パブリックコメントで寄せられた御意見に対する考え方

No.		提出者（種別）	該当箇所	御意見	御意見に対する考え方
1	1-1	不明	「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）」 P3　1-2-2 ペネトレーションテスト（侵入試験） サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の資格	情報セキュリティサービス提供者にかかる「資格要件」については、「情報セキュリティサービス」および「ペネトレーションテスト（侵入試験）サービス」においても「汎用資格」である「情報処理安全確保支援士」を必須要件とすべきである。	いただいた御意見は、情報セキュリティサービス基準の更なる検討を進めていくに当たって参考にさせていただきます。
2	2-1	個人	（案全体）	1. パブコメ段階からPDFは、少なくてもしおり付きPDFで公開して欲しい。本当はNativeなHTML＋利活用可能なWord,Excel書式での公開。現行の第3版は、しおり付きPDFで公開されている。しおり付きPDFにより、電子的な可読性が高まるため、公開版は当然として、パブコメ時においてもしおり付きPDFで公開して欲しい。	いただいた御意見については、情報セキュリティサービス基準及び情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示の更なる検討を進めていくに当たって参考にさせていただきます。
	2-2	個人	（案全体）	2. パブコメ時および公開時に変更履歴付きの版も同時に公開して欲しい。これにより従来の文書からの変更をより簡単に理解することができる。	いただいた御意見については、情報セキュリティサービス基準及び情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示の更なる検討を進めていくに当たって参考にさせていただきます。
	2-3	個人	「情報セキュリティサービス基準　第４版（案）」及び「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）」の表紙	3.「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示第3 版（案）」において、「本書が対応する情報セキュリティサービス基準：第4 版（案）（令和6 年 月 日公表）」と対応は記載されてはいるが、わかりにくい。同一の番号にして対応がわかりやすくするか、もしくはタイトルに情報セキュリティサービス基準の版数を記載してしまったらどうか。「情報セキュリティサービス基準：第4版に対する技術及び品質の確保に資する取組の例示」もしくは「情報セキュリティサービス基準に対する技術及び品質の確保に資する取組の例示：第4版」 または、情報セキュリティサービス基準に対する技術及び品質の確保に資する取組の例示を情報セキュリティサービス基準の付録にして一体化させる。例示といいつつ、サービス基準で引用されているので、一体化するメリットが高いものだと思います。	いただいた御意見については、情報セキュリティサービス基準及び情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示の更なる検討を進めていくに当たって参考にさせていただきます。
	2-4	個人	「情報セキュリティサービス基準：第4 版（案）」P10　5.（１）イ（ア）	4. 情報セキュリティサービス基準：第4 版（案）のP10の5.（１）イ（ア）において、「例示４-２」と記載されているが、今回の版では４-２は存在しない。４-２-１の修正漏れではないかと思われます。このような単純な間違いを防ぐためにも、前記にように1つのドキュメントにして、ハイパーリンクを設定するのがいいのではないかと思います。	ご指摘のとおり、当該箇所は本来「例示４－２－１」であるべきところですので修正いたします。ドキュメントの体裁及びハイパーリンクの設定につきましては、今後の改訂における参考とさせていただきます。
3	3-1	不明	「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）」 P3　1-2-1 脆弱性診断サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の資格	脆弱性診断サービスの専門資格の基準にOSWA,OSWEのようなWeb pentester資格などが含まれていないため、記載があってもいいのではないでしょうか。 その他、含めることができる資格はさらにあるかも追加を検討頂けると嬉しいです。	ご指摘を踏まえ、脆弱性診断サービスの専門資格の基準にOSWA,OSWEを追加いたします。その他の資格等の追加につきましては、今後の改訂における参考とさせていただきます。
4	4-1	法人	「情報セキュリティサービス基準　第４版（案）」P1　2 定義(3)及び(4)、P6　2-2 (1)ア(イ) 並びに「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）」P15　別表「テスト方法の選定は～」及び「想定されている脅威は～」	以下では「情報セキュリティサービス基準第 4 版（案）」を「基準」、「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示」を「例示」と表記いたします。 ■意見内容：「基準」および「例示」中で言及されるペネトレーションテストの定義が曖昧であり、事業者や受益者はその言葉が指し示すサービスを一意に判読することが困難です。その定義を見直し、補足を追加する等によりどのようなサービスを想定しているのかを読者が判断できるように明確に示していただくことを推奨いたします。 該当箇所：「基準」P.1 定義（３）と（４）、「例示」P.15 別表「テスト方法の選定は～」「想定されている脅威は～」、「基準」P.6 2-2(1)ア（イ） 理由：「基準」の定義から脆弱性診断とペネトレーションテストの違いは「攻撃者が実際に侵入等を行うために用いる手法と同様の手法により、（中略）セキュリティ機能を回避して攻撃の目的を達成できるかの観点から試験」であり、「例示」から攻撃者が実際に侵入等を行うために脅威モデリングやリスク分析を実施することが求められていると読み取りました。このようなテストをペネトレーションテストとして定義した場合、テスト内容だけでなく進め方（実施プロセス）もある程度規定されるように判読されます。その一方、専門性を有する者の在籍状況からは特定の攻撃に関する成立実績しか問うていないため、これでは脆弱性診断に加えて攻撃を成立させることのみがペネトレーションテストに必要な要素であるように読み取ることが可能です。したがって、読者や事業者は本書が想定するペネトレーションテストについて異なるサービスをイメージしてしまう可能性があります。	本基準におけるペネトレーションテストの定義は政府機関等のサイバーセキュリティ対策のための統一基準群との整合性を考慮して定めており、またペネトレーションテストサービス事業者の技術要件については書類審査により適合状況を判断可能な内容として規定していることから、いずれも原案のとおりとさせていただきますが、いただいた御意見は情報セキュリティサービス基準の更なる検討を進めていくに当たって参考にさせていただきます。
	4-2	法人	「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）」P15　別表「実施したテスト方法には～」	■意見内容：「例示」に記載されている満たすべき項目のうち実施内容に関する言及が網羅性を欠いており不十分であるため、このような制限を加える必要を読者は読み取ることが困難です。 該当箇所：「例示」P.15の別表「実施したテスト方法には～」 理由：ペネトレーションテストでは脅威や環境によって取り得る手段が異なるため、網羅的な攻撃手法を列挙することはできません。実際、当該項目は網羅性を欠いています（例：アカウントを持たないユーザが認証をされずに機微情報を窃取する等）。こ例示を満たすことでペネトレーションテストとして成立しうるかを読者は判断できないため、この条件を記載する必要があるかは改めて検討する必要があります。	ご指摘を踏まえ、別表の該当箇所から参照している情報セキュリティサービス基準２－２（１）ア（イ）の内容を拡充し、網羅性を確保するようにいたします。
	4-3	法人	「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）」P15　別表「テストを通じて検出された～」	■意見内容：ペネトレーションテスト報告書のエグゼクティブサマリなどを通じて、システム全体に対してリスクのランクを割り当てることにより読者がそのランクを誤って利用してしまう可能性があります。 該当箇所：「例示」P.15の別表「テストを通じて検出された～」 理由：ペネトレーションテストはシステム毎に異なるテストを実施するため、それら全てに対して一様に評価可能なリスク指標を示すことは極めて困難です。また、リスク評価を行う主体者によってもそのランクが異なる場合もあります。しかしながら、読者はエグゼクティブサマリに記載されたランクを読み、複数のシステム同士を比較し、それぞれのシステムのリスクの優先順位を付けてしまう可能性があります。これは適切なリスク評価が行われているとは言えないため、エグゼクティブサマリにおいてリスクのランク付けの強制を避けることを推奨します。	ご指摘の箇所はリスクのランク付けを強制するものではございませんが、原案が誤解を招きやすい表現であったこと及びご指摘のとおりペネトレーションテストの結果に基づくリスク評価の困難さが伝わりにくいことを踏まえ、記述内容を修正いたします。
	4-4	法人	「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）」P15　別表「想定されている脅威は～」及び「実施したテスト方法を～」	■意見内容：「例示」では記載されている参考情報を用いて脅威を想定する旨が示されていますが、当該参考情報では脅威に関する十分な記述がございません。 該当箇所：「例示」P.15の別表「想定されている脅威は～」「実施したテスト方法を～」 理由：例示4-2-1は脆弱性やその検出手法に関する情報を提示していますが、脅威そのものについては言及がほとんどなく、十分な情報源ではありません。（例示4-2-2のPTESには脅威についての言及があるため、こちらについてのポインタと取り違えている可能性もあります。）	ご指摘のとおり、当該箇所は本来「例示４－２－２」であるべきところですので修正いたします。

No.		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	4-5	法人	「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）　」 P8　4-2-2　ペネトレーションテスト（侵入試験）サービスの提供において用いる以下に例示する内容相当の基準等及びその明示方法の例示	■意見内容：ペンテストサービス提供内容に関する参考情報として「金融機関等におけるTLPT実施にあたっての手引書（FISC）」を追加することを推奨します。 該当箇所：「例示」P.8の4-2-2 理由：本書は、より実効性の高いサイバー攻撃対応態勢が求められる金融機関において、サイバーレジリエンスをもう一段引き上げることを支援する基準です。特に日本において「脅威ベースのペネトレーションテスト」を実施する際の有効な参考文書であるため、本書を参考情報として追加することをご提案差し上げます。	ご提案の脅威ベースのペネトレーションテスト（TLPT）サービスにつきましては、これを排除するものではありませんが、本制度の定義するペネトレーションテスト（侵入試験）サービスではTLPTに限定しないペネトレーションテスト（侵入試験）に関する内容を想定していることから、原案のとおりとさせていただきます。
5	5-1	個人	「情報セキュリティサービス基準　第４版（案）　」P1　２ 定義(4)	【ペネトレーションテストサービスの定義】 情報セキュリティサービス基準第４版（案）の第１章２項（４）ペネトレーションテスト（侵入試験）サービスの内容について、「脆弱性診断のサービスの定義を満たすサービスのうち」の記載がありますが、ペネトレーションテスト（侵入試験）が脆弱性診断に内包されるような表現になっていることについて、技術的に正確ではないものと考えます。 ペネトレーションテストは、以下の観点から脆弱性診断に内包されるものではなく、脆弱性診断とは異なるアプローチであるものと考えられます。 脆弱性診断はセキュリティ上の問題点の有無を調査するが、ペネトレーションテストでは攻撃者の目的の達成可否を調査するため、必ずしも脆弱性の有無に着目しない。 （一般的に）脆弱性診断のスコープはアプリケーション単位やホスト単位であるが、ペネトレーションテストではシステム全体がテストの対象になる。 （一般的に）脆弱性診断では対象となっているホストについてもれなく調査を行うが、ペネトレーションテストでは対象システムに含まれるホストについてもれなく調査を行うことは少なく、またホスト間の横断的侵害についても調査を行う。 つきましては、「脆弱性診断のサービスの定義を満たすサービスのうち」の表現を削除することを提案します。	本定義は、政府機関等のサイバーセキュリティ対策のための統一基準群においてペネトレーションテストが「高度な脆弱性診断」と位置付けられていることを踏まえた内容となっており、同基準群との整合性確保の観点から原案のとおりとさせていただきます。
	5-2	個人	「情報セキュリティサービス基準　第４版（案）　」P6　2-2(1) 技術要件	【ペネトレーションテストサービスの技術要件】 情報セキュリティサービス基準第４版（案）の第２章２項（１）技術要件の内容について、「２－１（１）に掲げる技術要件かつ」の記載がありますが、上記の「ペネトレーションテストサービスの定義」の内容に関連して、ペネトレーションテストサービスに従事する要員に対して、脆弱性診断事業の実施実績を求めることはそぐわないものと考えられます。つきましては、脆弱性診断サービスの技術要件はペネトレーションテストサービスの技術要件から除外することを提案します。	ペネトレーションテストの定義により、ペネトレーションテストサービスの実績をもって脆弱性診断サービスの実績として扱うことが可能であり、運用上の支障はないとみなされるため、原案のとおりとさせていただきます。
6	6-1	法人	－	今般の「情報セキュリティサービス基準(第4版)」の改定案につきましては、一昨年1月に弊社から同基準(第2版)の改定の際に提出させて頂きました「ペネトレーションテスト」の同基準への追加につきまして、2年近くに亘り、ご検討頂きました上に、今回の改定案にご反映を頂き、誠に有難うございます。 今回は、弊社の提案を踏まえて頂いたものであり、賛同致しますとともに、その際の留意点につきまして、以下のご提案をさせて頂きます。 今後も弊社は、同事例集を参考としつつ、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。	本基準に対する肯定的な御意見として承ります。
	6-2	法人	「情報セキュリティサービス基準　第４版（案）　」P6　2-2(2) 品質管理要件	（意見） 品質管理要件としてペネトレーションテストサービスに従事する要員に対して、高い倫理感を必須要件とすることを提案致します。 例示として、 ア 高い倫理観 イ 品質管理マニュアルの整備 のように高い倫理観を品質管理要件の１つとして記載することを提案致します。 （理由） ペネトレーションテストサービスに限らずですが、情報セキュリティサービス全般において、診断対象組織の情報資産へアクセスを行いながらサービスを提供します。そのため、診断サービスの計画、実施、分析及びレポート時に知り得た情報や攻撃手法を悪用しない高い倫理観が必要不可欠だと考えます。 今回の意見としてはペネトレーションテストサービスに必要とした意見にしておりますが、情報セキュリティサービス全般において高い倫理観が必要不可欠だと考えるため。	いただいた御意見については経済産業省でも重要と認識しておりますが、情報セキュリティサービス基準として審査時に倫理観の審査を行うのではなく、登録時に事業者からの誓約書等の徴求等を通じて要員に対して高い倫理観の維持を求めることが適切と判断することから、情報セキュリティサービス基準につきましては原案のとおりとさせていただきます。
	6-3	法人	「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）　」 P3　1-2-1　脆弱性診断サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の資格	（意見） 1-2-1に定める汎用資格として「CopmTIA Pentest+」を追加することを提案致します。 （理由） 「CompTIA Pentest＋」はネットワーク上の脆弱性を特定、報告、管理するための実践的なペネトレーションテストを取り扱う認定資格です。出題範囲は、汎用的な様々なIT環境での攻撃対象領域がカバーされており、クラウド、Webアプリケーション、IoT、オンプレミスなどに関連するペネトレーションテストのスキルとそれぞれの実施計画、報告などのスキルを評価することが可能です。本サービス基準において、ペネトレーションテスト（侵入試験）サービスが脆弱性診断サービスのオプションとして定義されていることもあり、脆弱性診断サービスの提供に必要な専門知識を「CompTIA Pentest+」から学ぶことで、脆弱性診断サービスで定義されている次のサービス「 Web アプリケーション脆弱性診断 、プラットフォーム脆弱性診断、スマートフォン／タブレット端末アプリケーション脆弱性診断」に対し、適切なサービスを提供できる専門性を身に着けることが期待できるため、「CompTIA Pentest+」を汎用資格として追加することを提案します。	いただいた御意見は、情報セキュリティサービス基準の更なる検討を進めていくに当たって参考にさせていただきます。
	6-4	法人	「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）　」 P5　2-3　講師又はリーダーの経験をもって、セキュリティ監視・運用サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の専門家コミュニティ	（意見） 専門家コミュニティの(ISC)2の名称をISC2 に変更することを提案致します。 （理由） (ISC)2の名称が 2023年8月にISC2 に変更になっております。	ご指摘のとおり、当該箇所は本来「ISC2」であるべきところですので修正いたします。

No.	提出者（種別）	該当箇所	御意見	御意見に対する考え方
7-1	法人	「情報セキュリティサービス基準　第４版（案）　」 P6　2-2(1)技術要件　ア　専門性を有する者の在籍状況（イ)次のいずれかのペネトレーションテスト（侵入試験）を含む事業に関して基準となる日から起算して過去３年間に合計で３件（契約件数。包括的な契約の場合は１年間分で１件とみなす。）以上の、顧客が管理しているシステムに対して以下のいずれかを実施した実績を有する者	【1】 〇該当箇所 情報セキュリティサービス基準　第4版（案）P.6 （１）技術要件　ア　（イ）　a～d 〇意見内容 箇条書きa～dでは、アカウントの侵害やそれを通じた情報漏洩、不正操作に絞られた内容となっているように見受けられます。 サーバーやシステムのミドルウェアやアプリケーションにフォーカスしたペネトレーションテストも含まれるよう、少し対象範囲が広がる表現にしていただくのはいかがでしょうか。 〇理由 脆弱性によっては、アカウントに関係なくミドルウェアやアプリケーションの不備をついてサーバーの改ざんや設定変更につながるものが存在するた	ご指摘のとおり、原案では実際に行われているペネトレーションテストサービスと比較して対象範囲が絞られておりましたので、項目を追加する等の修正を行います。
7-2	法人	「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）　」 P４　1-3　デジタルフォレンジックサービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の資格 1-4　セキュリティ監視・運用サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の資格 1-5　機器検証サービスの提供に必要な専門性を満たすことができる右に例示する内容相当の資格	【2】 〇該当箇所 情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示第3版（案）P.4 1-3、1-4、1-5 〇意見内容 記載の資格CISSPについて、（）内の正式名称の単語と単語の間隔が広いため、P.3の1-2-1のような体裁に統一できないでしょうか。 〇理由 表記の統一のため。	いただいた御意見のとおり、体裁を統一いたします。
7-3	法人	「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）　」 P13　7-2　脆弱性診断サービスの品質確保に資する教育又は研修	【3】 〇該当箇所 情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示第3版（案）P.13 7-2 〇意見内容 項目名および内容が「脆弱性診断サービス」のみとなっていますが、下記のような表現に変更するのはいかがでしょうか。 ・脆弱性診断サービスの品質確保に資する教育又は研修 ↓ 脆弱性診断サービスおよびペネトレーションテスト（侵入テスト）サービスの品質確保に資する教育又は研修 ・ 脆弱性診断サービスに従事する者 ↓ ・ 脆弱性診断サービスおよびペネトレーションテスト（侵入テスト）サービスに従事する者 〇理由 「情報セキュリティサービス基準　第4 版（案）」P.7　イ（イ）にて、ペネトレーションテストサービスに順次するものは前述の該当箇所の教育・研修を受講するように記載されています。しかし、前述の該当箇所では脆弱性診断サービスのみに関する例示のような表現となっているため。	ご指摘の箇所に関しては、政府機関等のサイバーセキュリティ対策のための統一基準群においてペネトレーションテストが「高度な脆弱性診断」と位置付けられていることを踏まえ、脆弱性診断サービスの品質確保に資する教育又は研修が、ペネトレーションテストサービスの品質確保に資する教育又は研修を包含するものとして扱っております。同基準群との整合性確保の観点から原案のとおりとさせていただきます。
7-4	法人	「情報セキュリティサービス基準　第４版（案）　」 P1　2(3)　脆弱性診断サービス	【4】 〇該当箇所 情報セキュリティサービス基準　第4版（案）P.1 2 定義 〇意見内容 「クラウドセキュリティ診断」を追加する 〇理由 2020年某SaaSサービスによる情報漏洩事故を起点として、現在までクラウドサービスの設定不備を原因とする数多くのセキュリティ事故が発生している。多要素認証やゲストユーザーの権限制限、共有設定などは既存の脆弱性診断というくくりではカバーしきれず、クラウドセキュリティ診断サービスを新たに定義する必要があると考えるため。	いただいた御意見については経済産業省でも重要と認識しておりますが、SaaS等のクラウドコンピューティングサービスを対象とする診断の定義や審査の方法について引き続き更なる検討が必要な状況であることから、原案のとおりとさせていただきます。

No.		提出者（種別）	該当箇所	御意見	御意見に対する考え方
7	7-5	法人	「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）」 P15　別表　ペネトレーションテスト（侵入試験）に関する試験実施報告書において満たすべき事項　テクニカルレポート又は相当するセクション	【5】 〇該当箇所 情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示第3版（案）P.15 別表　テクニカルレポート又は相当するセクション 箇条書きの上から5、6個目 〇意見内容 「例示4-2-1に例示する」とありますが、「例示4-2-2に例示する」が正しいのではないでしょうか。 〇理由 P.7　4-2-1は脆弱性診断サービスに関する記述であり、ペネトレーションテストサービスに関する記述はP.8　4-2-2に記載されているため。	ご指摘のとおり、当該箇所は本来「例示４－２－２」であるべきところですので修正いたします。
	7-6	法人	「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）」 P10　5-1-1　脆弱性診断サービスの提供において示す結果に関する取扱方法及びその明示方法	【6】 〇該当箇所 情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示第3版（案）P.10 ５．　結果に関する取扱方法及びその明示方法の例示 5-1-1 〇意見内容 5-2に記載の(1)、(2)と同等の内容を5-1-1にも含めるべき (1) 検証結果報告書において、検出された脆弱性に関する情報と、当該脆弱性が悪用された場合に想定される影響、攻撃の再現手順を記載する。 (2) 検証結果報告書において、検証結果に対する分析や考察等の追加情報を記載する。 〇理由 ツールで出た報告書をそのまま提出することしかできないベンダーは本資料記載の技術及び品質の確保ができていないと考えるため。	ご指摘の箇所につきましては、脆弱性診断サービスと機器検証サービスにおいてそれぞれ実施する診断及び検証の内容に関する相違を踏まえ、原案のとおりとさせていただきます。
	7-7	法人	「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）」 P8　4-2-1　脆弱性診断サービスの提供において用いる右に例示する内容相当の基準等及びその明示方法の例示	【7】 〇該当箇所 情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示第3版（案）P.8 4-2-1 箇条書きの一番最後 〇意見内容 Tripwire IP360/PureCloud は Tripwire IP360 へ変更すべきだと考えます。 〇理由 Tripwire PureCloudは提供終了しているため。 ・Tripwireの製品ページからOureCloudが削除されています。 ・ページ内検索でも該当製品が見つかりません。 　https://www.tripwire.com/ja/products	いただいた御意見のとおり、変更いたします。
	7-8	法人	「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示　第３版（案）」 P7　4-2-1　脆弱性診断サービスの提供において用いる右に例示する内容相当の基準等及びその明示方法の例示	【8】 〇該当箇所 情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示第3版（案）　P.7 4-2-1 〇意見内容 【クラウドセキュリティ診断において、次に示す内容相当の診断を行う旨の提示】 ・最新のCIS Benchmarksに準拠した診断内容 〇理由 2020年某SaaSサービスによる情報漏洩事故を起点として、現在までクラウドサービスの設定不備を原因とする数多くのセキュリティ事故が発生しています。多要素認証やゲストユーザーの権限制限、共有設定などは既存の脆弱性診断というくくりではカバーしきれず、クラウドセキュリティ診断サービスを新たに定義する必要があり、品質を担保するためには最新のCIS Benchmarksに対応している必要があると考えるため。	いただいた御意見については経済産業省でも重要と認識しておりますが、クラウドコンピューティングサービスを対象とする診断の定義や審査の方法について引き続き更なる検討が必要な状況であることから、原案のとおりとさせていただきます。