リスクマネジメントシステム研究分科会
ISO22301研究ワーキンググループ報告書

2017年10月1日

危機管理システム研究学会
リスクマネジメントシステム研究分科会
主査　指田　朝久

はじめに

1．研究経緯

危機管理システム研究学会リスクマネジメントシステム研究分科会ISO22301研究ワーキンググループでは、「JISQ22301社会セキュリティ　－事業継続マネジメントシステム－要求事項」につき、本学会の特色である企業の実務者と大学の研究者による共同議論方式を採りながら、詳細な逐条研究を行ってきた。

事業継続マネジメント（Business Continuity Management）は災害発生時の対応計画のひとつとして、1980年代より不測事態対応計画（Contingency Plan）として開発されたものが、要件が整備されBCPとして徐々に普及してきたものである。日本では2005年より内閣府防災担当や中小企業庁、経済産業省が相次いで事業継続に関するガイドラインを発表し、中でも内閣府防災担当では2020年に大企業100%、中堅企業50%の普及率を目指すなど、国を挙げて取り組みを進めてきた。

一方、世界的にもグローバル経済の進展により、サプライチェーンの事故災害などによる停止に連鎖して、工場などの生産が止まる影響が大きいことが判り、2012年に事業継続マネジメントシステム（BCMS）の国際標準規格ISO22301が制定され、同年、日本国内でもJISQ22301の認証制度がスタートした。

これらの規格は、それを順守することで認証取得を目指すものでもあるが、本来は何より実際に活用できることが求められるものである。そのため本報告書は、ワーキンググループメンバーである企業の実務者が、自社の企業活動やコンサルティング先の企業あるいは自治体での実践経験を踏まえ、大学の研究者と議論を重ねることによって、規格の箇条について、その意味するところ、日本の企業の実情に照らし合わせた場合の考慮点、場合によっては規格そのものへの改善に向けた提案事項などをまとめたものである。

このワーキンググループの活動期間中においても、常総市の水害や熊本地震、そして九州北部豪雨などの様々な災害が発生し、事業継続の取組の実践事例も出てくるようになった一方で、熊本地震では自治体や病院などで庁舎や病棟が被災し代替戦略の発動がままならないという、事業継続がうまくいかなかった事例も散見された。また、災害以外でも、工場や倉庫の火災事故に伴う事業継続計画の発動事例も見聞きするようになってきた。企業の事業継続マネジメントBCMが徐々に普及し実効性を挙げつつあることは認められるが、一方ではいまだにBCPを知ら

ない企業や、防災との区別がついていない、また形骸化している事例なども存在する。本報告書が、企業や自治体の事業継続マネジメントの普及発展の一助になれば幸いである。

2. 本研究報告書の留意点

本報告書の作成にあたっては、「JISQ22301社会セキュリティー事業継続マネジメントシステム-要求事項」の各箇条につき、研究会で合意できた理解の内容を「解釈」、企業や自治体が実際にこの規格を適用する際の方法例などを「方法例」、合意にいたらなかったものの貴重な着眼点や意見、および各企業や自治体などの実践を行う場合の参考を「意見」としてまとめた。特に今回の研究にあたっては、規格そのものが抽象的であるため、具体的に企業や自治体が取り入れる際のヒントになるものを「方法例」にまとめているので活用されたい。また、特に我々ワーキンググループの主張や苦労話、思い入れは「意見」に記載されているので、実務において本報告書を参照されるにあたっては、通常の図書にはない貴重な情報として活用できると考えている。

本報告書の活用にあたっては、JISQ22301と対比させて参照されることも多いと思われるが、国際規格準拠の規格であるがゆえの留意点も多い。以下に整理しておくので、併せて参考とされたい。

① マネジメントのニュアンスが日本と欧米では異なる

このJISQ22301のみならず、リスクマネジメント規格JISQ31000など、マネジメント規格に関しては、「マネジメント」のニュアンスが、日本の場合と規格策定の主流である欧米での特に経営の場面でのニュアンスとが異なっていることを理解する必要がある。Managementと綴られている英語が経営者を意味したり、管理者を意味したり、あるいは対応、やりくりなどの実践を意味するなど、対応するぴったりとした日本語がない。それ以上にマネジメントとは経営者および経営そのものであるというニュアンスが欧米では基礎にあることを前提に規格が作られていることを理解しなければならない。

② 欧米企業の経営構造と日本企業の経営構造の違い

経営に関する国際標準において決定的に異なるのは、企業経営における意思決定の方法の欧米と日本企業（特に伝統的な上場企業）との違いである。本規格ISO22301のほかJISQ9000、JISQ14001、JISQ27001の各種マネジメントシステム規格などにおいて、前提となっているのは欧米企業の経営の在り方である。このため、規格をそのまま現実の日本企業や自治体に合わせようとすると不適合を起こすことがある。経営のスタイルは欧米も日本もそれぞれメリット・デメリットがあり、個性があるものであり、それらは尊重されなければならない。経営者と現場の部長以下の管理職層、従業員層に一線が明確にひかれる欧米系のマネジメントスタイルを前提に本規格が構成されていることを前提に理解し、それを現実の日本流の経営と主要部門の部門長との間で交流が頻繁に行われる日本の企業経営に適合させるためには、十分理解し適切な応用を行うことが求められる。本規格にあたっても枠組みとプロセスでの各担い手の違いを意識する必要がある。

③ 規格用語

本研究報告書の中でも触れているが、規格作成のための特別な用語の使用法がある。本規格は認証規格であるため、第三者の認証機関が審査を行う条文がすべて「べきである」と記述される。べきであるという用語は認証を取得する場合には必須項目となる。認証規格である「すべきである」、認証規格でない場合および認証規格でも必須ではない場合の「望ましい」など、日常の日本語とは異なる用語使用法となっていることに留意する必要がある。

④ 日本語と英語

マネジメントのところでも触れたが、国際標準規格は英語圏の用語で作られている。(他に公用語はフランス語、ロシア語があるが、日本では英語がベースとなり理解されているので英語に絞る)そのため規格の各所で英語のニュアンスに対応する日本語が無いことが散見される。たとえばコミュニケーションという用語は英語では双方向、一方通行のどちらの意味も持ち適宜意味を適切にくみ取り使用されるが、日本語では適切に表現する言葉がない。このためわかりにくい表現や誤訳とはいえないまでも不適と思われる訳語となっている場合もある。そのため疑問を感じた場合はISOの原文に戻って英語での確認をすることをお勧めする。

⑤ ISOとJISの違い

国際標準規格ISO22301が制定された場合は日本工業標準調査会で議論し可決された場合、相同規格として日本工業規格JISが制定される。この場合日本で日常用いられる規格としては日本語のJISQ22301となる。このJIS規格を策定する場合に日本語への翻訳の問題のほかに規格用語としての制約が生じる。このためどうしても非英語圏の読者としては母国語と英語の間でくみ取りきれない意味が残ってしまうこととなる。なお、国際会議に参加した本ワーキンググループのメンバーの見解では、実は英語でもイギリスとアメリカおよびオーストラリアなどでニュアンスが違っていることもあり、同床異夢の解釈が行われていることもある。その意味で規格はあくまで実践性が求められるものであり5年で改定される生きたものであることを前提に活用していただきたい。

⑥ ハイレベルストラクチャー:マネジメントシステム規格の標準の適用

品質マネジメントシステムJISQ9001、環境マネジメントシステムJISQ14001、情報セキュリティマネジメントシステムJISQ27001、そして事業継続マネジメントシステムJISQ22301など、経営に関するマネジメントシステムの規格は国際標準規格では数十にのぼる。一方これらのマネジメントについての要求事項が同じ経営に関するものであっても規格ごとにばらばらであった。ほとんど同じ要求事項であるのに番号や記述内容などが少しづつ異なるため、複数のこれらのマネジメントシステムを導入している企業で混乱が生じていた。そのため国際標準機構では、これらの経営に関するマネジメントシステムの考え方を統一し、

HLSハイレベルストラクチャーにまとめ上げた。今後マネジメントシステム規格はすべてこのスケルトン・ひな形に準拠することとなり、その適用第一号がこのJISQ22301:ISO22301であった。今後その他のマネジメントシステム規格も5年毎の改定に合わせてHLS準拠に項目が改められていく。

一方、JISQ22301はその適用第一号であったため。解釈の誤解があったり、また文案が練れておらず、あとに改定されたその他のマネジメントシステムの文章のほうがより適切であったりということがある。これらについても適宜本研究報告書でHLSについても問題点としても指摘している。

3. 準拠したテキスト

この研究を実施するにあたり準拠したテキストは、「日本規格協会JISQ22301:平成25年10月21日第一刷発行」である。なお、日本語と英語のニュアンスの相違点を確認するため、必要に応じてISO22301(英語版)を参照した。

4. ワーキンググループメンバー

本ワーキンググループは2014年8月4日の活動開始以来17回の研究会を開催し、また4年にわたる研究期間を要したことからメンバーも一部変更になっている。ここでは報告書作成にあたったメンバーを以下に記載することとする。

WG主査	後藤和廣
WG副主査	長井健人
WGメンバー	有賀平、魚谷竜也、内田知男、北澤一保、笹子善平、指田朝久、 多田浩之、福田久治、眞崎達二朗、宮林正恭、宮崎昌和、山田喜代信、 山本祥司、吉川賢一

以上

目　　次

項目	序文 0.1 一般
内容	この規格は，2012 年に第 1 版として発行された ISO 22301 を基に，技術的内容及び構成を変更することなく作成した日本工業規格である。 なお，この規格で点線の下線を施してある参考事項は，対応国際規格にはない事項である。 0.1 一般 この規格は，組織が効果的な事業継続マネジメントシステム（以下，BCMS という。）を策定し，運用するための要求事項について規定する。 BCMS の重要事項を，次に示す。 － 組織のニーズ並びに事業継続マネジメントの方針及び目的を確立する必要性の理解 － 事業の中断・阻害を引き起こすインシデントへの組織の総合的な対応能力を活かすための管理策及び手段の導入及び運用 － BCMS のパフォーマンス及び有効性の監視及びレビュー － 客観的な測定に基づく継続的改善 BCMS は，他の全てのマネジメントシステム同様，次の重要な構成要素からなる。 a) 方針 b) 明確に定められた責任をもつ人員 c) 次の事項に関するマネジメントプロセス 1) 方針 2) 計画 3) 導入及び運用 4) パフォーマンスのアセスメント 5) マネジメントレビュー 6) 改善 d) 監査に必要な文書類 e) 組織にとって適切な事業継続マネジメントプロセス 事業継続は，社会のレジリエンス（resilience）の向上に寄与する。幅広いコミュニティ及び組織を取り巻く環境が組織に影響を与えており，したがって，場合によっては復旧のプロセスに他の組織の関与も必要となる。
解釈	【この箇条の狙い】 ・序文全体を通じて、この規格の固有の特徴（事業継続マネジメントのためのものであること）と全体像を要約して示すこと（序文自体、この規格に固有のものとなっている）。 ・序文はこの規格の全体像を示し重要であるが、いわば当然の事柄でもあるだけに、後の箇条を見ずにここだけで議論しても分かりにくいことに留意する。 【この箇条のポイント】 ・この規格は、ハイレベルストラクチャー設定後、これに準拠した最初の規格である。 ・この規格が、ISO22301 と同じものであること、並びにそこにはない参考事項が記載

	されていることを述べている。 ・この規格が ISO/IEC 専門業務用指針第 1 部統合版 ISO 補足指針―ISO 専用手順で示された「タイプ A のマネジメントシステム規格（要求事項を提供するマネジメントシステム規格）」であることを述べている。 ・この規格固有の特徴である BCMS の重要事項並びに事業継続の社会的意義について述べている。 ・規格の重要な構成要素を述べている。 ・「0.1　一般」にある重要事項の最初に「～方針及び目的を確立する」とあるが、原語が「establishing」であることから、組織のトップが行うべきことを示していると考えられる。
適用方法例等	特になし。
意見	・箇条6（計画）についての記述はかなり少量で自由度のある形になっているが、これは欧米流の経営スタイルを前提として具体的な方法を経営判断に委ねるものと考えられる。したがって自組織にとって必要と判断される部分だけを活用してもよい。 ・箇条8（運用）の部分は詳しく書かれているが、これは BCMS 固有の技術であるためここに記載している。そのため結果的に詳しくなったものと考えられる。
備考	特になし。

項目	序文 0.2 PDCA（Plan-Do-Check-Act）モデル

内容

この規格は，組織の BCMS の計画，確立，導入，運用，監視，レビュー，維持，及び有効性の継続的改善に“PDCA”（Plan-Do-Check-Act）モデルを適用する。

このことは，JIS Q 9001，JIS Q 14001，JIS Q 27001，JIS Q 20000-1，ISO 28000 など，他のマネジメントシステム規格とのある程度の一貫性を確保することによって，関連するマネジメントシステムと整合のとれた，統合的な導入及び運用を支援する。

図 1 は，BCMS が利害関係者及び事業継続マネジメントの要求事項をインプットし，必要な処置及びプロセスを通して，それらの要求事項を満たす継続性の結果（すなわち，運用管理された事業継続）をどのように生み出すかを示したものである。

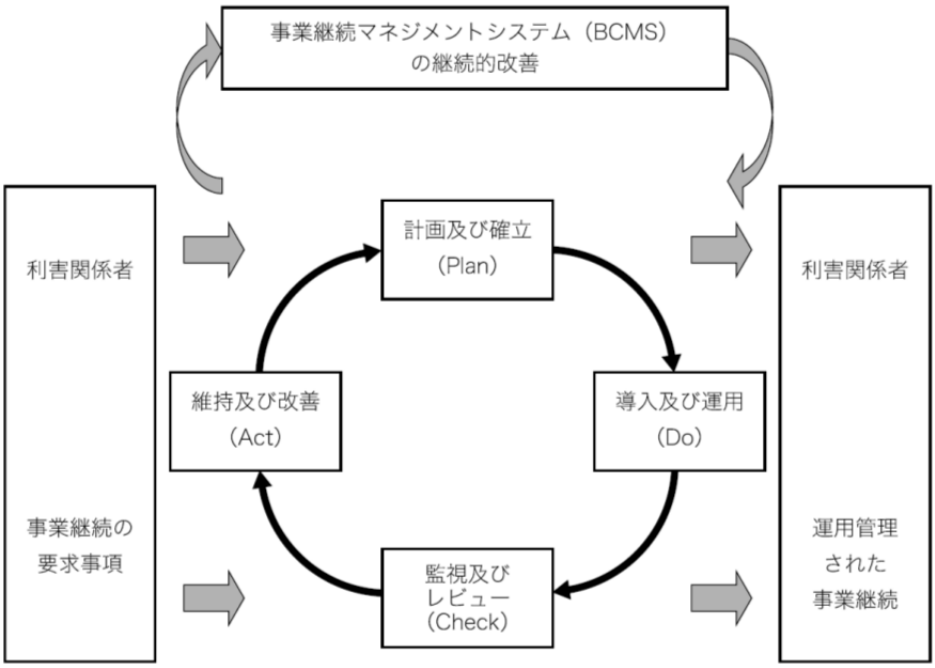


図 1－BCMS プロセスに適用される PDCA モデル

表 1－PDCA モデルの説明

計画及び確立（Plan）	組織の全体的な方針及び目的に沿った結果を出すために，事業継続の改善に適した事業継続の方針，目的，目標，管理策，プロセス及び手順を確立する。
導入及び運用（Do）	事業継続の方針，管理策，プロセス及び手順を導入し，運用する。
監視及びレビュー（Check）	事業継続の方針及び目的に照らしてパフォーマンスを監視及びレビューし，その結果を経営者に報告してレビューに付し，是正及び改善の処置を決定し，許可する。
維持及び改善（Act）	マネジメントレビューの結果に基づいた是正処置をとり，BCMS の適用範囲，事業継続の方針及び目的を再評価することによって，BCMS を維持し，改善する。

解釈	【この箇条の狙い】 ・この規格が、PDCA モデルに基づくマネジメントシステム規格であることを示す。 【この箇条のポイント】 ・この規格が、他のマネジメントシステム規格と整合的で統合的な導入・運用を意図し、そのことを前提として作られたものであることを意味している。 ・この規格における PDCA モデルの概要が示されている。 ・BCMS は組織における仕組み（事業継続のため、インプットを処理しアウトプットを生み出す組織の仕組みであり継続的改善が求められる）までを意味し、BCM（事業継続の活動プロセス）の概念にとどまらない。BCP という用語は、BCM における計画ないし手続き文書といえる。
適用方法例等	・既に一定程度確立された他の PDCA モデルのマネジメントシステムを有する場合には、それらを参考に適用を考えることも有効である。
意見	・PDCA という概念はマネジメントシステムとは異なる。継続的に取組み向上させていくための手法を意味し、ISO においては日本発の概念と考えられている。 ・PDCA モデルを適用することにより「関連するマネジメントシステムと整合性のとれた統合的な導入及び運用を支援する」とあるが、実際の活動では整合を取るのがなかなか難しく、それぞれのマネジメントシステムの目的により別々の活動となってしまう実態も見られる。 ・整合的・統合的とはいっても別々の目的のためのマネジメントシステムであることに変わりはなく、それぞれの整合性確保や統合のための負荷がかかる。また、システム間の関連性が高まれば高まるほど、あるシステムで修正を行ったときに、他のシステムにも影響が及ぶことになる。過度に緻密な整合性確保を図るよりも、実効性確保に意を払うことが特に導入当初は望ましいと考える。
備考	特になし。

項目	序文 0.3 この規格における PDCA の構成要素
内容	表 1 で示す PDCA モデルについては，箇条 4 から箇条 10 で次の構成要素を網羅している。 － 箇条 4 は，計画及び確立（Plan）の構成要素である。ここでは，組織に適用される BCMS の状況設定のために必要な要求事項，利害関係者のニーズ，適用法令等の要求事項及び適用範囲を規定する。 － 箇条 5 は，計画及び確立（Plan）の構成要素である。ここでは，BCMS におけるトップマネジメントの役割に固有の要求事項及び事業継続方針を表明し，リーダーシップによって，その期待をどのように組織に明確に伝えるかを規定する。 － 箇条 6 は，計画及び確立（Plan）の構成要素である。ここでは，BCMS 全体の戦略目的及び計画策定に関係する要求事項を規定する。箇条 6 の内容は，リスクアセスメントに基づくリスク対応の機会の設定，及び復旧目標の設定につながる事業影響度分析とは異なる。 注記 事業影響度分析及びリスクアセスメントプロセスについての要求事項は，箇条 8 で規定する。 － 箇条 7 は，計画及び確立（Plan）の構成要素である。ここでは，要求される文書類を文書化し，管理し，維持し，保持しながら，人々の力量，並びに利害関係者との反復的及び必要に応じたコミュニケーションを確立することを通じて，BCMS の運用の支援について規定する。 － 箇条 8 は，導入及び運用（Do）の構成要素である。ここでは，事業継続に関する要求事項を定め，それらへの対応方法，及び中断・阻害を引き起こすインシデントに対処する手順の策定方法を規定する。 － 箇条 9 は，監視及びレビュー（Check）の構成要素である。ここでは，事業継続マネジメントのパフォーマンス，BCMS のこの規格への適合，及び経営者の期待を測定するために必要な要求事項を規定し，期待に関して経営者のフィードバックを求める。 － 箇条 10 は，維持及び改善（Act）の構成要素である。ここでは，BCMS のこの規格への不適合を特定し，是正処置によって対応することを規定する。
解釈	【この箇条の狙い】 ・PDCA モデルと、この規格の箇条の対応状況を示す。 【この箇条のポイント】 ・PDCA の各プロセスがどの箇条に対応しているか、および各箇条の概要を述べている。
適用方法例等	特になし。
意見	・認証を取得する場合、日本と欧州の認証機関の考え方は異なり、日本の認証機関はかなり形式的なことを求める傾向がある。欧州では認証機関に対して自らの判断基準に照らして説明できれば OK。海外審査と国内審査では濃淡がある。 ・当初 ISMS 出身の人が多かったことからそのような傾向が見られたが、最近では認証技術の定着もあり極端な差はなくなった。 ・審査機関や審査員の性格やレベルによっても求められる詳細さが異なることがある。 ・同じ組織においても、最初に取り組む場合は目的に照らして行動をフレキシブルに考えられるが、後任者は当初の決定を見直さずそのまま遵守する傾向が強いことから、

	形式的にやらざるをえないと思われる。 ・審査員は、被審査側が書いてあることをそのまま遵守しているかを見るので、被審査側が細かく書けば細かく見る傾向が強い。 ・ハイレベルストラクチャーでは、品質や環境、情報セキュリティ、BCPなど各マネジメントステム固有の要素は原則、箇条8に記述することとし、この ISO22301 は HLS 適合の第 1 号のためにそれに従った。そのため本来計画段階で箇条 6 に記述すべきことが妥当なものも箇条 8 に記述されている。しかしこの ISO22301 の不便さが判明したためその後の品質や情報セキュリティなどでは箇条6にも必要なものは記述する方向に修正されている。「巻末参考:ISO22301,ISO27001,ISO14001 の目次構成の比較」を参照
備考	特になし。

項目	1 適用範囲
内容	この規格は，事業の中断・阻害を引き起こすインシデントを防止し，その発生の起こりやすさを低減し，発生に備え，発生した場合には対応し，事業を復旧するための文書化したマネジメントシステムを計画し，確立し，導入し，運用し，監視し，レビューし，維持し，継続的に改善するために必要な事業継続マネジメントに関する要求事項について規定する。 この規格に規定する要求事項は汎用的なものであり，組織の形態及び規模，並びに事業の性質にかかわらず，あらゆる組織又はその一部に適用できるように意図されている。これらの要求事項の適用度合いは，当該組織の事業環境及び複雑度によって異なる。 この規格の意図は，事業継続マネジメントシステム（BCMS）の構造の均一化を示唆することではなく，組織が，そのニーズにかな（適）い，利害関係者の要求事項を満たすBCMS を設計できるようにすることである。これらのニーズは，法令，規制，組織及び業界の要求事項，製品・サービス，使用するプロセス，組織の規模及び構造，並びに組織の利害関係者の要求事項によって形成される。 この規格は，次に示す事項を行おうとする，あらゆる形態及び規模の組織に適用できる。 a) BCMS を確立し，実施し，維持し，改善する。 b) 表明した事業継続方針とこの規格との適合を保証する。 c) この規格に適合していることを他者に実証する。 d) 第三者の認証機関に BCMS の認証・登録を求める。 e) この規格に適合していることを自己認証し，宣言する。 この規格は，自らの事業継続のニーズ及び義務を果たす組織の能力を評価するために用いることができる。 注記 この規格の対応国際規格及びその対応の程度を表す記号を，次に示す。 ISO 22301:2012，Societal security－Business continuity management systems－Requirements（IDT） なお，対応の程度を表す記号「IDT」は，ISO/IEC Guide 21-1 に基づき，“一致している”ことを示す。
解釈	【この箇条の狙い】 ・この規格の概要と制定の意図、並びに適用可能な組織の範囲を示す。 【この箇条のポイント】 ・この規格は、利用する組織のそれぞれが置かれた状況により最適なBCMSとなるよう、適切に設計されるためのものであり、単に同じようにやればよいというものではないことを述べている。 ・第三者による保証や評価に活用できるものであることを述べている。 ・この規格の活用は自組織にとって必要と判断される部分だけを活用しても良く、必ずしも全部について対応しなくても良い。ただ、認証を受ける場合は原則すべての要求事故について対応が必要であり、除外する場合はその理由を説明できることが必要となる。
適用方法例等	特になし。
意見	特になし。
備考	特になし。

項目	2 引用規格
内容	次に掲げる規格は，この規格に引用されることによって，この規格の規定の一部を構成する。これらの規格は，その最新版（追補を含む。）を適用する。 引用規格はない。
解釈	【この箇条の狙い】 ・引用規格がないことを示す 【この箇条のポイント】 ・特になし。
適用方法例等	特になし。
意見	特になし。
備考	特になし。

3 用語及び定義

この規格で用いる主な用語及び定義は，次による。

箇条	用語	用語の定義	出典
3.1	事業活動（activity）	一つ又は複数の製品・サービスを生産する又は提供する組織によって（又はその組織のために）行われるプロセス又は一連のプロセス。 例 このようなプロセスは，会計，コールセンター，情報技術（IT），製造，流通などがある。	
3.2	監査（audit）	監査基準が満たされている程度を判定するために，監査証拠を収集し，それを客観的に評価するための，体系的で，独立し，文書化したプロセス。 注記 1 監査は内部監査（第一者）又は外部監査（第二者・第三者）のいずれでも，又は複合監査（複数の分野の組合せ）でもあり得る。 注記 2 “監査証拠”及び“監査基準”は，JIS Q 19011 に定義されている。	Annex SL
3.3	事業継続（business continuity）	事業の中断・阻害などを引き起こすインシデントの発生後，あらかじめ定められた許容レベルで，製品又はサービスを提供し続ける組織の能力（JIS Q 22300 参照）。 注記 組織の能力だけでなく，組織の行為を示す場合もある。	
3.4	事業継続マネジメント（business continuity management）	組織への潜在的な脅威，及びそれが顕在化した場合に引き起こされる可能性がある事業活動への影響を特定し，主要な利害関係者の利益，組織の評判，ブランド，及び価値創造の活動を保護する効果的な対応のための能力を備え，組織のレジリエンスを構築するための枠組みを提供する包括的なマネジメントプロセス。	
3.5	事業継続マネジメントシステム，BCMS（business continuity management system）	マネジメントシステム全体の中で，事業継続の確立，導入，運用，監視，レビュー，維持及び改善を担う部分。 注記 マネジメントシステムには，組織の構造，方針，計画作成活動，責任，手順，プロセス及び資源が含まれる。	
3.6	事業継続計画（business continuity plan）	事業の中断・阻害に対応し，事業を復旧し，再開し，あらかじめ定められたレベルに回復するように組織を導く文書化した手順。 注記 多くの場合，この計画は，重要業務の継続を確実にするために必要な資源，サービス及び活動を対象とする。	
3.7	事業継続プログラム（business continuity program）	事業継続マネジメントを実施し，維持するための適切な資源が供給され，トップマネジメントによって支援される，継続的なマネジメント及び統治のプロセス。	
3.8	事業影響度分析（business impact analysis）	活動，及びその活動に対して事業の中断・阻害が及ぼし得る影響を分析するプロセス（JIS Q 22300 参照）。	

箇条	用語	用語の定義	出典
3.9	力量 (competence)	意図した結果を達成するために，知識及び技能を適用する能力(JIS Q 22300 参照)。	Annex SL
3.10	適合 (conformity)	要求事項を満たしていること(JIS Q 22300 参照)。	Annex SL
3.11	継続的改善 (continual improvement)	パフォーマンスを向上するために繰り返し行われる活動(JIS Q 22300 参照)。	Annex SL
3.12	修正 (correction)	検出された不適合を除去するための処置(JIS Q 22300 参照)。	Annex SL
3.13	是正処置 (corrective action)	不適合の原因を除去し，再発を防止するための処置(JIS Q 22300 参照)。 注記 望ましくない結果の場合，その原因の最小化又は除去，及びその影響の低減又は再発の防止のため，処置が必要である。この定義においては，このような処置は“是正処置”の概念には当てはまらない。	Annex SL
3.14	文書 (document)	情報及びそれを保持する媒体。 注記 1 媒体としては，紙，磁気，電子式若しくは光学式コンピューターディスク，写真若しくはマスターサンプル，又はこれらの組合せがあり得る。 注記 2 仕様書，記録などの一連の文書は，“文書類”ということが多い。	
3.15	文書化した情報 (documented information)	組織が管理し，維持するよう要求されている情報，及びそれが含まれている媒体。 注記 1 文書化した情報は，あらゆる形式及び媒体の形をとることができ，あらゆる情報源から得ることができる。 注記 2 文書化した情報には，次に示すものがあり得る。 － 関連するプロセスを含むマネジメントシステム － 組織の運用のために作成された情報(文書類) － 達成された結果の証拠(記録)	Annex SL
3.16	有効性 (effectiveness)	計画した活動を実行し，計画した結果を達成した程度(JIS Q 22300 参照)。	Annex SL
3.17	事象(event)	ある一連の周辺状況の出現又は変化(JIS Q 0073 参照)。 注記 1 事象は，発生が一度以上であることがあり，幾つかの原因をもつことがある。 注記 2 事象は，何かが起こらないことを含むことがある。 注記 3 事象は，“インシデント”又は“事故”と呼ばれることがある。 注記 4 結果にまで至らない事象は，“ニアミス”，“インシデント”，“ヒヤリハット”又は“間一髪”と呼ばれることがある。	

箇条	用語	用語の定義	出典
3.18	演習 (exercise)	組織内で，パフォーマンスに関する教育訓練を実施し，評価し，練習し，改善するプロセス(JIS Q 22300 参照)。 注記 1 演習は，次の目的に利用できる。 － 方針，計画，手順，教育訓練，装置又は組織間合意の妥当性確認 － 役割及び責任を担う要員の明確化並びにそれらの教育訓練 － 組織間の連携及びコミュニケーションの改善 － 資源の不足部分の特定 － 個人のパフォーマンスの改善及び改善の機会の特定 － 臨機応変な対応を練習するために統制された機会 注記 2 試験は，演習の独特かつ特有の形態であり，計画中の演習の到達点又は目的の枠内で，合否の要素を予想することが含まれている。 【BCM-WG 意見】 ・演習、訓練の定義案 －演習（エクササイズ）：組織としての実効性、力量・能力の確認のためのプロセス。実行して試してみること －訓練（トレーニング）：危機対応技能の組織的な習熟とその維持継続のためのプロセス。手順の実施能力を高めること －練習（ドリル）：手順を定着させ、習熟すること	

箇条	用語	用語の定義	出典
3.19	インシデント (incident)	中断・阻害，損失，緊急事態又は危機になり得る又はそれらを引き起こし得る状況(JIS Q 22300 参照)。 【BCM-WG 意見】 ・危機(crisis)は、ISO22300 社会セキュリティー用語－の2.1.12で「組織の中核となる活動、及び/又は組織の信頼性を中断・阻害させ、緊急の処置を必要とする、高レベルの不確かさを伴う状況」と定義されている。 ・インシデントとクライシスは概念が異なる。 あらかじめ想定されたリスクが、想定された被害程度の状況かそれ以内の小さな程度で発生した場合をインシデントと呼ぶ。クライシスは、想定外や想定を超えた被害程度における対応を指す。 ・英語では想定内の範囲がインシデントとエマージェンシーであり、想定外がクライシス、ディザスター、カタストロフィーとなる。 ・ISO では想定内の災害対応に対してエマージェンシーを用いている。ちなみにアメリカ連邦政府の危機管理庁と訳されるFEMAもエマージェンシーであり、想定内の範囲で有効に有事対応を行うことの意味合いである。 ・日本語の「危機管理」はこれらの2つの概念が明確に分かれておらず、さらにセキュリティの概念が含まれていると想定される。そのため文献を読む場合には用語の意味を確かめて意味をくみ取ることが必要である。 ・BCP では想定内の出来事に対して機能することを求めている。想定外のリスクが顕在化した場合や、想定したリスクではあるが規模が大きく手に負えないなどのいわゆる危機管理となる状況で機能することまでは求められていない。	
3.20	インフラストラクチャ (infrastructure)	組織の運営に必要な施設，設備及びサービスの基盤。	
3.21	利害関係者 (interested party)→(利害関係者が推奨用語、ステークホルダーは許容用語)	ある決定事項又は活動に影響を与え得るか，その影響を受け得るか，又は，その影響を受けると認識している，個人又は組織。 注記 組織のいかなる決定事項又は活動にも関心のある個人又は集団がなり得る。	Annex SL
3.22	内部監査 (internal audit)	組織自身又はその代理者によって，マネジメントレビュー及びその他組織内部の目的のために行う監査。 組織の自己適合宣言の根拠となることもある。 注記 多くの場合，特に比較的規模の小さい組織においては，監査の独立性は，その組織自身がその監査対象の活動に責任を負っていないことで実証できる。	

箇条	用語	用語の定義	出典
3.23	発動 (invocation)	重要な製品又はサービスの提供を継続するために，組織の事業継続の取決めを実施する必要があることを宣言する行為。	
3.24	マネジメントシステム (management system)	方針，目的及びその目的を達成するためのプロセスを確立するための，相互に関連する又は相互に作用する，組織の一連の要素。 注記 1 一つのマネジメントシステムは，単一又は複数の分野を取り扱うことができる。 注記 2 システムの要素には，組織の構造，役割及び責任，計画，運用などが含まれる。 注記 3 マネジメントシステムの適用範囲としては，組織全体，組織内の固有で特定された機能，組織内の固有で特定された部門，複数の組織の集まりを横断する一つ又は複数の機能，などがあり得る。	Annex SL
3.25	最大許容停止，MAO (maximum acceptable outage)	製品・サービスを提供しない，又は事業活動を行わない結果として生じる可能性のある悪影響が，許容不能な状態になるまでの時間。 注記 最大許容停止時間も参照。	
3.26	最大許容停止時間，MTPD (maximum tolerable period of disruption)	製品・サービスを提供しない，又は事業活動を行わない結果として生じる可能性のある悪影響が，許容不能な状態になるまでの時間。 注記 最大許容停止も参照。	
3.27	測定 (measurement)	値を決定するプロセス。	Annex SL
3.28	最小事業継続目標，MBCO (minimum business continuity objective)	事業の中断・阻害発生時に事業の目的を達成するために，組織にとって許容できる最低限のサービス及び／又は製品のレベル。	
3.29	監視 (monitoring)	システム，プロセス又は活動の状況を明確にすること。 注記 状態を明確にするために，点検，監督又は注意深い観察が必要な場合もある。	Annex SL
3.30	相互支援協定 (mutual aid agreement)	互いに助け合うため，二つ以上の主体の間であらかじめ取り交わした協定(JIS Q 22300 参照)。	
3.31	不適合 (nonconformity)	要求事項を満たしていないこと(JIS Q 22300 参照)。	Annex SL

箇条	用語	用語の定義	出典
3.32	目的 (objective)	達成する結果(JIS Q 22300 参照)。 注記 1 目的は, 戦略的, 戦術的又は運用的であり得る。 注記 2 目的は, 様々な領域[例えば, 財務, 安全衛生, 環境の到達点(goal)]に関連し得るものであり, 様々な階層[例えば, 戦略的レベル, 組織全体, プロジェクト単位, 製品ごと, プロセスごと]で適用できる。 注記 3 目的は, 例えば, 意図する成果, 目的(purpose), 運用基準など, 別の形で表現することもできる。また, 社会セキュリティ目的という表現の仕方もある。又は, 同じような意味をもつ別の言葉[例:狙い(aim), 到達点(goal), 目標(target)]で表すこともできる。 注記 4 社会セキュリティマネジメントシステムの場合, 組織は, 特定の結果を達成するため, 社会セキュリティ方針と整合のとれた社会セキュリティ目的を設定する。	Annex SL
3.33	組織 (organization)	自らの目的を達成するため, 責任, 権限及び相互関係を伴う独自の機能をもつ, 個人又は人々の集まり。 注記 1 組織という概念には, 法人か否か, 公的か私的かを問わず, 自営業者, 会社, 法人, 事業所, 企業, 当局, 共同経営会社, 非営利団体若しくは協会, 又はこれらの一部若しくは組合せが含まれる。ただし, これらに限定されるものではない。 注記 2 複数の業務ユニットがある組織は, 一つの業務ユニットを一つの組織として定義することがある。	Annex SL
3.34	外部委託する (outsource) (動詞)	ある組織の機能又はプロセスの一部を外部の組織が実施するという取決めを行う。 注記 外部委託した機能又はプロセスはマネジメントシステムの適用範囲内にあるが, 外部の組織はマネジメントシステムの適用範囲の外にある。	Annex SL
3.35	パフォーマンス (performance)	測定可能な結果。 注記 1 パフォーマンスは, 定量的又は定性的な所見のいずれにも関連し得る。 注記 2 パフォーマンスは, 活動, プロセス, 製品(サービスを含む。), システム, 又は組織の運営管理に関係し得る。	Annex SL
3.36	パフォーマンス評価 (performance evaluation)	パフォーマンスを判定するプロセス。	
3.37	要員 (personnel)	組織のために, その管理下で働く人々。 注記 要員の概念には, 従業員, パートタイムのスタッフ, 及び代理店のスタッフを含むが, これらだけに限らない。	
3.38	方針(policy)	トップマネジメントによって正式に表明された組織の意図及び方向付け。	Annex SL
3.39	手順 (procedure)	活動又はプロセスを実行するために規定された方法。	

箇条	用語	用語の定義	出典
3.40	プロセス（process）	インプットをアウトプットに変換する，相互に関連する又は相互に作用する一連の活動。	Annex SL
3.41	製品及びサービス（products and services）	組織が，その顧客，受領者及び利害関係者に供給する有益な結果（例 製造品，自動車保険，地域看護）。	
3.42	優先事業活動（prioritized activities）	インシデントの発生後，影響を軽減するため，優先的に実施しなければならない事業活動（JIS Q 22300 参照）。 注記 同種の事業活動を記述する際に一般的に使われる用語としては，“重要な”，“必須の”，“不可欠な”，“緊急の”，“主要な”，などがある。	
3.43	記録（record）	達成した結果，又は実施した活動の証拠を記述したもの。	
3.44	目標復旧時点，RPO（recovery point objective）	再開時に事業活動が実施できるようにするために，事業活動で使用される情報がどの状態まで復旧されなければならないかを示す時点。 注記 “最大データ損失”ともいう。	
3.45	目標復旧時間，RTO（recovery time objective）	インシデントの発生後，次のいずれかの事項までに要する時間。 － 製品又はサービスが再開される， － 事業活動が再開される， － 資源が復旧される。 注記 製品，サービス及び事業活動について，目標復旧時間は，製品・サービスを提供しない，又は事業活動を行わない結果として生じる悪影響が許容できなくなるまでの時間よりも短くなければならない。	
3.46	要求事項（requirement）	明示されている，通常暗黙のうちに了解されている又は義務として要求されている，ニーズ又は期待。 注記 1 “通常暗黙のうちに了解されている”とは，対象となるニーズ又は期待が暗黙のうちに了解されていることが，組織及び利害関係者にとって，慣習又は慣行であることを意味する。 注記 2 規定要求事項とは，例えば，文書化した情報の中で，明示されている要求事項をいう。	Annex SL
3.47	資源（resources）	組織が業務を運営し，目的を達成するために，必要なときに利用可能な状態になければならない全ての資産，人員，技能，情報，技術（工場及び設備を含む。），土地，供給品及び情報（電子的か否かを問わず。）。	

箇条	用語	用語の定義	出典
3.48	リスク(risk)	目的に対する不確かさの影響(JIS Q 0073 参照)。 注記 1 影響とは，期待されていることから，好ましい方向及び／又は好ましくない方向にかい(乖)離することをいう。 注記 2 目的は，例えば，財務，安全衛生，環境に関する到達目標など，異なった側面があり，戦略，組織全体，プロジェクト，製品，プロセスなど，異なったレベルで設定されることがある。 目的は，例えば，事業継続目的として，意図する結果，目標，運用基準，また，類似の意味をもつ言葉[例えば，狙い(aim)，到達点(goal)，目標(target)]などのように，別の方法で表現されることもある。 注記 3 リスクは，起こり得る事象(JIS Q 0073 の 3.5.1.3)及び結果(JIS Q 0073 の 3.6.1.3)，又はこれらの組合せについて述べることによって，その特徴を記述することが多い。 注記 4 リスクは，ある事象(周辺状況の変化を含む。)の結果とその発生の起こりやすさ(JIS Q 0073 の 3.6.1.1)との組合せとして表現されることが多い。 注記 5 不確かさとは，事象，その結果又はその起こりやすさに関する，情報，理解又は知識が，たとえ部分的にでも欠落している状態をいう。 注記 6 事業継続マネジメントシステム規格においては，事業継続目的は，明示された結果を出すために，事業継続方針に沿って組織で設定される。事業継続目的にリスクという用語及びリスクマネジメントの構成要素を適用するときは，6.2 に規定する事業継続目的を含み，これらだけに限らず，組織の目的に関連付けられる。 【BCM-WG 意見】 ・ISO22301 では risk に加えて機会(opportunity)が用いられており、ISO31000 の用語定義と齟齬がある。 ・損失や損害等のネガティブな影響の可能性が risk、利益や効用等のポジティブな影響の可能性が機会(opportunity)とされている。	Annex SL
3.49	リスク選好(risk appetite)	組織に追求する又は保有する意思があるリスクの量及び種類。	
3.50	リスクアセスメント(risk assessment)	リスク特定，リスク分析及びリスク評価のプロセス全体(JIS Q 0073 参照)。	
3.51	リスクマネジメント(risk management)	リスクについて，組織を指揮・統制するための調整された活動(JIS Q 0073 参照)。	

箇条	用語	用語の定義	出典
3.52	試験の実施 (testing)	ものの有無，品質又は正確さを見極めるための手順(JIS Q 22300 参照)。 注記 1 試験の実施は，“試験(trial)”ともいう。 注記 2 試験の実施は，支援計画に適用されることが多い。	
3.53	トップマネジメント(top management)	最高位で組織を指揮し，管理する個人又は人々の集まり。 注記 1 トップマネジメントは，組織内で，権限を委譲し，資源を供給する力をもっている。 注記 2 マネジメントシステムの適用範囲が組織の一部だけの場合，トップマネジメントとは，組織内のその一部を指揮し，管理する人をいう。	Annex SL
3.54	検証 (verification)	証拠を提示することによって，規定の要求事項が満たされていることを確認すること。	
3.55	作業環境 (work environment)	作業が行われる場の一連の諸条件(JIS Q 22300 参照)。 注記 条件には，物理的，社会的，心理的及び環境的要因が含まれる。例えば，温度，評価の仕組み，人間工学的側面，大気成分などがある。	

【BCM-WG で追加した用語定義】

用語	定義(BCM-WG 案)
警報(alert) 警告(warning)	・警報と警告は異なる。警報(alert)は一方的な通知、警告(warning)は幅広い情報提供である。
アカウンタビリティ(accountability)	・組織の長として、組織に関係性を持つ(ガバナンスの関係のある)ステークホルダーに対し、組織の実施したこと、実施することについて、ステークホルダーが判断できる最低限の情報提供を与える責任のこと。
ハイレベルストラクチャー (high level structure、HLS)	・「ISO/IEC 専門業務用指針 補足指針 (2012 年 5 月改正)」の中の「附属書 SL」において定められた、ISO マネジメントシステム規格についての構造、分野共通の要求事項及び共通となる用語・定義。 ・附属書 SL の附属書 3 で、「上位構造(High Level Structure[HLS])」、「共通の中核となるテキスト」、「共通用語及び中核となる定義」が定められている。一般に、慣用的にハイレベルストラクチャーと用いた場合、附属書 SL を意味することが多い。 ・ハイレベルストラクチャーでは、品質や環境、情報セキュリティ、BCP など各マネジメントステム固有の要素は原則、箇条 8 に記述することとし、この ISO22301 は HLS 適合の第 1 号のためにそれに従った。 ・そのため本来計画段階で箇条6に記述すべきことが妥当なものも箇条 8 に記述されている。しかしこの ISO22301 の不便さが判明したためその後の品質や情報セキュリティなどでは箇条6にも必要なものは記述する方向に修正されている。(巻末参考:ISO22301、ISO27001、ISO14001 の目次構成の比較)を参照のこと

用語	定義（BCM-WG 案）
レジリエンス （resilience）	・日常用語でも多義であり、医学用語では回復力として用いられる。 ・日本では強靭化と翻訳され、しなやかさや回復といったニュアンスの他に災害に立ち向かうなどのニュアンスをもち、地震や水害などへの事前対策として、ダムの建設や海岸堤防の津波対策などの公共工事への投資の正当化の意義も持っているように思われる。
レスポンシビリティ （responsibility）	・任務遂行責任。組織に所属しているすべての人々が持つ、自分に与えられた任務を遂行する責任のこと
risk advisory system	・JIS Q22301 では、risk advisory system を災害情報提供システムと訳しているが、ISO22301 では、災害だけを対象としている訳ではない。 ・災害情報提供システム（risk advisory system）は高度な意思決定を支援するようなシステムだけを指すのではなく、河川水位監視システムやアメダスなども該当する。地震でいえば地震後震度や倒壊家屋を推定し GIS（Geographic Information System）上に表示するシステムなども提供され始めている。
想定外 （unexpected）	・想定外という用語が東日本大震災以降用いられているが、言い訳として使われているように思われるため、用語は科学的な想定外と意図的な対応をしないことに決めた想定外などを区別するようにすべきである。 ・用語の使い分けの案としては以下のものがある。 1） 対応外： リスク評価をして経営判断として対応しないこととしたもの 2） サボタージュ： 故意に対応しないこととしたもの 3） 想定外： 科学的に想定できなかったもの(その時点での判断を含む) ・原子力分野のリスク解析では人工衛星の落下も考慮しており、東日本大震災の原子力事故は意図的に対応しないことを決めたという想定外（対応外）である。

項目	4 組織の状況 4.1 組織及びその状況の理解
内容	組織は，組織の目的に関連し，かつ，その BCMS の意図した成果を達成する組織の能力に影響を与える，外部及び内部の課題を決定しなければならない。 組織の BCMS を確立し，実施し，維持するに当たって，これらの課題を考慮しなければならない。 組織は，次の事項を特定し，文書化しなければならない。 a) 組織の事業活動，機能，サービス，製品，取引関係，サプライチェーン，利害関係者との関係，及び事業の中断・阻害を引き起こすインシデントに関係する潜在的な影響 b) 事業継続方針と，組織の目的及び組織の総合的なリスクマネジメント戦略を含むその他の方針とのつながり c) 組織のリスク選好 状況を明確にするに当たって，組織は次を実施しなければならない。 1) 事業継続に関係するものを含め，組織の目的を明確に述べる。 2) リスクを生じさせる不確かさを生む内部及び外部の要因を定義する。 3) リスク選好を考慮に入れて，リスク基準を設定する。 4) BCMS の目的を定義する。
解釈	【この箇条の狙い】 ・この箇条のアウトプットは「BCMS の目的」を明らかにすることであり、その手段として「組織及びその状況の理解」が求められている。 ・「4 組織の状況」全体を通じて、「我々はなぜ BCMS に取り組みたいのか」、「我々の BCMS には最低限何が要求されるのか」、「我々は何を BCMS の対象として守っていくのか」を明らかにする。 【この箇条のポイント】 ・組織及びその状況の理解のためには、サービスや製品などの内部の状況、サプライチェーンや利害関係者などの外部の状況の両方の理解が必要である。 ・組織の現状を見ることはすなわち、組織の目的、考え方、を明確にすることであり、これを最初にすべきこととしている。
適用方法例等	・IS022301 においては、各箇条において満点を目指すのではなく、まずは開始し、PDCA を回し、マネジメントシステムとして運用していく中で、レベルアップを図っていくという考え方を採用している。 ・BCMS の目的は根幹をなす重要なものであるが、作業としての「組織及びその状況の理解」においては、既存の情報(中期経営計画、CSR 報告書、各種委員会など)を利用することが効率的である。組織の内外の情報を詳細に集め現状分析するのではなく、「組織が内外の情報をどのように収集し、認識しているか」を理解することの方が、より重要であるためである。 ・BCMS の目的が明確になったらドラフトでも良いので、経営層に確認すべきである。BCMS にどこまで経営資源を注ぐのか、どこまでは割り切ってやらないのかは経営者の判断事項であるからである。
意見	特になし。
備考	・COSO では外部環境及び内部環境の認識をアピタイトと表現している。

項目	4 組織の状況 4.2 利害関係者のニーズ及び期待の理解
内容	4.2.1 一般 BCMS を確立するに当たって，組織は次の事項を決定しなければならない。 － BCMS に関連する利害関係者 － その利害関係者の要求事項（例えば，明示されているか，暗に示されているか，義務か否かに関わらない利害関係者のニーズ及び期待）
	4.2.2 法令及び規制の要求事項 組織は，その業務，製品及びサービスの継続並びに関係する利害関係者の関心のために，適用される法令及び規制の要求事項を特定し，入手し，評価するための手順を確立し，実施し，維持しなければならない。 組織は，これらの適用される法令及び規制の要求事項，並びに組織が同意するその他の要求事項を，BCMS の確立，実施及び維持において考慮することを確実にしなければならない。 組織は，この情報を文書化し，常に最新のものにしておかなければならない。法令，規制及びその他の要求事項の新規追加又は変更は，その影響を受ける従業員及びその他の利害関係者に周知しなければならない。
解釈	【この箇条の狙い】 ・自社と利害関係者の関係および利害関係者と社会の関係を通じて、自社の社会的責任を認識することが BCMS の目標設定にとって有用である。 【この箇条のポイント】 ・顧客はよくサプライヤーチェックリストで「BCM を構築・運用しているか」と聞いてくるが、顧客の一番の関心は「不測事態発生時に我々に優先的に製品やサービスを提供する意思と能力があるか」である。但し、すべての顧客に優先的に製品やサービスを提供することは本質的に不可能である。 ・一般的な態勢として BCM を構築しているか（人並みにできているか）ということと、一定の考え方の下で特定の顧客を優先すること(いざというときに何をすべきかが分かつていること)は別の問題である。
適用方法例等	・「BCMS の目的を定義すること」と「利害関係者のニーズを明確にすること」は表裏一体であり、「4.1 組織及びその状況の理解」と「4.2 利害関係者のニーズ及び期待の理解」は一体として取り組まれることが実務上は多い。 ・顧客の関心は「当該企業の対応において自社の順位はどう位置付けられているか」であり、これを合理的に説明できることが必要となる。 ・認証を取る場合と、自組織にとって必要なことを見極め実施する場合とでは、見方が変わってくるしコストも違う。 ・規格遵守の要請は、BCMS と ISMS とは違う。ISMS は、日常的に行われる活動であり準拠していることが重要であるが、BCMS は、非日常時の活動で取引先との関係が重要となる。
意見	特になし。
備考	・入札資格でない場合や、能力のある組織は、自分のやり方でやることもある。お墨付きがなくても自分のやり方でできる企業が増えたこともあるし、ISO のシェアが低下した可能性もある。

項目	4 組織の状況 4.3 BCMS の適用範囲の決定
内容	4.3.1 一般 組織は，BCMS の適用範囲を定めるために，その境界及び適用可能性を決定しなければならない。 この適用範囲を決定するとき，組織は，次の事項を考慮しなければならない。 － 4.1 に規定する外部及び内部の課題 － 4.2 に規定する要求事項 BCMS の適用範囲は，文書化した情報として利用可能な状態にしておかなければならない。 4.3.2 BCMS の適用範囲の決定方法 組織は，BCMS の適用範囲を決定するために，次に示す事項を実施しなければならない。 a)BCMS に含まれる組織の部署を明確にする。 b)組織の使命及び目標，組織内外の義務（利害関係者に関係するものを含む。），並びに法令及び規制上の責任を考慮し，BCMS の要求事項を決定する。 c) BCMS の適用範囲に入る製品及びサービス，並びにそれらに関連する全ての事業活動を特定する。 d)顧客，投資家，株主，サプライチェーン，公共及び／又は地域社会の意見，ニーズ，期待，利益（必要に応じて）など，利害関係者のニーズ及び利益を考慮に入れる。 e)組織の規模，性質及び複雑度の観点から，それらに適した BCMS の適用範囲を定める。 適用範囲を定めるに当たって，組織は，除外事項を文書化し，説明しなければならない。いかなる除外事項も，事業影響度分析，又はリスクアセスメント並びに適用される法令及び規制の要求事項によって決定された，BCMS の要求事項を満たす事業及び業務を継続できる組織の能力及び責任に影響を与えてはならない。
解釈	【この箇条の狙い】 ・事業継続の対象となる製品・サービスに関わる人・組織を決定する中で、BCMS の適用範囲を明確にする。 【この箇条のポイント】 ・「BCMS の適用範囲」で決定された範囲全てについて事業継続ができなければならないということではない。あくまで BCMS の対象領域を決めるものであり、実際にどこまで BCM に取り組むかはリスクアセスメント、事業影響度分析を通じて判断される。 ・社会環境やニーズの変化、法令・規制の改変に応じて適用範囲は定期的に見直す必要がある。
適用方法例等	・本規格を、どの組織部門、どの業務で実施するか等の問題であり、さらになぜ取り組むかのその答えを準備しておき、関係部門に周知する必要がある。
意見	・必ずしも全部門で取組む必要はなく特定部門だけでも認証は取得できるが、本社部門（経営判断が可能な人または組織）を認証の対象範囲に入れることが望まれる。 ・適用範囲の決定に当たっては、取組む前提条件と意味づけを明確にする。「枠」を決めると考えれば分かりやすい。
備考	特になし。

項目	4 組織の状況 4.4 BCMS
内容	組織は，この規格の要求事項に従って，必要なプロセス及びそれらの相互作用を含む BCMS を確立し，実施し，維持し，かつ，継続的に改善しなければならない。
解釈	【この箇条の狙い】 ・「IS022301 に準拠した BCMS を実施している」と宣言または認証を受けるのであれば、この規格の要求事項に沿う必要がある。 【この箇条のポイント】 ・逆に、独自の考えに基づき BCMS が十分であると考えるのであれば、規格の要求事項に従う必要はない。この意味においてIS022301を参照するにあたり、規格に準拠するのか、規絡を参考とするのかの立場を明確にする必要がある。
適用方法例等	特になし。
意見	特になし。
備考	特になし。

項目	5 リーダーシップ 5.1 リーダーシップ及びコミットメント
内容	トップマネジメントにある者，及びその他の関連する管理層の役割を担う者は，BCMS に関してリーダーシップを実証しなければならない。 例 このリーダーシップ及びコミットメントは，人員が BCMS の有効性に寄与できるよう動機付けし，権限を与えることによって示すことができる。
解釈	【この箇条の狙い】 ・トップマネジメントおよび BCM に従事する管理層の果たす役割を明確に示すことに狙いがある。 【この箇条のポイント】 ・BCM において、組織のトップマネジメントあるいはサブ組織のトップにあたるものがリーダーシップを発揮しなければならないことを強調している。 ・そのリーダーシップは実質的な内容を伴うものでなければならず、リーダーシップを発揮していることが誰にでも分かるようになっていなければならないという趣旨が、実証という言葉の中に秘められている。 ・また、“コミットメント”という表現によって、トップマネジメント及び管理職層が責任を持つことの必要性を述べている。 ・リーダーシップの具体的な発揮は、自らが作業をするというよりも、組織全体を BCM のために適切に動かしていく（マネジメントしていく）ことによって行われるべきものである。それが「動機付けし，権限を与えることによって示す」として表現されている。ただし、トップマネジメントに対して、次の箇条以降で、積極的にそれに参画することを求めており、責任者を決めて権限を与えれば済むという立場は取っていない。
適用方法例等	特になし。
意見	・この ISO による規格で想定しているマネジメントスタイルは、欧米、特に米英豪型のものである。その観点に立つと、至極当然の内容であるが、わが国の企業に持ち込む場合、これを実質化することはそう容易なことではない。 ・日本の経営者は、ボトムアップ型の組織の頂点にいて部下の補佐によって職務を遂行するケースが多い。日本の経営者が本規格で想定しているマネジメントスタイルを実行するためには、日本の組織を前提とした補完的なサポート策を加味したやり方を考えるべきである。 例えば、1950 年代、QC 導入に際し当時の関係者は我が国の製造現場におけるワーカーの自主性を活かした QC サークル等、日本の状況を活かした制度を独自に開発して成果を挙げた。 ・リーダーシップの実証という表現は、日本的経営においては抵抗感がある可能性がある。BCM についてのリーダーシップを実際に実証するためには、BCM の基本的な考え方を理解している必要があり、かつ、現場の苦労や抱える問題点について十分推理できることが必要である。しかし、日本の経営者はそこまでやっていないことが多いようだ。 ・一方、日本経済及びその担い手である企業のグローバル化が不可避であり、日本的経営の良いところは残しつつも、必要な部分については欧米流の経営に近づいていく必要がある。その意味で、トップマネジメントを中心とした経営層は、本規格で想定しているマネジメントスタイルを実行できる識見と能力を身につけるべきである。
備考	特になし。

項目	5 リーダーシップ 5.2 経営者のコミットメント
内容	トップマネジメントは，次に示す事項によって，BCMS に関するリーダーシップ及びコミットメントを実証しなければならない。 － BCMS の方針及び目的を確立し，それらが組織の戦略的な方向性と両立することを確実にする。 － 組織の事業プロセスへの BCMS の要求事項の統合を確実にする。 － BCMS に必要な資源が利用可能であることを確実にする。 － 有効な事業継続マネジメント及びBCMS の要求事項への適合の重要性を伝達する。 － BCMS がその意図した成果を達成することを確実にする。 － BCMS の有効性に寄与するよう指示を与え，支援する。 － 継続的改善を促進する。 － その他の関連する管理層がその責任の領域においてリーダーシップ及びコミットメントを実証するよう，管理層の役割を支援する。 注記 1 この規格で“事業”という場合，それは，組織の存在の目的の中核となる活動という広義の意味で解釈することが望ましい。 トップマネジメントは，BCMS の確立，導入，運用，監視，レビュー，維持及び改善へのコミットメントの証拠を次の事項によって示さなければならない。 － 事業継続方針を策定する。 － BCMS の目的及び計画が策定されることを確実にする。 － 事業継続マネジメントのための役割，責任及び力量を決定する。 － BCMS の実施及び維持に責任を負うために適切な権限及び力量を備える 1 名以上の者を，BCMS の責任者に任命する。 注記 2 BCMS の責任者は，組織内で他の職務と兼務することができる。 トップマネジメントは，関連する役割に対して，責任及び権限を割り当て，組織内に伝達することを次に示す事項によって確実にしなければならない。 － リスク許容基準及びリスクの許容可能レベルを定める。 － 演習及び試験の実施に積極的に関与する。 － BCMS の内部監査の実施を確実にする。 － BCMS のマネジメントレビューを実施する。 － 継続的改善へのコミットメントを明確に示す。
解釈	【この箇条の狙い】 ・BCMS に関するリーダーシップ及びコミットメントを実証するためにやるべき内容を示している。 ・トップマネジメントがリーダーシップを発揮するとともに BCMS に関し参画する具体的な中身及びその方法を明確にすることに狙いがある。 【この箇条のポイント】 ・BCMS の方針及び目的を明確にし、それを組織内の拘束的条件とすること及びそれが組織の戦略的な、進んできた方向に合致するものであることを明確に示し、それに則って業務が行われるようにすることはトップマネジメントの責務であるとしている。 ・BCMS が要求する内容が確実に事業実施の一部として行われるようにすることはトップマネジメントの責務であると明確にしている。 ・人材、資金等の組織の資源が BCMS において必要とする量だけ確保できるようにする

	ことはトップマネジメントの責務であるとしている。 ・組織内において、十分役に立つ事業継続マネジメント及び BCMS であるためには、それらの求める条件に適合することが必要であることを関係者に伝達し認識させることがトップマネジメントの役割の一つと指摘している。 ・BCMS によって果たそうとした目的が間違いなく達成されるようにすることはトップマネジメントの責務であるとしている。 ・BCMS の活動が効果的なものとなるように指示、支援することはトップマネジメントの責務であることを明確にしている。 ・BCMS の改善が継続的に行われるようにする役割をトップマネジメントが担っていることを明確にしている。 ・管理層がその各々の所掌に応じて BCM をしっかりと行うように支援することがマネジメントの責務であることを明らかにしている。 ・トップマネジメントは、BCMS の確立、導入、運用、監視、レビュー、維持及び改善を行う必要があり、その具体的なやり方としては、以下のことを行うことによって、自らの責任において事業継続マネジメントを行っていることを証拠立てる必要がある。 － 事業継続方針を策定する。 － BCMS の目的及び計画がその責任のある者によって作成されること確実にする。 － 事業継続マネジメント実施における組織内の者の役割、責任を決めるとともにその力量を評価し明確化しておく。 － それを実行するに相応しい能力を持った BCMS 責任者を少なくとも 1 名任命する。 ・トップマネジメントは BCMS に関連する業務に従事する者および部局に、責任及び権限を割り当て、その旨を組織内に伝達するが、それは、具体的には、以下のような内容のことを行うことによって、それが実効性のあるものとする必要がある。 － リスク許容基準及びリスクの許容可能レベルの決定 － 演習及び試験の実施への積極的関与 － BCMS の内部監査の確実な実施 － BCMS のマネジメントレビューの実施 － 継続的改善へのトップマネジメントの明確な参画
適用方法例等	特になし。
意見	・ここで示されていることをトップマネジメントが実施するという考え方は欧米流の経営におけるアプローチの方法であり、欧米のプロ経営者としての方法論である。日本の多くの経営者はこのようなシステムアプローチをするように教育を受けていない。むしろ、このようなアプローチをするタイプの者は、それぞれの部門の中から選抜して役員になる日本流のシステムの下においては、途中で排除されることが少なくないように思われる。 ・創業者型の経営者、欧米の子会社のトップを経験し、欧米型の経営に同感している経営者を除き、現状、日本の経営者の多くは、ここで要求されていることが実行出来ない可能性が高い。経過的措置としては、部下がサポートをして実行可能となるような対応策を講ずるのが妥当である。 ・しかし、リスクマネジメントを行って危機による被害を少なくすることは経営の重要な一部であり、トップマネジメントが自らの発意によって、BCMS の最適運用が行われるよう、人材力の涵養、組織運営のあり方の改善などが行われることが求められている。そのために、日本経済団体連合会等の経営者団体の積極的取組が好ましい。
備考	特になし。

項目	5 リーダーシップ 5.3 方針
内容	トップマネジメントは，次の事項を満たす事業継続方針を確立しなければならない。 － 組織の目的に対して適切である。 － 事業継続目的の設定のための枠組みを示す。 － 適用される要求事項を満たすことへのコミットメントを含む。 － BCMS の継続的改善へのコミットメントを含む。 BCMS 方針は，次に示す事項を満たさなければならない。 － 文書化した情報として利用可能である。 － 組織内に伝達される。 － 必要に応じて，利害関係者が入手可能である。 － 定期的に及び大きな変更があった場合に，継続的に適切であるかをレビューする。 組織は，事業継続方針に関して文書化した情報を保持しなければならない。
解釈	【この箇条の狙い】 ・組織のトップである経営者に事業継続方針及び BCMS 方針の作成を要求するとともに、その内容について必要要件を示し、それらを文書化したものとして保持することを求めている。 【この箇条のポイント】 ・事業継続方針の作成はトップマネジメントの責務であることをはっきりさせている。 ・事業継続方針については次のような条件を満たすものでなければならない。 － 組織の目的に対して適切なこと － 事業継続目的の設定のための枠組みを示すものでなければならないこと － 適用される要求事項を満たすことを確保することを経営者として宣言をすること － BCMS の継続的改善が確保されることについて経営者としての宣言をすること ・事業継続方針に関しては、文書化した情報として、維持管理される必要がある。 ・BCMS 方針では以下のような条件が満たされていなければならない。 － 文書となっていて、文書として利用可能である － 組織内で各方面にしっかりと伝えられている － 利害関係者も必要があれば入手することができる － 継続的に適切性についてレビューされる必要がある。その継続性は、定期的および大きな変更があった場合にレビューを行うことによって確保される ・事業継続方針に関して文書化した情報を保持しなければならない。
意見	・事業継続方針及びBCMS方針を文章化して示すことになる。その内容は、曖昧なものでは困るし、逆に、必要以上に拘束的で、弾力性のないものでも困る。また、内部矛盾の存在は絶対に避けなければならない。一方、この作成のために長時間を要し、その作成に多くのスタッフが関わるようでは、マネジメントとはいえない。 ・文書化した情報の保持は、我が国企業は得意ではない点には要注意。 ・関係者に対して、いかに情報を伝達し、又、意見を汲み上げることが出来るかという問題を伴っている。そして、その伝達する内容は、トップマネジメントの覚悟と責任意識を伝えるものである。また、その内容は、社内だけではなく、利害関係者にも伝えられる可能性があるものであり、利害関係者も納得できるものでなければならない。これは日本の企業経営者がこれまで必ずしも「得意」として来た事ではない。 ・日本的経営における補完措置を考えるべきである。

項目	5 リーダーシップ 5.4 組織の役割，責任及び権限
内容	トップマネジメントは，関連する役割に対して，責任及び権限を割り当て，組織内に伝達することを確実にしなければならない。 トップマネジメントは，次の事項に対して，責任及び権限を割り当てなければならない。 a) BCMS が，この規格の要求事項に適合することを確実にする。 b) BCMS のパフォーマンスをトップマネジメントに報告する。
解釈	【この箇条の狙い】 ・BCMS に関わる業務を行う者や部門の責任や権限の明確化がトップマネジメントの責任であることを明確化する狙いがある。 【この箇条のポイント】 ・トップマネジメントが BCMS に関し、関連する業務を実施する者および部門に対して、その責任と権限を割り当てるとともにその事実を組織内に広く伝達しなければならないことを明確にしている。 ・その責任と権限の割り当てについては、特に、①BCMS がこの規格の要求事項に適合することを確実にする、②BCMS のパフォーマンスをトップマネジメントに報告する、の 2 点に言及し、これら 2 事項の重要性を強調している。
適用方法例等	・明確な役割分担を整理し、それに伴う必要な権限も明確化するとともに、そのタスクがいつまで有効であるか、その全体の調整は誰が行うのか、その報告はどのように行われるのかなども、明確化しておく必要がある。 ・例えば、我が国と欧米の金融機関の「job description（職務記述書）」を比較すれば、明確な役割分担を整理し、それに伴う必要な権限を明確化することは我が国ではあまり行われていないと考えられる。 ・こうした状態を前提として、BCMS に関わる業務を行う者や部門についてだけでも責任や権限の明確化を図るか、或いはこうした組織において本規格の要求を満たすためにはいかなる補完策を講ずるべきかの検討が必要となる。
意見	・一見すると当たり前のことのような気もするが、「関連する役割に対して，責任及び権限を割り当て，組織内に伝達することを確実にしなければならない」ということは、何とでも取れるような曖昧な責任や権限ではなく、明確に責任や権限を示すということであり、日本ではあまりこれまで行われてきていないように思われる。トップマネジメントが、やるべき内容について十分理解をしており、責任を持っていることを示すものである。 ・繰り返しになるが、日本の経営者が本規格で想定しているマネジメントスタイルを実行するためには、現在の日本的なやり方では対応できないところが出る可能性があり、その補完のための方法論を考える必要がある。
備考	特になし。

項目	6 計画 6.1 リスク及び機会に対処する活動
内容	BCMS の計画を策定するとき，組織は，4.1 に規定する課題及び 4.2 に規定する要求事項を考慮し，次の事項のために対処する必要があるリスク及び機会を決定しなければならない。 － BCMS が，その意図した成果を達成できることを確実にする。 － 望ましくない影響を防止又は低減する。 － 継続的改善を達成する。 組織は，次の事項を計画しなければならない。 a) 上記によって決定したリスク及び機会に対処する活動 b) 次の事項を行う方法 1) その活動の BCMS プロセスへの統合及び実施（8.1 参照） 2) その活動の有効性の評価（9.1 参照）
解釈	【この箇条の狙い】 ・ここでいう「計画」は、対策の立案実施などにおける「Plan」とは意味が異なり、経営層が示すべき「Plan」に限定され、BCM の方針策定に近い実施項目を規定している。 ・組織全体に対する BCMS の対応方向性の絞込み「有効性」に触れている。6.1b では次の事項を「行う方法」という表現で上層のフレーム的な発想を窺わせる。 ※ ISO31000 の構成要素と構造を対比的に示すと以下のようになる。（4.3~4.6 がサイクリックな PDCA である。） 【原則】【枠組み】 【プロセス】 4.2 指令及びコミットメント 5.3 組織の状況の確定 4.3 RM の枠組みの設計 5.4 リスクアセスメント 4.4 RM の実践 5.5 リスク対応 4.5 RM の枠組みのモニタリング及びレビュー 4.6 RM の取り組みの継続的改善 【この箇条のポイント】 ・ISO22301 では「Plan」と「Planning」が区別されている。 ・ISO22301 の解説「4 規定項目」の内容で、Plan 計画及び確立）として、箇条 4～7 の各項目、つまり「組織の状況」、「リーダーシップ」、「計画」、「支援」を規定している。 ・一方で、解説で触れられているように、「計画段階のプロセスとして、事業影響度分析、リスクアセスメント、事業継続戦略、演習の実施へと続く重要なプロセスを一連の取り組みとして、まとめて規定するほうがよい」として、箇条8の「運用（Do）」に移しているので、日本的な PDCA の捉え方とは違和感がある。 なお、「ハイレベルストラクチャーの標準化の方針（MSS）」の構成上は、箇条 8 で「計画」のプロセスを詳細化することになる。 ※ 上記のリスクマネジメントの実践にあたるのが、箇条 8 の「運用」であり、プロセスとして事業影響度分析（BIA）やリスクアセスメント（RA）を規定している。

適用方法例等	・日本的なボトムアップ前提の計画ではなく、トップダウンの指令計画の策定が特徴的である。 ・なお、ISO22301 の規格内容を実際に適用するにあたって、規格が作成された時代的推移および背景を理解することがきわめて肝要であり、上記【ポイント】に述べているように、この規約の構成は認証規格の性格を帯びている点に注目を要する。ISO22301 はハイレベルストラクチャーの考えを最初に適用された規格であり、忠実にその構想に則った構成となっている。認証規格の視点であり、認証もしくは監査の審査員のチェックリストに適している。一方で、事業運営の現場で、この構成・手順の通りに適用・実践していくのは無理がある。実践に当たっては、あくまでも実行可能な手順に則って運用すべきである。
意見	・わかるようで日本的な慣行ではわかりにくい表現がある。（下記参照） ・「リスク及び機会」 機会（opportunity）はポジティブリスクの捉え方であり、ISO22301 としてのリスクの捉え方の一貫性が崩れている。なお、ポジティブの意味は、事業運営にとって、有形無形の利益を生み出す意図・志向を有するということである。 例えば、一般に規格を導入するという場合、管理的な志向に傾きがちであるが、導入することにより事業体の信用度が高まり、事業の社会的価値を付加していくことができるとの点に視点を置けば、立案者や現場の人のモチベーションアップにつながる。 この視点を経営の立場にある人が持っていれば、推進が容易だが、そこまでに至っていない場合、立案者、推進責任者が経営層にプレゼンテーションすることが必要となる。 ・「BCMS プロセスへの統合」 8.1 と対応させてみると、以下のようになる。 a）プロセスに関する基準の設定 b）その基準に従った，プロセスの管理の実施 c）プロセスが計画どおりに実行されるような必要な程度の「情報の文書化」と保持 ※組織での、“計画に対する「変更管理」”は重要点であるが、特に意図しない変更によって生じた結果をレビューし、必要に応じて有害な影響を軽減する処置をとらなければならない。 ※組織は，「外部委託したプロセス」までも視野に入れて確実に管理する。サプライチェーンマネジメントは必要である。
備考	特になし。

項目	6 計画 6.2 事業継続目的及びそれを達成するための計画
内容	トップマネジメントは，事業継続目的が設定され，組織内の関連する部門及び階層において伝達されていることを確実にしなければならない。 事業継続目的は，次の事項を満たさなければならない。 a) 事業継続方針と整合している。 b) 組織が目的を達成するために許容できる製品及びサービスの最低限のレベルを考慮する。 c) (実行可能な場合)測定可能である。 d) 適用される要求事項を考慮に入れる。 e) 監視し，適切に更新する。 f) 伝達する。 （BCM-WG 注） 点線の下線を施してある参考事項は，対応国際規格にはない事項を示す。（序文参照） 組織は，事業継続目的に関する文書化した情報を保持しなければならない。 組織は，事業継続目的をどのように達成するかについて計画するとき，次の事項を決定しなければならない。 － 責任者 － 実施事項 － 必要な資源 － 達成期限 － 結果の評価方法
解釈	【この箇条の狙い】 ・この箇条は、日本的な PDCA の「P」と違和感はない。 【この箇条のポイント】 ・「伝達」つまり、組織内に考え方を徹底し、浸透させる経営者的な特色が出ている。
適用方法例等	特になし。
意見	・「伝達する」という項目があることが ISO22301（事業継続マネジメントシステム）らしい。 ・なお、BCMS の方針を伝達するとともに、経営層としてはその取り組みの心構えを継続的に保持することも、組織に伝達・浸透させなければならない。 ・本文の主語に「トップマネジメント」の表現が用いられており、ハイレベルストラクチャーでの表現である「組織」とは異なっている。経営的時点が重視されていることが窺える。
備考	特になし。

項目	7 支援 7.1 資源
内容	組織は、BCMS の確立、実行、維持及び継続的改善に必要な資源を決定し、提供しなければいけない。
解釈	【この箇条の狙い】 ・BCMSを構築・維持しやすくするために必要な資源を検討し、準備を行う必要があるということを示している。 【この箇条のポイント】 ・BCMS の構築・維持だけでなく、有事の際に必要となる資源についても検討し確保する必要があると述べている。
適用方法例等	・BCM の資源について事前の資源の洗い出しは可能だが、有事の際に必要となる資源については、事業影響度分析（BIA）やリスクアセスメント（RA）を行わないと洗い出しが難しい。
意見	・少し大げさにいうと、ここでの資源の決定・確保は BCMS に必要な資源と限定したほうがよい。
備考	特になし。

項目	7 支援 7.2 力量
内容	組織は，次の事項を行わなければならない。 a) 組織のパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。 b) 適切な教育，教育訓練及び経験に基づいて，それらの人々が力量を備えていることを確実にする。 c) 該当する場合には，必ず，必要な力量を身につける処置をとり，とった処置の有効性を評価する。 d) 力量の証拠として，適切な文書化した情報を保持する。 注記 適用される処置には，例えば，現在雇用している人々に対する教育訓練の提供，指導の実施，配置転換の実施などがあり，また，力量を備えた人々の雇用，そうした人々との契約締結などもある。
解釈	【この箇条の狙い】 ・BCMS の構築及び有事の際に携わる人たちのスキル管理について記載している。 【この箇条のポイント】 ・BCMS を構築するための力量、実際に対応する力量について、教育・訓練を実施し、その実効性の評価と課題解決を定期的に行っていくことが必要と記載している。
適用方法例等	・BCMS の人の力量については、一般的にプロジェクトマネジメント(ファシリテーション・問題解決能力等)ができる力量があれば、業務的知識は不要である。 ・有事の人の力量についてはその業務に精通している必要がある。 ・経験が必要である。 ・会社全体の業務を理解、もしくは、俯瞰的に見られる立場の人が好ましい(例えば IT 部門)。
意見	・必要となる力量の定義は非常に難しい。理由は、被害想定・目標復旧時間等により要求される力量は大きく変化するからである。 従って力量は定期的に見直し、スパイラルアップするべきものと考える。
備考	特になし。

項目	7 支援 7.3 認識
内容	組織の管理下で働く人々は，次の事項に関して認識していなければならない。 a) 事業継続方針 b) BCMS，パフォーマンスの向上によって得られる便益を含む，BCMS の有効性に対する自らの貢献 c) BCMS の要求事項に適合しないことの意味 d) 事業の中断・阻害を引き起こすインシデント発生時の自らの役割
解釈	【この箇条の狙い】 ・この箇条は、BCMS 関係者へ本活動を周知させることを狙いとしている。 【この箇条のポイント】 ・上記で求める内容について深めていき、リスク感性(危機感・想像力)の向上を図っていくことが重要であると記載している。
適用方法例等	・認識を持ち力量を高めていくサイクルが必要である。具体的には危機感を感じさせる訓練を行ない、その上で必要な対策を考え、実施していくことが重要である。
意見	・認識について周知されていないと、活動目的・目標が定まらないため関係者のモチベーションが上がらず、活動が形骸化してしまう恐れがある。 ・BCMS 導入時、導入後も認識の維持・向上は必要な対応である。
備考	・「c) BCMS の要求事項に適合しないことの意味」の解釈は、2 通り考えられる。 「説明責任を果たす」と「会社の事業継続が出来なくなる状況を理解する」のどちらの場合も考えられる。

項目	7 支援 7.4 コミュニケーション
内容	組織は，次の事項を含め，BCMS に関連する内部及び外部のコミュニケーションを実施する必要性を決定しなければならない。 a) コミュニケーションの内容（何を伝達するか。） b) コミュニケーションの実施時期 c) コミュニケーションの対象者 組織は，次のための手順を確立し，実施し，維持しなければならない。 － 組織内の利害関係者及び従業員の間の内部コミュニケーション － 顧客，取引先，地域社会，及びメディアを含むその他の利害関係者との外部コミュニケーション － 利害関係者からのコミュニケーションの受け入れ，文書化及び対応 － 全国又は地域の災害警報システム又は同等システムの計画及び運用への採用及び組入れ（それが適切な場合） － 事業の中断・阻害を引き起こすインシデント発生時におけるコミュニケーション手段の確保 － 必要に応じて，関係当局との体系的なコミュニケーションの促進，及び複数の緊急対応機関と要員との相互運用性の確保 － 平時のコミュニケーションが中断・阻害されたときに使用するコミュニケーション機能の運用及び試験の実施 注記 インシデントに対応するコミュニケーションについては，これら以外の要求事項を8.4.3 に規定している。
解釈	【この箇条の狙い】 ・災害時、誰が・いつ・どういう手段で・何を伝えるかを決めておかなければならないことを示している。また平時の資源が毀損しても対応できるよう、利害関係者からそれぞれの手段を明確にし、実行できるよう訓練が必要であることを示している。 ・事前対策として災害を早期に知る手段についても整備する必要があると記載している。 【この箇条のポイント】 ・社内外・利害関係者とのコミュニケーションについて整理し、事業中断が起きてもコミュニケーションが出来るよう、対策を構築しそれを維持していくことが必要である。 ・特に災害警報の早期入手についても本コミュニケーションの一部としている。
適用方法例等	・被害想定を定めその際必要なハード・マニュアルを整備していく。被害想定を定める理由は、被害想定のレベルにより対策（コミュニケーション手段）にかかるコスト・準備が大きく異なるため。 ・またブラインド訓練を取り入れ、実行性の検証が必要である。
意見	・コミュニケーションの構築については、誰が・何の目的で使用するかを明確にする必要がある。また代替手段を多く準備し過ぎると実効性に欠けるリスクがあるため、出来れば平時から利用しているものを活用すると効果的である。
備考	特になし。

項目	7 支援 7.5 文書化した情報 7.5.1 一般
内容	組織の BCMS は，次の事項を含まなければならない。 － この規格が要求する文書化した情報 － BCMS の有効性のために必要であると組織が決定した，文書化した情報 注記 BCMS のための文書化した情報の程度は，次のような理由によって，それぞれの組織で異なる場合がある。 － 組織の規模，並びに活動，プロセス，製品及びサービスの種類 － プロセス及びその相互作用の困難さ － 人々の力
解釈	【この箇条の狙い】 ・BCMS の活動において、文書を作成し共有することは、関係者間の対応力の標準化に利用できるとともに、担当者が変更となった場合や、担当者が手順等を忘れた場合にも有効であることを記載している。 【この箇条のポイント】 ・企業の実情にあった文書を作成しても良い。
適用方法例等	・BCMS 活動で作成される、マニュアル・規程・体制図等のすべての情報を指している。
意見	特になし。
備考	特になし。

項目	7 支援 7.5 文書化した情報 7.5.2 作成及び更新
内容	文書化した情報を作成及び更新する際，組織は，次の事項を確実にしなければならない。 a) 適切な識別及び記述（例えば，タイトル，日付，作成者，参照番号） b) 適切な形式（例えば，言語，ソフトウェアの版，図表）及び媒体（例えば，紙，電子媒体），並びに適切性及び妥当性に関するレビュー及び承認
解釈	【この箇条の狙い】 ・BCM活動で作成された最新の文書を組織内で管理していく上での注意点について記載している。 【この箇条のポイント】 ・バージョン管理と、関係者で最新文書を共有するために必要な事項について記載している。
適用方法例等	特になし。
意見	・文書化する際、メンテナンスが必要となるような個別名称などは極力避けるべきである。例えば体制図の場合、個人名を記載するのでなく、「○○組織の責任者」と記載すれば、人事異動があってもメンテナンスが不要となる。
備考	特になし。

項目	7 支援 7.5 文書化した情報 7.5.3 文書化した情報の管理
内容	BCMS 及びこの規格で要求されている文書化した情報は，次の事項を確実にするために，管理しなければならない。 a) 文書化した情報が，必要なときに，必要なところで，入手可能かつ利用に適した状態である。 b) 文書化した情報が十分に保護されている（例えば，機密性の喪失，不適切な使用及び完全性の喪失からの保護）。 文書化した情報の管理に当たって，該当する場合には必ず，組織は，次の行動に取り組まなければならない。 － 配付，アクセス，検索及び利用 － 読みやすさが保たれることを含む，保管及び保存 － 変更の管理（例えば，版の管理） － 保持及び廃棄 － （削除） － 判読性（例えば，はっきりと読めること）の保護 － 廃止情報の誤使用の防止 注記 対応国際規格には“検索及び利用”が箇条に記載されているが重複するために削除した。 BCMS の計画及び運用のために組織が必要と決定した外部からの文書化した情報は，必要に応じて，特定し，管理しなければならない。 文書化した情報の管理を確立するに当たって，組織は，文書化した情報の適切な保護を確実にしなければならない（例 セキュリティ侵害，無断の変更又は削除の防護）。 注記 アクセスとは，文書化した情報の閲覧だけの許可に関する決定，文書化した情報の閲覧及び変更の許可及び権限に関する決定，などを意味する。
解釈	【この箇条の狙い】 ・文書が必要な人に、必要な時に必要な文書が確実に提供できるようなプロセスについて記載している。 【この箇条のポイント】 ・情報の機密性・完全性・可用性について記載されているが、それに加え判読性についても明記されている。これは、緊急時の状況を想定して記述せよとの意図といえる。
適用方法例等	・非常時の状況も十分に考慮し、停電でもアクセスが出来るような配慮も重要である。また廃止情報の誤使用の防止も人命にかかわることもあるので配慮すべきである。
意見	・緊急時に使用する文書と平時の運用管理で使用する文書を意識して作成していくことが必要である。特に緊急時用の文書は混乱している中での使用となることに十分配慮することが必要である。
備考	特になし。

項目	8 運用 8.1 運用の計画及び管理
内容	組織は，次に示す事項の実施によって，要求事項を満たすため，及び 6.1 で決定した活動を実施するために必要なプロセスを計画し，実施し，管理しなければならない。 a) プロセスに関する基準の設定 b) その基準に従った，プロセスの管理の実施 c) プロセスが計画どおりに実行されたという確信をもつために必要な程度の，文書化した情報の保持 組織は，計画した変更を管理し，意図しない変更によって生じた結果をレビューし，必要に応じて，有害な影響を軽減する処置をとらなければならない。 組織は，外部委託したプロセスが管理されていることを確実にしなければならない。
解釈	【この箇条の狙い】 ・箇条 6 で経営層が認識すべき枠組みを示し、箇条 8 で具体的にどうするのかを記載している。 【この箇条のポイント】 ・実務においては、計画段階では、BCP の仕組みの整備を行い、運用段階では、BCP の策定やその実施等が行われると考えるが、ISO22301 では、これらの整備事項と策定事項が全て箇条 8 に記載されている。 ・認証のしやすさを高めるために、ハイレベルストラクチャー（HLS）がつくられた、という背景がある。つまり毎年確認すべき部分をまとめてほしい、という要請があり、箇条 8 にまとめることが指向された。BCM を作る際には分かりにくいが、一度できたものを点検する際には、まとまっていた方がよい。 ・外部委託したプロセスが管理されていることを確実にする、について、ひとつの製品やサービスの提供にあたって、外部委託先やサプライヤーが機能しない場合に連鎖して自社が機能停止してしまうことを認識する必要がある。そのため外部委託したプロセスやサプライヤーが BCP を持ち機能するか、あるいはそこが機能停止した場合の対処策を持つことが必要である。
適用方法例等	・箇条 8.2～8.5 は、BCMS 固有の事項であるため箇条 8 に入れられているが、これらは計画についての事項と解釈すべきである（箇条 6 に入れてもおかしくない）。計画と運用という視点から整理すると、箇条 8 に入るのは、箇条 8.1 だけとなる。箇条 8.2～8.5 は「運用」だから箇条 8 に置かれた訳ではなく、BCMS 固有の事項であるため箇条 8 に入れられていると考えるべきである。 ・実務的には、毎年行うことは箇条 8 に、毎年行うことの前提となる事項を箇条 6 に置くという理解もできる。 ・会社においては、それぞれの組織ごとに BCP を作成するが、それに該当することを箇条 8 に、その前提として会社全体の上位概念的事項・共通事項を箇条 6 と考えることもできる。BCP は、全社が一斉に整備するのではなく、徐々に整備していくのが現実であるが、その場合には、上位概念と各組織で実施することがそれぞれ別にまとまっていた方が良い。
意見	【箇条 6 と箇条 8 の位置付け】 ・ISO22301 以降に改定された ISO27000 や ISO14000 の改訂版では、マネジメントシステム（MS）の仕組み作り等は箇条 6 に記載される傾向にある。（参考：ISO22301、ISO 27001、ISO 14001 の目次構成の比較）ハイレベルストラクチャー

	（HLS）の解釈において、当初、MS の個別事項は全て箇条 8 に記載する方針だった。この傾向は、ISO の動きであり、日本だけの話ではない。 ・計画でも細かいことになると箇条 8 に示した方が良いかもしれない。 ・箇条 8 において計画的な部分をどこまでとするのかについては議論がある。 【外部委託したプロセスが管理されていることを確実にする】ことの意味 ・「外部委託したプロセスが管理されていることを確実にする」とは、自分の事業に必要不可欠なリソースを特定することを求めているのではないだろうか。委託先を何段階までさかのぼる必要があるのかということは本質ではない。 ・「外部委託先の管理」と書いてあれば、外部委託先の BCP にまで踏み込んで管理するという意味や「複数の委託先を確保しておく」等の委託政策の管理という意味になる。しかし規格には「外部委託したプロセスの管理」と書かれており、工程に対して BCP 的な管理が適用されているかどうか確認する（委託先に BCP の整備を要請し内容を確認する等）と理解すべきだろう。 ・トヨタでは、納品不能になった場合罰金を科す方針を出しているが、それは委託政策の管理に相当する。 ・調達先を「外部委託したプロセス」とは理解しにくい。外部委託とはそもそも自分の所で行うべきことを外に出したものであり、責任を負うべき範疇と整理すべき。8.2.2 では外部委託先とサプライヤーを書き分けている。 ・現実の現場を見ると、倉庫業のピッキングリストのシステムは顧客企業のシステムを用いていたりする。またコンビニの弁当の容器製造会社はコンビニからの需要計画に基づいて生産している。このように自らの意思ではなくして外部に依存している部分も多い。通関業等のシェアードサービスの利用も同じように考えられる。このような外部依存に対して日本企業は責任の所在があいまいであり、責任を追及することが苦手である。
備考	特になし。

項目	8 運用 8.2 事業影響度分析及びリスクアセスメント
内容	8.2.1 一般 組織は，事業影響度分析及びリスクアセスメントのために，次の内容を含む正式に文書化したプロセスを確立し，実施し，維持しなければならない。 a) アセスメントの状況を設定し，基準を定め，事業の中断・阻害を引き起こすインシデントの潜在的な影響を評価する。 b) 法的，及び組織が同意するその他の要求事項を考慮する。 c) 体系的な分析，リスク対応の優先順位付け，及びそれらに係るコストを含める。 d) 事業影響度分析及びリスクアセスメントから必要とされるアウトプットを定義する。 e) a)～d)の情報を常に最新に保ち，機密扱いにするための要求事項を規定する。 注記 事業影響度分析及びリスクアセスメントを実施する順序を決める様々な手法がある。
	8.2.2 事業影響度分析 組織は，事業継続及び復旧の優先順位付け，目的及び達成目標を設定するために，正式に文書化した評価プロセスを確立し，実施し，及び維持しなければならない。このプロセスには，組織の製品・サービスを支える活動が中断・阻害された場合の影響の評価が含まれていなければならない。 事業影響度分析には，次を含めなければならない。 a) 製品及びサービスの提供を支援する事業活動（4.3.2 (c)で規定）を特定する。 b) これらの事業活動を実施しないことによる経時的な影響を評価する。 c) これらの事業活動が再開しないことによる影響が許容できなくなるまでの時間（最大許容停止時間）を考慮し，明示した最低限の許容できるレベルでこれらの事業活動を再開するために優先順位付けされた時間枠（目標復旧時間）を設定する。 d) サプライヤー，外部委託先，及びその他該当する利害関係者を含め，それらの活動の依存関係及びそれらの事業活動を支える資源を特定する。
	8.2.3 リスクアセスメント 組織は，組織に事業の中断・阻害を引き起こすインシデントのリスクを体系的に特定し，分析し，評価するために正式に文書化したリスクアセスメントプロセスを確立し，実施し，維持しなければならない。 注記 このプロセスは，JIS Q 31000 に準拠して実施できる。 組織は，次を実施しなければならない。 a) 組織の優先事業活動，並びにそれらを支えるプロセス，システム，情報，人，資産，外部委託先，及びその他の資源に対する事業の中断・阻害のリスクを特定する。 b) リスクを体系的に分析する。 c) 対応を必要とする，事業の中断・阻害を引き起こすリスクを評価する。 d) 事業継続目的に合致し，組織のリスク選好に応じた対応策を特定する。 注記 組織は，金融又は行政上の特定の義務として，これらのリスクを様々な詳細度で開示する必要があることを認識しなければならない。加えて，特定の社会的なニーズから，この情報を適切な詳細度で開示することが求められることがある。

解釈	【この箇条の狙い】 ・事業継続マネジメントシステムは、何が継続しなければならない事業なのかを決めることから始まる。それを決めるのが事業影響度分析（BIA）であり、なぜそれが起こるのかを分析するのがリスクアセスメント（RA）である。これを踏まえて、事業影響度分析に関して文書化すべき評価プロセスの要件及びリスクアセスメントに関して文書化すべきプロセスの要件を示している。 【この箇条のポイント】 ・BIA と事業継続戦略が ISO22301/BCMS の特徴といえる。リスクアセスメントだけであれば ISO31000 と差がない。ISO22301 は事業中断に焦点をあてた具体的な対応策のための規格である。 ・リスクアセスメントは、「こんなことが原因でこんなことになりそうです。それについてこんな措置が考えられます」、事業継続戦略は、「これとこれを組み合わせて対応することにしましょう」というイメージである。 ・「8.2.1 一般」の a)の「アセスメントの状況」は、Context of Assessment であり、状況ではなく「文脈、中身」と理解する必要がある。 ・「アセスメントの状況」のアセスメントは、The assessment となっており、事業影響度分析（BIA）とリスクアセスメント（RA）の両方を指している。 ・リスクアセスメントは、identify、estimate、analysis を合わせたもの。規格の中での用語の意味と日常での用語の意味は異なることに注意を要する。 ・実務では、BIA において重要業務を特定することが重視されているが、規格の中に重要業務に関する記載は少なく、重要業務が明確にされていない。 ・BIA は、実務的には、顧客から契約を切られないための条件という形で行われることが多い。何かの複雑な計算をするわけではない。 ・企業では、BIA において、企業内の業務が重要業務であるか否かの切り分けを行うが、自治体の場合は、業務自体が公的なものであり、すべての業務が重要であることから、BIA においては重要業務の優先順位付けを行うことが必要になる。
適用方法例等	【一般】 ・「8.2.1 一般」で、「事業影響度分析及びリスクアセスメントから必要とされるアウトプットを定義すること」が要求されているが、アウトプットに至るプロセスや情報は、監査等に提示するための証拠資料、あるいは、事業影響度分析及びリスクアセスメントの条件や分析結果の詳細を示した付属資料として記録に残す必要がある。このため、事業影響度分析及びリスクアセスメントの条件や結果を論理的にかつわかりやすく整理するためのフォーマットを作成することが重要となる。 ・「8.2.1 一般」の a)の「基準」として、事業が継続するための判断基準（クライテリア）を定義する必要がある。 ・8.2.1 の注記「事業影響度分析およびリスクアセスメントを実施する順序」については、いろいろな考え方がある。現在は、経営にとって何が重要事業/重要業務かを決めて、そのためのリスクがどこにあるのかを分析し対策を策定するという流れが一般的であり、規格としても、リスクアセスメントよりも BIA を先に行う。しかし、規格を検討した当時は、先ずハザードを決め、それの経営への影響を分析し必要な対策を取るという流れも取られていた。例えば、日本の内閣府 BCP(地震)、経産省の情報システム BCP（システム停止）、2000 年問題当時の世界中の企業における対応のとり方等が後者の考え方である。経営も後者の方が理解しやすい傾向があるので、コンサルも後者の手法で展開しているところが多かった。これらのことから、どちら

	が先かを明確にすることを避けた背景があり、この表現となっている。 【BIA】 ・BIA に取組む際は、重要事業/重要業務を対象にして取組むことが望ましい。試行的に脇役的業務を対象にしても意味のある BCP は出来ない。 ・BIA のアウトプットは、重要事業/重要業務と目標復旧時間、目標復旧レベル。8.2.2 の c)がアウトプットとなる。 【リスクアセスメント】 ・リスクアセスメントのアウトプットは、8.2.3 の a)～d)である。具体的には、障害要因候補の一覧と対応策候補の一覧表（対応策選択肢一覧）である。ここでいう選択肢は、リスクが現実のものとなった場合の対策だけでなく、事前の予防策や低減策も併せた対策（あるいは措置）の選択肢と考える。 ・ISO31000 は、事前対策までであり、事後対策は含まれていない。しかし、ISO23301 においては、中断を起こすリスクが現実のものとなった場合の対策が対象となる。アウトプットとしてはその候補が示される。 ・事業継続戦略として、事業が止まっても顧客に製品が届くようにしておくことも対応策の一種となる。また、会社を存続させるためにあえて製品供給を制限するという方策も考えられる。
意見	・ISO31000 の検討では、「なぜリスクマネジメントをするのか、何が目的なのかをきちんと把握し、共通の理解を得ること」が context の意味とした。 ・ユーザー側から見ると、環境マネジメントシステムや品質マネジメントシステム、ISO31000 等にリスクアセスメントはあるが、BIA はない。BCMS にしか BIA が入ってこないことの意味を明確にするべきである。 ・大きなリスク分類を特定しないで BIA を行うには、実務的には限界がある。地震なりシステム停止なりを想定せずに BIA を行っても有意義な BIA は出来ない。 ・リスクアセスメントには、地震やシステム停止等の原因事象を特定するレベルのアセスメントと具体的な障害要素を特定するレベルのアセスメントの二つのレベルがある。 ・ISO31000 では 4 つの対応の選択肢（回避、保有（受容）、移転、低減（抑止、軽減）があったが、事後対応についても ISO31000 に含めるという議論をした。ここでの検討事項については、2 つの意見が出た。 ①ここでは、事象が発生しないようにするためにどうするのかの選択肢の検討が求められている。事象が発生した後の対策は、事業継続戦略において検討する。 ②ここでは、事象の発生防止だけでなく、発生時も含めた対策の選択肢を検討する。次の事業継続戦略では、それらの選択肢をどう組み合わせて対応するのかについて検討する。 ・「8.2.1 一般」で、事業影響度分析及びリスクアセスメントに係る情報（入力、出力、それらのプロセス等に関するすべての情報）を最新に保つことが要求されているが、これらの情報を見直し、アップデートするための考え方や頻度について規定することが必要である。 ・本規格では、「リスクアセスメントは、JISQ31000 に準拠して実施できる」と注記されているが、本規格とJISQ 31000 ではリスクアセスメントの定義が異なるので注意を要する（JIS31000 では、リスクアセスメントに「リスク対応」が含まれない）。この注記は、ISO31010 を意識している。
備考	・「8.2.2 事業影響度分析」で製品及びサービスの提供を支援する事業活動は、4.3.2（BCMS の適用範囲の決定方法） (c)で規定している。

項目	8 運用 8.3 事業継続戦略
内容	8.3.1 決定及び選択 戦略の決定及び選択は、事業影響度分析及びリスクアセスメントのアウトプットに基づかなければならない。 組織は、次のために必要な事業継続戦略を決定しなければならない。 a) 優先事業活動を保護する。 b) 優先事業活動及びそれらの依存関係、並びに支援する資源を安定させ、継続し、再開し、復旧する。 c) 影響を軽減し、対応し、対処する。 戦略の決定には、活動再開のための優先順位を定めた時間が承認されていなければならない。 組織は、サプライヤーの事業継続の能力の評価を実施しなければならない。
	8.3.2 資源に関する要求事項の設定 組織は、選択した戦略を実施するための資源に関する要求事項を決定しなければならない。考慮される資源の種類には次のものが含まれるが、これだけに限らない。 a) 人 b) 情報及びデータ c) 建物、作業環境及びユーティリティ d) 施設、設備及び消耗品 e) 情報通信技術(ICT)システム f) 交通機関 g) 資金 h) 取引先及びサプライヤー
	8.3.3 保護及び軽減 対応が必要であると特定されたリスクに対して、組織は次のような事前対策を考慮しなければならない。 a) 事業の中断・疎外の発生の起こりやすさを低減する。 b) 事業の中断・疎外の時間を短縮する。 c) 事業の中断・疎外が組織の重要な製品及びサービスに及ぼす損害の大きさを抑制する。 組織は自らのリスク選考に応じて、適切なリスク対応策を選択し、実施しなければならない。
解釈	【この箇条の狙い】 ・事業継続戦略は、運用の計画と管理を具体化するための実際の手順のフレームワークを特定するプロセスである。この箇条の狙いは、BIA と RA の分析を経て得られた、BCMS の適用範囲に含まれる事業のプロセスと、その脆弱性をカバーする戦略を決定することである。 【この箇条のポイント】 ・戦略とは、事業を継続するためのソリューション（代替サイト、遠隔業務、人員配置の置き換え等）を意味する。ソリュ―ションを特定することで実際の手順のフレームワークが定まる。 ・組織は BIA で特定したそれぞれの活動の時間的なフレームワークを満たし、かつ BIA と RA で特定した業務プロセスとそれを支える経営資源の脆弱性を補う戦略を

	選択することが求められる。
意見	・選択すべき戦略は、組織の状態の変化や、BIA や RA の見直しなどによって、変化する可能性を常に持っているため、定期的に見直しが必要である。さらに、大きな変化があった場合も、タイムリーな見直しが必要である。 ・8.3.1c)は、英文と日本文が異なる。「(前箇条で明らかにした、対応策の選択肢を駆使して)影響を軽減し、インパクトをやりくりする」という意味と捉えるべき。 ・8.3.3a)にあるように事業の中断・阻害の発生の起こり易さを低減する取組みも、事業継続戦略の要素となる。 ・BCM の取組み初期はきちんとやるが、プロジェクト案件から業務部門の取組みに落とし込まれた途端に取組みが希薄になっていく。業務に落とし込まれた後でもきちんとモニタリングする仕組みが必要である。日本企業では、やらないことについてはモニタリングやレビューが行われないことが多い。 ・「8.運用」の中に書いてあるのでマネジメント案件ではないように見えるが、事業継続戦略はマネジメントの関与が不可欠である。 ・事業継続戦略は、代替と復旧などであるが、中堅中小企業では、OEM しか選択肢はないのが一般である。米国でも、状況は同じ。 ・米国は、あまり予防策にお金を掛けない傾向にある。合理的な判断のもとに、法律などで定められた最小の予防策だけを事前対策で行う。その結果事象が発生したら、利益保険と同業他社への OEM で頑張る。予防等にお金を掛けずにリスクをテイクしていくという思想が一般的である。 ・内閣府も中小企業庁もこのような中小企業の状況を理解し始めており、OEM 先との提携を要請している。しかし、OEM 先を作ることは市場を分け与えることであり、依頼する側は簡単には選択できない対策といえる。 ・トヨタなども、協力会社に OEM 先等の提携を促したり、生産工場の複数拠点化を促したりしている。それが難しい場合(海外等)には、適正在庫という考え方で在庫を確保している。
備考	・上記 8.3.2 資源に関する要求事項の設定について、ISO22313(推奨規定)には、組織がなすべきこととして以下が挙げられている。 －インシデントへの準備、対応、復旧のための権限を持った適切なチームまたは数名の個人(小組織の場合)の設定 －BCMS をサポートするためのサービス、要員、資源、物資、施設の設定、人手、保管、配送、維持、テスト、検討を行うためのロジスティックスの能力と手順の設定 －業継続対策をサポートする財務上・ロジスティック上・管理上の手順の策定 －対応の時期、要員、装備、訓練、施設、資金、保険、賠償責任、の対策、専門家の知見、物資、タイムフレームに関する資源管理の目標の設定 －利害関係者の支援、コミュニケーション、戦略的連携、相互援助に関する手順の策定

項目	8 運用 8.4 事業継続手順の確立及び実施 8.4.1 一般
内容	組織は，事業影響度分析で設定された復旧の目標に基づいて事業の中断・阻害を引き起こすインシデントに対処し，事業活動を継続するための事業継続手順を確立し，実施し，維持しなければならない。 組織は，事業活動の継続及び事業の中断・阻害を引き起こすインシデントへの対応を確実にするための手順（必要な取組みを含む。）を文書化しなければならない。 手順は，次のようなものでなければならない。 a) 組織内部及び外部の適切なコミュニケーション手順を確立する。 b) 事業の中断・阻害時の緊急の処置が明示されている。 c) 不測の脅威，及び組織内外の状況変化に柔軟に対応する。 d) 潜在的に事業の中断・阻害を引き起こすおそれのある事象の影響に焦点を当てる。 e) 所定の前提及び相互依存の分析に基づいて策定される。 f) 適切な軽減戦略の実施によって影響を最小限に抑えることに効果的である。
解釈	【この箇条の狙い】 ・事業継続計画のマネジメントを含む全体の文書を作成しその実行および維持することを求めている。 ・計画は文書を作成し見える化を行い、要員が代替わりしても継承されるようにすることを求めている。 ・有事の対応とともに日常時のリスク軽減が求められている。 ・8.4.1b)の緊急の処置とは原文では immediate step で、直ちに取るべき段階を意味する。 【この箇条のポイント】 ・事業継続計画などの計画の策定・実施・維持に必要な一般論が述べられている。組織を構築し計画を策定するには情報の共有が必要であり、そのために適切なコミュニケーション手順が必要である。 ・緊急時の処置とはいわゆる災害対策本部の設営と運営を意味する。 ・事業の影響に焦点を当てるのは BIA のことであり、所定の前提や相互依存とは、リスクの認識や被害想定であり、サプライチェーンなどの分析を意味する。 ・軽減戦略（mitigation strategies）の実施とあるのは、そもそも事業中断を引き起こすリスク、例えば地震や水害、火災などの抑止策などのことであり、その様々なリスクにつき経営資源をどのように投入して対策をとるかを意味する。事前にリスク軽減の対策を実施し BCP（事業継続計画）の発動に至らないようにリスク発現時の被害を小さくすることも BCP においては重要である。
適用方法例等	・適切な BCP であればこの項目は達成されている。個別の要素は他の項目と重なるので省略する。 ・BCP の策定にあたっては、BCP 促進のためのプロジェクトチームを策定するのが一般的である。BCP をよく勉強し理解し経営者を説得できる中核人材の育成をしたところが成功している。 ・BCP を実行・維持するにはプロジェクトチームを解散することは望ましくなく、平時の推進と有事の災害対策本部要員を兼ねた常在する組織または役職・役割としているところが成功している。

	・8.4.1 のみならず全体に関する重要な取組である。
意見	・事業中断に至らないようにすることは、火災や地震が発生しても事業が中断するような事態に陥らないように、被害抑止策が有効に働くようにすることである。 ・事業継続計画とは、ISO22301 では事業継続計画の全体像を記述した書類・文書のことを表す。
備考	特になし。

項目	8 運用 8.4 事業継続手順の確立及び実施 8.4.2 インシデント対応の体制
内容	組織は，インシデントに対処するために必要な責任，権限及び力量をもつ要員を用い，事業の中断・阻害を引き起こすインシデントに対応するための手順及び運営管理体制を確立し，文書化し，実施しなければならない。 対応の体制は，次のようなものでなければならない。 a) 正式な対応を発動させる事態のレベルの基準を決定する。 b) 事業の中断・阻害を引き起こすインシデント及びその潜在的な影響の性質及び程度を評価する。 c) 適切な事業継続対応策を発動する。 d) 対応の発動，運用，調整及びコミュニケーションのためのプロセス及び手順を備える。 e) 影響を最小限に抑えるために，事業の中断・阻害を引き起こすインシデントに対処するプロセス及び手順を支える利用可能な資源を確保する。 f) 利害関係者及び関係当局，並びにメディアとのコミュニケーションを行う。 組織は，人命を最優先とし，また関係する利害関係者と協議し，重大なリスク及び影響について外部に伝えるか否かを決定し，その決定を文書化しなければならない。伝える決定を下した場合には，組織は，必要に応じて，メディアを含め外部へのコミュニケーション，警報及び警告のための手順を確立し，実施しなければならない。
解釈	【この箇条の狙い】 ・いわゆる災害対策マニュアル、危機管理マニュアルを策定することを求めている。 ・権限が切り替わることが多いことから発動基準、非常事態宣言の発動などを規定することを求めている。 ・災害対策に必要な体制、物資の準備、マスコミ対策などを整備することを求めている。 ・インシデントとは ISO22300 社会セキュリティー用語－の 2.1.15 で「中断・阻害、損失、緊急事態または危機になり得る又はそれらを引き起こし得る状況」と定義されている。一方危機（crisis）は同じく 2.1.12 で「組織の中核となる活動、及び/又は組織の信頼性を中断・阻害させ、緊急の処置を必要とする、高レベルの不確かさを伴う状況」と定義されている。 【この箇条のポイント】 ・多くの企業では地震対策マニュアルとして、インシデント対応を行っている。ただし BCP においてはハザード毎に準備するのではなく、何らかの現象で製品やサービスの供給が提供できなくなったときに共通の対策を準備することが望ましい。ただし地震対策マニュアルで火災や水害などに応用できれば、文書名は問わない。
適用方法例等	・地震対策マニュアルとして多くの企業で準備されている。 ・c）の適切な事業継続対応策とは事業継続計画（代替策や早期復旧戦略などの具体的な対応策）のことである。 ・対策本部の立ち上げ基準例として以下の事例がある（本社、工場の立地地域が震度 6 弱の地震、960hpa 以下で台風が上陸した場合、火災、水害などで拠点が被災した場合など）。 ・マスコミ対策は広報部門でマニュアル化されている場合が多い。必要に応じて記者会見訓練を行うことも有効である。

意見	・一般的に利害関係者とは、株主、消費者、取引先、顧客、銀行、債権者、市民、自治体、消防、警察、官公庁、従業員など様々である。 ・f)では利害関係者と当局を分けている。また関係する利害関係者と協議をするということから、さらにここでは対象となる利害関係者は限定される。 ・ここでは外部の利害関係者を取り上げており、具体的に念頭にあるのは一般市民である。 ・情報の開示においては、第何報など都度更新していくことが望ましい。 ・トンネルの開通や橋の開通状況など都度更新していくことが東日本大震災でも求められた。 ・情報を実際に利用する実需がどこにあるのかを見極めることが大切である。 ・インシデントとクライシスは概念が異なる。あらかじめ想定されたリスクが、想定された被害程度の状況かそれ以内の小さな程度で発生した場合をインシデントと呼ぶ。クライシスは、想定外や想定を超えた被害程度における対応を指す。英語では想定内の範囲がインシデントとエマージェンシーであり、想定外がクライシス、ディザスター、カタストロフィーとなる。ISO では想定内の災害対応に対してエマージェンシーを用いている。ちなみにアメリカ連邦政府の危機管理庁と訳される FEMA もエマージェンシーであり、想定内の範囲で有効に有事対応を行うことの意味合いである。日本語の「危機管理」はこれらの2つの概念が明確に分かれておらず、さらにセキュリティの概念が含まれていると想定される。そのため文献を読む場合には用語の意味を確かめて意味をくみ取ることが必要である。 ・インシデントとは想定内の災害規模およびリスクが顕在化したときのことを指す。もともと BCP では想定内の出来事に対して機能することを求めている。想定外のリスクが顕在化した場合や、想定したリスクではあるが規模が大きく手に負えないなどのいわゆる危機管理となる状況で機能することまでは求められていない。 ・想定外という用語が東日本大震災以降用いられているが、言い訳として使われているように思われるため、用語は科学的な想定外と意図的な対応をしないことに決めた想定外などを区別するようにすべきである。 ・用語の使い分けの案としては以下のものがある。 1）対応外： リスク評価をして経営判断として対応しないこととしたもの 2）サボタージュ： 故意に対応しないこととしたもの 3）想定外： 科学的に想定できなかったもの(その時点での判断を含む) ・想定外は unexpected であるが、原子力では人工衛星の落下も考慮しており、東日本大震災の原子力事故は意図的に対応しないことを決めたという想定外である。
備考	・事後対応の ISO22320：Societal security-Emergency management-Requirements for incident response. ・危機管理対応の BS 規格：BS-PAS200：Crisis management. Guidance and good practice ・企業の災害対策・危機管理について解説した図書；リスクマネジメントがよ～くわかる本第2版；東京海上日動リスクコンサルティング著；秀和システム第5章

項目	8 運用 8.4 事業継続手順の確立及び実施 8.4.3 警告及びコミュニケーション
内容	組織は，次のための手順を確立し，実施し，維持しなければならない。 a) インシデントの検知 b) インシデントの定期的な監視 c) 組織内部のコミュニケーション，並びに利害関係者からのコミュニケーションの受け入れ，文書化及び対応 d) 全国若しくは地域の災害情報提供システム，又は同等のシステムからの勧告の受理，文書化及び対応 e) 事業の中断・阻害を引き起こすインシデント発生時の通信手段の確保 f) 緊急事態対応機関との組織化されたコミュニケーションの促進 g) インシデント，実施された処置，及び下された決定に関する重要な情報の記録 次の事項についても考慮し，該当する場合は必ず実施しなければならない。 － 事業の中断・阻害を引き起こすインシデントの発生又はそれが差し迫っているとき，影響を受ける利害関係者への警報 － 複数の緊急事態対応機関と要員との相互運用性の確保 － 通信設備の運用 コミュニケーション及び警告の手順を定期的に演習しなければならない。
解釈	【この箇条の狙い】 ・インシデント発生において多くの人間が情報を共有して同じ目標に向かって力を結集する必要がある。そのために事態の発生を知り共有する情報処理が極めて重要である。 ・情報処理は、重要性の理解、ステークホルダーの把握、通信手段、リテラシー、記録などがすべて整っている必要がある。 ・多くの人が関与するので、そのリテラシーを育成し保つためには演習が継続的に必要である。 ・いつどこで誰に何をどのようにして伝えるかというソフトな能力が必要である。 ・d）災害情報提供システムの原文は risk advisory system である。リスクに関するアドバイスを与えるシステムであり、災害に限定されるものではない。システムは仕組みのことであり、必ずしも IT のことだけではないことに注意する。 ・警告とは warning のことである。 ・g）の警報は alert のこと 【この箇条のポイント】 ・インシデントが発生するあるいは発生するおそれをいかに把握するかを重要視している。日本の多くの企業では地震を対象にすることが多いため、事前の把握「警告」段階は比較的注目度が低い。しかし部品の不良品などでの操業停止などじわりとくるものについては、早期把握が重要であり、悪い情報が早く入手できることが不可欠である。 ・気象災害など、あるいは津波など早期把握が可能な災害においては、情報の入手手段を整備する必要がある。 ・化学物資漏洩事故など自分が加害者になることが想定される場合、また事業中断をした場合にお客様に迷惑をかけるため、必ずお客様をはじめ周辺住民などを含めた

	利害関係者に情報提供できる仕組み必要である。 ・インシデントの検知・監視に一番なじむのは情報システム障害のリスクである。
適用方法例等	・お客様に情報を伝えるためには、ホームページの活用がある。 ・営業社員を含め現場の従業員はお客様への情報提供の重要な役割を担う。 ・近隣の警察・消防の連絡先を把握しておく。避難訓練などを通じて消防と連携する。 ・上場企業等においては業績に影響があると予測される場合、適時開示が求められる。
意見	・c)利害関係者の最たるものは株主であり、上場企業等では適時開示が求められる。自治体や株主が少ない中小企業などでは劣後する。 ・想定するリスクが地震などの自然災害であれば特にコミュニケーションが重要である。 ・周辺住民などに情報提供できる仕組みを持つことが重要であるが、組織内部のコミュニケーションも重要である。内部の人間は特に正確な情報を共有することが必要である。 ・日本では自然災害に偏ってリスクをとらえがちであるが、オールハザードに目を向ける必要がある。 ・鳥インフルエンザの場合は WHO の情報や基準が重要になる ・情報をどこまで開示するかの調整は重要である。情報統制は情報を「隠している」と組織に対するマイナスの風評を生む危険がある。 ・警告と警報の違いは何にあるのか。alert は一方的な通知、warning は幅広い情報提供である。 ・情報の取扱いには、情報を受け入れる局面と発信する局面の2つがある。 ・g)の複数の緊急事態対応機関と要員の相互運用性の確保とあるが、これは欧米の緊急時対応の標準である ICS(Incident Command System)のことを指す。日本では国で自治体などへの導入の検討会が開催されているが、まだ普及していないため現時点では対応が難しい。 ・化学物質の漏洩事故のアラームを事前に構築することを企業などに義務付ける法律は日本にはない。現実には環境マネジメント ISO14001 の認証の中の緊急時対応の中で整備が進められている。 ・災害情報提供システム(risk advisory system)は高度な意思決定を支援するようなシステムだけを指すのではなく、河川水位監視システムやアメダスなども該当する。地震でいえば地震後震度や倒壊家屋を推定し GIS(Geographic Information System) 上に表示するシステムなども提供され始めている。
備考	特になし。

項目	8 運用 8.4 事業継続手順の確立及び実施 8.4.4 事業継続計画
内容	組織は、事業の中断・阻害を引き起こすインシデントへの対応，及びあらかじめ設定した時間枠内で事業活動を継続又は復旧する方法について，文書化した手順を確立しなければならない。 このような手順には，それらを使用する者に関する要求事項を含めなければならない。 事業継続計画には，全体として次の事項が含まれていなければならない。 a) インシデント発生時及びその後について権限をもつ者及びチームの明確に定められた役割及び責任 b) 対応策を発動するプロセス c) 次のことに相当な配慮をし，事業の中断・阻害を引き起こすインシデントの直接的影響に対処するための詳細事項 1) 個々人の福祉 2) その中断・阻害に対応する戦略的，戦術的及び運用面の選択肢 3) 波及する損害又は優先事業活動が実施できなくなることの防止 d) 組織がどのように，またどのような状況で，従業員及びその近親者，主要な利害関係者，並びに緊急連絡先と連絡をとるかについての詳細事項 e) 組織があらかじめ定めた時間枠内で優先事業活動を継続又は復旧する方法 f) 次を含む，インシデント発生後の組織のメディア対応に関する詳細事項 1) コミュニケーション戦略 2) メディアに対する優先連絡窓口 3) メディアに対する声明文を作成するための指針又はひな(雛)形 4) 適切な広報担当者 g) インシデント終了後の解除プロセス 各計画は，次の事項を定義しなければならない。 － 目的及び適用範囲 － 達成目標 － 発動基準及び手順 － 実施手順 － 役割，責任及び権限 － コミュニケーションに関する要求事項及び手順 － 組織内外の相互依存及び相互作用関係 － 資源に関する要求事項 － 情報の流れ及び文書化のプロセス
解釈	【この箇条の狙い】 ・事業継続計画の具体的な要件が示されている。 ・事業継続計画においては、文書化した手順を確立することが目的になる。 【この箇条のポイント】 ・事業継続計画は、事業を中断あるいは阻害するインシデントへの対応及び目標復旧時間内に事業活動の継続又は復旧するための文書化された手順となる。 ・具体的には、7 項目の要求事項と盛り込まれるべき定義要件が 9 項目示されてい

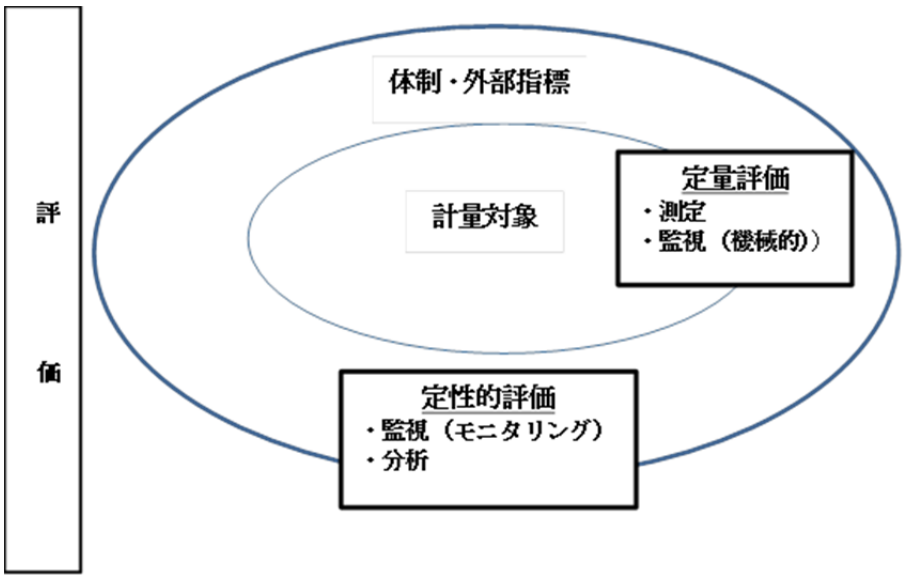
	る。事業継続計画は、これらの事項を全体として含めた内容とすることが求められる。 ・事業継続計画は、インシデント発生後の暫定処理と位置づけられる。 ・緊急時の処置としてのインシデント対応の手順に加えて、事業活動を継続するための戦略、方法、防止対策など事前の備えとしての諸対策を織り込んでいくことが求められる。 ・8.4.4 g)の後の「各計画」は、各インシデントに対する計画、あるいは各対応手順と捉えられる。 ・8.4.4 f)2)の優先連絡窓口は、「preferred」「より望ましい窓口」というくらいの意味である。窓口の一元化までは意図されていない。
適用方法例等	・目標復旧時間内に事業活動の継続又は復旧を図るためのインシデント対応として事業継続計画は策定される。このため、役割を明確にした各チームが、優先事業活動を継続、復旧するために対応していくべき目標、手順、資源、情報伝達の方法等を明確に確立しておく必要がある。 ・具体的な手順は、組織内外の相互連携について時間軸に沿った形で策定しておくことが望ましい。 ・クリティカルな状況における危険を伴う現場対応についても予め手順を策定しておくことが望ましい。 ・メディア対応コミュニケーションに当たっては、社内状況を整理したポジションペーパーに基づき一元的に対応していくことが望まれる。また、利害関係者等に情報を発信していくうえでポジティブな姿勢が求められる。 ・各チームの手順は担当者とその代替者を明確にした上で、資源や情報に関する事項、情報エスカレーションの手順、方法などを明確かつ簡潔に作成されることが望ましい。 ・各チームの手順は演習等を通じて見直し、改善が図られていくことが望まれる。 ・ISO22301 は、企業あるいは組織単位、事業単位を対象とすることが基本となる。地震、火災、テロ等対象とするべき事象については、各々の組織の事情により決まる。特定の事象についての BCP であっても差し支えない。但し、なぜその事象を特定したのか明確にしておく必要がある。 ・基本的には企業における優先事業活動の継続確保が目的であるため、優先事業に関連するサプライチェーンおよびその経営判断の根底である本社が含まれることが自然の流れといえる。
意見	・コミュニケーションについては、メディアに加えて外部利害関係者並びに組織内部に向けたコミュニケーション対応が求められる。（ISO31000、4.3.6、4.3.7 参照）
備考	特になし。

項目	8 運用 8.4 事業継続手順の確立及び実施 8.4.5 復旧
内容	組織は，インシデント発生後，採用された暫定的処置から，平常の事業活動の要求事項を満たすことができるまでに，事業活動を回復し，復帰させるための手順を文書化して備えなければならない。
解釈	【この箇条の狙い】 ・復旧は、インシデント対応並びに暫定処置としての事業継続計画の後を受けて、事業活動を平常状況に回復、復帰させるまでの対応として位置づけられる。 ・復旧対応においても、手順の文書化が求められる。
適用方法例等	特になし。
意見	・事業継続計画は、インシデント発生後の暫定処理として位置づけられているが、本格復旧においても、人、モノ、金の確保はインシデント対応時よりも重要な要素となる可能性があり、事業継続計画策定時において復旧のための計画の策定並びに具体的な対応策の検討、準備を進めておくことが課題となる。 ・暫定処理においても、インシデント発生後目指すべき一次目標としての業務レベルまでの復旧が対象となる。 ・工場火災などでは火災の程度により工場を復旧せずに移転や外部依存等色々な対応が取られる。様々な可能性への検討が必要となる。 ・全ての可能性への対応策を検討しておくことは困難であるため、対応策設定の方式、手順、考え方等を整理しておくことが有効である。 ・インシデントにより事業復旧のスコープは大きく異なることになるが、情報システムダウンを基本に整理すると理解が深まる可能性がある。 ・欧米ではシステムダウンがすなわち BCP 発動に繋がる。その認識の下で規格が作成されていることを理解しておく必要がある。 ・BCP が発動された場合はその結果についての評価をしておくことも重要課題と考えられる。
備考	特になし。

項目	8. 運用 8.5 演習及び試験の実施
内容	組織は、事業継続手順が事業継続目的に合致していることを確実にするために、手順を演習し、試験しなければならない。 組織は、次のような演習及び試験を実施しなければならない。 a) BCMS の適用範囲及び目的と合致している。 b) 明確に定められた狙いと達成目標をもって、周到に計画された適切なシナリオに基づいている。 c) 該当する利害関係者を含めた事業継続の取組みについて、長期にわたる総合的な妥当性を確認する。 d) 事業の中断・阻害のリスクを最小限に抑える。 e) 結果、提言、及び改善を実施するための処置を含めた正式な演習実施報告書を作成する。 f) 継続的な改善を促進する観点からレビューする。 g) あらかじめ定めた間隔、及び組織又は組織が活動する環境に大きな変化があった場合に実施する。
解釈	【この箇条の狙い】 ・組織が、事業継続計画の目的に合致した手順を確立し、その手順を演習・試験して実効性を確認することを求めている。 【この箇条のポイント】 ・事業継続計画の目的に合致した手順の確立が重要である。 ・その実効性を確認する演習・試験を実施が重要である。 ・継続的改善であることが重要である。
適用方法例等	・明確に定められた狙い(目的)と達成目標とは、たとえば指標の設定がある。 ・周到に用意されたBCP関連文書とは、たとえば各部署において、および各部所間で連携してよく練られた「行動計画書」、「インシデントマネジメント計画書」、「演習・訓練手順書」等を作成することがある。 ・利害関係者を含めた事業継続の取組みでは、直接的利害関係者(例. B2B)、および、間接的利害関係者(例. B2B2B)も巻き込んで実施することが考えられる。
意見	・本文中の「演習・試験の実施」は、「演習・試験および訓練の実施」とすべきと考える。理由は、「危機対応技能の組織的な習熟とその維持継続」も必須だからである。 ・演習・試験、訓練は、下記のように目的(再定義案)が異なることを明確にするべきと考える。 ・演習・試験＝組織としての実効性、力量・能力の確認のため。 ・訓練＝危機対応技能の組織的な習熟とその維持継続のため。 ・日本語で「演習」と「訓練」は明確に区別して使われていないが、海外では明確に区別されている。 ・エクササイズ:実行して試してみること。 ・トレーニング:手順の実施能力を高めるもの。 ・ドリル:手順を定着させ、習熟すること。 ・本規格の演習の定義では、その中に臨機応変な対応の練習や訓練も含んでおり、かなり広範な意味を含んでいる。 ・本当に「使えるBCP」にするためには、具体的な復旧手順まで演習・訓練に含めておくことが重要である。(注)東日本大震災でもその重要性が実証された。

	・「長期にわたる総合的な妥当性を確認」を具体的に実施するには、綿密なリスクアセスメントとそれに見合った計画策定が必要である。 ・「あらかじめ定めた間隔、及び組織活動環境に大きな変化があった場合に実施」の方が、規格の解釈として分かりやすく対応もしやすい。これを実施し、定着させるべきである。
備考	・特になし。

項目	9 パフォーマンス評価 9.1 監視，測定，分析及び評価
内容	9.1.1 一般 組織は，次の事項を決定しなければならない。 a）必要とされる監視及び測定の対象 b）該当する場合には必ず，妥当な結果を確実にするための，監視，測定，分析及び評価の方法 c）監視及び測定の実施時期 d）監視及び測定の結果の，分析及び評価の時期 組織は，この結果の証拠として，適切な文書化した情報を保持しなければならない。 組織は，BCMS，パフォーマンス及びBCMS の有効性を評価しなければならない。 さらに，組織は次を実施しなければならない。 － 好ましくない傾向又は結果に対処する必要がある場合，不適合が生じる前に処置をとる。 － 結果の証拠として，文書化した関係情報を保持する。 パフォーマンスを監視する手順は，次の事項を規定しなければならない。 － 組織のニーズに適したパフォーマンス測定基準の設定 － 組織の事業継続方針，目的及び目標の達成程度の監視 － 優先事業活動を保護するプロセス，手順及び機能のパフォーマンス － この規格及び事業継続目的に対する適合の監視 － BCMS のパフォーマンス不足に関する過去の証拠の監視 － その後の是正処置を促進するための，監視及び測定のデータ及び結果の記録 注記 パフォーマンス不足には，不適合，ニアミス，誤報，実際のインシデントなどがある。
	9.1.2 事業継続手順の評価 事業継続手順は，次によって評価する。 a）組織は，事業継続手順及び能力の適切性，妥当性及び有効性の継続を確保するために，それらの評価を実施しなければならない。 b）これらの評価は，定期的なレビュー，演習，試験，インシデント発生後の報告，及びパフォーマンス評価を通して行われなければならない。大きな変更があった場合は，遅滞なく手順に反映しなければならない。 c）組織は，適用される法令及び規制の要求事項の順守，業界のベストプラクティスとの適合，並びに組織の事業継続方針及び目的との適合を定期的に評価しなければならない。 d）組織は，あらかじめ定めた間隔で，また大きな変更があった場合にも，評価を実施しなければならない。 事業の中断・阻害を引き起こすインシデントが発生し，事業継続手順の発動に至った場合，組織は，インシデント発生後のレビューを実施し，結果を記録しなければならない。
解釈	【この箇条の狙い】 ・MSS（Management System Standard）の枠組みでの、実施（D）が計画（P）に適合しているかというPDCAのC（チェック）に該当する部分であることを明示する。 ・チェックは、文書化されたプロセスと基準により、定期的に行われなければならないとし、この機能が組織的に担保された持続可能なものとすべきことを求めている。

	・BCMの手順としてのチェック機能の留意点をプロセスに沿って示している。 ・9.1.1の中段「さらに・・」以下及び9.1.2は、本規定の独自性に鑑み、他の規定にない特有部分である。 【この箇条のポイント】 ・パフォーマンス評価のために行う行動は多数あるが、特に以下の構造に留意すべきである。  ・チェック機能は、大きな経営レベルのマクロの管理フレームと現場でのインプリケーションのミクロの管理フレームの双方を含んでいる。 ・COSO-ERMでのモニタリングとコミュニケーションに対するものであり、具体的説明としては、自主点検と内部監査として、次の箇条以降で展開されている。 ・BCMでの対応として、特に有効な演習とそのフィードバックとビジネス環境等の変化を常に念頭におくことを注意喚起している。 ・パフォーマンスとは、「3. 用語及び定義」では「測定可能な結果」と定義されているが、具体的には、9.1.1に記載された「・・・を監視する手順は次の事項を規定・・・」に記載されている各内容である。また、注記されている「パフォーマンス不足」の事例からも判断することになる。 ・測定は定量的なものだけでなく定性的であっても良いが、日本の場合、定量測定が難しいものが多い。欧米のように情報システムを中心に企図とした規定とは考えていないからである。
適用方法例等	・CSA（Control Self Assessment：統制自己評価）を活用する。 ・会社法上の内部統制システムの言明を行う。
意見	・いわゆる説明責任（見せるための統制システム）と実質的な管理責任（リスクコントロールとしての統制システム）の双方の必要性を満たさなければならない。 ・文書化な基準明示は組織的対応としてのBCMを意識している記述であるが、属人的・黙示的・非言語的ノウハウやコントロールを否定するのではなく、むしろ演習等の実践を通して双方含めて有効性をチェックするものである。 ・事業は生き物であり森羅万象と繋がりがあるため、マネジメントシステムとしては目的と対象の適切な設定と見直しが、後続のプロセス以上に重要である。 ・この前提として、利害関係者とのコミュニケーションを通して、外部内部情報や期待が円滑に相互に伝達され、各層でのPDCAのAにつながることが期待されている。

	・何のためにパフォーマンス評価をするのか、ここだけの記述では分かりにくいので、9.1.2 a) 一般　に改めて説明したほうが分かりやすい。その場合、例えば、9.1.2 a)に記述された内容あるいは9.3に記載された「・・・次の事項を考慮・・」の内容を踏まえた説明が考えられる。 ・9.1.1中段に「BCMSのパフォーマンス及びBCMSの有効性を評価・・」とあるので、タイトルに「有効性評価」を加えたほうが明確になる。 ・9.1.1注記の「パフォーマンス不足」事項には列記事項以外にもあるので、「・・を含む」と記述することが妥当である。 ・9.1.2 c)にある「ベストプラクティス」とは、一般に言われる「最善慣行・最良慣行」ではなく、業界の「自主基準」と考える。 ・パフォーマンス評価は通常状態下で行うものであるので、有事において設計されたとおりのパフォーマンスを発揮できるかを日常時に正しい評価をすることは実際には難しい。 ・注記されている「「パフォーマンス不足」事例はレベルが不揃いであるが、これは本規格がもともとITを対象としてスタートしたことに由来している。BCMS規格の認定取得において、欧米ではIT関連が多い。これは、欧米において現実にシステムダウン障害による被害が多く発生しているからである。相対的に日本ではシステムダウン障害は多くない
備考	特になし。

項目	9 パフォーマンス評価 9.2 内部監査
内容	組織は，BCMS が次の状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施しなければならない。 a）次の事項に適合している。 1）BCMS に関して，組織自体が規定した要求事項 2）この規格の要求事項 b）有効に実施され，維持されている。 組織は，次に示す事項を行わなければならない。 － 頻度，方法，責任及び計画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。監査プログラムは，関連するプロセスの重要性及び前回までの監査の結果を考慮に入れなければならない。 － 各監査について，監査基準及び監査範囲を明確にする。 － 監査プロセスの客観性及び公平性を確保するために，監査員を選定し，監査を実施する。 － 監査の結果を関連する管理層に報告することを確実にする。 － 監査プログラムの実施及び監査結果の証拠として，文書化した情報を保持する。 あらゆるスケジュールを含めた監査プログラムは，組織の活動に関するリスクアセスメントの結果及び前回までの監査結果に基づかなければならない。監査手順には，監査の実行及び結果報告に関する責任及び要求事項だけでなく，範囲，頻度，方法及び力量も含めなければならない。 監査対象の部門に責任をもつ管理層は，検知した不適合及びその原因を除去するために，必要な修正及び是正処置が不当に遅延することなく実施されることを確実にしなければならない。フォローアップ活動には，実施された処置の検証及び検証結果の報告を含めなければならない。
解釈	【この箇条の狙い】 ・組織としてのチェックの重要な機能である内部監査について、再確認として概要を述べている。 【この箇条のポイント】 ・内部監査に求めている事項自体は、IIA（国際内部監査人協会）基準で示されているものの概要とほぼ同じものになっている。 ・求められる監査の深度は、形式チェック・プロセス確認にとどまらない、実質的に有効性を確認し改善余地の認識に及ぶPDCAのAのマネジメントアクションにつながる有用かつ付加価値のある監査である必要がある。 ・このため、人的資源を含めた適切な組織対応と深度ある監査をするための的を外さない「リスクアプローチ」が求められる。
適用方法例等	・内部監査の専門職的実施の国際基準が参考となる。
意見	・内部監査はどのような管理システムでも今や一般的に求められているが、その深度は必ずしも深くなく、プロセスの実在性・準拠性を証跡をもとに確認するような、評価を伴わないものも多い。これは管理システムがマネジメントシステムのフレームワークの設定に偏重し、実質的な有効性まで目が向かない実態との裏表である。 ・しかし、BCMのような範囲の広い課題では、形式的な準拠性はその定義によってい

	かようにもできるため、あまり意味はない。 ・フレームワーク設定の有効性はもちろん目的とスコープに及ぶ監査人の評価、少なくとも限定されたスコープであればその旨の意見表明が必要である。 ・内部監査の目的は「・・・BCMSが次の状況にあるか否かに関する情報を提供・・・」とあるが、提供の客体の記述があると分かりやすい。 ・組織の行うべき事項に「・・頻度、方法、責任及び・・」とあるが、この「責任」には、responsibility（何をするかの責任）のほか、accountability（結果に対する責任）も含むと考えられる。 ・下段の「あらゆる・・」以下は、BCMSの難しさに鑑み特に設けられた特有の規定であるが、実際に行うのは難しい。また、「・・方法及び力量も含む・・」の力量は監査者の力量と考えられる。
備考	特になし。

項目	9 パフォーマンス評価 9.3 マネジメントレビュー
内容	トップマネジメントは，組織の BCMS が，引き続き，適切，妥当かつ有効であることを確実にするために，あらかじめ定めた間隔で，BCMS をレビューしなければならない。 マネジメントレビューは，次の事項を考慮しなければならない。 a) 前回までのマネジメントレビューの結果とった処置の状況 b) BCMS に関連する外部及び内部の課題の変化 c) 次に示す傾向を含めた，事業継続パフォーマンスに関する情報 1) 不適合及び是正処置 2) 監視及び測定の評価の結果 3) 監査結果 d) 継続的改善の機会 マネジメントレビューでは，次の事項を含む組織のパフォーマンスを考慮しなければならない。 普及－ 前回までのマネジメントレビューからのフォローアップ処置 － 方針及び目的を含む，BCMS に変更を加える必要性 － 改善の機会 － 必要に応じて，重要なサプライヤー及び取引先を含めた，BCMS の監査及びレビューの結果 － BCMS のパフォーマンス及び有効性の改善に組織内で利用できる技術，製品又は手順 － 是正処置の状況 － 演習及び試験の結果 － 過去のいずれのリスクアセスメントでも適切に取り上げていなかったリスク又は問題点 － BCMS の適用範囲内であるか否かを問わず，BCMS に影響を与える可能性のある変化 － 方針の妥当性 － 改善のための助言 － 事業の中断・阻害を引き起こすインシデントから学んだ教訓，及び実施した処置 － 新しい優れた実践及び指針 マネジメントレビューからのアウトプットには，継続的改善の機会，及び BCMS のあらゆる変更の必要性に関する決定を含めなければならない。また，次も含めなければならない。 a) BCMS の適用範囲の変更 b) BCMS の有効性の改善 c) リスクアセスメント，事業影響度分析，事業継続計画及び関連する手順の更新 d) 次の事項の変更を含め，BCMS に影響を与える可能性のある組織内外の事象に対応するための手順及び管理策の修正 1) 事業及びその活動に関する要求事項 2) リスク軽減及びセキュリティに関する要求事項 3) 事業活動の条件及びプロセス 4) 法令及び規制の要求事項 5) 契約上の義務

	6) リスクのレベル及び／又はリスクの許容基準 7) 資源のニーズ 8) 資金及び予算の要求事項 e) 管理策の有効性の測定方法 組織は，マネジメントレビューの結果の証拠として，文書化した情報を保持しなければならない。 組織は，次を行わなければならない。 － マネジメントレビューの結果を該当する利害関係者に伝達する。 － それらの結果に関する適切な処置をとる。
解釈	【この箇条の狙い】 ・BCM におけるマネジメントレビューの重要性を強調する。 ・MSS（Management System Standard）の枠組みでの、PDCA の C（チェック）に該当するパフォーマンス評価におけるマネジメントレビューの中身を明示する。 【この箇条のポイント】 ・トップマネジメントの役割は、全体の BCM の有効性の評価を内部監査や管理部門の自己点検・演習のフィードバックを総括することに留めずに、マネジメント自らチェックしアクションすることを求めている。 ・BCM のカバー範囲の大きさに鑑みて、スコープ設定と改善にフォーカスしており、静態的なコントロールの評価ではなく、動態的な改善活動そのものが重視されている。
適用方法例等	・統合報告書（※）の作成が有用である。 ※企業において売上などの財務情報と、環境・CSRなど非財務情報をまとめて投資家などに伝えるための報告書
意見	・ここで規定するマネジメントレビューの実行は難しい。このため、本規格固有の記述が3個所ある。 － 考慮すべき組織のパフォーマンスに含むべき事項 － アウトプットに含めるべき事項で、追加して含むべきもの － マネジメントレビューの結果の利害関係者に伝達すること及び結果に関する処置をとること ・BCM はシステムではなく経営そのものである。経営者が主体的にスコープを設定し優先順位を決めて対応するべき課題である。 ・コストと時間をかければやれることは際限なくある。外部利害関係者の要請等は流動的であり、常にムービングターゲットを追うものである。 ・実際のインシデント対応において、日ごろから BCM に主体的に取り組んでいない経営者ができることは極めて限定的である。 ・トップマネジメントが実施すべきことであるが、日本の経営の現状は不十分なため、これを確実に行うための体制・対策の具体化が重要といえる。 ・BCMS 規格の認定取得において、欧米では IT 関連が多い。これは、欧米において現実にシステムダウン障害による被害が多く発生しているからである。相対的に日本ではシステムダウン障害は多くない。
備考	特になし。

項目	10 改善 10.1 不適合及び是正処理
内容	不適合が発生した場合、組織は、次の事項を行わなくてはならない。 a) 不適合を特定する。 b) 不適合に対処し、該当する場合は必ず、次の事項を行う。 1) その不適合を管理し、修正をするための処置をとる。 2) その不適合によって起こった結果に対処する。 c) その不適合が再発又は他のところでも発生しないようにするため、次の事項によって、その不適合を除去するための処置をとる必要性を評価する。 1) その不適合をレビューする。 2) その不適合の原因を明確にする。 3) 類似の不適合の有無、又はそれが発生する可能性を明確にする。 4) 不適合の再発、又はほかでの発生の防止を確実にするための是正措置の必要性を評価する。 5) 必要な是正措置を決定し実施する。 6) (削除) 7) (削除) 注記 対応国際規格には 6)及び 7)が記載されているが、下記 e)及び f)は重複するために削除した。 d) 必要な処置を実施する。 e) とった全ての是正措置の有効性をレビューする。 f) 必要な場合には、BCMS の変更を行う。 是正措置は、検出された不適合のもつ影響に応じたものでなければならない。 組織は、次に示す事項の証拠として、文書化した情報を保持しなければならない。 ― 不適合の性質及びとった処置 ― 是正処置の結果
解釈	【この箇条の狙い】 ・PDCA の A(Act)プロセスの内容を明示した条文となっている。 【この箇条のポイント】 ・「前ステップに確認された事項を修正、改善して、BCMS が適切に、かつ、有効に機能しているかどうかを継続的に改善してく取り組みを実施する。」(「社会セキュリティ事業継続マネジメントシステム-要求事項 解説」) ・BCMS が意図した成果をもたらさない組織のマネジメントシステム上の原因を調査し、その原因を排除する修正、改善を実施しなければならない。 ・実際に発生している不適合の修正・改善だけにとどまらず、同様の不適合が他のところで発生しないように処置をする、すなわち、一箇所に不適合が発生した場合には同様の視点で全体を見直すことを求めている。 (参考)注記の英語表記 c) 6) review the effectiveness of any corrective action taken and 7) making changes to the BCMS, if necessary. e) review the effectiveness of any action taken f) make changes to the business continuity management system, if necessary.

適用方法例等	・具体的に不適合が発生している場合は、この不適合とこれを原因として生じている問題を解決する修正および改善を実施することを第一優先として行う。 ・同様の不適合が他でも発生する可能性があることを前提として、起こりうる具体的な不適合を想定し、その原因とこれを防止するための処置をおこなう。 ・修正および改善をした場合は、その後の一定期間後の有効性の検証をして、必要に応じた再修正を実施する。
意見	・小さな組織については、e)および f)を全体の PDCA と一体として実施することが許されても良いと考える。 ・不適合が他のところで発生しないように適切に処置するには、リスクマネジメントに関する知識と経験が必要であり、人材の育成が必要である。
備考	特になし。

項目	10 改善 10.2 継続的改善
内容	組織は、BCMS の適切性、妥当性及び有効性を継続的に改善しなければならない。 注記 組織は、リーダーシップ、計画、パフォーマンス評価など BCMS のプロセスを使って改善を達成することができる。
解釈	【この箇条の狙い】 ・PDCA は一回転するだけでなく、何回も継続的に回転させることを求めている。 【この箇条のポイント】 ・継続的に修正と改善を繰り返すことで、徐々に BCMS の意図した成果を達成するマネジメントシステムに近づいていくという考え方が基本となっている。 ・取り巻く環境は絶えず変化するため、マネジメントシステムはこの変化に応じて適宜修正や改善を必要とするという考え方も含意している。 ・注記では、BCMS のプロセスのうち、「組織の状況」「支援」「運用」の活用についての言及がないが、これらは重要なプロセスであり改善の達成のために活用することが当然といえる。
適用方法例等	・予め、修正と改善を実施する期間を設定する(実情に合わせて無理のない期間を設定)。 ・実施時に修正と改善の必要がないと判明した場合でも、行った作業手順を記録する。
意見	・継続性を確保するために組織の規模や要員に見合った仕組みの構築が重要である。
備考	特になし。

参考:ISO22301、ISO 27001、ISO 14001 の目次構成の比較

	ISO22301	行		ISO 27001	行		ISO 14001	行
	序文	3	0	序文	3		序文	3
0.1	一般	23	0.1	概要	17	0.1	背景	9
						0.2	環境マネジメントシステムの狙い	17
						0.3	成功のための要因	14
0.2	PDCA(Plan-Do-Check-Act)モデル	8				0.4	Plan-Do-Check-Act モデル	11
0.3	この規格における PDCA の構成要素	20				0.5	この規格の内容	26
			0.2	他のマネジメントシステム規格との両立性	5			
1	適用範囲	-	1	適用範囲	-	1	適用範囲	-
2	引用規格	-	2	引用規格	-	2	引用規格	-
3	用語及び定義	-	3	用語及び定義	-	3	用語及び定義	-
						3.1	組織及びリーダーシップに関する用語	-
						3.2	計画に関する用語	-
						3.3	支援及び運用に関する用語	-
						3.4	パフォーマンス評価及び改善に関する用語	-
4	組織の状況		4	組織の状況		4	組織の状況	
4.1	組織及びその状況の理解	14	4.1	組織及びその状況の理解	4	4.1	組織及びその状況の理解	3
4.2	利害関係者のニーズ及び期待の理解	8	4.2	利害関係者のニーズ及び期待の理解	4	4.2	利害関係者のニーズ及び期待の理解	4
4.3	BCMS の適用範囲の決定		4.3	情報セキュリティマネジメントシステムの適用範囲の決定	6	4.3	環境マネジメントシステムの適用範囲の決定	12
4.3.1	一般	5						
4.3.2	BCMS の適用範囲の決定方法	12						
4.4	BCMS	2	4.4	情報セキュリティマネジメントシステム	2	4.4	環境マネジメントシステム	5
5	リーダーシップ		5	リーダーシップ		5	リーダーシップ	
5.1	リーダーシップ及びコミットメント	4	5.1	リーダーシップ及びコミットメント	12	5.1	リーダーシップ及びコミットメント	15
5.2	経営者のコミットメント	28						
5.3	方針	11	5.2	方針	9	5.2	環境方針	16
5.4	組織の役割, 責任及び権限	5	5.3	組織の役割, 責任及び権限	7	5.3	組織の役割, 責任及び権限	5
6	計画		6	計画		6	計画	

	ISO22301	行		ISO 27001	行		ISO 14001	行
6.1	リスク及び機会に対処する活動	10	6.1	リスク及び機会に対処する活動		6.1	リスク及び機会への取組み	
			6.1.1	一般	10	6.1.1	一般	17
			6.1.2	情報セキュリティリスクアセスメント	21	6.1.2	環境側面	17
			6.1.3	情報セキュリティリスク対応	22	6.1.3	順守義務	7
						6.1.4	取組みの計画策定	11
6.2	事業継続目的及びそれを達成するための計画	17	6.2	情報セキュリティ目的及びそれを達成するための計画策定	16	6.2	環境目標及びそれを達成するための計画策定	
						6.2.1	環境目標	9
						6.2.2	環境目標を達成するための取組みの計画策定	9
7	支援		7	支援		7	支援	
7.1	資源	1	7.1	資源	1	7.1	資源	2
7.2	力量	9	7.2	力量	10	7.2	力量	11
7.3	認識	5	7.3	認識	5	7.3	認識	7
7.4	コミュニケーション	15	7.4	コミュニケーション	7	7.4	コミュニケーション	
						7.4.1	一般	12
						7.4.2	内部コミュニケーション	5
						7.4.3	外部コミュニケーション	2
7.5	文書化した情報		7.5	文書化した情報		7.5	文書化した情報	
7.5.1	一般	8	7.5.1	一般	8	7.5.1	一般	9
7.5.2	作成及び更新	4	7.5.2	作成及び更新	4	7.5.2	作成及び更新	4
7.5.3	文書化した情報の管理	20	7.5.3	文書化した情報の管理	15	7.5.3	文書化した情報の管理	15
8	運用		8	運用		8	運用	
8.1	運用の計画及び管理	8	8.1	運用の計画及び管理	7	8.1	運用の計画及び管理	22
8.2	事業影響度分析及びリスクアセスメント		8.2	情報セキュリティリスクアセスメント	3			
8.2.1	一般	9						
8.2.2	事業影響度分析	10						
8.2.3	リスクアセスメント	12						
8.3	事業継続戦略		8.3	情報セキュリティリスク対応	2	8.2	緊急事態への準備及び対応	15
8.3.1	決定及び選択	8						
8.3.2	資源に関する要求事項の設定	10						

	ISO22301	行		ISO 27001	行		ISO 14001	行
8.3.3	保護及び軽減	5						
8.4	事業継続手順の確立及び実施							
8.4.1	一般	11						
8.4.2	インシデント対応の体制	15						
8.4.3	警告及びコミュニケーション	15						
8.4.4	事業継続計画	30						
8.4.5	復旧	2						
8.5	演習及び試験の実施	10						
9	パフォーマンス評価		9	パフォーマンス評価		9	パフォーマンス評価	
9.1	監視，測定，分析及び評価		9.1	監視，測定，分析及び評価	10	9.1	監視，測定，分析及び評価	
9.1.1	一般	18				9.1.1	一般	14
9.1.2	事業継続手順の評価	12				9.1.2	順守評価	17
9.2	内部監査	20	9.2	内部監査	14	9.2	内部監査	
						9.2.1	一般	6
						9.2.2	内部監査プログラム	9
9.3	マネジメントレビュー	44	9.3	マネジメントレビュー	16	9.3	マネジメントレビュー	27
10	改善		10	改善		10	改善	
						10.1	一般	2
10.1	不適合及び是正処置	20	10.1	不適合及び是正処置	16	10.2	不適合及び是正処置	16
10.2	継続的改善	3	10.2	継続的改善	1	10.3	継続的改善	2
				附属書 A(規定)管理目的及び管理策			附属書 A(参考)この規格の利用の手引	
							附属書 B(参考)JIS Q 14001:2015 と JIS Q 14001:2004 との対応	
	参考文献			参考文献			参考文献	
	解 説							
							用語索引(五十音順)	
							用語索引(アルファベット順)	