府省庁等が「意図しない」のか、CSPによる要求事項の理解のため、ご例示頂けますと幸いです。 また、リスク評価結果･内容について、どのような情報が要求されているか（例えば、国外の当局からアクセス要請があった場合に一般にクラウドサービス事業者がどう対応するのか、という対応プロセスなど）、本規則に記載頂くか、調達要件において記載するよう、お願い申し上げます。 理由： まず、「意図しないまま」という要件については、入札に際してその「意図」を事前にお示し頂けませんと、クラウドサービス事業者にとって、リスクの特定および評価が困難となります。また、日本国以外の当局が日本法以外の法令に基づき情報にアクセスする典型例は、その情報が犯罪または犯罪者に関するものである場合に、令状に基づく捜索がなされるケースですが、こうした事態は調達府省庁等としても通常「意図しない」と考えられる一方、令状発布に際しての司法審査を踏まえたものである以上、セキュリティの観点からは事前のリスク評価が重要若しくは、効果的なのかについては、別途慎重な議論が必要かと思われます。 よって、調達府省庁等の「意図しない」という要件は明確性を欠くだけでなく、調達時に必ずしも必要ではない情報を要求する結果となりかねないものと思料します。また、仮に「意図しないまま」が「調達府省庁等の与り知らぬところで」という意味であれば、「意図」という言葉を「関与」に変更することで、直接または（クラウドサービス事業者を通じて）間接的に関与しうる上記の捜索のようなケースは除外することができるものと考えます。 また、この点で要求されている情報について、国外の当局からアクセス要請があった場合に一般にクラウドサービス事業者がどう対応するのか、という対応プロセスに関する情報を提供することが考えられます。本登録の申請時に、調達府省庁等のクラウドサービスのご利用内容の詳細が決定されていない以上、かかる事態への対応に関するクラウドサービス事業者のスタンスが最も「セキュリティ評価」に資するものと思料します。	クラウドサービスの利用にあたっては、調達側がその利用目的や業務の性質に照らして、リスクに応じてサービスの性質を見極めながら利用することが大前提となりますので、調達側がリスク評価を行うにあたって必要な情報提供がなされるよう、次のとおり修正致します。 ・クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用され、調達府省庁等が意図しないまま当該調達府省庁等の管理する情報にアクセスされ又は処理されるリスクについて、ISMAP運営委員会及び当該省庁等がリスク評価を行うために必要な情報 なお、具体的にどのような情報を求めるのかについてはFAQ等で例示したいと思います。

192	ISMAPクラウドサービス登録規則	２） 該当箇所： 第3章申請者に対する要求事項3.5（P1：30～33行） 意見内容： 「申請者は、調達府省庁等との調達交渉時に、調達機関の求めに応じて、言明書の詳細、申請するクラウドサービス従事者の所属、専門性、実績、国籍に関する情報を調達機関に対して提出すること。」とありますが、①「クラウドサービス従事者」の範囲を調達府省庁等において必要最小限の範囲に限定して明確にして頂きたい他、②クラウドサービス従事者の「国籍」についてはこの要件を削除するか、または特定の国籍を有する従事者がいるかどうかの開示をCSPが可能な範囲でお伝えするなど、特定の個人に紐付かない情報の提出で足りるものをご記載頂ければ幸いです。 理由： ①クラウドサービス事業者においてクラウドサービスに従事する者は多数にのぼりますが、ISMAPの制度趣旨からすれば、管理部門や営業部門等の人員に関わる情報は提出の必要が無いと考えられます。個々の従業員のプライバシー保護の観点から、安易に外部に個人情報を開示することは難しい旨ご理解頂ければ幸いです。 また、挙げられている情報の中でも②「国籍」については、クラウドサービス従事者の能力に本来関係しないと考えられるところ、特定の国籍を有する特定の従事者を、それを理由として排除することは国籍に基づく差別となりかねません。また、在留資格は当然確認するとしても、国籍に関する情報の聴取は差別につながりかねないことから、従業員の国籍に関する情報を収集しないクラウドサービス従事者も存在する旨伺っております。よって、かかる情報を要求事項とすることは避けて頂きたくお願い申し上げます。 仮に国籍情報の要求についてセキュリティ上止むを得ない理由があったとしても、入札は個別の従事者を判断するのではなく事業者を判断するものである以上、当該事業者において特定の国籍を有する従事者がいるかどうか開示が可能な限りで回答する、といった個人を特定しない形での情報提供で十分であると考えております。	御指摘を踏まえ、次のとおり修正致します 。 (1)申請者は、調達府省庁等との調達交渉時に、調達機関の求めに応じて、言明書の詳細、申請するクラウドサービスの従事者のうち、利用者の情報又は利用環境に影響を及ぼす可能性のある者の所属、専門性、実績、国籍に関する情報を調達機関に対して提出すること。国籍については、個々人に紐付かない形で該当する国名を提出すること
193	ISMAPクラウドサービス登録規則	３） 該当箇所： 第3章申請者に対する要求事項3.7（P2：17行目） 意見内容： 「後発事象」が指す内容を補足頂ければ幸いです。 理由： 求められる言明内容が不明であるため。	後発事象とは言明書の対象期間以降、実施結果報告書の日付までに発生した事象であって、当該監査期間を対象とした言明書の内容や監査の前提に影響を与えるような事象を想定しており、いただいた御意見も踏まえて、FAQ等において説明を示したいと考えています。
194	ISMAP管理基準	4.<別添3>ISMAP管理基準（案） １） 1.2「基準の特質」（P1：13～14行） 意見内容： こちらに記載されている「国際規格（JISQ27001:2014、JISQ27002:2014、14JISQ27017:2016）」という箇所ですが、これは日本工業規格であって、国際規格（ISO等）で無い旨申し添えておきます。 理由： （意見内容で述べた通り）	御指摘を踏まえ、以下のとおり、修正をいたします。 ＜修正後＞ こうした観点から、本管理基準は、国際規格に基づいた規格（JIS Q 27001:2014、JIS Q 27002:2014、 JIS Q 27017:2016）に準拠して編成された「クラウド情報セキュリティ管理基準(平成２８年度版)」(以下、「クラウド情報セキュリティ管理基準」という)を基礎としつつ、「政府機関等の情報セキュリティ対策のための統一基準群（平成30年度版」）(以下、「統一基準」という)、及び「SP800-53 rev.4」(以下、「SP800-53」という)を参照して作成されている。
195	ISMAP管理基準	２） 該当箇所： 2.2.8経営者確認書に記載すべき内容（P6：34～37行） 意見内容： 「業務依頼者は、言明の対象となるクラウドサービスに関して、サービスの内容及びセキュリティリスク分析の結果を踏まえて、管理基準に準拠して統制目標及び詳細管理策を選択し、対象期間にわたりそれらを有効に運用していることの言明を行う責任を有している旨」とありますが、こちらの「業務依頼者」とは誰を指すのかご教示頂ければ幸いです。 理由： 「業務依頼者」ではなく、クラウドサービス事業者が詳細管理策を定義するのではないかと想定しております（もし、「業務依頼者」がクラウドサービス事業者を指すのであれば、特段問題ございません）。	御質問の件については、「業務依頼者」は「クラウドサービス事業者」と同義です。
196	ISMAP管理基準	３） 該当箇所： 7「人的資源のセキュリティ」7.1.1.（P27：45～46行） 意見内容： 「全ての従業員候補者についての経歴などの確認は、関連する法令、規制及び倫理に従って行う」とありますが、ここにおける「関連する法令」及び「倫理」について、具体的な内容をご教示頂けますでしょうか？ 理由： 従業員のバックグラウンドチェックに関する法令の存在が不明であることに加え、「倫理」については各CSPが有している「行動原則」の様なものを参照すればよいのか、確認させて頂きたい次第です。	御質問の件について、本管理策では、従業員の選考において、労働基準法や男女雇用機会均等法、その他厚生労働省の指針などの関連法規制や倫理にしたがって、適切に行うことを要求しています。 また、経歴などの確認については、盗難や不正行為又は施設の不正利用のリスクを低減するために、重要なセキュリティプロセスに従事する予定の従業員等には、それらのリスクを考慮した確認をすることを意図して、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行うことを要求しています。

197	ISMAP管理基準	4） 該当箇所： 供給者関係15.1.1.16B（P34：28～32行） 意見内容： 「クラウドサービス事業者は、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内法以外の法令が適用された結果、クラウドサービス利用者の意図しないまま当該利用者の管理する情報にアクセスされ、又は処理されるリスクを評価して外部委託先を選定し、必要に応じて委託業務の実施場所及び契約に定める準拠法・裁判管轄を指定する。」とありますが、①この項目を削除、若しくは②「意図」ではなく「関与」に変更、の何れかに変更願います。変更されないのであれば、どういうケースを調達府省庁等が「意図しない」のか、CSPによる要求事項の理解のため、ご例示頂ければ幸いです。 理由： ISMAPクラウドサービス登録規則案の第3章「申請者に対する要求事項」3.4へのコメントと同様である旨ご理解頂ければ幸いです。なお、こうした日本以外の当局のアクセスは当該国の公法に基づくものですので、私法上の関係を規律する契約の準拠法や裁判管轄の指定の影響を受けるものでは無いという理解です。その意味では、契約の準拠法・裁判管轄の指定に関する要求事項はあまり意味をなさないものと思料致します。	クラウドサービスの利用にあたっては、調達側がその利用目的や業務の性質に照らして、リスクに応じてサービスの性質を見極めながら利用することが大前提となりますので、調達側がリスク評価を行うにあたって必要な情報提供がなされるよう、次のとおり修正致します 。 ・クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用され、調達府省庁等が意図しないまま当該調達府省庁等の管理する情報にアクセスされ又は処理されるリスクについて、ISMAP運営委員会及び当該省庁等がリスク評価を行うために必要な情報 なお、具体的にどのような情報を求めるのかについてはFAQ等で例示したいと思います。
198	ISMAP管理基準	5） 該当箇所： 16.1.7.13.PB（P35：19～21行） 意見内容： 「クラウドサービス事業者は、クラウドサービス利用者と、クラウドコンピューティング環境内の潜在的なディジタル形式の証拠、又はその他の情報の要求に対応する手順を合意する。」とありますが、「潜在的なディジタル形式の証拠」とは具体的に何を指しますでしょうか？（監査ログ等の「デジタル証跡」を残して欲しい、とのことでしょうか） 理由： 定義が不明なため、内容をご説明頂けますと幸いです。	御意見を踏まえ、今後予定をしておりますガイドライン等作成時の参考とさせて頂きます。
199	ISMAP情報セキュリティ監査ガイドライン	6.<別添5>ISMAP情報セキュリティ監査ガイドライン（案） 1） 該当箇所： 第2章独立性、客観性と職業倫理 意見内容： 「業務実施者に対する独立性、客観性及び職業倫理に関する要求事項は、情報セキュリティ監査基準の定めによる。」とありますが、「独立性」に関して、具体的にCSPとどのような関係にあることが独立性を害する事情と捉えられるのかご例示頂ければ幸いです。 理由： 弊社が本件に関する監査法人さまとの会話から、業務の性質（保証か助言か）に加え、「独立性」の要件が不明確であることから、評価業務の受任に支障が出る可能性がある旨コメントを頂戴したので、記載させて頂きました。	いただいた御意見も参考に、ISMAP情報セキュリティ監査ガイドラインの独立性に関する記載を修正致します。
200	ISMAP基本規程	対象文書：政府情報システムのためのセキュリティ評価制度（ISMAP）基本規程（案） 御指摘内容については別表を参照	本御意見については、別表にて個別に回答致します。
201	ISMAPクラウドサービス登録規則	対象文書：ISMAPクラウドサービス登録規則 御指摘内容については別表を参照	本御意見については、別表にて個別に回答致します。
202	ISMAP管理基準	対象文書：ISMAP管理基準（案） 御意見内容については別表を参照	本御意見については、別表にて個別に回答致します。
203	ISMAP管理基準	対象文書：ISMAP管理基準（案）別表3 御意見内容については別表を参照	本御意見については、別表にて個別に回答致します。
204	ISMAP監査機関登録規則	対象文書：ISMAP監査機関登録規則（案） 御意見内容については別表を参照	本御意見については、別表にて個別に回答致します。
205	ISMAP情報セキュリティ監査ガイドライン	対象文書：ISMAP情報セキュリティ監査ガイドライン（案） 御意見内容については別表を参照	本御意見については、別表にて個別に回答致します。

206	制度全般	■意見内容 本制度への対応のため、毎年、IaaS、PaaS、SaaSの全クラウド事業者に費用負担、人件費への負担が大きいです。更新も義務付けられており、クラウドの利用費用を押し上げる要素となる危険性があります。 また毎年対応するためのコスト（費用面、人員面）を持っていないが、利用するクラウドサービスとしては競争力のあるものである場合、調達元としてはそれらのサービスが利用できないことが構想力を失うリスクを許容させられることになります。 よって、監査性を担保しつつ、対応のためのコストを下げるための仕組みが必要であると考えます。 ■改善提案 認定監査法人による申請・登録だけではなく、FISC安泰基準のように、セルフアセスによる登録も認め、2段階の認定制度を認める、とすると良い。 また、有効期間を1年とせず、3年として、対応ベンダー側の費用削減をすべきである。	登録更新の要否の判断は申請者の判断によって行われるべきものであり、制度として更新を義務づけるものではありません。 また、本制度への対応コストに関しては、制度としても運用評価対象の例示を行うなど、効率化に向けた対応を行っているところですが、通常、継続的な監査を行う過程で、工程については一定の効率化が図られるものと考えております。 その上で、制度全体としてのコストのさらなる効率化については運用状況も踏まえ適切に検討していきたいと考えています。 なお、監査の有効期間に関しては、SOC2等の監査においても、1年を超える期間で監査の有効性を認めているものは、主要なものとしては存在しないと考えております。
207	制度全般	■意見内容 ISOやSoCレポートなど国際的に認知され利用されている各種の認証は、それぞれ定期的に見直され、認定されています。 本制度において、監査対象とする項目の内容もそれらの認定を参照されて作成されているので、それらの認定を取得していること自体を証跡とすることで監査に必要な期間、および費用を大幅に圧縮することができます。 これはCSPのみならず、監査法人側、および制度運営側の労力も最適化できると考えられます。 特定の取得済みの認定があれば、特定の項目について改めての監査証跡の提出は不要である旨を記載していただければ、全体的な効率化を図りつつも、制度としての位置づけを損なわないと認識しています。 ■改善提案 特定の取得済みの認定があれば、特定の項目について改めての監査証跡の提出は不要である旨を記載していただきたい。 特に、以下のような条件において不要であれば、監査性を確保しつつ、コストも抑えられると考えています。 ・更新においては、不要である。 ・該当の国際標準の監査法人主体が、ISMAPにおける監査法人と同じ場合（または、認定監査法人である場合）、改めての監査証跡の提出は不要である。	クラウドサービスの安全性評価に関する検討会とりまとめにも記載しているとおり、本制度において、業務実施者は、言明の範囲において、監査対象から直接入手した証跡を本制度で定める標準監査手続に従って評価を行うことが原則となります。その上で、監査人が標準監査手続を実施する際に適切と見なす場合には、他の認証・監査制度等において収集された証跡を利用することを認めることが監査の効率化の観点から有効であると考えます。 その上で、制度全体としてのコストのさらなる効率化については運用状況も踏まえ適切に検討していきたいと考えています。
208	制度全般	日本政府が、セキュリティリスクについてクラウドベンダーと共有する正式なプロセスを作ってほしい。	御指摘を踏まえ、今後の制度運用の参考とさせていただきます。
209	制度全般	セキュリティインシデントの報告義務について、義務の対象を明確化してほしい。個人情報漏洩も伴う場合は個人情報保護法上の報告義務と同期をとってほしい。	いただいた御意見も踏まえて、インシデント報告を求めるのはどのような場合かが明らかとなるよう、FAQ等において例示を行うものとします。
210	制度全般	ISMAPのステコミは守秘義務を守るということになっているが、それがどのように担保されるのか知りたい。	御質問の件について、例えば、クラウドサービス事業者が登録や登録の更新等を行うために制度運営側に提供した自社のサービスのセキュリティ等に関する機微な情報は全て「秘密情報」に該当します。その上で、当該「秘密情報」については、本制度の運用にあたって、ISMAP運営委員会、制度所管省庁、ISMAP運用支援機関がアクセスする可能性がございますが、これらの職員については、国家公務員法第100条第１項及び情報処理の促進に関する法律第41条の秘密保持義務の規定が適用されます。 その上で、いただいた御意見を踏まえて、制度運営に関わる者の範囲が明確となるよう、記載を修正致します。 「ISMAP 運営委員会及び制度運営に携わる者」⇒「ISMAP運営委員会、制度所管省庁、ISMAP運用支援機関及びその委託を受けた者」
211	制度全般	クラウドベンダーは申請書を郵送することになっている。オンライン申請を認めていただきたい。	今後、本制度ホームページの構築を予定しており、その中でご要望のオンライン申請につきましても、対応を検討して参ります。
212	ISMAP基本規程	■意見内容 29行目 第三者による検査（ペネトレーションテストを含む）の実施に関する情報が示しているものが不明瞭であり、提出される情報に偏りが出る可能性がある。 ■改善提案 具体的にどういう情報が必要となるか、例えば実施できる・できない、という情報なのか、実施した結果についての情報なのかを明示するとよい。	本項における「第三者による検査（ペネトレーションテストを含む）」とは、脆弱性対策としての脆弱性検査ツールを用いた手法やペネトレーションテスト等を想定しております。また、「実施に関する情報」とは、その実施状況や受入に関する情報を指しており、実施結果内容の提供は想定しておりません。 いただいた御意見も踏まえて、上記の趣旨が明確になるよう、記載を修正致しました。

213	ISMAP基本規程	■意見内容 16行目 更新の申請をしなければならない、という強制力は不要であると考えます。 ■改善提案 更新するかしないかの判断は申請者にゆだねられるべきです。	御指摘の点について、ISMAPクラウドサービス登録規則の8.1の記述は、「登録者が登録の有効期限以降も登録のステータスを維持する意向がある」ということを前提としている記述です。 御指摘の点を踏まえ、以下のとおり、記述を修正いたします。 ＜修正後＞ 8.1　登録者は、登録の更新を希望する場合は、登録の対象となった監査の対象期間の末日の翌日から1年4ヶ月後までに、更新の申請をしなければならない。
214	ISMAPクラウドサービス登録規則	■意見内容 29行目 第三者による検査（ペネトレーションテストを含む）の実施に関する情報が示しているものが不明瞭であり、提出される情報に偏りが出る可能性がある。 ■改善提案 具体的にどういう情報が必要となるか、例えば実施できる・できない、という情報なのか、実施した結果についての情報なのかを明示するとよい。	本項における「第三者による検査（ペネトレーションテストを含む）」とは、脆弱性対策としての脆弱性検査ツールを用いた手法やペネトレーションテスト等を想定しております。また、「実施に関する情報」とは、その実施状況や受入に関する情報を指しており、実施結果内容の提供は想定しておりません。 いただいた御意見も踏まえて、上記の趣旨が明確になるよう、記載を修正致しました。 ＜修正後＞ （４）ペネトレーションテストや脆弱性診断等の第三者による検査の実施状況と受入に関する情報
215	ISMAPクラウドサービス登録規則	■意見内容 16行目 更新の申請をしなければならない、という強制力は不要であると考えます。 ■改善提案 更新するかしないかの判断は申請者にゆだねられるべきです。	御指摘のとおり、登録更新の要否の判断は申請者の判断によって行われるべきものですが、8.1は登録の有効期間に関する規定であり、登録の更新を検討している場合において、本項に定める期間内に更新申請が行われない場合には自動的に登録が削除される旨を規定するものとなります。そのため、原案のとおりとします。
216	ISMAP管理基準	■意見内容 9.5.2.1.PB 責任分界点上（または、責任共有モデル上）、IaaSでは、OS以上の要塞化は利用者の責任です。この項目は、IaaS、PaaS、SaaSによってクラウドサービス事業者の責任範囲とならない可能性があります。また、言及している対象が、仮想マシン、となっているが、それがIaaSなのか、PaaSなのか、SaaSを指すのか定かではない。現行の表現では、仮想マシン（IaaS）のみを対象としているようにも読み取れるため、PaaSやSaaSの利用者にとって有効な質問とならない可能性があります。 ■改善提案 クラウドサービス事業者は、利用者に提供する環境やサービスについて、適切に要塞化し(例えば、クラウドサービスを実行するのに必要なポート、プロトコ ル及びサービスのみを有効とする）、適切な技術的管理策(例えば、マルウェア対策、ログ取得）を実施する、もしくは、利用者の責任範囲において適切に要塞化し、各種管理策を実施できること。	9.5.2.1.PBは仮想マシンを念頭においた管理策であり、CSPが仮想マシンを設定しないのであれば、対象外となります。そのため、原案のとおりとします。
217	ISMAP管理基準	■意見内容 10.1 暗号において、保管中のデータ(Data at Rest)と通信中のデータ (Data in Motion)についての暗号化の定義は各所で定められている。しかし使用中のデータ (Data in Use) についての定めがありません。10.1.1.9.PBでカバーされているとも読み取れますが、保管中及び通信中のデータの暗号化については別で述べられているので、使用中のデータについても明示的に追記すべきだと思われます。 ■改善提案 マルチテナントの環境において、使用中のデータであっても利用者の必要に応じて暗号化ができる機能を有すること。もしくは、マルチテナントのように使用中のデータの傍受が不可能なサービスである、シングルテナントの環境が利用できること。	御指摘の点については、使用中のデータ（Data in Use）については、海外において広く参照されているガイドラインがまだ存在しない分野と認識しております。今後、国際的な動向を踏まえつつ、必要に応じて要件化を検討していきたいと考えております。