パブリックコメントに寄せられた御意見の概要と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	個人	情報セキュリティサービス基準　第３版（案） 第１章　２（２）	『マネジメント』を『管理』と置き換えては、どうか。 ＜理由＞ 横文字は格好良いかもしれませんけれども、漢字の方が意味がはっきり分かるから、です。	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あたって参考にさせていただきます。
	1-2		情報セキュリティサービス基準　第３版（案） 第１章　２（２）	『リスクアセスメント』を『リスクの評価・分析』と置き換えては、どうか。 ＜理由＞ 熟語を混ぜてもらった方が意味が分かりやすいから、です。	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あたって参考にさせていただきます。
2	2-1	個人	情報セキュリティサービス基準　第３版（案） 第１章　２（７）ウ	情報セキュリティーに関する研修修了と受講実績について、国際規格ISO9001を認証している企業が比較的多い経済団連の人権と雇用についての報告書を照らしあわせ社内だけで報酬や賞状などをもらう仕組みは多いが、外部及び外国の学びを継続する仕組みと制度をつなげたいです。学びたい人が実際には研修を受けていらっしゃらない現状があり有期雇用社員や外国人財をふくめストップオプションではないため差別の格差を縮めるためにも有効である。国際会計財務基準での情報セキュリティーの意味と内容が日本とは異なり、有価証券を含みまた、tipが組み込まれている場合あります。tipについては、欧州最大の国際規格の認証機関が研修を提供されており正当である。 受講料も日本だけ突出し高額であり欧州や欧米では誰もが学ぶことができるようになっておりCPD(certificate professional Development)の認証が研修してその後に実践したコースは認証をもらいプライバシーに配慮され楽しみまた安全に履歴を残す事ができます。基準はENが良いのは具体的であり審査も厳しいです。 研修の過程とステップについては、ISO27001→NIST→各国または専門性高い情報セキュリティーの資格が地球上には存在します。受け取る側も学ぶ体制を経済産業省は支援する必要がある。派遣労働会社と一般企業でプライバシー認証や情報セキュリティー認証と内容が区別されているため統一なさることにより雇用形態による現場の差別はなくなるでしょう。	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あたって参考にさせていただきます。
3	3-1	個人	-	今回、「機器検証サービス」の追加の改訂をされたことは、機器検証の重要性の観点からも評価されるべき取組みだと認識しています。	本基準に対する肯定的な御意見として承ります。
	3-2		-	今回、2つのドキュメントがPDFのみで提供されています。以下のようにすると読者にとって、デジタルでの恩恵をさらに得られ、便利になると思います。 (a) しおり付きPDFでの提供 デジタルでの可読性が非常にたかくなります。 (b) 前回の版とのマイクロソフトワード等の変更履歴付き文書 変更箇所の特定、変更内容が非常にわかりやすくなります。	いただいた御意見を踏まえ、「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」の公表に際しては、しおり付きPDFでの提供といたします。変更履歴の公表につきましては、今後の改訂における参考とさせていただきます。
	3-3		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２版（案）	「情報セキュリティサービス基準」と「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」との版数 今回の案では、前者が第3版、後者が第2版になっている。これらの2つの文書は、どれとどれとが対応しているかを簡単にわかるようにすべき。 案1「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「情報セキュリティサービス基準」の最後に付録として1文書化 案2「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」の版数以外に、対応する「情報セキュリティサービス基準」の版数を明示する。	いただいた御意見を踏まえ、「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」の改訂版の公表にあたっては、対応する「情報セキュリティサービス基準」の版数を表紙に明示することといたします。
4	4-1	法人	-	平成30年2月に策定されました「情報セキュリティサービス基準」を昨年1月に改定され、今般、新たに「機器検証サービス」を基準に追加する改定に向けた御省の取り組みは、誠に時宜を得たものであります。改定案につきましては、特段の意見はなく、賛同致します。	本基準に対する肯定的な御意見として承ります。
	4-2		-	弊社が昨年度の同基準(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は、「情報セキュリティサービス普及促進に関する検討会」にてご検討を頂いているとお伺いしておりますが、引き続き、ご検討の程、宜しくお願い申し上げます。	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、対象サービスの追加について検討しておりますが、ペネトレーションテストサービスの定義ならびに一定のサービス品質を確保するための技術要件及び品質管理要件について、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。
	4-3		情報セキュリティサービス基準　第３版（案） 第１章　２（３）	脆弱性診断サービスの１つとしてスマートフォンアプリケーション脆弱性診断が定義されていますが、モバイルアプリケーション脆弱性診断の名称が適切ではないかと考えます。 ＜理由＞ iOS、Android搭載のスマートフォンアプリケーションだけではなくタブレット端末を対象としたアプリケーションの脆弱性診断を実施しているため。 また、スマートフォンアプリケーションという呼び名が日本固有の呼び名と想定されるため海外でも広く使用される呼び名のモバイルアプリケーションが相応しいと考えるため。	いただいた御意見をもとに名称を「モバイルアプリケーション脆弱性診断」とした場合、例えばリモートセンシングデバイスのような当該サービスの対象として想定されていない機器の脆弱性診断も対象に含まれるとの誤解が生じる恐れがあります。一方、ご指摘の通り、現行の名称では通話機能を有しないタブレット端末等が対象に含まれないという誤解が生じる恐れがあるため、御意見を踏まえ名称を「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」に変更することといたします。
5	5-1	法人	情報セキュリティサービス基準　第３版（案） 第２章　５（１）ア	「なお、（ア）と(イ）の要件を同一人物が満たす場合には、兼務者としての人数を明らかにすること」 この要件については、１から４のサービスと異なる基準になっています。 機器検証サービスのみ限定する理由はなく、記載する必要はないと考えます。	機器検証サービスに関する技術要件は、機器検証サービスの提供に必要な専門性を有する者に加えて、脆弱性診断サービスの提供に必要な専門性を有する者が業務に従事することを求めている点で他のサービスと異なります。したがって、これら２種類の専門性を同一の者が兼務している場合は審査において兼務による要件の充足状況について確認する必要があることから、機器検証サービスのみについて兼務者の人数を明らかにすることを求めています。したがって原案のとおりといたしますが、兼務者としての人数を明らかにする趣旨を当該箇所に追記することといたします。
6	6-1	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２版（案） ４-２ 【Web アプリケーション脆弱性診断において、次に示すツールを使用して診断を行う旨の提示】	株式会社エーアイセキュリティラボが提供するSaaS型Webアプリケーション脆弱性診断ツール「AeyeScan」を追加いただきたい。 ＜理由＞ 国内スタートアップが国内で自社開発・運用するツールであり、ASVS等主要な診断項目を充足しつつ現在急速に発展しているクラウド型の Webアプリツール市場にてNo.1（※）となっているため。 （※）富士キメラ総研調べ「2022 ネットワークセキュリティビジネス調査総覧 市場編」(Web アプリケーション脆弱性検査ツール<クラウド> 2021年度実績)	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に記載するツールの選定にあたっては、これまでに審査登録機関において同等性の判定を行った実績のあるものを対象とすることとしており、御提案のツールはこの条件を満たさないことから、原案のとおりとさせていただきます。しかしながら御意見の趣旨を踏まえ、当該ツールを用いる申請がなされた場合に、例示相当とみなせるようにするために審査登録機関との間で当該ツールの実績等に関する情報共有等を進めてまいります。