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	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
1-1	システム監査基準	6	（1） 1列目	・意見 『若しくは』を『もしくは』としては、どうか。 ・理由 普通には使われない表現だから、です。	今後の検討の参考にさせていただきます。
1-2	システム監査基準	20	全体	・意見 PDF１９P目にがんばってねじ込んでは、どうか。 ・理由 このために１枚紙を使うのがもったいないように感じるため、です。	御意見を踏まえ、調整いたします。
1-3	システム監査基準	29,30	最終行	・意見 『コンピータ支援監査技法』は『コンピュータ支援監査技法』にしては、どうか。 ・理由 ケアレスミスだと思ったため、です。	御意見のとおり、修正いたします。
1-4	システム監査基準	33	＜解釈指針＞ 3.	・意見 回付ではなく、回覧にしては、どうか。 ・理由 見るかどうかを相手の判断と責任にするのではなく、見ましたよね、とチェックをつけたほうが責任の所在が明らかになるので、今後のためになるように感じるから、です。	本基準は監査人における実施方法等を示すものであることから、原案のままとさせていただきます。
1-5	システム管理基準	17	最終行	・意見 ＜カバナンス活動の例＞　は、次のページの頭に持って行っては、どうか。 ・理由 ぱっと見で頭の中の認識が繋がるから、です。	御意見のとおり、修正いたします。
1-6	システム管理基準	30	最終行	・意見 ＜管理活動の例＞　を次のページの頭に持って行っては、どうか。 ・理由 一目で、その項目が一覧できるようになるため、です。	御意見のとおり、修正いたします。
1-7	システム管理基準	36	最終行	・意見 ＜達成目標＞　を次のページの頭に移動しては、どうか。 ・理由 一覧できるようにしておくと、頭の中での認識速度が上るため、です。	御意見のとおり、修正いたします。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
1-8	システム管理基準	37,48,52,56,58,75,78,82	最終行	・意見 ＜管理活動の例＞や＜達成目標＞を次のページの頭に持って行っては、どうか。 ・理由 タイトルと、その内容が一覧できた方がそれを早くそれと認識できるようになるから、です。	御意見のとおり、修正いたします。
1-9	システム管理基準	77	Ⅱ.9.1リスクアセスメント	・意見 海外に視点を置いている会社も日本は多いと思うので、その国に関するリスクマネジメントを策定するのは、どうか。 ・理由 俗に言われるチャイナリスクとかコリアリスクから会社を守ることは重要だと感じたから、です。	御意見を踏まえ、リスクアセスメントにおいて、地政学的要因やサプライチェーンに関連する要因を考慮する必要性について追記します。
2-1	両方	全体		提出意見： 情報処理技術者試験にも影響があるので、改訂にあたっては十分な周知とともに、情報処理推進機構からの案内も検討願う。	御意見ありがとうございます。今後の検討の参考にさせていただきます。
3-1	両方	全体		提出意見： 「システム監査基準（案）」のフォントではなく、 「意見公募要領」のフォントを使ってほしい。 「システム監査基準（案）」1ページ 「デジタル・トランスフォーメーション」 ここまでではないがスペースが開いている。 そして文字の線が細くて見にくいのである。 つまり読めるが、読み進める事は不可能なのである。 資料で（箇所ではなく）フォントを使い分けている理由はなんなのか？ 取り決めはないのか？ 「デジタル・トランスフォーメーション」これだとスムーズに読めるが、 「デジタル・トランスフォーメーション」は、 つまり「デ・ジ・タ・ル・ト・ラ・ン・ス・フ・ォ・ー・メ・ー・シ・ョ・ン」と読む羽目になるのである。	御意見を踏まえ、字間を調整いたします。
4-1	システム監査基準	37	共通用語集	「システム監査基準・システム管理基準の共通用語集（分類別）」の用語「ガバナンス」の「定義」として、“・・・IT 戦略と方針を実現するために必要な責任と資源等を組織体内へ割り当て、期待する効果(IT パフォーマンスの期待値を含む)を示し、その実現と想定されるリスクへの対処を経営者に指示すること（指示：Direct)こと、・・・”の記載は、経営者が目的語となっているが、経営者の役割期待として、経営者が主語となるべきではないかと思われる。対案として、上記の“経営者に”を削除し、（評価：Evaluate）→（指示：Direct)→(モニタ：Monitor)の記載の冒頭部分で、“経営者の役割として、”を追記すればよいのではないか。具体的には、2行目後半から、“経営者の役割として、ステークホルダーを特定し、協議し、そのニーズを明確にして対応する（ステークホルダーへの対応： Engage Stakeholders）・・・”	ガバナンスの主たる担い手は、経営者ではなく、取締役会等の統治機関と考えますので、原案のままとします。 なお、この点を明確にするために、ガバナンスの定義に仕組みという言葉を明記します。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
5-1	システム監査基準	全体		２０P 監査計画の適切性を維持するためには、監査対象の変化（ リスクや重要性等の変化）に応じて、適時適切に見直し、変更されるとも必要である。 ⇒ 監査計画の適切性を維持するためには、監査対象の変化（ リスクや重要性等の変化）に応じて、適時適切に見直し、変更されることも必要である。 ２２P 必要な場合は、組織体の目的に達成を効果的かつ効率的に支援するIT システムの目的が達成されるようにガバナンス、マネジメント、コントロールが体系的に統合されて有効に機能しているかも監査の視点に含めなければならない。 ⇒ 必要な場合は、組織体の目的の達成を効果的かつ効率的に支援するIT システムの目的が達成されるようにガバナンス、マネジメント、コントロールが体系的に統合されて有効に機能しているかも監査の視点に含めなければならない。 ２５P IT システムの利活用に係る助言業務を依頼された場合には、助言業務提供による組織体への貢献度、保証型監査実施への影響、上限提供能力等について検討する必要がある。 ⇒ IT システムの利活用に係る助言業務を依頼された場合には、助言業務提供による組織体への貢献度、保証型監査実施への影響、助言提供能力等について検討する必要がある。 ２７P　２８P 監査手続の適用に際しては、チェックリスト法、ドキュメントレビュー法 インタビュー法、ウォークスルー法、突合・照合法、現地調査法、コンピータ支援監査技法等が利用できる。 ⇒ 監査手続の適用に際しては、チェックリスト法、ドキュメントレビュー法、インタビュー法、ウォークスルー法、突合・照合法、現地調査法、コンピュータ支援監査技法等が利用できる。 ４１P 監査の結論 監査員が発見した客観的証拠を基に、監査目的及び業務の運用状況を加味した上で下す監査の結果を指す。 ⇒ 監査人が発見した客観的証拠を基に、監査目的及び業務の運用状況を加味した上で下す監査の結果を指す。	御意見のとおり、修正いたします。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
5-2	システム監査基準	5	前文	倫理は最終的には個々の監査人に帰せられるべき事項であるのに対して、監査はシステム監査機能（ 監査人や監査チーム等の提供する機能） のあり方を示す必要があるからである。 ⇒ 倫理は最終的には個々の監査人に帰せられるべき事項であるのに対して、基準はシステム監査機能（ 監査人や監査チーム等の提供する機能） のあり方を示す必要があるからである。 （提案理由） 前段のなお書きにおいて、「監査人の倫理」は監査人の立場から、「システム監査の基準」はシステム監査機能の立場から記述している。これを受けての文章であるから、倫理に対比すべきは監査ではなく基準ではないかと判断した。	御意見のとおり、修正いたします。
5-3	システム監査基準	26	基準6	判断過程の適切性と判断内容の合理性を確保するために、各取締役は相互監視しかつ取締役会等として監督機能を果たすことになり、これらがガバナンスに係るコントロールの役割を果たすこととなる。 ⇒ 判断過程の適切性と判断内容の合理性を確保するために、各取締役は相互監視しかつ取締役会等として監督機能を果たすことにより、これらがガバナンスに係るコントロールの役割を果たすこととなる。 （提案理由） 取締役会等として監督機能を発揮することを観点として考えると、「監督機能を果たすことになり」よりは、「監督機能を果たすことにより」が表現として適切と判断した。	御意見のとおり、修正いたします。
5-4	システム監査基準	28	基準7	個別監査計画とは、年度の基本計画に基づいて、個々のシステム監査対象ごとに、具体的な監査スケジュールまで落とし込んだ詳細計画書をいう。 ⇒ 個別監査計画とは、年度の基本計画に基づいて、個々のシステム監査対象ごとに、具体的な監査スケジュールまで落とし込んだ詳細計画をいう。 （提案理由） 監査計画については、計画書という記述はされていないので、この箇所も「詳細計画書」とするよりは「詳細計画」とした方が記述の整合性がとれると判断した。	御意見を踏まえ、修正いたします。
5-5	システム監査基準	32	基準10	監査調書に基づいて、論理の飛躍がないようにする必要がある。 ⇒ 監査調書に基づいて、監査の結論は、論理の飛躍がないようにする必要がある。 用語解説 本文」（２１P）のマネジメントの視点のPDCAサイクルと、用語解説（３６P）のマネジメントおよび用語解説（３７P　３８P）ITマネジメントのPBRM とが整合していない。	御意見のとおり、修正いたします。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
5-6	システム管理基準	全体	全体	２Ｐ 同ガイドラインについては、迅速なアップデートが可能とするためには、民間団体が策定し公表することとした。 ⇒ 同ガイドラインについては、迅速なアップデートを可能とするためには、民間団体が策定し公表することとした。 ２６Ｐ IT 戦略に関わる意思決定を支援するための情報を経営者に提供されている。 ⇒ IT 戦略に関わる意思決定を支援するための情報が経営者に提供されている。 ３３Ｐ 思決定の根拠及び前提が明確にされている。 ⇒ 意思決定の根拠及び前提が明確にされている。 ３５Ｐ 契約に基づいて製品・サービスを納入されている。 ⇒ 契約に基づいて製品・サービスが納入されている。 ７０Ｐ （インシデント報告）外部サービスにおけるインシデント等の発生時に適切内対応を行うために、インシデント報告書を受領し、業務影響度を分析するとともに、原因究明及び再発防止策を外部サービス提供者に要請する。 ⇒ （インシデント報告）外部サービスにおけるインシデント等の発生時に適切な対応を行うために、インシデント報告書を受領し、業務影響度を分析するとともに、原因究明及び再発防止策を外部サービス提供者に要請する。	御意見のとおり、修正いたします。
6-1	システム管理基準	83	Ⅱ.10.6 要員のエンゲージメント向上	・「要員のエンゲージメント」について 「要員の態度/心構え、行動はどうあるべきか。」についても記載してほしい。 「監査人やプロセス・オーナー等の行動はどうあるべきか。」は記載されている。 「要員をどう行動させるか、要員をどう管理するか」についての記載はある。	ここでの「エンゲージメント」は「ワーク・エンゲージメント」の趣旨で記載しており、行動基準については、Ⅱ.1.1 体制と機能の管理活動の例9.（IT システムの利活用の行動基準等）に記載しておりますので、明確化の観点から、「エンゲージメント」を「ワーク・エンゲージメント」に修正いたします。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
7-1	システム監査基準	3	前文	１．前文のページ１下部にあります 組織体の監査役（会）等（監査役設置会社の監査役会及び監査役、等）は不要ではないでしょうか？ 現文では、監査役（会）等が内部監査部門等と同様にシステム監査を実施するように読めます。監査役が本「システム監査基準」を参照させていただくことはありますが、これにもとづき、システム監査を実施することはないと考えます。	監査役（会）等も必要な場合はITシステムに係る監査を行うため、「適用」の文言は残し、「適用又は参考」に変更させていただきます。
7-2	システム監査基準	全体	全体	２．ページ４の上部にあります 監査役（会）等は、法令の定めるところにより株主からの委任により、取締役の業務執行に対する監査の一環として、ここまでは、教科書通りの文言ですが、これ以降の「システム監査に係る監査を行う。」これは、監査役に対する拡大な解釈だと思います。ガバナンスに対する監査を実施するのは現実にあっておりますが。結論としては、この３行の記述は、不要ではないでしょうか。 ページ２４の下部にも、類似の記載がありますが、これも教科書通りで問題ないですが、本基準書に記述の必要性があるか疑問です。執行の立場にないため。 監査人の意味が、ページを重ねていくに従い、希薄になっているように読みとれます。監査人に、監査役を含めることが、監査役の機能の誤解があるように思えます。本基準は、内部監査部門を含め執行部門が参照すべき基準で、監査役（会）は、含むべきではないのではないかと思います。 ただ、ページ３１にあります監査報告書を監査役（会）に、報告書を提出することを記載していただけるのは、良いこと思います。	監査役（会）等も必要な場合はITシステムに係る監査を行うため、「適用」の文言は残し、「適用又は参考」に変更させていただきます。
7-3	システム管理基準	6	前文	１．ページ２の真ん中下　取締役会等（監査役・・・ 取締役会等に執行とは別の役割の監査役、監査等委員を含めるのは、間違いではないでしょうか。 監査役は、ページ７にあります、取締役（会）（監査役はふくまず）が、・・予算や人材といった資源の配分やITシステムの利活用から得られる効果の実現をしているかを監視するのが役割だと思っております 本管理基準は、本指摘とは別に、監査役監査の際の、参考させていただけると思っております。	御意見のとおり、修正いたします。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
8-1	両方	全体	全体	今回のパブコメ版はしおりなしのPDFで提供されています。ITのリテラシーの高い方々が作成され、読者もそのような方が多いのではないかと思います。例え、パブコメ版でもしおり付きPDFで提供して、デジタルでの可読性を高めるべきかと思います。 今回、実践部分のガイドラインを別冊化することに関して、基本は賛同いたします。要件等の基準は、できるだけすきっきりさせ明確化が図れ、実践部分はガイドラインでより具体的に示させていてわかりやすくなるのではないかと思います。しかし、あくまで従前のデジタルではない、紙での基準、ガイドライン等の書籍のイメージになってしまっているのかと思います。せっかくデジタルに詳しい方が作成し、デジタルに詳しい方が読者であることが想定されるので、それに合わせた書式にすべきではないかと思います。例えば、NativeなHTMLでの提供。これにより、本編だけを見るかた、別冊だけを見る方、両方を見る方に適切な情報提供が可能なしかけになるのかと思います。 例えば、英国では国民のために国はＰＤＦでの公開を禁止していると認識しています。 せめて、各基準毎に本編から別冊へのハイパーリンクや、現在、別冊に本編の内容をコピーしてしまっていますが、参照するようにするなど。	改訂版の公開に当たっては、しおり付きのPDF形式で公開予定です。そのほか、お寄せいただいた御意見は、今後の検討の参考にさせていただきます。
8-2	システム監査基準	全体	全体	基準の記載において、基準はより明確かつシンプルに記載されなければならない。例えば、「等」「適切な」をさける、必ず1文で記載する。記載ができない点、補足等は必要に応じて主旨、解釈指針に記載する。 (削除を検討したほうがいいと思われる用語等の例) 基準1 文書化された規定等 基準2 1文に。「その他の能力」「その」　「備えているか、又は備えるようにしなければ」 基準3 「システム監査の実施に際し、」「システム監査業務を行い」 基準4 1文に。誠実性を記載するなら、タイトルにも誠実性を追加。「配慮され」	御意見につきましては、今後の検討の参考にさせていただきます。
8-3	システム監査基準	14	基準2	基準2 解釈指針 1 (1) 他の部分は、「例えば」からの記載でない修正がされている。ここは、(1)の後に「例えば」と始まってしまっている。「例えば」の例示は、非常にわかりやすくなるのですが、まずは、例えばではなく要件を記載した上で、その後に「例えば」を記載したほうがわかりやすいと思います。	御意見につきましては、今後の検討の参考にさせていただきます。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
8-4	システム管理基準	全体	全体	参考資料に「アジャイル開発やAI活.等の新たな.法・技術等にも対応できるよう、国際規格の考え.なども踏まえながら、各プロセスを細分化して再整理」と記載されています。しかし、国際規格等との関係をもっと明確にすべきではないかと思います。極端には、日本独自の「システム管理基準」を作成することなく、国際標準に基づいた日本産業規格(ＪＩＳ)を制定すべきではないかと思います。もちろんJIS化には手間がかかる、更新に時間がかかる等の課題もありますが、同じ職掌の経産省内で、それはJISの課題として取り組むべきではないかと思います。	御意見につきましては、今後の検討の参考にさせていただきます。
9-1	システム監査基準	4	前文	・２ページの２１行目「更に」は「さらに」のほうがよい。他の箇所の例と同様に。	ここでは副詞の意で使用しているため、公用文に関する要領等を踏まえ、原案のままとさせていただきます。
10-1	両方	全体	全体	いつの間にか締め切りぎりぎりになっていたのでざっと読みでコメントしておきます。 対象とされる範囲がイマイチわかりませんが、内容は総じて空論だらけに感じました。 範囲外のために入っていないということなら申し訳ないですが、threat injectionに基づく正常性確認すら一文字も入っていないのは、日本の古式ゆかしい性善説に立った禊の儀式を連綿と継承する気しか感じませんでした。 ごく少数の人のみに通知した状態で、実際にデータの盗み出しや改ざんを行い、それが計画通りに検出され対応されるのか、といったことを監査に取り入れようとしない時点で、日本のセキュリティ・情報安全性に未来はないなと思いました。	本基準については、監査人が、一定の基準に基づいて IT システムの利活用に係る検証・評価を行い、ガバナンスやマネジメント等について、一定の保証や改善のための助言を行うものでありますところ、お寄せいただいた御意見につきましては、今後のサイバーセキュリティに関する施策の検討に当たり、参考にさせていただきます。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
10-2	両方	全体	全体	いつの間にか締め切りぎりぎりになっていたのでざっと読みでコメントしておきます。 対象とされる範囲がイマイチわかりませんが、内容は総じて空論だらけに感じました。 範囲外のために入っていないということなら申し訳ないですが、監査人や管理者や運用者に対する信用チェックといった概念が全く出てきていませんでした。 正直、図面もなく家を外から見て外観だけで建築基準法に違反していないかチェックしろ、みたいなろくでもない方法を延々使い続けるんだろうなとしか思えないです。 監査する側に対する信用チェックとして、監査される側の一部に「監査で引っかかること」をわざと行わせて監査人が検出できるかを調べたり、管理者や運用者に対して動機と機会を与えてデータの盗み出しや改ざんや運用手順の無視等の不正行為を行うかどうかをチェックしたり、実際に行った結果それが検知されるか、検知されるまでどれくらいかかるか、といったことを検証する手法が一ミリも出てきていませんでした。 それこそ、IDカード忘れたからちょっと代わりに認証通してドア開けてくれとか、上司から「その運用手順は飛ばしていいから」と、勝手なアレンジをする指示を受けたらどう行動するかなど、現場の人間（監査人を含む）に対する実際の検証を行う手法が影も形も見えないあたり、これから先も後進国化が止まらないだろうなって思いました。	本基準については、監査人が、一定の基準に基づいて IT システムの利活用に係る検証・評価を行い、ガバナンスやマネジメント等について、一定の保証や改善のための助言を行うものでありますところ、お寄せいただいた御意見につきましては、今後のサイバーセキュリティに関する施策の検討に当たり、参考にさせていただきます。
11-1	システム監査基準	16	基準3 解釈指針１． （１）	（１）システム監査の目的は、以下のようなニーズに基づいて決定される。 の箇所で、１は保証型のニーズ、２は助言型のニーズが記載されている。どちらも、企業経営者が自組織を評価するニーズ、つまり組織内部のニーズに限定されている。現監査基準に記載されている、以下のニーズは削除すべきではない。 さらに、システム監査のニーズは、以上に限らず、例えば、委託先の管理レベルによって大きな損害を被る可能性があり、その管理レベルが自社の望むレベルであるか判断する材料として、第三者の評価が欲しいというシステム委託者のニーズ、システムを受託するに当たって、委託元が委託先の管理レベルを重視するようになり、委託元に自社のシステム管理レベルを判断してもらう材料として開示したいというシステム受託者のニーズ、社会的責任を負う重要インフラや多数の生命・財産に影響を及ぼす分野及び行政組織など、不特定多数の利害関係者に向けて、説明責任を果たすことを担保したいという社会的責任を負う者のニーズ等がある。 ・理由 基準で組織外部のニーズを排除してしまうと、システム監査にそのようなニーズが無いことになってしまう。 今日のシステム開発においては、自社開発だけではなく委託、受託による開発も多い。また、本監査基準の前文で、地方公共団体等なども対象としていることから、社会のニーズに対応したシステム監査も想定する必要がある。利用者を自組織の経営者に限定せず、外部監査、特に保証型システム監査を活用した組織外部の利害関係者を守るためのニーズもあることに留意すべきである。組織内部の利用者のニーズと組織外部の利用者のニーズは、本質的に異なるものなので、事例ではなく基準で説明することが望ましい。	御意見を踏まえ、修正いたします。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
11-2	システム監査基準	40	システム管理基準の共通用語集（分類別）ステークホルダー	・意見内容 説明を次のように改めるべきである。 組織体の活動により影響を受ける利害関係者のことを指す。一般には、株主、投資家、顧客、従業員、取引先、地域社会、行政機関等など、組織体を取り巻く、外部の様々な組織、団体、個人などがあげられる。 ・理由 広義の意味に記載されている法令や指針等は、適切ではなく誤解を招く恐れがある。組織体に影響を及ぼすものではなく、組織体が影響を与える先の人や組織が対象となる。	御意見を踏まえ、修正いたします。
11-3	システム監査基準	44	システム管理基準の共通用語集（分類別）助言を目的としたシステム監査	・意見内容 次のような説明に改めるべきである。 被監査組織と監査人が合意した判断規準に基づいて、ＩＴシステムに係わるガバナンス、マネジメント、及びコントロールの状況について検証・評価を行い、問題がある事項、不十分と思われる事項を検出し、必要に応じてその検出事項に対応した改善勧告及び助言を行う監査である。依頼者は改善を目的にシステム監査を依頼し、その監査結果は主に内部目的に利用される。 ・理由 前文の冒頭にあるとおり、ＩＴシステムの利活用に係わる証拠を客観的に検証・評価するプロセスは、助言型も保証型も同じである。助言型と保証型の違いがもっと明確になるよう、その検証・評価された結果がどのように使われるのかを記述すべきである。	御意見を踏まえ、修正いたします。なお、システム監査の意義との整合性、保証を目的としたシステム監査の定義とのバランスを考慮して、一部を修正しております。
11-4	システム監査基準	44	システム管理基準の共通用語集（分類別）助言を目的としたシステム監査	・意見内容 次のような説明に改めるべきである。 被監査組織による言明書の範囲内で、ＩＴシステムに係わるガバナンス、マネジメント、及びコントロールの状況について検証・評価を行い、一定の判断規準により監査手続を実施した限りにおいて、その主張が適切であるか否かを監査意見として表明する監査である。依頼者は、その主張に信頼性が付与されることを目的にシステム監査を依頼し、その監査結果は、内部目的にも利用されるが、組織体を取り巻く利害関係者向けの外部目的に利用されることもある。 ・理由 【基準３】＜解釈指針＞１．（１）１の事例と整合性がとれる内容にすべきである。 前文の冒頭にあるとおり、ＩＴシステムの利活用に係わる証拠を客観的に検証・評価するプロセスは、助言型も保証型も同じである。助言型と保証型の違いがもっと明確になるよう、その検証・評価された結果がどのように使われるのかを記述すべきである。	御意見を踏まえ、修正いたします。なお、システム監査の意義との整合性、助言を目的としたシステム監査の定義とのバランスを考慮して、一部を修正しております。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
11-5	両方	39	共通用語集（分類別）	IT ガバナンスの説明の後に、以下の文章を追記する。 なお、ITガバナンスを中核として、情報セキュリティガバナンス、プライバシーガバナンス、データガバナンス、アジャイルガバナンス等の拡がりがあり、これらのガバナンスを含めて用いている。 ・理由 ２０１８年のシステム監査基準及びシステム監査基準は、ITガバナンスを中核においていた。しかし、近年、経済産業省は、ITガバナンスをはじめして、情報セキュリティガバナンス、プライバシーガバナンス、データガバナンス、アジャイルガバナンス等について、公表しその考え方を定義している。ITガバナンスが国際標準（ISO/IEC38500）として公表されたことで、ＥＤＭモデルでの、システム監査・監督を、監査役の責任のもとですすめられることは、これまでと変わらない、今回の改訂で、さらに、ITガバナンスの監査が重要性と示しているが、ITガバナンスのみならず、情報セキュリティガバナンス、プライバシーガバナンス、データガバナンス、アジャイルガバナンス等の拡がるガバナンスの概念を明記すべきである。 　なお、アジャイルガバナンスについては、ITガバナンスに含めずに、新たな概念とする考え方もある。	御意見を踏まえ、修正いたします。
12-1	システム管理基準	6	「基準」の適用	■意見内容 「基準」の適用方法　の部分には、具体例の箇条書きがあると良いのではないか？ 改定した「基準」の実際の利用者に対し、再構成した基準文書類に意図が容易に伝わるように、再構成した基準文書類（ガバナンス編、マネジメント編、ガイドライン側の主な構成単位等）を一覧化して示したうえで、どの文書は、誰が、どのように利用することを想定しているかについて、箇条書きでいくつか具体例を示した方が良いのではないか。 基準文書類一覧 ・管理基準・ＩＴガバナンス編 ・管理基準・ＩＴマネジメント編 ・管理基準ガイドライン・ＬＬＬ 。。。 活用の一例 ・管理基準・ＩＴガバナンス編　は、〇〇〇が、ｘｘｘの目的で参照し、ＡＡＡする。 ・管理基準ガイドライン　は、〇〇〇が、ｘｘ目的のチェックリストを作成する際に参照する。 ETC. ■理由 今回の改定の趣旨・目的の１つは、「様々な組織」が「容易に」本基準を参照できるようにし、「多様な場面でのITシステムの利活用が適切に行われるように後押しすること」（それが、本基準が意図する適切な形で広く行われること）であると理解した。 また、今回、基準を複数の文書に再編成しているため、改定後の基準文書類群の一覧を明示し、具体的に、どの文書は、誰が、どのような場面でどう利用するかの例示があった方が利用する側がイメージしやすく、基準改定の意図を正しく理解し、正しく活用しやすくなると考える。	御意見につきましては、今後のガイドラインの作成等における参考にさせていただきます。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
12-2	（参考資料1）システム監査基準・管理基準の改訂概要	3	システム監査基準・管理基準の改訂の背景・目的	■意見内容 改定後の基準文書類群の一覧（想定メンテナンス頻度付）がどこかに説明としてあった方がわかり易い。以下のイメージであっているか？ 従前は２つのみ ・システム監査基準 ・システム管理基準 改定後は、多数に分割し、ガイドライン部分は民間団体がおおむねＸ年ごとに見直しを想定 ・システム監査基準　＋　・システム監査基準ガイドライン ・システム管理基準（ＩＴガバナンス編） システム管理基準（ＩＴマネジメント編）　＋　システム管理基準ガイドライン（現段階で、具体的な単位が不明？ ■理由 今回の改定の目的の１つは、　今後の変化にも柔軟に対応できるように、また、多様な利用者が必要な時に必要な箇所を参照しやすいようにすることであると理解した。従前の構成から大きな見直しが行われているため、従前の基準を利用していた側に混乱が生じないよう対策が必要であると考える。特に、ガイドラインとして分離する部分については、メンテナンスの主体が民間団体に変わり、メンテナンス頻度も基準側の頻度よりも頻繁になるとのことだが、あらかじめ具体的な更新サイクル（現時点での想定サイクル）を明示しておいた方が、利用者側の活用するモチベーションが上がるのではないか。	改訂後はシステム監査基準、システム管理基準（ITガバナンス、ITマネジメント両方を含む）及びこれらの基準のガイドラインを予定しております。 そのほかお寄せいただいた御意見につきましては、今後の検討の参考にさせていただきます。
12-3	（参考資料3）システム管理基準ガイドライン（案）抜粋			■意見内容 ガイドライン側に記載（引用）している、基準側の「達成目標」と「（ガバナンス/管理）活動の例」の部分は、引用していることがわかり易いように、四角の枠線で囲うなどもう少し工夫してほしい。 ■理由 改定後の構成では、ガイドラインには、基準の記載内容を引用する形で包含しており、　そこに加えて、ガイドライン側の独自の記載内容として、「リスク」と「着眼点」という形で整理されていることを理解した。 対応策（着眼点）がうまくいかない場合に、具体的にどのようなリスクが想定されるか、非常にわかり易く、現場で活用しやすくなると考える。 ガイドライン（案）抜粋を見たところ、基準からの引用部分は、そのことがわかるように、太字で強調されているが、もう少し明確に、例えば、枠線で囲うなどしてほしい。その方が、初めて基準やガイドラインを参照する人にも文書間の関係（引用している部分であるということ）が容易に伝わり、「リスク」と「着眼点」を参照しやすくなるのではないか。	《今回の意見公募対象外》

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
13-1	両方	3,5	前文	・意見内容 　但し書きに、下記内容を追加すべきと考えます。 システム監査基準およびシステム管理規準は民間企業を事例とした記述となっているが、広くICTシステムを導入している組織・団体（民間企業、公共団体、医療機関、学校等）にも適用でき、活用を推奨するものである。 ・理由 　提示されたシステム監査基準(案)およびシステム管理規準（案）は、その対象を民間企業に限定した記述となっている。ICTシステムの利活用および情報資産の保護が求められるのは民間企業に限らない。 政府機関、自治体、病院、学校および各種団体など、ICTシステムを導入している組織、団体は数多くあり、今日の社会ではこれらの組織団内による不適切なICT利用や情報の流出等のリスクが、社会への脅威となっている。従い、システム監査基準およびシステム管理規準の対象は、広くICTシステムを導入している組織・団体とすべきである。	御意見を踏まえ、修正いたします。 なお、システム監査基準の前文において、政府機関のほか、病院、学校法人等においても利用・参考となる基準であることを明示しております。
13-2	システム監査基準	3	前文	・システム監査基準の意義と適用上の留意事項 「今日社会での IT や情報システム、さらにはデータ・情報(本監査基準におい て、IT、情報システム、データ・情報をまとめた概念として「IT システム」と いう。)の利活用は、会社やその他組織体の諸活動全般に及んでいる。IT シス テムの戦略的利活用は、組織体の価値の向上や会社の競争力の維持、向上を図 る上で不可欠である一方、それに伴いリスクも増大している。組織体が適切に リスク・マネジメントを行い、価値向上のために IT システムの利活用を適切に 行うことを確実にするために、システム監査が効果的・効率的に行われること が必要である。」 ・意見内容 該当箇所を、次の様に変更することで、システム監査の目的がより明確になります。 ⇒「今日社会での IT や情報システム、情報資産（コンピュータシステム上で扱うデータおよび財務情報、個人情報、営業秘密、クレジット情報や医療情報などの機微情報を含む情報）の利活用は、企業やその他組織体の諸活動全般に及んでいる。ITシステムの戦略的利活用は、組織体の価値の向上、企業の競争力の維持向上や社会生活の利便性向上を図る上で不可欠である一方、それに伴いリスクも増大している。組織体が適切にリスク・マネジメントを行い、価値向上のために ITシステムの利活用を適切に行うことを確実にするために、システム監査が効果的・効率的に行われることが必要である。(本監査基準において、IT、情報システム、情報資産をまとめた概念として「ITシステム」という。)」 ・理由 　システム監査の目的として、ITシステムの利活用を適切に行う目的の他に、情報資産を適切に保護し、利活用することがある。 　情報資産に該当するデータ・情報として、財務情報、個人情報、営業秘密、クレジット情報や医療情報などの機微情報などがあり、システム監査ではこれら情報資産の適切な利活用と保護を監査対象とすることが求められている。情報資産の利活用の監査を明記しておく必要があると考えます。 情報セキュリティ監査では情報資産の保護を対象としています　システム監査ではより広く利活用まで含めて、有効性の監査を行っています。	御意見の趣旨を踏まえ、ガイドラインの作成において、データ・情報の具体例を記載いたします。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
14-1	システム監査基準	10	監査人の倫理	・意見内容 「・・・システム監査が結果として、広く社会的な信用につながるには、個々の依頼人の要請を満たすだけではなく、・・・」とあるが、システム監査は依頼人の要請を満たすのではなく、利用者の要請を満たすものである。 --- ・理由 5頁に掲載された図を使って説明する。依頼者の要請を満たさなければならないのは、依頼者イコール利用者である助言を目的としたシステム監査の場合である。保証を目的とするシステム監査（特に外部監査の場合）での依頼者はプロセスオーナーと同一であることがほとんどである。その場合、依頼人の要請を満たすとは、監査されるプロセスオーナーの要請を満たせとのことになり、そもそも監査の独立性が毀損されることになる。 これは、システム監査とは助言を目的としたシステム監査が主要であるとの思い込みが背景にあるように思われる。今回の改訂では、助言を目的としたシステム監査を前提に記述されているのではないかと思われる箇所が極めて多く、普遍的であるべきシステム監査基準とは言い難い内容となっている。	御意見を踏まえ、修正します。
14-2	システム監査基準	11	基準１	・意見内容 システム監査に係る権限と責任等の明確化という基準であるが、システム監査人の権限に関する記述がほとんど無い。 どのような権限が持つ必要があるのか、その権限を維持するのにどのような仕組みを構築しないといけないのかをシステム監査基準は記述する必要がある。 --- ・理由 権限という語句が、システム監査基準（案）全文中に7語あるのみで、システム監査人の権限を明確にし周知するという意味以上のことは記述されていない。 旧システム監査基準（2018年）から、情報システムのガバナンスが監査対象となっている。上場会社ではガバナンス・コードに沿った対応が求められている。ガバナンスとは経営を監督することなので、会社法では監査役等に広範囲の権限を与えることで実行可能な環境を用意している。しかし、システム監査人が情報システムのガバナンスを監査しようとするときに、どのような権限を持っているかといえば、制度的には何もないのが現状である。外部監査人で経済的独立性を保持できる者であれば、経営者トップに監査意見を表明することが可能だろうが、内部監査人が経営者トップに意見することは、ガバナンス・コードが適用される上場会社ではほぼ非現実である。 システム監査基準にガバナンスを謳うなら、システム監査人にどのような権限を付与しなければならないのか、権限を守るためにどのような仕組みを構築しなければならないのかを記載し、組織内でシステム監査を実施する組織体に遵守を求めるべきであろう。	御意見につきましては、今後の検討の参考にさせていただきます。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
14-3	システム監査基準	16	基準3 主旨	・意見内容 「システム監査は、任意監査（略）であることから・・・」と理由付けに任意監査であることを言っているが、任意監査に限定する理論的根拠はない。 （旧基準と文言は変わっていないが、間違いがあるので意見を述べる。） --- ・理由 　法定監査であっても、法律で定められる利用者のニーズを十分に踏まえたシステム監査が求められることに変わりはなく、任意監査に限定して、利用者のニーズを把握することの理由にしてはならない。 現在、法定されたシステム監査は存在しないが、将来法定される可能性はあるので、任意監査に限定してシステム監査基準を公表する意義はない。任意監査に限定するなら、前文及びシステム監査の意義と目的にその旨を記載する必要があるだろう。	御意見を踏まえ、修正いたします。
14-4	システム監査基準	16	基準3	・意見内容 システム監査の目的を経営者のニーズだけで解釈しているが、組織体の外部からのニーズによる場合が抜けている。旧監査基準に記載されていた以下のニーズは削除すべきではない。 「さらに、システム監査のニーズは、以上に限らず、例えば、委託先の管理レベルによって大きな損害を被る可能性があり、その管理レベルが自社の望むレベルであるか判断する材料として、第三者の評価が欲しいというシステム委託者のニーズ、システムを受託するに当たって、委託元が委託先の管理レベルを重視するようになり、委託元に自社のシステム管理レベルを判断してもらう材料として開示したいというシステム受託者のニーズ、社会的責任を負う重要インフラや多数の生命・財産に影響を及ぼす分野及び行政組織など、不特定多数の利害関係者に向けて、説明責任を果たすことを担保したいという社会的責任を負う者のニーズ等がある。」 --- ・理由 　保証を目的としたシステム監査の究極の姿は、社会がさまざまな組織体に対してシステム監査を求める形態であると考えられる。 　ところが、この解釈指針では経営者のニーズしか述べていない。組織体を取り巻く利害関係者には、取引先、地域住民、構成員（社員など）、出資者、官公庁などさまざまな者がおり、監査される組織体には、会社だけでなく非営利法人や地方自治体や政府がある。 　そのことを網羅していないこの解釈指針は、監査基準を規範とするシステム監査人に誤解を与えてしまうので、理論的に整理し直す必要がある。（少なくとも、旧基準の削除部分は復活すべきである。）	御意見を踏まえ、修正いたします。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
14-5	システム監査基準	30	基準8解釈指針5	・意見内容 「5. アジャイル手法を用いたシステム開発プロジェクト等、ドキュメントの作成に重きが置かれない開発手法が採用されている場合には、・・・開発現場への負荷増とならないように考慮することが望ましい。」と被監査現場への斟酌が記載されているが、主旨に反しており、解釈指針として記載するには相応しくなく削除すべきである。 （旧基準にも同様の文言があるが、間違いがあるので意見を述べる。） --- ・理由 ＜主旨＞に「監査手続に基づく監査証拠の入手は、監査の結論を得るために必要不可欠なものである。」と述べているとおりであって、監査対象の部署に斟酌して監査証拠としてのドキュメントを入手しなくてもよいと誤解されるような解釈指針を記載するべきではない。 基準8を否定しているかの文脈になっている。 アジャイル手法について述べたいなら、具体的な監査証拠の入手方法を例示すべきであろう。 なお、今回の基準改定では、保証を目的としたシステム監査への言及が非常に少ない。アジャイル手法を採用している監査対象が（保証を目的とした）システム監査で監査できるかどうかの判断は、監査実施前にしなければならないはずである。可監査性が認められなければ、（保証を目的とした）システム監査は実施してはならないからだ。	御意見を踏まえ、修正いたします。
14-6	システム監査基準	32	基準10解釈指針4	・意見内容 旧基準にあった監査対象部門との間で意見交換をするの「は監査対象部門の承認を得るためではなく、事実確認をするためです。」という解釈は必要なので、今回の改訂で削除すべきではない。 --- ・理由 被監査対象と意見交換する場を監査意見を承認してもらう場だと誤解している人達が未だ一定数ある現状で、このことを注意喚起する意義は失せていない。削除する意味は全くないと考える。	御意見を踏まえ、修正いたします。
14-7	システム監査基準	42	システム監査基準の用語集（五十音順）　監査対象先	・意見内容 「監査人が実施する監査の対象となる組織体、部門、部署、業務、機能、プロセス、個別の情報システム、等の監査対象を指す。」とあって、「監査対象先」の定義に「監査対象」を使っており、定義になっていない。 --- ・理由 同義語を反復することは定義にならない。「監査対象先」とは聞き慣れない言葉であるので、「監査対象先」の「先」が何を限定するものかを定義しなければならない。	御意見を踏まえ、修正いたします。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
14-8	システム監査基準	42	システム監査基準の用語集（五十音順）　監査人	・意見内容 「システム監査を行う者を指し、専門職としてのシステム監査人だけでなく、何らかの形でシステム監査を行う人やチーム、集団等を指す。」の中で、「何らかの形でシステム監査を行う人」の意味が明瞭でない。 （修正案）「システム監査を行う者をいう。専門職としてのシステム監査人（狭義の監査人）とさまざまな分野に特化した専門家でシステム監査人を補助する者（広義の監査人）から構成される。」 --- ・理由 「何らかの形でシステム監査を行う人」は補助者のことかと想像して書いたのが上記修正案である。システム監査を行うには、監査対象の業務の知識も必要であり、例えば銀行業に通暁している者がチームにいることが必要な場合がある。 ただ、「監査人」の定義の中に補助者を含めることには問題がある。システム監査基準は、システム監査をする場合に監査人が遵守しなければいけない規範であり、「何らかの形でシステム監査を行う人」に【基準2】で求められる監査の専門的能力を求めることには無理があるからだ。	御意見を踏まえ、修正いたします。
15-1	システム監査基準	7	前文	・意見内容 システム監査の当事者は下記のように記されている。 保証型システム監査の当事者は、プロセスオーナー、監査人、利用者 助言型システム監査の当事者は、監査人、依頼者 監査タイプにより、当事者を定義する必要は無く、 依頼者、監査人、プロセスオーナー、監査結果の利用者の四者を記載すべきである。 ・理由 依頼者は、システム監査の結果に基づいて改善を指示する立場であり、一般に経営者である。 また、被監査対象は、プロセスオーナーであるというところは合意できる。 しかし、監査結果の利用者は、自組織に限定するのは不合理である。　依頼者である経営者の場合もあれば、組織・団体の特性に応じて、取引先やITサービスの一般利用者など広く社会の利害関係者が監査結果の利用者となることもある。 その点を考慮して、依頼者、プロセスオーナー、監査人とは別に監査結果の利用者を当事者に含めることが必要である。 ただし、「監査結果の利用者」として、依頼者がなることもあり、助言型システム監査では「依頼者＝監査結果の利用者」となる場合が普通である。	この文言の目的は、保証を目的とした監査と助言を目的とした監査の違いの一つを示すことにあること、また、組織体外の方が利用者になることも想定して、「一般的には」を入れていることから、原案のままといたします。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
16-1	システム監査基準	5	前文	文言の訂正　頁３ （現）監査人は高い倫理が要求される （願）監査人は強い倫理が要求される	御意見を踏まえ、修正いたします。
16-2	システム監査基準	10	監査人の倫理	文言の追加 （現）社会的役割を自覚し、自らを律し、かつ社会の期待に応え、公共の利益に資することができなければならない。 （願）社会的役割を自覚し、自らを律し、かつ社会の期待に応え、是非に鑑みて、公共の利益に資することができなければならない。	御意見の内容は、監査人として当然のことであることから、原案のままとさせていただきます。
16-3	システム監査基準	9	システム監査の意義と目的	文言の追加　頁７ （現）システム監査の目的は、ITシステムに係るリスクに適切に対応しているかどうかについて、監査人が検証・評価し、 （願）システム監査の目的は、ITシステムが健全に稼働して、ITシステムに係るリスクに適切に対応しているかどうかについて、監査人が検証・評価し、	御提案の内容については、例えば、システム開発に関する監査であると対象外と考えられる可能性があるため、原案のままとさせていただきます。
16-4	システム監査基準	25	基準６解釈指針2(2)	文章の移動　頁２３ ・システム監査に係るリスクには、監査対象に対するリスクと監査実施に係るリスクがある。 　適切な位置へ移動をお願いいたします。	御意見を踏まえ、修正いたします。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
16-5	システム監査基準	28,43,44	基準7主旨、システム監査基準の用語集	・頁２６ （現）年間監査計画 （願）年度計画 ・頁４１ （現）監査員 （願）監査人 ・頁４２ （現）公認システム監査人、 （願）公認システム監査人(CSA)、	御意見のとおり、修正いたします。
16-6	システム監査基準	36	基準12解釈指針4	文言の追加　頁３４ （現）が適切かつ適時におこなわれない場合のリスクを明確にして、取締役会等及び経営者等に報告することが必要な場合もある。 （願）が適切かつ適時におこなわれない場合のリスクを明確にして、取締役会等及び経営者等に報告することが必要な場合もある。その際に監査対象先又は改善責任部門にも通知することが必要な場合もある。	既に通知されていることを前提としているため、このような表現としております。この点を明確にするために、一部表現を修正いたします。
17-1	両方	全体	全体	（１）方向性について サイバー攻撃の激化」を受け、我が国においても「サイバーセキュリティリスク」が社会的な大きな課題になっています。世界の潮流は、「セキュアなシステム開発」として、システムライフサイクルの中に対象組織の「情報セキュリティの達成も含めて継続的に実現」するためのＳＳＤＬＣ（セキュリティバイデザインを包含したシステムのライフサイクル管理）ないしはＤｅｖＳｅｃＯｐｓを目指しており、システム監査基準、システム管理基準も、その実現に向けた施策を盛り込むべきではないかと思いました。 （２）ガイドライン化について 今回の改定で、ガイドライン化はシステム監査の機動性と多様性を高める重要なポイントであると思います。ガイドラインは、様々な組織が、様々な監査シーンを想定して用意することが望ましく、例えばシステム監査制度参加者において自主的に策定したガイドラインがあれば公開し、経済産業省に一定の基準を満たすものを認定してもらうことで、システム管理やシステム監査のノウハウが、組織を超えて広く共有されるような取り組みを考えてもよいのではないかと思いました。そのためにも基準本体は幅広い受け皿となれるよう、抽象度を高め、簡潔かつ骨太であってほしいと考えます。	(1)について 御意見を踏まえ、修正いたします。 (2)について 今後の参考にさせていただきます。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
17-2	システム管理基準	全体	全体	システム管理基準について システム管理基準は、システムライフサイクルに立ち戻ったことで、対象プロセスが特定しやすくなり、とてもわかりやすくなりました。 一方で、「サイバーセキュリティリスク」に対しての対応は不十分なものと思われます。 システムライフサイクルを通じてセキュリティを実現するためには「システム監査」が必要です。また、情報セキュリティに関する”マネジメントシステムの有効性”を説明するには「情報セキュリティ監査」が必要です。二つの監査制度はその説明目的に応じて視点を変えているだけで、監査対象の実体は同じものですので、もし制度をすみ分けようとしてセキュリティを除いたのだとすれば、それは誤りだと思います。すべての組織にとってサイバーセキュリティ対応は喫緊の課題であり、システム監査においても「セキュリティ」は最重要の品質項目でなければならないのではないでしょうか。システム管理基準も「サイバーセキュリティへの対応」をもっと前面に出していただけるとよいと思います。	御意見につきましては、今後の参考にさせていただきます。また、付録として、情報セキュリティ管理基準参照表を公表する予定です。
17-3	システム管理基準	前文	前文	（前文） 異常に長いので、１～２ページ程度に短くなるとよいと思います。	基準の活用にあたっての解説を十分に行うために現状の分量となっておりますが、御意見につきましては、今後の検討の参考にさせていただきます。
17-4	システム管理基準	ITガバナンス	全体	（ITガバナンス） 銀行組織をもとにした説明になっているようで、大多数の組織にとってはフィット感がないと思います。冗長な部分も多いので、どのような組織でも必要な要素に絞って抽象度を高くし、より汎用性のある記述とすることが望まれます。	御意見につきましては、今後の参考にさせていただきます。但し、御意見を踏まえて、一部文章による説明を修正させていただきます。
17-5	システム管理基準	ITマネジメント	全体	（ITマネジメント） （１）セキュリティへの対応 今回の改定の柱になった「システムライフサイクル」の国際規格ではそれぞれのプロセスで「セキュリティ」への関連を明確に記述しているのですが、今回の基準からはその記述が抜け落ちており、これらは継承すべきと思いました。 また、「インシデント管理」はシステム障害、セキュリティ事故、サイバー攻撃、すべてのハンドリングの要なので、その観点で「インシデント対応」を含めたものとする必要があるのではないでしょうか。すくなくともこの２点は「サイバーセキュリティへの対応」として欠かせないと思います。	御意見につきましては、今後の参考にさせていただきます。また、付録として、情報セキュリティ管理基準参照表を公表する予定です。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
17-6	システム管理基準	ITマネジメント	全体	（２）サプライチェーンへの対応 供給プロセスがないので、システムサービス等を供給する観点での視点に欠けていると思います。取得プロセスもプロジェクトレベルの記述になってしまっており、「合意」の概念とその監査がないのが残念です。サプライチェーンを監査対象にするためには必須の概念ではないでしょうか。	御意見を踏まえ、修正いたします。
17-7	システム管理基準	ITマネジメント	全体	（３）国際化への対応 残念ながらシステム管理基準には英語版もなく、海外での知名度もないため、海外当局向説明や海外拠点での管理や監査には使いにくいものとなっています。今回の改定で、柱は国際基準に近いものとなったので、参照した国際基準（ISO/IEC/IEEE15288・12207orJISQ0170/0160）とのリファレンスを付けていただくと、説明しやすくなるのではないでしょうか。あわせてNISTのCSFもしくは経済産業省のCPSFとのリファレンスをご検討いただけると、サイバー対策の評価について、海外でも説明がしやすいものになるように思います。	御意見につきましては、今後の検討の参考にさせていただきます。
17-8	システム監査基準	前文	前文	（前文） 異常に長いので、１～２ページ程度に短くすべきであると思います。 また、判断尺度として「情報セキュリティ管理基準」だけでなく、CPSFやサイバーセキュリティ経営ガイドラインなど、経済産業省が現在そして今後発行する基準やガイドライン、各種国際基準、関連する業界基準なども対象として使用しやすくする記述を加えるのが良いのではないでしょうか。 なお「汎用性のある内容となっている」と言う一方で、前文全体は銀行のような重厚長大な組織体制が前提となっており、大多数の組織にはフィット感がないように思います。より抽象度を高くして、種々の組織および多様なシステム監査に共通なものだけを残し、それ以外のものは外部の団体が「ガイドライン」とするのが今回の改定の趣旨に合うのではないでしょうか。	御意見につきましては、今後の検討の参考にさせていただきます。
17-9	システム監査基準	全体	全体	（情報セキュリティ監査基準との項目の差異が妥当かどうかの検証） 二つの監査基準に差異があること自体が問題とは思いませんが、その差は説明可能なものであることが望ましいと思います。例えば「品質管理」は「情報セキュリティ監査基準」にあって、「システム監査基準」にないのですが、これはあまり調子が良くないように思いました。	品質管理に関しては、基準3に記載されているところ、御意見を踏まえて、前文にも追記いたします。

No	対象 （監査基準/管理基準）	PDF ページ数	該当箇所	意見	御意見に対する考え方
17-10	システム監査基準	28	基準7	（不要な基準の削除） 基準７は銀行の内部監査に向けたＦＩＳＣの基準に倣ったものと思われますが、そもそもすべての組織に内部監査部門があるわけではなく、ましてやシステム監査の専担者がいる組織はもっと少ないのが実態です。外部に依拠せざるを得ない組織も多い中で、この基準は「汎用性のある内容となっている」とする前文とは矛盾するのではないでしょうか。あった方が望ましいかもしれませんが少なくとも「基準」とすべきものではないと思います。	基準７については、原則実施されることが望ましいと考えられ、本基準では実務上望ましい対応等を記載しておりますので、原案のままとさせていただきます。