事業継続マネジメントシステム（BCMS）について

一般社団法人レジリエンス協会
黄野吉博

はじめに

2011年の12月と2013年の5月に、以下の事業継続マネジメントシステム（BCMS）関係文書がISOの国際規格（IS）として公表されました。

【国際規格（IS）となった文書】

- ISO22300 社会セキュリティ ― 用語
- ISO22301 社会セキュリティ ― BCMS ― 要求事項
- ISO22313 社会セキュリティ ― BCMS ― ガイドライン
- ISO22320 社会セキュリティ ― 危機対応に関する要求事項

1.「社会セキュリティ」とはなにか

2006年にISO/TC223（ISO223技術委員会）が「社会セキュリティ」をテーマに国際規格の開発を始めてから、この発行に至るまでに6～7年が過ぎました。一般的にISOの国際規格の開発は3年が目安ですから、その倍の年月がかかったことになります。これは「社会セキュリティ」の目的である「命を守る」と「事業を守る」を国際規格にすることの困難性の現れでもあります。

BCMSは品質ISOや環境ISOと同様のマネジメントシステム規格ですが、「命を守る」機能は企業や組織（以下、「企業等」という）の枠を超え、行政・医療機関・インフラ提供者などとの協力と連携が必要ですし、サプライチェーンやICT（Information and Communication Technology）などの「事業を守る」機能も企業等の間で協力と連携が必要になります。この協力と連携を整理・調整して初めて国際規格になりますが、この整理・調整が容易ではありませんでしたし、今も他の「社会セキュリティ」関係文書ではこの整理と調整が進められています。

企業等間の協力と連携が容易ではない理由の一つは、国際的にも国内的にも特定の企業なり組織を中心と設定したとして、他の企業等がその中心に合わせるというハブ・アンド・スポーク方式が取れないことにあります。勢い、企業等の組合せが網の目のように無数に存在し、ひいては企業等の対応方針も組合せも無数に存在することになり良い対応方針を選ぶには多大で困難な作業が必要となります。

ここで「良い」対応方針の「良い」は、利害得失や文化背景が異なる国際社会では、理解の幅が広く、調整作業に多くの時間がかかりましたし、今もかかっています。「命を守る」は明確な目標ですから、異論はないのですが、命を守る「機能」になりますと、現状の災害等の情報把握機能、医療機

能、行政機能、インフラ機能などが含まれ、その優先順位は複雑になります。更に、後方支援となる医薬品や食料・生活必需品の供給機能、情報伝達機能、その他の災害対応機能を含めるとより複雑になります。

民間企業でも、従業員や関係者の「命を守る」は明確ですが、命を守る「機能」になると複雑さが増加し、「事業を守る」になると事業の維持と再開の優先順位がかなり複雑になります。

忘れてならないのは、「命を守る」と「事業を守る」は時により対立することがあることです。「命を守る」が常に優先しますが、例えば新型感染症の防疫のケースのように感染防止のためには全従業員・関係者が自宅などで安全が確認できるまで待機する方法が望まれますが、そうすると医薬品や食料・生活必需品の供給も、医療や警察・消防・行政の機能も電力・上下水道・通信も止まることになり、社会が維持できなくなります。このような事例では、「命を守る」を超えて、「事業を守る」ために活動する人々が必要になります。

2. ISO22301（BCMS）について

ISO22301の開発は以下の6文書を比較検討することから始まりました。

- ANSI/NFPA1600:2007　米国規格協会
- BS/PAS56:2003　英国規格協会
- HB211:2001　豪州規格協会
- SS507:2008　シンガポール規格協会
- 事業継続計画策定ガイドライン　経済産業省、2005 年
- 事業継続計画ガイドライン　内閣府、2005 年

この6文書は、それぞれ「命を守る」面と「事業を守る」面が含まれていますが、その重みと対策に違いがありましたし、「事業を守る」機能としてのサプライチェーン関係とICT関係を含む程度にも、差がありました。

3. ICTの事業継続性

ICTの事業継続性について触れているのは、シンガポール規格の「SS507」と経済産業省の「事業継続計画策定ガイドライン」でした。このICTの事業継続性の取り扱いは、審議の途中からISO/TC223とは別にあるISO/IECの合同委員会に移動しました。

その後、合同委員会は2011年5月、その検討成果を「ISO/IEC27031:2011　情報技術－セキュリティ技術－事業継続のための情報通信技術の準備態勢に関する指針」として公表しました。

この文書の特徴は、ICT]障害を地震や火災時と同時に発生する障害ではなく、ICT単独での障害として、その考え方と対策を記述していることです。 なお、広域災害時における企業および組織

間のICT機能の維持は、TC223で引き続き検討されています。

4. TC223で続く検討

命が関係する災害・事故・事件（以下「災害等」）は極めて大きな影響を企業・組織に与えます。東日本大震災も、今後発生が強く懸念されている首都直下型地震、東海・東南海・南海地震も同様です。

これとは別に命に直接的な影響はないが、事業には大きな影響を及ぼす災害等もあります。2011年春に発生した日本の銀行での大規模システム障害、同年秋に発生したバンコック大水害などがその一例です。前者はICT障害であり、人命に直接影響を及ぼすことはありませんが、企業活動を混乱させ最悪の場合は企業活動を停止させ、失業者を生むこともありえました。後者も人命には直接的な影響を与えませんでしたが、部品の供給停止は企業活動を停止させる可能性があります。

日本は地震の多発地帯であり、台風も毎年2～3個は接近・上陸し水害・風害を与えますので、欧米と比較しても自然災害への対策は進んでいると国連大学の専門チームも評価しています。ただ、事業に強く影響をあたえるICT障害とサプライチェーン中断の対策については、日本よりも米国と英国が先行していると同チームは指摘しています。

日本の多くの方は、TC223は地震や水害など大規模な自然災害リスクのみを対象としていると理解されていますが、実は、自然災害の他に、ICT障害、サプライチェーン中断、各種の操業リスク、役員誘拐やテロ、ICTのサイバーテロや情報の窃盗なども検討範囲に含んいることに留意しなければなりません。

5. BCMSの概要とマネジメントシステム規格（MSS）との関係

ISO 22301は、マネジメントシステム規格（MSS）に準拠した規格です。今後は、品質ISO（ISO9001）、環境ISO（ISO14001）を始め、全てのマネジメントシステムはこのMSSに準拠することになります。

表1 MSSとISO 22301の比較

MSS （マネジメントシステム規格）の構成		ISO 22301の構成	
1	適用範囲	1	適用範囲
2	引用文献	2	引用文献
3	用語と定義	3	用語と定義
4	組織の状況	4	組織の状況
4.1	組織とその状況の理解	4.1	組織とその状況の理解

4.2	利害関係者の要求事項と期待の理解	4.2	利害関係者の要求事項と期待の理解
4.3	マネジメントシステムの適用範囲の決定	4.3	BCMSの適用範囲の決定
4.4	XXXマネジメントシステム	4.4	BCMS
5	リーダーシップ	5	リーダーシップ
6	計画	6	計画
7	支援	7	支援
8	運用	8	運用
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
9.2	内部監査	9.2	内部監査
9.3	マネジメントレビュー	9.3	マネジメントレビュー
10	改善	10	改善
10.1	不適合及び是正処置	10.1	不適合及び是正処置
10.2	継続的改善	10.2	継続的改善

懸念すべきは、品質ISO、環境ISOではパフォーマンス評価としてある程度明確な指標がありますが、BCMSのパフォーマンス評価の指標であるレジリエンス量の明確な尺度がないことです。このレジリエンス量は今後の検討テーマになると思います。

表 3 MSS の有効性評価に用いる指標

MSS	目的	指標
品質 ISO	品質に配慮した経営	顧客満足度、不良品率など
環境 ISO	環境に配慮した経営	電力使用量、廃棄物量など
BCMS	レジリエンスに配慮した経営	レジリエンス量

6. BCMSが求める文書類

BCMSは次の文書、資料を求めています。

表4 BCMSが求める文書類

セクション	文書類の内容
4.1.a	組織の活動、機能、サービス、製品、連携、サプライチェーン、利害関係者との関係、事業を中断させる緊急事態に関係する潜在的な影響

4.1.b	総合的なリスクマネジメント戦略を含む、事業継続方針、組織の目的その他の方針
4.1.c	組織のリスク選好
4.2.2	法令及び規制の要求事項
4.3.1	適用範囲
4.3.2	適用除外
5.3	事業継続方針
6.2	事業継続目的
7.2	力量の証拠
7.4	コミュニケーション手順
7.5.1	組織がBCMSの有効性に必要と判断した文書
8.2.2	事業影響度分析（BIA）
8.2.3	リスクアセスメント（RA）実施手順書
8.4.1	インシデントへの対応を確実にするための手順
8.4.3	警告及びコミュニケーションに関する文書
8.4.4	事業継続計画書（必要事項がすべて網羅されているBCP）
8.4.5	復旧手順書
8.5	演習実施報告書
9.1.1	BCMのパフォーマンス・有効性の評価結果
9.1.2	インシデント発生後のレビューの実施記録
9.2	内部監査実施結果
9.3	マネジメントレビュー実施結果
10.1	不適合及び是正処置の結果

ここでは、今までの BCM（少し紛らわしいですが、「システム」がない事業継続マネジメント：Business Continuity Management）との比較をします。

今までの BCM は「マネジメントシステム（MS：Management System）の部分」と「事業継続性の向上部分」の二つから構成されていました。

この二つの部分が BCMS では分化し、「MS の部分」は品質 ISO や環境 ISO の MS 部分との共通化が明確になりました。また、「事業継続性の向上部分」は、PDCA（Plan–Do–Check–Act）サイクルの活用が明記されました。（図1 参照）

PDCA サイクルの活用とは、前年度の事前対策（具体的には地震対策、水害対策、教育訓練など）を評価し、改善すべき点を明確にし、翌年度に改善策を実行し記録するということで、これを毎年度繰り返すことになります。（図2 参照）

PDCA サイクルの実行を評価するために、各対策や教育訓練の実施記録と改善記録を複数年度分、保管・管理することが必要になります（従って、管理する文書類が増えます）。

また、PDCA サイクルは、個人・所属部門・工場等の施設・全社などのレベルに存在しますが、経営者の PDCA サイクルが最優先されます。

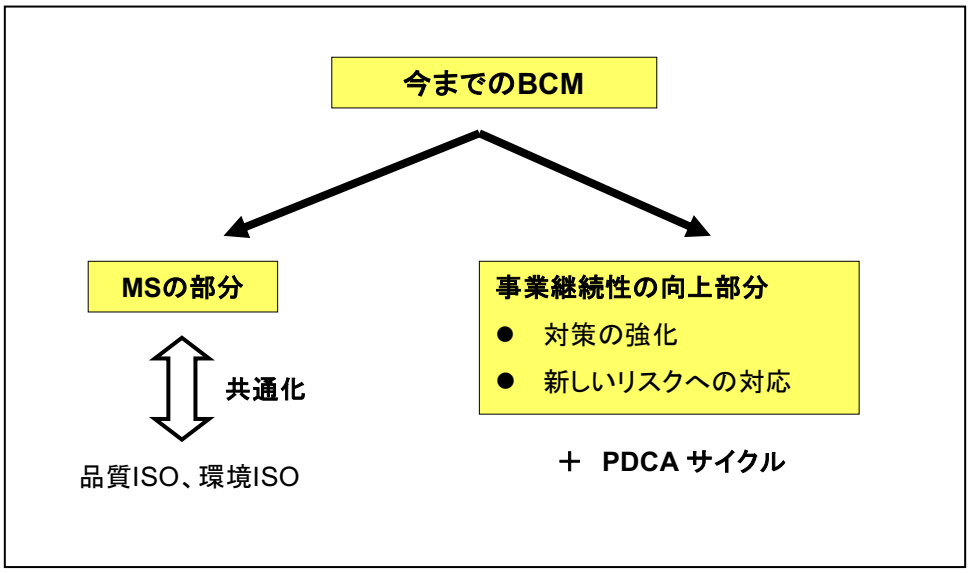

図1 今までの BCM の構成

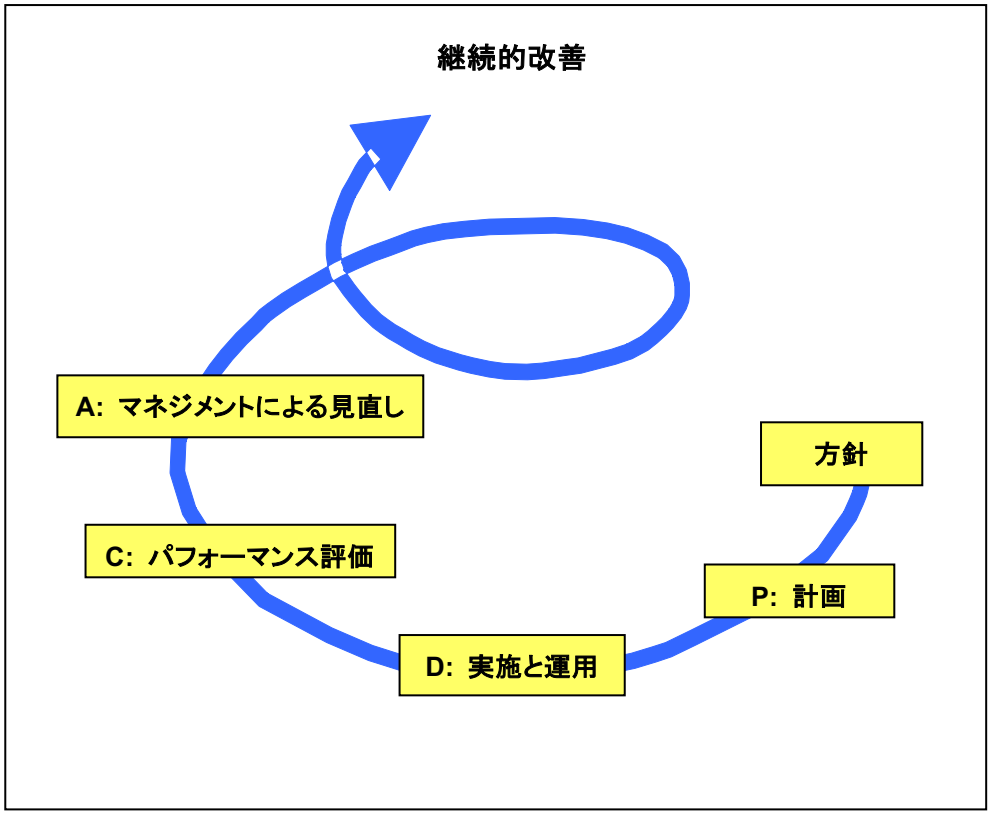

図2 PDCA サイクル