「情報セキュリティ監査基準改正案等」に対する意見募集結果の概要及び具体的な修正内容

パブリックコメントに対してお寄せいただいた意見と、提出意見に対する考え方は以下のとおりです。皆様の御協力に厚く御礼申し上げます。

No	御意見の箇所	御意見の内容	御意見に対する考え方
1	全体	情報処理技術者試験への影響が大きいので周知を徹底することを強く求める。	御意見いただきありがとうございます。情報セキュリティ監査基準等の改訂がされた際は周知を図ってまいります。
2	全体	1. 提供フォーマットについて 現在の情報セキュリティ監査基準・管理基準については原則的にpdfでのテキスト提供になっていますが、新たな基準に対してはGRCツール等での利用を考慮し機械判読可能な形式での提供を希望します。Excel提供は検討済みとの噂を聞きましたが、OSCAL形式（JSON、YAML）での提供もご検討いただきたいです。	御意見いただきありがとうございます。いただいた御意見は、情報セキュリティ監査制度の普及を進める上での参考とさせていただきます。
3	全体	2. ISMAP管理基準との接合 情報セキュリティ管理基準については従来通りJISQ27001/27002に軸足を置く公開基準と捉えています。一方で、クラウドサービスに対するISMAP管理基準はJISQ27017/27002/27014を直接参照していることで詳細管理策の公開範囲が限定される状況になっており、今回策定する情報セキュリティ管理基準をJISQ27002の大体として参照する、または情報セキュリティ管理基準をクラウドに拡張した基準を新たに作成する、といった基準同士の接合を期待しております。	御意見いただきありがとうございます。いただいた御意見は、情報セキュリティ管理基準の活用策を検討する際の参考とさせていただきます。
4	全体	3. リスク基準の明示または例示 今回の改訂でリスクベース監査記述が全体的に追加されていますが、リスクマネジメントの基準の明示あるいは例示があるとリスクアセスメントのスコープやレベル感が具現化すると思います。考えつくところでJISQ31000、COBIT、NIST RMFなどの全方位向け基準、FISC安対などの業界標準、あとは企業独自で導入するリスクマネジメント方針などがあり、それらに一定のレベルを要求することでリスクベース監査の質を担保できると良いなと考えるものです。	御意見いただきありがとうございます。御意見を踏まえ、情報セキュリティ管理基準活用ガイドライン Ⅰ. 3.（3ページ）の脚注に次の内容を追記いたします。「2 リスク対応のための方針に基づくリスクマネジメントが行われていると、リスクベース監査がより効果的に実施できる。リスクマネジメントの基準として、JIS Q 31000、COBIT、NIST RMF（Risk Management Framework）などの例が挙げられる。また、業界で固有の基準を定めている例もある。」
5	情報セキュリティ管理基準案　属性一覧（P144…	■意見内容 属性の一覧の2つ目の表（P144の下段…P147まで）にタイトルがついていない。活用しやすいよう、タイトルを付けてほしい。 例えば、 ・管理策・属性対応表 ・管理策・属性マトリクス など ■理由 利用場面で関係者間で、 「あの下段のやつ」で「運用機能」が、「L：＃法令及び順守」の管理策を網羅した というような、あいまいな意思疎通ではなく、明確に、 「管理策・属性対応表」で「運用機能」が、「L：＃法令及び順守」の管理策を網羅した というような意思疎通ができた方が良いと考える。	御意見いただきありがとうございます。当該表は「Ⅶ. 属性一覧」として識別可能と考えられることから、原案のとおりとさせていただきます。

No	御意見の箇所	御意見の内容	御意見に対する考え方
6	情報セキュリティ管理基準活用ガイドライン案 3. 管理基準のさらなる活用 2. 管理策に関する属性情報の活用 表1　属性の一覧	■意見内容 　属性の一覧には、管理基準の「属性一覧　＜記号凡例＞」と合わす形で、記号を入れてほしい。 　具体的には、 　「管理策タイプ　＃予防」　　→「管理策タイプ　P　＃予防」 　「運用機能　　＃ガバナンス」→「運用機能　　G　＃ガバナンス」 　など。 ■理由 　2. 管理策に関する属性情報の活用　では、旧管理基準から見直された部分として、JIS Q 27002:2024　にて個々の管理策に新たに定義された属性を紹介し、これらの属性を手掛かりに、現場のリスク低減に資する、個別管理基準を策定する際の活用方法を提示しているのだと理解した。 　そうであれば、新管理基準の「属性一覧　＜記号凡例＞」と合わす形しておいた方が、読者に容易に伝わるのではないか。	御意見いただきありがとうございます。御意見のとおり追記させていただきます。
7	情報セキュリティ管理基準活用ガイドライン案 3. 管理基準のさらなる活用 2. 管理策に関する属性情報の活用 (1)個別管理基準を策定する際の活用方法	■意見内容 「【属性による管理策の分類】属性により、管理策を分類することができる。例えば、表の「管理策タイプ」では、…」と属性を使った活用例を文章で説明している。この部分が、より読者に容易に伝わるように、簡単な表（例えば、管理策タイプ「P　＃予防」の属性を持つ管理策を抽出した例など）を付けるとよいのではないか。 ■理由 　この後に続く、(2)監査を実施する際の活用方法　の部分で、「表2　属性を用いた管理策の抽出例」がついている。 　この表による例示は、いきなり、2軸で整理した表（サイバーセキュリティ概念×運用機能の2軸）になっており、JIS Q 27002:2024　に馴染みの浅い読者にとっては、いささか解読が複雑ではないかと考える。 　先に、1軸（例えば、管理策タイプの1軸で）で整理抽出した表の例を提示し、属性を手掛かりに、多数ある管理策を絞り込んでいく活用例を先に見せておいた方が、読者が理解しやすいと考える。	御意見いただきありがとうございます。御意見を踏まえ表1を修正させていただきます。
8	情報セキュリティ管理基準活用ガイドライン案 3. 管理基準のさらなる活用 2. 管理策に関する属性情報の活用 表2　属性を用いた管理策の抽出例	■意見内容 「表のタイトル」と「行見出し・列見出し」を少し改善してはどうか。 　具体的には、 　表のタイトル 　　属性を用いた管理策の抽出例　　→　　属性を用いた管理策の抽出例（サイバーセキュリティ概念×運用機能の2軸） 　列見出し 　　ガバナンス　　→　　G　＃ガバナンス　　など 　行見出し 　　識別　　→　　I　＃ガバナンス　　など ■理由 　今回改定する　情報セキュリティ管理基準　が、今後広く活用されるためには、JIS Q 27002:2024　にて個々の管理策に新たに定義された属性が、いかに上手く活用されるか（理解されるか）ではないかと個人的には考える。 　2. 管理策に関する属性情報の活用　の部分で、属性の説明や、表による説明があり、この点が考慮されているが、新たに定義された属性にまだ不慣れな読者が、ガイドラインなど通読しながら理解しやすいように、文書間のつながりが容易にわかるように、記号なども省略せず、表現を統一しておいた方が良いと考える。 　（管理基準の「属性一覧　＜記号凡例＞」と「下段の対応表（管理策＆属性）」と管理基準活用ガイドラインの各説明や各図表　の表現を統一化する）	御意見いただきありがとうございます。御意見を踏まえ、表1を修正するとともに、表2のタイトルを「運用機能「#資産管理（As）」に該当する管理策の抽出例」と修正させいただきます。

No	御意見の箇所	御意見の内容	御意見に対する考え方
9	「情報セキュリティ監査報告基準ガイドライン改正案」のp12「2.社会的合意方式のアシュアランス型情報セキュリティ監査報告書【様式2】の雛型」の「1.実施した手続の概要」	他の【様式2】の雛型では、リスクベースの監査）委託元が情報セキュリティリスク評価して管理策を選んだこと）への言及があるが、本様式では、その言及が薄いように思える。監査では、整備状況を適切に記載し、記載された整備状況通りに運用していることの確認をしているを述べているが、整備・運用する管理策そのものが、委託元のリスク評価によって選択されていることの記載が欠けているように思える。（段落「会社の情報せきゅりtえ位に関わるマネジメント管理策の有効性・・・マネジメントと管理策との関連によって異なる」では、上記の趣旨は伝わらないので）	御意見いただきありがとうございます。御指摘の箇所については雛形という性質上、記載する内容を典型的なものに絞っていることもあり、原案のとおりとさせていただきます。
10	「情報セキュリティ監査報告基準ガイドライン改正案」のp12「2.社会的合意方式のアシュアランス型情報セキュリティ監査報告書【様式2】の雛型」の「3.マネジメントと管理策の変更による影響と統制の限界」 と 「情報セキュリティ監査報告基準ガイドライン改正案」のp18「2.利用者合意方式のアシュアランス型情報セキュリティ監査報告書【様式2】の雛型」の「3.マネジメントと管理策の変更による影響と統制の限界」	「情報セキュリティ監査実施基準ガイドラン改正案」のp4「アシュアランス型監査」の説明で、「当該意見に一切の誤りがないという絶対的な保証ではないことに留意する。特に、被監査主体である組織体において、「インシデントが発生しないことを保証する」という誤解が生じることがないよう、監査の実施に先立って十分な理解を得るよう努めることが望ましい。」とある。 それに対し、該当箇所の文章例、マネジメントや管理策に変更がった場合と、それとは別に、不正や誤謬の発生が発見されない可能性があるとは記載しているが、文章が続いているため、後者が、前者の変更があった場合の話と解釈される可能性があるのでは。 前半の「変更があった場合のその影響を考慮したものではない。」と「また、マネジメントと・・・」を改行・段落を変えて、別モノであることを強調する、あるいは、前半の末尾に「影響については再度監査する必要がある」など何等か補足を入れた方が誤解を招かなくてよいのでは。	御意見いただきありがとうございます。御意見を踏まえ、「2.社会的合意方式のアシュアランス型情報セキュリティ監査報告書【様式2】の雛型」の「3.マネジメントと管理策の変更による影響と統制の限界」について、「また」の前後で改行を加えることにより、読者の誤解を生じさせないように修正させていただきます。
11	情報セキュリティ監査実施基準ガイドラン改正案	いずれ、AIや他の監査ツールの利用による監査負担の軽減やそれらツールを利用する際の、各基準の著作権の整理、ツール利用におけるセキュリティ（監査情報の漏えいの防止等）について追記が必要になると思われる。 ただし、これらは技術の進歩・変化によって記載内容も変わるカノ可能性が高いので、原則・方針だけ記載し、他の内容は、補足や付録等の篤明で、頻繁に差し替えが可能なようにするなどの工夫必要と思われる。	御意見いただきありがとうございます。いただいた御意見は、今後、情報セキュリティ監査基準等改訂の際の参考とさせていただきます。
12	「情報セキュリティ監査実施基準ガイドラン改正案」のp11「3. 監査手続の実施」の最終段落	「管理策が適切でないと判断した場合には、監査の目的や設定した目標の達成に対する影響の重要性や広範性を判断する」とあるが、各監査基準ガイドラインを読むと 委託元（被監査組織）がリスクアセスメントを実施する場合と 監査人自らがリスクアセスメントを実施する場合を想定している。 上記文章は、両方を指すと思われるが、前者については、委託元が一定のリスクアセスメントの手法・基準に則って実施していることの確認が主と思われる。が、文章からは、そのような内容が読み取れない。	御意見いただきありがとうございます。御意見を踏まえ、「管理策が適切でないと判断した場合には、監査の目的や設定した目標の達成に対する影響の重要性や広範性を判断する。」を「監査人が入手した監査証拠の評価に当たっては、監査人が適切と判断したリスクアセスメントの結果との関連づけが考慮されることが望ましい。」に修正させていただきます。
13	「情報セキュリティ管理基準改正案」のp6「詳細管理策」の説明	「詳細管理策」の説明で、詳細管理策[Xx-X.X.X]内の、a), b), c), d),e)・・・の扱いも追記した方がよいと考える。（a)b)・・・以下全てを満たす必要がある等）	御意見いただきありがとうございます。御意見を踏まえ、御指摘の箇所に箇条書きの説明として、「詳細管理策に含まれる箇条書き形式の項目には、列挙されている項目をすべてに対処すべきもの、包含した上でさらに追加を考慮すべきもの、又は例示にとどまるものなどの種類があり、詳細管理策の内容によって意味が異なるため留意する必要がある。」を追記させていただきます。
14	「情報セキュリティ管理基準改正案」のp31「V.管理策基準」の冒頭	「管理策基準に記載される管理策[Xx-X.X]は、情報セキュリティマネジメントの単位毎に、リスク管理方針に基づき適切に選択すべき事項である」との説明はあるが、委託元（被監査組織）の認識が薄くなりがちのため、冒頭文章でもう少し強調した方がよいと考える。 また、説明文で、「1.情報セキュリティ監査基準」「情報セキュリティ監査実施基準」「3.情報セキュリティ監査報告基準」のどこにも使用されていない「リスク管理方針」という言葉出てきている。 「情報セキュリティ管理基準」でも初出かつ本箇所のみで使用している。本用語よりも、リスクアセスメントをした上で、リスクに応じて取捨選択するなどの説明に差し替えた方が分かり易いのでは。（[5.情報セキュリティ管理基準活用ガイドライン]では「リスク管理方針」が何回か使用されている）	御意見いただきありがとうございます。御意見を踏まえ、情報セキュリティ管理基準及び情報セキュリティ管理基準活用ガイドラインのそれぞれにおいて、「リスク管理方針」を「リスク対応のための方針」に修正させていただきます。

No	御意見の箇所	御意見の内容	御意見に対する考え方
15	1_情報セキュリティ監査基準_改正案 P.3 前文	『これまで「保証」及び「助言」と記載していた箇所について、それぞれ「アシュアランス」及び「アドバイザリー」と表記を改めることとした。』とありますが、妥当であるか再考いただきたいです。 特に「アシュランス」に関して、監査業務で一定程度利用されている用語であることは理解していますが、日本国内において必ずしも理解されやすい用語とは言えません。用語自体が難解になってしまっており、従来の「保証型」が『保証（英語のguaranteeに相当）として誤解される』という問題の解消にもつながらないと思われます。 「2_情報セキュリティ監査実施基準ガイドライン_改正案」のp.4にあるように、「保証」の位置づけについてしっかりとした説明がなされれば、従来の「保証型」でよいのではないでしょうか。	御意見いただきありがとうございます。御指摘の点は十分に理解できるところではありますが、「保証」の位置付けに関する正しい認識が監査の関係者で共有されておらず、誤解が生じている実態を踏まえ、新たに「アシュアランス」という用語を用いて情報セキュリティ監査制度の活用を推進することといたしました。そのため原案のとおりとさせていただきますので、御理解のほどよろしくお願いします。
16	1_情報セキュリティ監査基準_改正案 P.6 4. 他の専門職の利用	用語が統一されていない箇所があります。 ×「情報セキュリティ監査人」 ○「監査人」	御意見いただきありがとうございます。御意見のとおり修正させていただきます。
17	3_情報セキュリティ監査報告基準ガイドライン_改正案　P.11 上記雛型における下線部15について	以下は誤記と思われます。 ×「理由を導くに至った証拠の標目明らかにするものである。」 ○「理由を導くに至った証拠の標目を明らかにするものである。」	御意見いただきありがとうございます。御意見のとおり修正させていただきます。
18	3_情報セキュリティ監査報告基準ガイドライン_改正案　P.14 上記雛型における下線部4について	以下は誤記と思われます。 ×「経営者が責任を追う。」 ○「経営者が責任を負う。」	御意見いただきありがとうございます。御意見のとおり修正させていただきます。
19	3_情報セキュリティ監査報告基準ガイドライン_改正案　P.15 項番「n-1」の「情報セキュリティ監査手続」	以下は誤記と思われます。 ×「持込み・持出しは記録の査閲。」 ○「持込み・持出し記録の査閲。」 ※なお、p.19にも同様の記述があります。	御意見いただきありがとうございます。御意見のとおり修正させていただきます。
20	3_情報セキュリティ監査報告基準ガイドライン_改正案　P.20 上記雛型における下線部3について	以下は誤記と思われます。 ×「利用者に要求事項に基づいた管理手続を被監査主体が作成し、」 ○「利用者の要求事項に基づいた管理手続を被監査主体が作成し、」	御意見いただきありがとうございます。御意見のとおり修正させていただきます。
21	3_情報セキュリティ監査報告基準ガイドライン_改正案　P.8 及び P.11	用語が統一されていない箇所があります。 ×「情報セキュリティ監査人」 ○「監査人」	御意見いただきありがとうございます。御意見のとおり修正させていただきます。
22	4_情報セキュリティ管理基準（令和7年改正版）_改正案　P.10 3.2 情報セキュリティガバナンスの目的	「目的3：投資の方向性を設定する」とありますが、表現上、以下の方が適切ではないかと思われます。 「投資の方向性を示す」「方向性を決定する」	御意見いただきありがとうございます。御意見のうち、「方向性を決定する」にて修正させていただきます。

No	御意見の箇所	御意見の内容	御意見に対する考え方
23	4_情報セキュリティ管理基準（令和7年改正版）_改正案　P.14 4.4.1.1	以下は誤記と思われます。 ×「マネジメントビュー議事録等」 ○「マネジメントレビュー議事録等」	御意見いただきありがとうございます。御意見のとおり修正させていただきます。
24	4_情報セキュリティ管理基準（令和7年改正版）_改正案　P.15 4.4.2.1 a) 外部状況	「国際、国内、地方又は？」とありますが、表現上、以下の方が一般的ではないかと思われます。 「海外、国内、地方又は？」 「国外、国内、地方又は？」 ※なお、p.16 にも同様の記述があります。	御意見いただきありがとうございます。御意見のうち、「国外、国内、地方又は」にて修正させていただきます。
25	4_情報セキュリティ管理基準（令和7年改正版）_改正案　P.18 4.4.7.1 d)	以下は誤記と思われます。 ×「情報セキュリティアセスメント」 ○「情報セキュリティリスクアセスメント」 ※なお、p.19 の 4.4.8.1 にも同様の記述があります。	御意見いただきありがとうございます。御意見のとおり修正させていただきます。
26	4_情報セキュリティ管理基準（令和7年改正版）_改正案　P.25 4.6.2.1	以下は誤記と思われます。 ×「利用可能な状態とするとともにに、」 ○「利用可能な状態とするとともに、」	御意見いただきありがとうございます。御意見のとおり修正させていただきます。
27	4_情報セキュリティ管理基準（令和7年改正版）_改正案　P.26 4.6.2.3	以下は誤記と思われます。 ×「組織は、頻度、方法、責任及び計画策定に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持する。」 ○「組織は、頻度、方法、責任及び計画策定に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持を行う。」 ○「組織は、頻度、方法、責任及び計画策定に関する要求事項及び報告を含む、監査プログラムを計画、確立、実施及び維持する。」 もしくは、以下のようにしてもよいかもしれません。 「組織は、監査プログラムの計画、確立、実施、及び維持を行う。このプログラムには、監査の頻度、方法、責任、計画策定に関する要求事項、及び報告が含まれる。」	御意見いただきありがとうございます。御意見のうち、「組織は、頻度、方法、責任及び計画策定に関する要求事項及び報告を含む、監査プログラムを計画、確立、実施及び維持する。」にて修正させていただきます。
28	4_情報セキュリティ管理基準（令和7年改正版）_改正案　P.36 5a-5.7.2	以下の記述がありますが、a)だけ「情報の交換」となっており、b)にはないため、統一してはいかがでしょうか。 a) 戦略的脅威インテリジェンス：脅威の動向に関する大局的な情報の交換 b) 戦術的脅威インテリジェンス：攻撃者が使う手法、ツール及び技術に関する情報	御意見いただきありがとうございます。御意見のとおり「情報の交換」に統一させていただきます。
29	1_情報セキュリティ監査基準_改正案	情報セキュリティ監査の目的 アドバイザリーの定義を「同様の検証を根拠とした基準不適合の事項に対する改善のための助言を行うこと」としていますが、必ずしも不適合とまでは言えなくても、よりよい管理のために助言することもあり得ると考えます。「基準不適合の事項に対する…」とすることは、アドバイザリーの定義として狭義にすぎるのではないかと思われますので、再考いただけますと幸いです。	御意見いただきありがとうございます。御指摘の点は十分に理解できるところではありますが、基準不適合の事項以外についての指摘や助言を目的に含めることで、アドバイザリーの意図が適切に伝わらなくなることが懸念されるため、原案のとおりとさせていただきますので、御理解のほどよろしくお願いします。

No	御意見の箇所	御意見の内容	御意見に対する考え方
30	1_情報セキュリティ監査基準_改正案	報告基準 3. 監査報告書の記載事項 「アシュアランス意見又はアドバイザリー意見」と、二つの意見が併記されていますが、「情報セキュリティ監査の目的」ではアシュアランスのみが意見表明するものとされ、アドバイザリーでは助言に留まります。 アシュアランスの意見が、被監査側の利益になるか不利益になるかにかかわらず監査主体として表明すべきものであるのに対し、アドバイザリーの助言とは、被監査側が改善に向けた取り組みを行うためのトリガーを提供するものであり、被監査側の利益となることを前提に伝達するものであるから、アシュアランスの意見とアドバイザリーの助言とは本質的に異なるものと思料します。英語では、前者が「opinion」、後者が「advice」に当たるでしょう。これを同じ「意見」という言葉でくくるのは混乱を招きやすく、読み手に誤解を生じるおそれがあることから、見直していただきたく存じます。 「2_情報セキュリティ監査実施基準ガイドライン_改正案」においては、「助言」、「助言意見」、「意見（アドバイザリー）」と表記が揺れており、甚だ不自然でもあります。 もしも「アドバイザリーの意見」というものが想定し得るということであれば、「助言」ではなく「意見」という用語を使う是非を含めて、その定義を明確にするようお願いします。	御意見いただきありがとうございます。御意見を踏まえ、情報セキュリティ監査基準及び関連ガイドライン文書において、アドバイザリー型監査の報告書において監査人が表明するものは「助言」の表記で統一することとさせていただきます。
31	2_情報セキュリティ監査実施基準ガイドライン_改正案	I. 情報セキュリティ監査実施上の前提事項 2. 情報セキュリティ監査の目的設定 アシュアランス型監査とアドバイザリー型監査について、「この2つの目的は排他的なものではないため、アシュアランスとアドバイザリーの2つを監査の目的とすることができる」と書かれており、あたかも一つの業務(1本の契約)の中でアシュアランスとアドバイザリーの両方を行うことができるかのように読めます。 しかし、監査主体が助言を行い改善させた管理策を当該監査主体が保証するのでは、実質的に監査主体が自分の提案した改善策を自分で保証しているも同然となり、マッチポンプと言いますか、お手盛りにすぎ、独立性が損なわれると思料します。 情報セキュリティ監査にはアシュアランス型とアドバイザリー型の二種類があるということと、同じ監査主体が同じ被監査主体に二種類の情報セキュリティ監査を同時提供できるということは異なるでしょうから、この点を明確にすることが望ましいです。ここを明確に読み取れる制度にしないと、情報セキュリティ版のエンロン事件のような事態を引き起こしかねません。 被監査主体はアシュアランス型監査とアドバイザリー型監査とで異なる監査主体に発注するであるとか、同じ監査主体が提供するなら実施期間が異なるべきであるとか、対象領域が重ならないことであるとかの一定の考慮がなされるべきですし、それは明文化されてしかるべきと考えます。	御意見いただきありがとうございます。御意見を踏まえ、「この2つの目的は排他的なものではないため、アシュアランスとアドバイザリーの2つを監査の目的とすることができる。」を「この2つの目的を同時に実現しようとすることは、監査における独立性や客観性の確保の観点で不適切である。ただし、あらかじめアドバイザリー型監査を実施し、改善が図られた後でアシュアランス型監査を実施する、又はその逆のような形で、それぞれの監査の独立性が担保されることを条件に、実施することは考えられる。」に修正させていただきます。
32	2_情報セキュリティ監査実施基準ガイドライン_改正案	アシュアランス型監査 「誤解が生じることがないよう、監査の実施に先立って十分な理解を得るよう努めることが望ましい」とありますが、この書き方ではあたかも監査主体が誤解させているかのようです。また、非常に重要な点でありながら「望ましい」で済ませるのは、問題の大きさに比して扱いが小さすぎると思料します。基準かガイドラインかのいずれかにおいて、次の点も定める必要があると考えます。 ・被監査主体が、意見に一切の誤りがないという絶対的な保証を求めないことを確認し、文書化する責務 ・監査依頼者又は被監査主体が監査主体と結ぶ契約において、意見に一切の誤りがないという絶対的な保証ではないと両者が確認することを条項に盛り込むこと	御意見いただきありがとうございます。御意見を踏まえ、「誤解が生じることがないよう、監査の実施に先立って十分な理解を得るよう努めることが望ましい」を「誤解が生じることがないよう、監査の実施に先立って、監査主体は被監査主体がこの点について理解していることを確認する」に修正させていただきます。

No	御意見の箇所	御意見の内容	御意見に対する考え方
33	2_情報セキュリティ監査実施基準ガイドライン_改正案	「監査人と監査報告書利用者の間における、監査リスク受容の程度についての合意の形態により、アシュアランスの水準が異なる可能性があることにも留意する」と書かれていますが、「監査リスク受容の程度」、「アシュアランスの水準」という未定義の用語が出てくるために、意味を汲むのが困難です。 「3_情報セキュリティ監査報告基準ガイドライン_改正案」にも「水準」という言葉は出てきますが、そちらは「委託元の期待する水準」という形で、被監査主体における情報セキュリティの水準を表していると考えられる一方、こちらの「アシュアランスの水準」とは監査主体が行うアシュアランス型監査に様々な水準があり得ることを意図しているように読めることから、何ら解説することなく言葉だけ登場させるのは情報セキュリティ監査基準及び情報セキュリティ監査実施基準ガイドラインの役割として不適切と考えます。 そも、「1_情報セキュリティ監査基準_改正案」に「アシュアランスとは証拠等の客観的な検証を根拠とした事実認定に基づき信頼性についての意見表明をすること」をいうと定義され、「2_情報セキュリティ監査実施基準ガイドライン_改正案」ではアシュアランスを「評価に対して証拠等の客観的な検証を根拠として信頼性を付与すること」(p.4 脚注1)と定義している中で、アシュアランスに様々な水準があるということであれば、確固とした信頼性が存在しないかのようであり、それがアシュアランスといえるのか疑問です。甘いアシュアランスと厳しいアシュアランスとか、弱い信頼性と強い信頼性とかが自由に選べ、それらが等しくアシュアランス型監査を名乗ることになれば、情報セキュリティ監査制度そのものの信頼が保てないのではないかと危惧します(「弱い信頼性を付与するだけの甘いアシュアランス」というものが認められるはずはないと思いますが)。 なお、「3. リスクの特徴に基づく監査目標設定の考え方」の「アシュアランス型監査における目標設定」において、利用者合意方式と社会的合意方式の二つの方式が紹介されておりますが、方式が複数あることとアシュアランスの水準に幅があることとは、もとより異なる概念であると理解しております。	御意見いただきありがとうございます。御意見を踏まえ、「アシュアランス型監査」に関する説明文において、「また、監査人と監査報告書利用者の間における、監査リスク受容の程度についての合意の形態により、アシュアランスの水準が異なる可能性があることにも留意する。」としていた箇所を「なお、アシュアランス型監査ではどの程度の厳密さで監査意見を述べるかについて、報告書利用者と監査人の間であらかじめ、合意しておく必要がある。合意には複数の形態があることに留意する必要がある。」に修正させていただきます。
34	2_情報セキュリティ監査実施基準ガイドライン_改正案	II. 情報セキュリティ監査の実施手順 2. 監査計画の立案 監査計画立案における監査対象のリスクアセスメント 「なお、アドバイザリー型監査においては、被監査主体におけるリスクアセスメントの適切性、及び監査人によるリスクアセスメントの結果とそれに応じたマネジメント又は管理策の整備及び運用に対する助言が重要な指摘事項となることがある。」 末尾の、なお書きで始まる上の文の意味が分かりませんでした。「…適切性、…助言が重要な指摘事項となる」とは、どういうことでしょうか。助言をする中で、指摘すべき事項に気づくことがある、といったことでしょうか。平易な表現で説明していただけると幸いです。	御意見いただきありがとうございます。御意見を踏まえ、「被監査主体におけるリスクアセスメントの適切性」を「被監査主体におけるリスクアセスメントの適切性に関する助言」に修正させていただきます。
35	2_情報セキュリティ監査実施基準ガイドライン_改正案	3. 監査手続の実施(監査証拠の入手と評価) 「監査証拠は、…その時の状況に応じてもっとも適切な監査手続を選択適用した結果得られたものでなければならない」と書かれていますが、この文は因果関係を適切に表現してはいないと考えられます。監査証拠を得るためにその時の状況に応じてもっとも適切な監査手続を選択適用することは重要ですが、この文では、監査手続の選択いかんでは現に存在する証拠が認められなくなるかのように読まれかねません。念入りに検討された監査手続を選択適用した結果ではなく、偶然発見した事実が重要な性質を帯びていることもあり得ます。 ここでは、もっとも適切な監査手続を選択適用した結果得られたものが監査証拠であると述べるのではなく、監査証拠はもっとも適切な監査手続によって十分かつ適切なものであることが裏付けられなければならない、ということを述べるほうが望ましいと思料します。そのほうが、この文に続く段落の趣旨とも整合すると考えます。	御意見いただきありがとうございます。御意見を踏まえ、「監査証拠は、アシュアランス意見又はアドバイザリー意見の根拠となるものであるから、その時の状況に応じてもっとも適切な監査手続きを選択適用した結果得られたものでなければならない。」を「監査証拠は、結果の表明の根拠となるものであるから、もっとも適切な監査手続によって十分かつ適切なものであることが裏付けられなければならない。」に修正させていただきます。

No	御意見の箇所	御意見の内容	御意見に対する考え方
36	2_情報セキュリティ監査実施基準ガイドライン_改正案	6. アシュアランス型監査を行う場合の品質管理システム 「審査担当の要否を含む個別業務の品質維持方法」という文言からは、審査担当が不要なケースもあり得るように読めます。しかし、アシュアランス意見を表明することの重要性と責任を考えれば、最低でも、独立性を担保した上での受嘱や、計画立案、報告書発行等に係る審査は実施してしかるべきだと考えます。この審査とは、たまたまそのとき審査担当を名乗る者が1人いればよいということではなく、一定以上の品質の監査業務を恒常的に提供し続ける仕組み・体制が整っていてはじめて真に品質を維持する方法と言えるものと思料します。 したがって、「審査担当の要否を含む個別業務の品質維持方法」ではなく、「厳格で恒常的な審査制度・審査体制の構築を含む品質管理体制の確立と、その体制に基づく個別業務の品質維持方法」としていただくのがよろしいと存じます。	御意見いただきありがとうございます。御意見を踏まえ、「審査担当の要否を含む個別業務の品質維持方法」を「品質管理体制の確立とその体制に基づく品質維持方法」に修正させていただきます。
37	2_情報セキュリティ監査実施基準ガイドライン_改正案	アドバイザリー型監査においても品質管理システムは重要なはずです。アドバイザリー型監査の品質管理システムについての言及がないと、アドバイザリー型監査では品質を重視しなくてよいとの誤った受け取り方をされるおそれがございます。監査主体の規模の大小にかかわらず、業務の性質やリスクに応じた品質確保の仕組みや、監査主体の改善提言を受けて被監査主体が構築した管理策を当の監査主体が保証してしまうような独立性違反を回避する仕組みが講じられるべきであることを、明記する必要があると思料します。	御意見いただきありがとうございます。御意見を踏まえ、「6」の見出しを「アシュアランス型監査を行う場合の品質管理システム」を「監査の品質管理システム」に修正するとともに、当該項目の内容についても外部監査と内部監査における違いを考慮して記述するように修正させていただきます。
38	3_情報セキュリティ監査報告基準ガイドライン_改正案	IV. アシュアランス報告書作成上の留意事項 2. アシュアランス意見の類別 末尾において、「監査人が必要と認めた監査手続が制約され、アシュアランス意見の合理的な根拠を得ることができなかった場合には、アシュアランス意見を述べてはならない」と書かれていますが、一方で、限定付肯定意見の説明に「監査人が必要と認めた監査手続が制約されたがその部分を除けば適切である旨のアシュアランス」とあります。意見を述べてはならないのか、限定付肯定意見を述べればいいのか、大変分かりにくくなっていますので、より詳しい説明が必要だと存じます。 このことは、「4. 内部監査におけるアシュアランス報告書」においても同様です。	御意見いただきありがとうございます。御意見を踏まえ、「監査人が必要と認めた監査手続が制約され、合理的な根拠を得ることができなかった場合には、アシュアランス意見を述べてはならない。」を「監査人が必要と認めた監査手続が制約され、合理的な根拠を得ることができなかった事項には、肯定意見及び否定意見を述べてはならない。」に修正させていただきます。
39	3_情報セキュリティ監査報告基準ガイドライン_改正案	V. アシュアランス報告書の雛型 脚注に「アシュアランス方式の監査報告書の記載事項の検討にあたっては、日本公認会計士協会が以下にて公表している実務指針等を参考とすることができる」と書かれていますが、「…できる」という表現だと、参考としてもしなくてもよいように読めます。 しかしながら、まずは当該実務指針等を読んでみないことには、実務指針等に準拠するかどうかの判断すらできません。ここでは、日本公認会計士協会が公表している実務指針等を参考にした上で、監査人の業務に当てはまる適切な報告書の形態を検討することを求めるべきだと存じます。	御意見いただきありがとうございます。御意見を踏まえ、「日本公認会計士協会が以下にて公表している実務指針等を参考とすることができる」を「以下も参照のこと」として日本公認会計士協会の実務指針の情報源を紹介するように修正させていただきます。
40	3_情報セキュリティ監査報告基準ガイドライン_改正案	同じ脚注に「必要に応じて米国公認会計士協会の定めるService and Organization Control (SOC)レポートのうち、SOC2 及びSOC3 の規定内容も考慮すべきである」と書かれていますが、「必要に応じて」という書き出しと「すべきである」という結びが整合していないと思われます。考慮することの重要性を考えれば、「必要に応じて」という文言を削除して文意を明瞭にするべきだと存じます。	御意見いただきありがとうございます。御意見を踏まえ、御指摘の脚注について、「必要に応じて」及び「も考慮すべきである」を削除する形で記載内容を修正させていただきます。
41	3_情報セキュリティ監査報告基準ガイドライン_改正案	2. 利用者合意方式のアシュアランス型情報セキュリティ監査報告書【様式2】の雛型 見出しの番号は、「2」ではなく「4」ではないでしょうか。	御意見いただきありがとうございます。御意見のとおり修正させていただきます。
42	3_情報セキュリティ監査報告基準ガイドライン_改正案	報告書雛型の宛先が「[監査主体]殿」となっていますが、正しくは「[被監査主体]殿」ではないでしょうか。	御意見いただきありがとうございます。御意見のとおり修正させていただきます。

No	御意見の箇所	御意見の内容	御意見に対する考え方
43	情報セキュリティ監査基準（前文） ･･･監査の目的として示されている「保証の付与」について、「セキュリティインシデントが発生しないことを保証する」という文脈における保証（英語のguarantee に相当）として誤解される事例があることが指摘されるようになった。そこでVer2.0 への改訂にあたり、これまで「保証」及び「助言」と記載していた箇所について、それぞれ「アシュアランス」及び「アドバイザリー」と表記を改めることとした。	【意見内容】 「アシュアランス」の動詞（assure）について、Cambridge Dictionaryによると以下のように定義されており、今回の改訂趣旨にも合致すると思われる。 to tell someone that something is definitely true, especially so that they do not worry: to make something certain to happen: その一方で、英国では、生命保険のように何か問題が発生した時にお金が支払われるようなニュアンスでも用語が利用されており、当該文化圏の影響を受けている人には誤解が生じる恐れがあることから、注釈が必要であると思われる。 【理由】 https://dictionary.cambridge.org/dictionary/english/assure	御意見いただきありがとうございます。Assuranceについては米語圏のみでなく、英国を含めて広く用語として用いられおり、注釈の必要はないと考えられることから、原案のとおりとさせていただきます。 （ご参考：英国財務報告評議会（FRC）によるAssuranceについての説明ページ） https://www.frc.org.uk/library/standards-codes-policy/audit-assurance-and-ethics/
44	情報セキュリティ管理基準（令和7年改正版）Ⅲ.ガバナンス基準、Ⅳ.マネジメント基準	Ⅲ.ガバナンス基準では、「トップマネジメント」と「各情報セキュリティマネジメントシステムの責任者」を明確に分けて記載している。 一方で、Ⅳ.マネジメント基準以降では、「各情報セキュリティマネジメントシステムの責任者」に関する説明がないため、「トップマネジメント」に含まれているのか、或いは、別の役割となるのか判断することが困難であると感じた。	御意見いただきありがとうございます。御意見を踏まえ、トップマネジメントを「情報セキュリティマネジメントを行う組織の長」の意味で用いることとし、情報セキュリティ管理基準における初出箇所の脚注において、「情報セキュリティマネジメントを行う組織の長（または責任者）。（注）「情報セキュリティマネジメントを行う組織」は部門単位であることがあり、複数の組織が一つの企業や機関の中に存在することがある。」と明示するよう修正させていただきます。また、ガバナンス基準においてトップマネジメントを用いていた箇所は、「ガバナンス主体」とさせていただきます。
45	情報セキュリティ管理基準（令和7年改正版）Ⅱ.構成　2.2 マネジメント基準	2.2 マネジメント基準 “「マネジメント基準」は、原則、全て実施すべき事項である。”と記載されているが、例示としての記載に留めておいた方が良いものが含まれている。 例1： 4.5.2.4 教育及び訓練を実施した結果、必要な力量が持てたかどうかを確認するために、以下を実施する。 ・知識の確認テスト ・スキルの実習テスト ・チェックリストなどによるベンチマーク ※力量の内容によっては、目的が達成されるのであれば、知識の確認テストだけでも十分である場合が想定される。また、全体の傾向分析を実施している事例は、多く確認しているが、チェックリストなどにベンチマークを実施しているような事例は少ないと思われる。（チェックリストなどによるベンチマークが実施されていないと「不適合」になる？） 例2： 4.5.2.5 　教育、訓練については以下を検討し、定期的に実施する。 ・教育・訓練基本計画 ・教育・訓練実施計画 ※小規模の組織では、基本計画と実施計画に分けて検討していない事例が多いと思われる。（分けて検討しないと「不適合」になる？）	御意見いただきありがとうございます。御意見を踏まえ、マネジメント基準全体について、必ず実施することを求めるのではなく例示として記載されているものについて、「以下の例示を参考に」等、その旨がわかるように修正させていただきます。
46	情報セキュリティ管理基準改正案 p.75 6a-6.3.15【教育及び訓練】について	「会議及びイベントに参加し、自らの知識を最新の状態に保つ」だけではなく、「IPA情報処理技術者試験などの公的あるいは民間の情報セキュリティに関する資格試験にも積極的に取り組み、外部評価に耐える専門性を向上させることも推奨される」を追記してはどうか。	御意見いただきありがとうございます。当該箇所はJIS Q 27002における規定内容から大きく乖離しないことを前提としていることから、原文のとおりとさせていただきます。

No	御意見の箇所	御意見の内容	御意見に対する考え方
47	全体	今般、情報セキュリティマネジメントに関わる国際規格の改正を踏まえた改正及び情報セキュリティ監査制度を取り巻く環境に変化を踏まえた所要の改正が行われたことは、誠に時宜を得たものであり、改正内容に賛同致します。 今後、弊社は、今回の改正内容を踏まえつつ、ITとサイバーセキュリティの力で、社会的課題に立ち向かい、国の発展を支え、人々の暮らしを守ってまいります。	御意見いただきありがとうございます。本基準に対する肯定的な御意見として承ります。
48	情報セキュリティ管理基準活用ガイドライン Ⅱ. 個別管理基準の策定手順 1. 情報セキュリティ管理基準の参照・項目の抽出　最終段落（p5冒頭）において	【意見内容】 「それぞれの作業の後には、監査人への説明、あるいは後任の担当者への引継のため、 修正理由を記述しておくことが望ましい。」とありますが、 必須とされたほうが良いと考えます。 【理由】望ましい＝監査における指摘事項＋組織体での是正対象ではない？といった ややあいまいな印象を受けるため。 管理基準の「4.8文書化した情報の管理」の内容との整合性を図るため。	御意見いただきありがとうございます。御意見を踏まえ、「修正理由を記述しておくことが望ましい。」を「修正理由を記述しておく。」に修正させていただきます。