No	頁	項番		引用原文	修正案	理由	回答
1		全般		下線箇所	下線箇所の削減	全体的に下線が多過ぎる為、着目すべき点が曖昧となるため	下線は、JIS Q 27001/27002に追記または変更を加えた部分にのみ付しており、差分を明確にするために原案通りとしたいと思います。 なお、序文の下に下記の注記を付けます。 注記　本書では、JIS Q 27001:2014またはJIS Q 27002:2014との差分を明確にするため、追記した記述の箇所にアンダーラインを付している。
2		序文、 ほか		この規格は,・・・	この文書は,・・・ 本文書は,・・・ このガイドラインは,・・・　など	規格とガイドラインの関連性がわかりにくい	ご指摘の通り規格と紛らわしため、”本書”に修正します。
3	1	1	4行目	箇条4及び箇条5	第4条及び第5条	箇条という表現は分かりにくいため	箇条はJIS規格固有の言い回しであるため、ここでは一般的な表現である、4章、5章に修正します。
4	2	3.2		「サイバーセキュリティ」	サイバーセキュリティについては用語の定義から削除	「サイバーセキュリティ」という言葉単独で用いた場合に、「管理された状態」まで含むことに違和感があります。特に、次に続く、3.3と3.4について、上記定義で置き換えると、意味をなさなくなってしまいます。 3.3：「サイバーセキュリティリスクが管理された状態のリスク管理」 3.4：「サイバーセキュリティリスクが管理された状態のリスク」 サイバーセキュリティの定義についてはISOでも明確な定義はできていないと思いますので、ここでは敢えて定義に載せない方が良いのではないかと思います。	ガイドラインを構成するための基本的な概念であり、定義は欠かせないと考えております。”管理された状態”についても、サーバーセキュリティ基本法の定義において、”必要な措置が講じられ、その状態が適切に維持管理されていることをいう”と記されており大きな乖離はないと考えています。 なお、3.3サイバーセキュリティマネジメントは本文から参照されていないため削除し、また、4.2.3項のサイバーセキュリティをサイバーセキュリティリスクに修正します。
5	2	3.2		サイバーセキュリティリスクが管理された状態	サイバー攻撃に対する防御行為	3.3 サイバーセキュリティマネジメントが「サイバーセキュリティのリスク管理」と定義されているのにも関わらず、「サイバーセキュリティ」の定義が、「サイバーセキュリティマネジメントが出来ている状態」を表現している点が不明瞭であるため。	防御行為は管理された状態の一部であり、定義としては原文のままとしたいと思います。
6	2	3.4		サイバー攻撃により生じるリスク	サイバー攻撃により損害や影響が発生する可能性	ガイドライン導入部分でリスクという文言を日本語で具体的に表現することにより、ガイドライン全体に対する読者の解釈精度が高まることを期待する。	”リスク”は本書のベースであるJIS Q 27001/27002でそのまま使われている用語であるため、原案通りとしたいと思います。

7	2	4.2	21行目	以下に記述されていないJIS Q 27001:2014のすべての要求事項は適用されなければならない。	以下に記述されていないJIS Q 27001:2014のすべての要求事項は、原文のまま適用される。	後続の５章等の記載と書きぶりを合わせる方が良いと思います。	ご提案の通り、”以下に記述されていないJIS Q 27001:2014のすべての要求事項は、原文のまま適用される”で統一するように修正します。
8	~~1~~ 3	4.2.2	a)	a) 組織の目的に対して適切である。	a) 組織の目的及び社会的責任に対して適切である。	「4.2.1 JIS Q 27001:2014 :2014 の 4.14.1 （組織及びその状況理解） 4.1 組織及びその状況理解 組織は，組織の目的及び社会的責任に関連し（以下略）」 において、「組織の社会的責任」について明記しているため、それら組織において確立されるべき情報セキュリティ方針は組織の社会的責任に対して適切であるべきと考える。 また、後のP5 5.4との整合性を保つ意味もある。	ご指摘頂いた通り、”組織の目的及び社会的責任”に修正します。
9	3	4.2.3	28行	組織は，情報セキュリティリスク対応のプロセスについての文書化した情報を保持しなければならない。	組織は，サイバーセキュリティを含む情報セキュリティリスク対応のプロセスについての文書化した情報を保持しなければならない。	３～４行目の 組織は，次の事項を行うために，サイバーセキュリティを含む情報セキュリティリスク対応のプロセスを定め，適用しなければならない。 という文章との整合性を図るため。	ご指摘頂いた通り、”サイバーセキュリティを含む情報セキュリティリスク対応”に修正します。
10	3	4.2.3	d)	附属書 A 又は本規格の付属書 A に規定する管理策を除外した理由	附属書 A 及び本規格の付属書 A に規定する管理策を除外した理由	どちらも除外した理由が必要だと思われるため	各々の管理策は附属書 A 又は本書の附属書 A のどちらかに記述されるため、原案通りとしたいと思います。
11	3	4.2.3	i) j)	・～復旧計画を立案し、実施する。 ・～事業継続計画を立案し、実施する。	・～復旧計画を策定し、実施する。 ・～事業継続計画を策定し、実施する。	大切なプロセスであり、計画立案後、実施は現実的ではないため。	ご指摘頂いた通りであり、直前の記述に合わせそれぞれ、 ”普及を計画し、実施する”、 ”事業継続を計画し、実施する” に修正します。
12	3	4.2.3	11	附属害A及び本規格の附属書A	付属書A及び本規格の付属書A	害は誤記と思われるため	誤記です。修正します。
13	4	4.2.4	a)	a) コミュニケーションの内容（何を伝達するか。）	a) コミュニケーションの内容（伝達内容）	括弧内の説明を簡潔にするため	”伝達内容”に修正します。
14	4	4.2.4	e)	a)コミュニケーションの実施プロセス サイバーセキュリティ対応計画に従った活動は次を含む 1)（以下略）	a)コミュニケーションの実施プロセス サイバーセキュリティ対応計画に従った活動は次を含む 1)（以下略） ※5）として以下を追加 5）サイバーセキュリティが侵害された場合の事業継続についての規定と実施	「JIS Q 27001:2014 :2014 の 7.4.（コミュニケーション）」に関して、日本規格協会出版の「ISO IEC270：2013　情報セキュリティマネジメントシステム要求事項の解説」において　既に顧客からの苦情や情報セキュリティインシデントなどの事象への対応は迅速に処理する必要があるため、手順を定めて、対象者に徹底することが必要である」と記載されており、また、「処置及び改善策以外でもコミュニケーションの必要性を特定することが要求される」と続けられている。 このことからも、組織の事業継続に関するコミュニケーションも含めた方がよいのではないかと考える	ご提案の通り、”サイバーセキュリティが侵害された場合の事業継続についての規定と実施”を追記します。

15	4	4.2.4	e) 2)～4)	2) サイバーセキュリティに関する状況認識を深めるための外部関係者との間の任意の情報共有 3) サイバーセキュリティが侵害された場合の広報についての規定と実施 4) イベント発生後の評判の回復	2) サイバーセキュリティに関する状況認識を深めるための外部機関（パートナ）との間の任意の情報共有 3) サイバーセキュリティが侵害された場合の広報 4) イベント発生後の組織の信用・信頼の回復	2) 外部関係者と利害関係者との相違を明確化するため。また、5.19（P.8）の表現を合わせる方が望ましい。 3) 当該条文の「規定と実施」は他の条文にも該当するため。（条文の表記統一） 4)「評判」よりも一般的な表現と考えるため。	ご指摘頂いた通りであり、ご提案の内容に修正します。
16	4	4.2.4	14行目	4) イベント発生後の評判の回復	4) インシデント発生後の評判の回復	「イベント」発生時点ではそれが有害か無害か、有害だとして組織として対応が必要か、事業継続に影響を及ぼすかなどは確定されていない状況にあると思われます。 発生後に評判の回復が必要となるのはイベントの中でも組織の利害関係者に対して何らかの不利益を生じさせたり、信用の失墜につながるような「インシデント」と考えます。	ご指摘頂いた通りであり、インシデント”に修正します。
17	4	4.2.4	14	イベント発生後の評判の回復	情報セキュリティインシデンド発生後の評判の回復	イベントというとイメージが沸かないため	ご提案通り、インシデント”に修正します。
18	4	5.2	f)	f) リスク一覧に基づくリスクオーナーの明確化	f) リスク一覧に基づくリスク所有者の明確化	JIS Q 27001におけるリスク所有者と同義だと思われる	ご指摘頂いた通りであり、リスク所有者”に修正します。
19	5	5.4	3	h)インシデント対応が必要になった時の自己の役割と行動の順番	f)インシデント対応が必要になった時の自己の役割と行動の順番	元の文章ではe)までなため	編集ミスです。修正します
20	5	5.5	5～6行目	注記 1　資産目録には,・・・ 注記 2 資産目録には,・・・	注記 1　資産目録には,・・・ 注記 2　資産目録には,・・・	見た目だけの問題です。注記1の後は全角スペース、注記2の後は半角スペースで半角分ずれているので全角に統一します。	修正します
21	5	5.6	3行目	目的 所定の保存期間を過ぎたデータを不当な利用や漏えいから保護するため。	目的 所定の保存期間を過ぎたデータの不当な利用や漏えいを防止するため。	大辞林によると「保護」は「危険・破壊・困難などが及ばないように、かばい守ること」とあります。 データ破壊の目的を「保護するため」とすると、「破壊から守るために破壊する」という意味になり、違和感があります。 「不当な利用や漏えいを防止するために破壊する」とした方が自然ではないでしょうか。	データの不当な利用や漏洩の予防も含め防止preventionすることに越したことはありませんが、ここではそこまでは要求しておらず、データの不当な利用や漏洩からの保護protectionが主眼であるため、原文のままとしたいと思います。
22	5	5.6	13行	係争中または実際の訴訟または法的措置または調査に関連する文書は、その訴訟が進行中または発生している間は破壊されない措置が取られることが望ましい。	係争中または実際の訴訟または法的措置または調査に関連する文書は、その訴訟が進行中または発生している間は破壊されない措置が取られることが望ましい。 また、法律で保存期間が決まっている「法定保存文書」は、その保存期間中、破壊されない措置を取る。	税法や労働基準法、医療・医師法などは、所定の期間、文書が保存されていないと罰則が適用される場合もあり、破壊に関し厳密な管理を要するから。	この一文の意図は、保存期限が過ぎて廃棄する文書であっても、係争中は破壊しないようにする例外措置であり、保存期間中の安全な保存とは意図するところが異なりますので、原文のままとしたいと思います
23	5	5.6	15	WORM光学ディスクなど	CD-ROMといった、書き込んだデータを削除したり書き換えたりすることはできないメディアなど	WORMは一般に分かりにくいため	WORMは、その直前の”個々のデータを破壊されないようにした媒体やシステム”と同義の技術用語であるため、ここでは原文通りとしたいと思います。

24	5	5.6	15～17行目	注記 1 当該データが,個々のデータを破壊されないようにした媒体やシステム（WORM光学ディスクなど）に保存されている場合は,破壊待ちデータへのアクセスを防ぐ適切なプロセスが実装されるか,あるいは,破棄するデータをコピーせずに,媒体上の他のデータを新しい媒体にコピーする手順を用いる。	プロセスと手順の例を追記。	注記1の内容が具体的にどのようなプロセスや手順を要求しているかが難解です。 具体例を追記いただけないでしょうか。	文の後半を次の様な表現に改めます。 ”破壊待ちデータへのアクセスを防止するプロセスを実装するか,あるいは,破壊待ちデータ以外のデータを新しい媒体にコピーし、元の媒体を本管理策に従って処分する。”
25	5	5.7	g)	g) 装置の保守と修理は，承認・管理されたツールを用いてタイムリーに実施し，ログを記録する。	g) 装置の保守と修理は，タイムリーに実施し，ログを記録する。	Excel管理でもツール利用といえるが、ツール利用を前提とする記述は不要と考える。（ツール前提とする場合は、他の項目でも該当して、同様の表記とするケースがあると考えるため。例えば、フォレンジックの項目等）	本管理策の意図は、管理の方法が承認されていることにあります。承認・管理されたツールという部分が削除されると管理策の意図が伝わらないこと、Excelもツールであるというのはその通りであり、意味が通るので原文のままとしたいと思います。
26	6	5.7	h)	h) 装置に対する遠隔保守は,承認を得て,ログを記録し,不正アクセスを防げる形で実施する。	h) 装置に対する遠隔保守は,〇〇の承認を得て,ログを記録し,不正アクセスを防げる形で実施する。	ログを記録するためには誰の承認を得るのか、装置の管理者、供給者、保守要員などさまざまな解釈が可能です。 修正案の「〇〇」の中で承認者を明確にするのが望ましいと考えます。	JIS Q 27002では、承認すべき人は、6.1.1 情報セキュリティの役割及び責任においてすべて定めることになっていることから、重複を避けるため、ここは原文通りとしたいと思います。
27	6	5.9	15行目、他	4) 情報技術/産業用制御システムのモニタリング	「情報システム」と「情報技術/産業用制御システム」の使い分けについて解説を別記。	JIS Q 27002:2014の「情報システム」と、本ガイドライン案の「情報技術/産業用制御システム」は同義で使用しているように見えます。 意図的に用語を使い分けるのであれば、解説が必要と考えます。 特に14.1.1項のように既に「情報システム」という表記があり、そこに今回「情報技術/産業用制御システム」を追加して同じ項の中で混在する場合は使い分けについて別記するのが望ましいと考えます。	ご指摘の点を踏まえ、情報システムで統一し、注記として”NIST-SP800では「情報技術/産業用制御システム」と記述されている”を追記します。
28	6	5.10	3～5行目	・・・適切なログ取得及び監視を適用する。これには次の事項を含む。 1) 継続的モニタリング 2) サービス妨害からの保護	・・・適切なログ取得及び監視を適用する。これにはサービス妨害から保護するための継続的モニタリングを含む。	「継続的モニタリング」は監視の方法・態様であり、「サービス妨害からの保護」は監視の目的であることから、同列に並べるものではないと思われます。 ～のために～するという形で文章として構成してはどうかと思います。	ご指摘内容を踏まえ、次のように修正します。 d) 情報セキュリティに影響を及ぼす可能性のある行動（サービス妨害を含む），又は情報セキュリティに関連した行動を記録及び検知できるように，継続的モニタリングを含む適切なログ取得及び監視を適用する。
29	7	5.13	3行目	n) 重要サービス提供を支援するレジリエンスに関する取り決め	本細別は、15.1.2に追加する。	本細別は組織が提供するサービスの可用性支援を供給者に要求しているように見えます。 その場合、「組織の資産にアクセスする供給者」への要求を定める15.1.1より、「組織の情報のための IT 基盤を提供する供給者」への要求を定める15.1.2が適切と考えます。	ご指摘の通りであり、15.1.2への追記に修正します。
30	7	5.13		n）重要サービス提供を支援するレジリエンスに関する取り決め	n）重要サービス提供を支援するサイバーレジリエンスに関する取り決め	用語が定義されていないので違いがわかりにくい	修正します。 用語定義については#31参照。

31	7	5.13	3	重要サービス提供を支援するレジリエンスに関する取り決め	重要サービス提供を支援する取り組みに関する取り決め	レジリエンスは一般には分かりにくい 直訳すると、「精神的回復力」「抵抗力」「復元力」「耐久力」などとなるが、“取り組み”としてみた。	3章の用語及び定義に”レジリエンス”を追加します。 3.6 レジリエンス（resilience） 複雑かつ変化する環境下での組織の適応できる能力。 注記 レジリエンスは，中断・阻害を引き起こすリスクを運用管理する組織の力である。 （JIS Q 22300）
32	7	5.14	2行目	q) 適切なパートナとの間の・・・	q) 適切なパートナーとの間の・・・	JIS Q 27002:2014の中では「パートナー」と表記しています。 ※P8、5.19も同様	修正します。
33	7	5.15	1行目	JIS Q 27002:2014:16.1.1（責及び手順） の・・・	JIS Q 27002:2014:16.1.1（責任及び手順）の・・・	脱字です。	修正します。
34	7	5.16	下から３行目	JIS Q 27002:2014の16.1.4(情報セキュリティ事項の評価及び決定)の実施の手引を,次とおり読み替える。	JIS Q 27002:2014の16.1.4(情報セキュリティ事項の評価及び決定)の実施の手引を,次のとおり読み替える。 ※”の”を追加	誤記	修正します。
35	8	5.16	3行目	情報セキュリティ事項の評価及び決定には・・・	情報セキュリティ事象の評価及び決定には・・・	3行上に「各情報セキュリティ事象を評価し,」とあることから、「事項」ではなく「事象」で統一するのが望ましいと考えます。	ご指摘の通りであり、修正します。
36	8	5.16	3行目	必要に応じてエスカレーションを考慮することが望ましい。	必要に応じて段階的取扱い（escalation）を考慮することが望ましい。	元のJIS Q 27002:2014では「エスカレーション」は「段階的取扱い（escalation）」と表記していることから、合わせるのが望ましいと考えます。	ご指摘の通りであり、修正します。
37	8	5.1.7	3	事業継続マネジメント（以下，BCM という。）	修正案 事業継続マネジメント：Business Continuity Management（以下，BCM という。）	BCMの原語を表記すべき	当該部分は、JIS Q 27002をそのまま引用している部分であり、正確さを期すため、原案通りとしたいと思います。
38	8	5.1.7	4	災害復旧管理（以下，DRM という。）	災害復旧管理：Disaster Recovery Management（以下，DRM という。）	DRMの原語を表記すべき	同上
39	8	5.1.7	8	事業影響度分析（以下，BIA という。）	事業影響度分析：Business Impact Analysis（以下，BIA という。）	BIAの語源を表記すべき	同上
40	8	5.17	8～17行目	太字になっている10行全て	太字を通常の字体に変更	太字の意図が不明であるため	編集ミスです。修正します。
41	8	5.17	5～7行目	通常の業務状況とは異なる困難な状況においても,情報セキュリティ要求事項は変わらず存続することを,情報セキュリティマネジメントの前提とすることが望ましい。別の方法として,困難な状況に適用できる・・・	通常の業務状況とは異なるサイバー攻撃の発生時においても,情報セキュリティ要求事項は変わらず存続することを,情報セキュリティマネジメントの前提とすることが望ましい。別の方法として, サイバー攻撃の発生時に適用できる・・・	本ガイドラインでは元のJIS Q 27002:2014 17.1.1の「困難な状況（adverse situation）（例えば，危機又は災害）」を「サイバー攻撃」に置き換えていることから、本文中で「困難な状況」を使用している他の箇所も「サイバー攻撃」に置き換えるのが適切と考えます。 「困難な状況」は17.1.2、17.1.3でも使用していることから、これらの扱いも検討が必要です。	ご指摘の通り”サイバー攻撃の発生時”に修正します。 また、17.1.1～17.1.3の管理策についても”困難な状況”を”サイバー攻撃”に読み替えるよう修正します。

42	8	5.18	2行目	h) イベントの発生中又は後についても対応計画を実施する。	h) インシデントの発生中又は後についても対応計画を実施する。	本項は「情報セキュリティインシデントへの対応」であり、「a)情報セキュリティインシデントの発生後,・・・」という記述もあることから、イベントではなくインシデントで統一するのが望ましいと考えます。	ご指摘の通り、インシデントに修正するとともに、他の項目の記述に合わせ、”インシデントの発生中又は後の対応を計画し、実施する”に修正します。
43	8	5.18	i)	i) 発生したインシデトを封じ込める。	i) 発生したインシデトの拡大・発散を防ぐ。	「封じ込め」よりも、一般的な表現と考えるため。	ご提案の”拡大・発散を防ぐ”に修正します。
44	8	5.20	2行目	h) フォレンジックの実施	~~h) フォレンジックの実施~~（削除）	本項は「証拠の収集」として「証拠となり得る情報の特定，収集，取得及び保存のための手順」を要求していますが、フォレンジックは証拠収集だけでなく調査・分析までを含むことから、本項の範囲を逸脱しているように見えます。 現状のa)～g)でもフォレンジックにつながる証拠収集としては十分だと考えます。	ご指摘の通り範囲を逸脱する恐れがあることから、フォレンジックの実施を本文から削除し、それに替えて、関連情報として、下記を追記したいと思います。 証拠の収集と分析手段として、ディジタルフォレンジックがある。
45		5	（追加の管理策と実施の手引）	N/A	JIS Q 27002:2014 の 9（アクセス制御）に細分箇条 9.4.6（システムの要塞化）を追加する。 9.4.6　システムの要塞化 管理策 情報技術/産業用制御システムは、事業上のニーズを満たすために要塞化することが望ましい。 実施の手引 情報技術/産業用制御システムを設定する際には，適切な側面からの要塞化（例えば，必要なポート，プロトコル及びサービスだけを有効とする。）及び利用するシステムへの適切な技術手段（例えば，マルウェア対策，ログ取得）の実施を確実にすることが望ましい。	追加の管理策が必要だと思われる	要塞化という視点は重要ですが、管理策の観点からは既に規定されている管理策で対応可能と考えられますので、特に追加は行わないこととしたいと思います。