国際規格「ISO 22301」はどのようなものか？

「ISO 22301」の可能性とは

西出 三輝 Mitsuteru Nishide
リスクコンサルティング事業本部 ERM 部
主任コンサルタント

井口 洋輔 Yosuke Iguchi
リスクコンサルティング事業本部 ERM 部
主任コンサルタント

はじめに

2011 年 3 月 11 日、東日本を襲った未曾有の大災害「東日本大震災」は、事業中断や原材料の供給不足による業務レベルの低下など、多くの企業の事業に影響を与え、災害発生による事業停滞リスクの大きさを改めて認識させた。

また、海外においてもタイの洪水やアイスランドの火山噴火による欧州航空網の麻痺など、事業に影響を及ぼすリスクが顕在化しており、大企業だけではなく中小企業においても事業継続への対応を考える機会が増えたのではないだろうか。

このような中、事業継続マネジメントシステム（BCMS）の国際規格 「ISO22301:2012　社会セキュリティー事業継続マネジメントシステムー要求事項」が、ISO（国際標準化機構）から、2012 年 5 月 15 日に発行された。

国際規格の発行により、今後日本だけでなく世界各国で ISO 22301 の第三者認証制度が始まり、様々な業種・業態において認証を取得する企業が増加するものと予想される。

そこで、本稿では ISO 22301 がどのような規格なのか、また ISO 22301 が企業にとってどのような有効性が期待できるのかについて述べる。

1. ISO 22301 の概要

1.1. ISO 22301 の構成

社会セキュリティに関する国際規格は、「TC 223」という ISO の専門委員会のワーキンググループで開発された。

ISO 22301 は、事業継続マネジメントシステムの要求事項であり、「0 Introduction」から「10 Improvement」で構成されている（表 1）。このうち要求事項にあたるのは、箇条 4～箇条 10 である。

なお、TC 223 において開発している ISO 22301 に関係する規格として、「ISO/DIS 22313:2011　社会セキュリティー事業継続マネジメントシステムーガイダンス」がある。

これは、ISO 22301 のガイドラインとしての位置付けであり、要求事項の各項目について採用することが望ましい事項を示しているため、ISO 22301 の要求事項に基づく体制構築時の具体的な指針として利用できる。

ISO のプレスリリース[1]によると「ISO/DIS 22313:2011　社会セキュリティー事業継続マネジメントシステムーガイダンス」は、2013 年初頭の発行に向けて準備を行なっている。

表 1　ISO 22301 目次と概要[2]

箇条	項目	概要
0	Introduction／序文	BCMS の重要性や本規格の構成要素について説明している。
1	Scope／適用範囲	本規格の趣旨や適用可能な範囲について説明している。
2	Normative reference／引用規格	本規格が引用している文書について示している。
3	Terms and definitions／用語及び定義	ISO ガイド 73[3]、ISO 22300[4]に規定する以外の用語について定義している。
4	Context of the organization／組織の状況	PDCA サイクルの PLAN に関する要求事項であり、BCMS における組織の適用範囲を決定するために必要となる事項を示している。
5	Leadership／リーダーシップ	PDCA サイクルの PLAN に関する要求事項であり、BCMS におけるトップマネジメントの役割責任について示している。
6	Planning／計画	PDCA サイクルの PLAN に関する要求事項であり、BCMS 全体の目的や指針の設定について示している。
7	Support／支援	PDCA サイクルの PLAN に関する要求事項であり、BCMS を運用するにあたり、文書化、力量の保持、利害関係者とのコミュニケーションに関する事項を示している。
8	Operation／運用	PDCA サイクルの DO に関する要求事項であり、事業継続を実現するための対応方法、手順の策定方法、策定後の演習について示している。
9	Performance evaluation／パフォーマンス評価	PDCA サイクルの CHECK に関する要求事項であり、BCMS のパフォーマンスや適合性の確認について示している。

[1] ISO（International Organization for Standardization）.“ISO publishes new standard for business continuity management.” ISO（International Organization for Standardization）,http://www.iso.org/iso/pressrelease.htm?refid=Ref1587（アクセス日：2012-07-10）

[2]ISO（International Organization for Standardization）. ISO 22301:2012. ISO（International Organization for Standardization）2012,Pⅰ-P24,Pⅲ　（表内の「項目」は、ISO/FDIS 22301:2012 をもとに行った当社の仮訳であり、「概要」は当社の見解である）。

[3] 一般財団法人 日本規格協会 ISO Guide 73:2009 リスクマネジメントに関する一般的な用語及びその定義についての規定

[4]一般財団法人 日本規格協会 ISO 22300:2012　社会セキュリティに関する用語規格集

箇条	項目	概要
10	Improvement／改善	PDCA サイクルの ACT に関する要求事項であり、BCMS の不適合を特定し是正処置によって対応することを示している。

1.2. ISO 22301 の特徴

ISO 22301 は、マネジメントシステム規格であるため、PDCA サイクルや継続的改善といった ISO 9001 や ISO 14001 など従来の国際規格でも示されている要求事項の他に、有事の事業継続を目的としたマネジメントシステムの性格上、以下のような特徴的な要求事項が見受けられる。

① 演習

事業継続マネジメントは、他のマネジメントとは違い、有事が発生しなければ BCP の有効性や実効性を確認する機会が発生しない。

しかし、有事は頻繁に発生するものではないため、平時でも BCP の有効性や実効性を確認する「演習」の実施が求められている。

演習実施は箇条 8.5 に明記されている要求事項であるが、演習を単に実施するだけではなく、演習実施の目標を定め、シナリオを計画・実施し、その結果をまとめ、改善を促進する観点からレビューすることも求められている。

また、演習はあらかじめ定められた間隔で実施され、また組織に大きな環境の変化があった場合にも実施が求められている。

② 平時と有事の要求事項

ISO 22301 では、演習以外にも平時における要求事項と有事における要求事項、両方が示されており、文書策定や体制構築において適切に構築する必要がある。

例えば、箇条 7.4 と箇条 8.4.3 はどちらもコミュニケーションについての要求事項であるが、平時に準備する内容と有事に実施する内容が示されている。

箇条 7.4 は、平時において BCMS に関する内部及び外部のコミュニケーションの必要性を判断することを求めており、平時において有事に備えて伝達事項、伝達時期、伝達相手についてどのように対応するか手順化することを求めている。

箇条 8.4.3 では、有事発生のコミュニケーション手順を確立することを求めており、組織が決めた手順については演習実施の対象にすることを求めている。

1.3. 他のガイドラインとの比較

事業継続に関する規格やガイドラインとしては、2004 年に NFPA 1600（米国防火協会）、2005 年に事業継続ガイドライン（内閣府）[5]と事業継続計画策定ガイドライン（経済産業省）[6]、2007 年に BS 25999-2（英国規格協会）、2009 年に ANSI/ASIS SPC.1（米国規格協会）が、そして、2012 年 5 月に ISO 22301 というようにこれまで数多くの規格やガイドラインが発行されている。そして、ISO 22301 は、ISO 9001 や ISO 14001 など

[5]事業継続ガイドライン 第二版 （内閣府）平成 21 年 11 月発行 http://www.bousai.go.jp/MinkanToShijyou/guideline02.pdf
[6]事業継続計画策定ガイドライン （経済産業省）平成 17 年 6 月発行
http://www.meti.go.jp/policy/netsecurity/downloadfiles/6_bcpguide.pdf

従来の国際規格や海外の事業継続に関するガイドラインのみならず、国内のガイドラインも参考に開発されてきた。

そこで、ISO 22301 と国内の多くの企業が事業継続に取り組む際に一つの指針として活用されている事業継続ガイドライン（内閣府）を比較してみると、双方でカバーしている項目に大きな違いがないことが分かる（表 2）。

表 2 ISO 22301 と事業継続ガイドライン（内閣府）の対応表[7]

ISO 22301:2012	事業継続ガイドライン 第二版 （内閣府）
1 適用範囲	1.2.3 本ガイドラインにあげた各項目の位置づけ
2 引用規格	―
3 用語及び定義	―
4 組織の状況	
4.1 組織とその状況の理解	2.1 方針 2.2.2 影響度の評価
4.2 利害関係者のニーズ及び期待の理解	1.2.2 事業継続と共に求められるもの 2.2.6 事業継続と共に求められるもの
4.3 マネジメントシステムの適用範囲の決定	2.2.1 検討対象となる災害の特定
4.4 事業継続マネジメントシステム	Ⅱ 事業継続計画および取組みの内容
5 リーダーシップ	
5.1 一般	2.1 方針
5.2 経営者のコミットメント	2.1 方針
5.3 方針	2.1 方針
5.4 組織の役割、責任及び権限	2.3.1 事業継続計画に従った対応の実施
6 計画	
6.1 リスク及び機会に対応するための処置	2.2 計画
6.2 事業継続目的及び達成計画	2.3.1 事業継続計画に従った対応の実施 2.3.2 文書の作成 2.4 教育・訓練の実施
7 支援	
7.1 資源	2.2.4 重要な要素の抽出
7.2 力量	2.4 教育・訓練の実施
7.3 認識	2.4 教育・訓練の実施
7.4 コミュニケーション	2.2.5.3 対外的な情報発信および情報共有
7.5 文書化した情報	2.3.2 文書の作成
8 運用	
8.1 運用の計画及び管理	2.3.1 事業継続計画に従った対応の実施
8.2 事業影響度分析及びリスクアセスメント	2.2.2 影響度の評価 2.2.3 重要業務が受ける被害の想定
8.3 事業継続戦略	2.2.4 重要な要素の抽出
8.4 事業継続手順の確立及び導入	2.2.5 事業継続計画の策定

[7]ISO（International Organization for Standardization）. ISO 22301:2012. ISO（International Organization for Standardization）2012,Pⅰ-P24,Pⅲ （表内の「ISO 22301:2012」の欄については、ISO/FDIS 22301:2012 をもとにした当社による仮訳）。
ISO22301 と事業継続ガイドライン第二版の対応表については当社の見解である。

ISO 22301:2012	事業継続ガイドライン 第二版 （内閣府）
8.5 演習及び試験の実施	2.3.4 計画が本当に機能するかの確認 2.4 教育・訓練の実施
9 パフォーマンス評価	
9.1 監視、測定、分析及び評価	2.5 点検及び是正処置
9.2 内部監査	2.5 点検及び是正処置
9.3 マネジメントレビュー	2.5 点検及び是正処置
10 改善	
10.1 不適合及び是正処置	2.5 点検及び是正処置
10.2 継続的改善	2.6 経営層による見直し

しかしながら、解説されている詳述レベルという点では差異が見受けられる。例えば、事業影響度分析及びリスクアセスメントを見ると、事業継続ガイドラインの方が検討する際の考え方を示しているが、ISO 22301 ではアプローチ方法を示すに留まっている。一方、パフォーマンス評価については、ISO 22301 のほうがより詳しく示されている。これらの違いは、第三者認証に利用可能な国際規格とガイドラインという、それぞれの位置付けによって生じているもので、事業継続への取組を進めていく上での目的・アプローチはほぼ同じであると考える。

2. ISO 22301 の活用方法

ISO 22301 は、認証取得のための要求事項としてだけでなく様々な活用方法が考えられており、規格の「1. 適用範囲」では、ISO 22301 が以下の事項を実施するあらゆる組織に適用できるとしている。

① BCMS を確立し、導入し、維持し、改善する[8]。
② 表明した事業継続方針との適合性を保証する。
③ 適合を他者に示す。
④ 第三者の登録認証機関に BCMS の認証・登録を求める。
⑤ この国際規格との適合を自己決定し、自己宣言する。

よって、企業において ISO 22301 を活用する場合、どのような活用方法が考えられるかを以下に示す。

2.1. 認証取得

ISO 22301 が発行されたことにより、ISO 22301 を審査基準とした BCMS の第三者認証制度が、各国にて開始するものと考えられる。

第三者認証制度において ISO 22301 認証を取得するためには、制度で認定を受けた認証機関からの審査が必要となる。そのため、認証取得した組織の事業継続マネジメント体制は、客観的に事業継続の能力があり、その能力に対する継続的な改善がなされ、かつ、その管理の仕組みがあることへの宣言につながる。

[8] ISO（International Organization for Standardization）. ISO/FDIS 22301:2012　社会セキュリティー事業継続マネジメントシステムー要求事項. ISO（International Organization for Standardization）2012,P ⅰ -P24,P1

その結果、取引先などの利害関係者から事業継続性への客観的な評価を得やすくなる効果が期待できる。

2.2. 事業継続マネジメント体制の構築のガイドライン

ISO 22301 は、内閣府の事業継続ガイドラインや中小企業庁の中小企業 BCP 策定運用指針[9]など、様々な事業継続のガイドラインと同様に活用することが可能である。

ISO 22301 は国内のガイドラインとは違い、国際標準であるため、国内だけでなく海外の企業と取引をする企業であれば、海外の顧客より事業継続の取り組みを質問された場合でも、国際標準に則った事業継続マネジメント体制を維持していることを説明することで、国内ガイドラインの解説など、自社が採用したガイドラインについて解説する手間や国際標準との比較をする必要がなく、迅速に対応する事が可能と考えられる。

今後の ISO 22301 の認証取得を条件とされた場合でも、既に要求事項に基づいた体制を構築しておけば、これまでの活動結果を元に審査を受け、認証取得することも可能となる。

2.3. 事業継続マネジメント体制のチェックツール

委託先や供給先が事業継続にどの程度取組んでいるかを測る指標の一つとして、ISO 22301 の活用が考えられる。

実際に有事が生じた場合でも、あらかじめ定めたレベルで重要な業務を継続できることを評価するためには、実効性のある BCP が策定されているか、平時においても教育・訓練、演習、レビューや改善などの継続的な諸活動が実施されているかをチェックすることが重要である。

ISO 22301 では、事業継続マネジメント体制の構築・運用だけでなく実効性のある BCP の維持・改善に向けた諸活動についても要求事項に示されていることから、委託先や供給先の事業継続の取組状況が一過性ではないことも含め、網羅的に確認することが可能である。

また、ISO 22301 と合わせて ISO/DIS 22313 を参考にすることで、委託先や供給先に実施して欲しい諸活動の具体例を示すことも可能である。

2.4. 統合マネジメントシステムの基礎ツール

ISO 22301 の章立ては、ISO Guide 83[10]で示されている規格構造で構成されている。ISO Guide 83 とは、マネジメントシステム規格の共通要素を定めたガイドラインである。今後改訂または新規発行されるマネジメントシステム規格は、ISO Guide 83 に示された構造、用語等が適用される。

ISO Guide 83 で示されている章立てのうち、箇条 8 については各マネジメントシステム規格が対象としている事象ごとに内容が異なるが、それ以外の箇条については共通の章立てとなる。

そのため、複数のマネジメントシステム認証を受けている組織において、ISO 22301 の章立てはマネジメントシステム文書や活動の統合における基礎ツールとして参考となる。

3. まとめ

ISO 22301 の発行により、今後様々な企業が認証取得することも予想されるが、他の第三者認証と同様、認証取得が『有事における事業継続』を保証するものではなく、『有事における事業継続』の目的達成に向けた

[9] 中小企業 BCP 策定運用指針（中小企業庁）2006 年公開　http://www.chusho.meti.go.jp/bcp/
[10] High level structure and identical text for management system standards and common core management system terms and definitions

取り組みを ISO 22301 の要求事項に基づき実施していることを認証していることにとどまる。

そのため、認証取得を目的とせずに、自社にあった事業継続マネジメント体制を構築し、『有事における事業継続』に向けて継続的な活動を行うことが本来の事業継続の趣旨として重要である。

『有事における事業継続』に向けた体制作りや BCP 策定は、ISO 22301 でも国内のガイドラインでも大きな違いはないことから、まずは自社にあったガイドラインを参考とし、その内容に基づいて網羅性のある事業継続マネジメント体制を構築し、維持し続ける事が重要である。

そのためにも、一度 ISO 22301 の内容を確認し、自社の事業環境などを考慮した上で、採用の是非を図ることをお勧めしたい。

参考文献

ISO 22301:2012　Societal security — Business continuity management systems — Requirements
ISO/DIS 22313:2011　社会セキュリティー事業継続マネジメントシステムーガイダンス
ISO/FDIS 22301:2012　社会セキュリティー事業継続マネジメントシステムー要求事項
事業継続ガイドライン 第二版（内閣府）

執筆者紹介

西出　三輝　Mitsuteru Nishide

リスクコンサルティング事業本部 ERM 部
主任コンサルタント
専門は BCM、情報セキュリティ

井口　洋輔　Yosuke Iguchi

リスクコンサルティング事業本部 ERM 部
主任コンサルタント
専門は BCM、情報セキュリティ

NKSJ リスクマネジメントについて

NKSJ リスクマネジメント株式会社は、株式会社損害保険ジャパンと日本興亜損害保険株式会社を中核会社とする NKSJ グループのリスクコンサルティング会社です。全社的リスクマネジメント（ERM）、事業継続（BCM・BCP）、火災・爆発事故、自然災害、CSR・環境、セキュリティ、製造物責任（PL）、労働災害、医療・介護安全および自動車事故防止などに関するコンサルティング・サービスを提供しています。詳しくは、NKSJ リスクマネジメントのウェブサイト（http://www.nksj-rm.co.jp/）をご覧ください。

本レポートに関するお問い合わせ先

NKSJ リスクマネジメント株式会社
リスクコンサルティング事業本部 ERM 部
〒160-0023 東京都新宿区西新宿 1-24-1 エステック情報ビル
TEL：03-3349-4226（直通）

