

よくわかる ISO22301 の概要とポイント

はじめに

2012 年 5 月、BCP の ISO 規格として ISO22301(事業継続マネジメントシステム—要求事項)が発行されました。これにより、BCP 及び BCMS 導入をめぐる取り組みは ISO22301 規格に準じた取り組みへと進化を遂げ、各社・組織・団体での事業継続マネジメントシステム構築に向けた動きは一層活性化していくことが予想されます。

“様子見”から実行へ、迅速かつ適正で実効性のあるシステム構築が必須の時代となっていきます。

本ドキュメントでは、ISO22301 の特長、取り組みにあたってのポイントとなるところを弊社の視点で読み解き、整理したものです。

BCP の策定、BCMS 構築に向けた最前線で活躍されている皆様にお役立ていただければ幸いです。

《 INDEX 》

1. BCP の規格・ガイドラインの歴史
2. ISO22301 5つの特長
3. ISO22301 の基本は PDCA にもとづいた「BCMS の構築による事業継続のスパイラル作成」
4. PDCA に当てはめると見えてくる ISO22301 全 10 章
5. ISO22301 構築の鍵は 8 章「運用」にあり
6. ISO22301 認証取得に役立つ参考ガイドライン
7. ISO22301 認証取得のための15ポイント

付録 1 よくある BCMS、BCP の失敗の原因

付録 2 弊社サービスの特徴

付録 3 資料

1. BCP の規格・ガイドラインの歴史

● BS25999-2:2007（事業継続マネジメント:仕様）

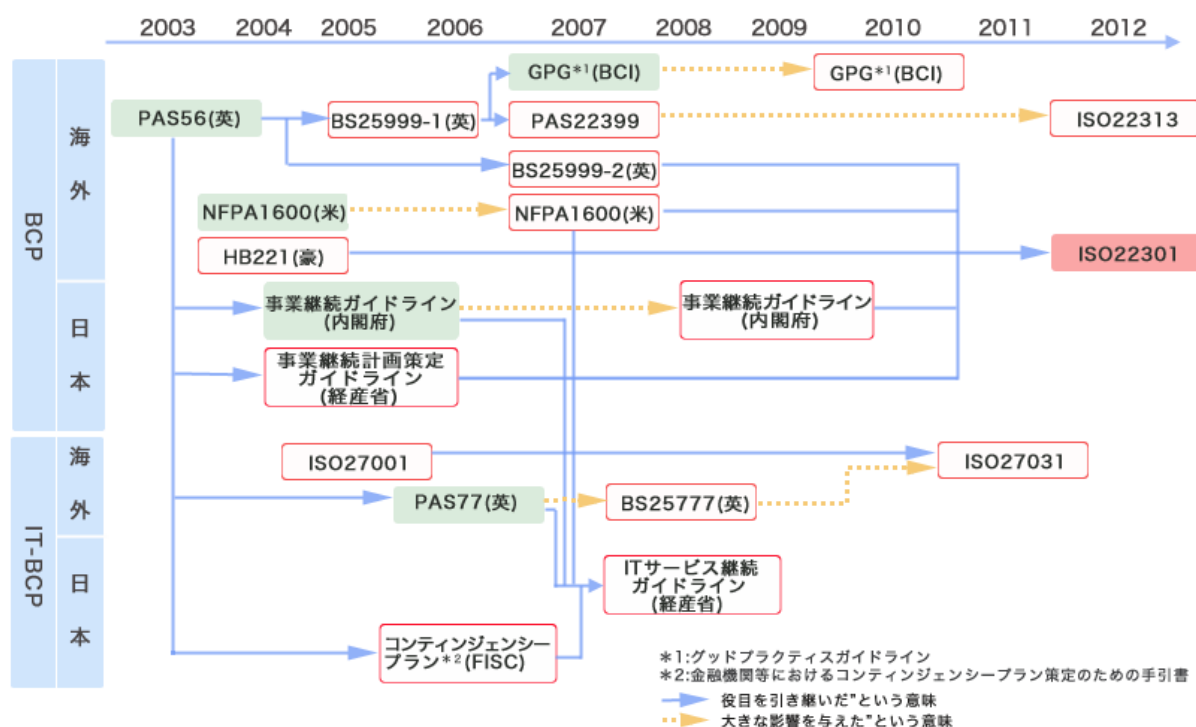
2007 年 11 月に英国規格協会が発行した事業継続マネジメントシステム（BCMS）の規格です。規格としては現在、世界で最も利用されているものです。

日本国内では 2008 年 7 月から BCMS 適合性評価制度がスタートしていますが、この制度の中で当該規格が採用されています。

● ISO22301:2012(事業継続マネジメントシステム—要求事項)

BCMS 規格の ISO 版で、BS25999-2:2007 の後継とも言えるものです。2012 年 5 月に発行されました。

今後の国内外の認証制度は全てこの規格に基づいたものへと移行される予定です。



2. ISO22301 5つの特長

ISO22301 では、事業を中断させるインシデントが発生した場合の行動、対処として下記を適用範囲に掲げ、文書化されたマネジメントシステム(BCMS)を計画、確立、運用、監視、レビュー、維持、および継続的に改善するための要求事項が規定されています。

● インシデント発生に際しての行動、対処の適用範囲 ●

- ・ インシデントからの保護
- ・ インシデント発生の可能性の低減
- ・ インシデントに対する準備
- ・ インシデントへの対応
- ・ インシデントからの復旧

ここで、ISO22301 の主な特長をまとめてみたのが下記の①～⑤です。

- ① 事業継続性を継続的に向上させるマネジメントシステム(BCMS)の構築に重点
 - ・ 事業継続を保証するために必要なリソースの計画や準備決定
 - ・ 実践的な活動のマネジメントシステムの確定と実効性確保
- ② 第三者認定用規格である。
 - ・ 抜け、漏れのない事業継続マネジメントシステムを構築
 - ・ 事業継続への取り組み姿勢を対外的にアピール
 - ・ ステークホルダーへ安心感を与える
- ③ 認証規格として、経営者が実施／関与すべき項目を明確化
- ④ リスク選択・判断は組織に委ねられている
- ⑤ BCMS(事業継続マネジメントシステム)は、他のマネジメント規格(QMS、EMS、ISMS等)と一貫性が保たれている。

補足すれば、⑤については、他のISO規格と構造を共通化することにより、BCPに関して新たに開発するマネジメントシステムの開発期間を短縮するとともに、ISOの複数のマネジメントシステムの導入・統合を簡素化するという、ISO化の大きな目的がここで達成されているといえます。

また、ISO22301では「演習とテスト」の重視や、コミュニケーションやリーダーシップなどボトルネックとなりやすい項目に対する要求が明確になったことも特長としてあげていいでしょう。

3. ISO22301 の基本は PDCA にもとづいた

「BCMS の構築による事業継続のスパイラル作成」

ISO22301 では特に、組織における事業継続マネジメントを継続的に改善していくための手法として、PDCA サイクル*を取り入れて、PDCA サイクルにもとづいた「BCMS の構築による事業継続のスパイラル作成」が、事業継続能力を継続的に高める上での要となる仕組みとして位置づけられています。

*「PDCA サイクル：Plan（計画）、Do（実行）、Check（点検）、Action（改善）のプロセスを実行し、継続的に改善を行うマネジメント手法。」

BCMS の PDCA サイクルで Plan（計画）、Do（実行）、Check（点検）、Action（改善）の各プロセスに該当するものは以下の通りです。

Plan 「計画のプロセス」 BCMS 計画の策定となります。 BCMS の計画では、 ① BCMS の目的、BCMS の適用範囲の決定 ② BCM 方針の決定 ③ BCMS 運用体制の確立 ④ BCMS 文書体系 ⑤ 関係者の周知 などを行います。	Do 「実行のプロセス」 BCMS の導入及び運用となります。 BCMS の実行では、 ① 事業影響分析 ② リスク分析 ③ BCP 戦略の決定 ④ BCP の策定 などを行います。
Check 「点検のプロセス」 BCMS の監視及びレビューとなります。 BCMS の確認では、 ① BCMS 内部監査 ② BCMS 訓練 ③ BCMS マネジメントレビュー などを行います。	Action 「改善のプロセス」 BCMS の維持及び改善となります。 BCMS の改善では、 ① 予防処置 ② 是正処置 ③ 改善計画 などを行います。

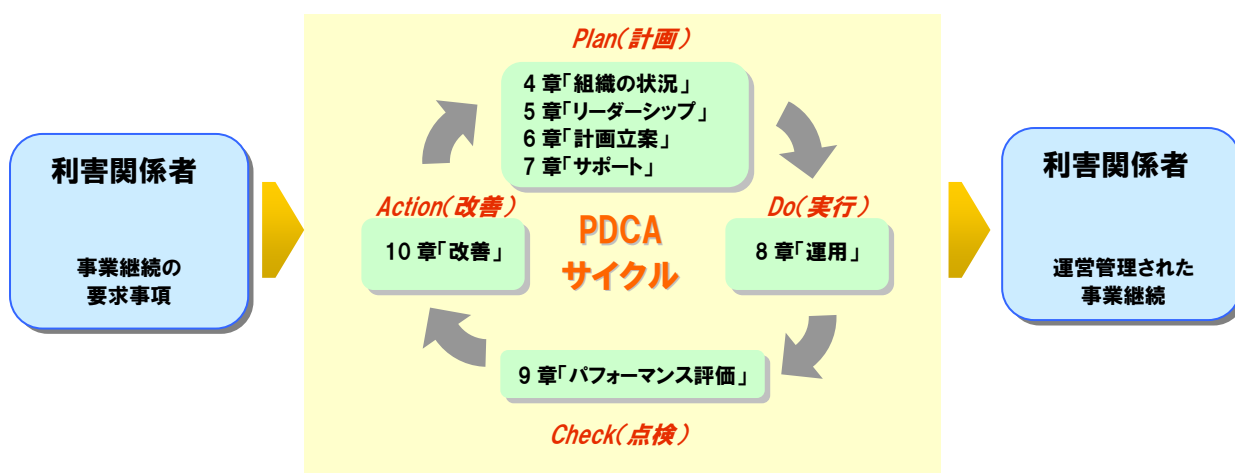
4. PDCA に当てはめると見えてくる ISO22301 全 10 章

ISO22301 は以下の全 10 章からなり、このうち規格要求事項は 4 章から 10 章となります。

序文	
1 章. 適用範囲	(この規格が適用できる組織について記載)
2 章. 引用規格	(この規格内で引用している他規格)
3 章. 用語および定義	(この規格内で使用されている用語の説明)
4 章. 組織の状況	
5 章. リーダーシップ	
6 章. 計画立案	
7 章. サポート	
8 章. 運用	
9 章. パフォーマンスの評価	
10 章. 改善	

ISO22301 の規格は、マネジメントシステムの基本である PDCA サイクルを意識して読んでいくと、非常に分かりやすくなります。

ISO22301 の規格の各章を PDCA サイクルに当てはめると、以下の図になります。



Plan 「計画のプロセス」

4 章「組織の状況」には、事業継続の一般要求事項となります。

5 章「リーダーシップ」は、事業継続の方針に関して記述されています。

6 章「計画立案」は、事業継続の計画に関して記述されています。

7 章「サポート」は、BCMS の運用を支える仕組みに関して記述されています。

Do 「実行のプロセス」

8 章「運用」には、事業継続の運用に関して記述されています。

Check 「点検のプロセス」

9 章「パフォーマンスの評価」には、事業継続の点検に関して、評価方法が記述されています。

Action 「改善のプロセス」

10 章「改善」には、事業継続の維持・改善に関して記述されています。

5. ISO22301 構築の鍵は 8 章「運用」にあり

ISO22301 の規格の中身の大部分は、マネジメントシステム全般に共通で求められる記述となっています。しかしながら、8 章「運用」に関しては、BCMS 独自の記述がされており、ISO22301 構築の鍵となると言えます。

8 章の構成は、以下の図のとおりとなっています。

8. 運用	8.1 運用の計画立案及び管理	
	8.2 事業インパクト分析及びリスク評価	8.2.1 一般
		8.2.2 事業インパクト分析
		8.2.3 リスク評価
	8.3 事業継続の戦略	8.3.1 決定及び選択
		8.3.2 経営資源の確立
		8.3.3 保護及び軽減
	8.4 事業継続の手順の確立及び実施	8.4.1 一般
		8.4.2 インシデント対応体制
		8.4.3 警告及びコミュニケーション
		8.4.4 事業継続対策
		8.4.5 復旧
	8.5 演習及び試験	

8 章では、組織が事業継続計画（BCP）を経営方針に沿った形で策定・導入・維持していくための内容を記述しています。具体的には、BCP を運用するための計画の立案が 8.1 章に記述されており、事業継続の影響およびリスク評価が 8.2 章に記述されています。

また、8.2 章の分析結果に基づく戦略の決定が 8.3 章に記述されており、その戦略を基にした BCP の手順が 8.4 章に記述され、事業継続計画の実効性を検証する為の演習及び試験が 8.5 章に記述されています。

このように 8 章全体には BCP 運用のための PDCA に沿った記述がされており、運用自体の見直しの仕組みが入っているのです。ここに記述されている要求事項をどのように読み取り、マネジメントシステムの構築に反映していくかは、ISO22301 の導入に向けた重要な検討事項といえるでしょう。

6. ISO22301 認証取得に役立つ参考ガイドライン

ISO22301 は、BCMS に関する要求事項であり、第三者（審査機関）のお墨付きをもらうためには、ISO22301 に記述されている要求事項の内容を満たす必要があります。

しかし、要求事項の記述内容は簡潔であり、規格を読みなれていないと具体的にイメージしにくい場合もあります。そういう場合に参考になる物を以下に記します。

- ISO22301 のガイドラインとして、ISO22313 が策定されています（現在は、DIS 版として刊行）。
ここには、具体的な事例が数多く記述されているので、自分たちの組織に当てはまりそうな事項を選んで採用すると、非常に参考になります。
- ICT-BCP のガイドラインとして、ISO/IEC27031 が策定されています。
ここには、ICT の具体的な指針が記載されており、システムの対策に非常に参考になります。
- ICT の障害復旧のガイドラインとして、ISO/IEC24762 が策定されています。
ここには、ICT の障害復旧の具体的な指針が記載されており、システム障害復旧対策の検討に非常に参考になります。
- ISO22301 構築後内部監査を行う際の指針として、ISO19011「マネジメントシステム監査のための指針」が策定されています。
- ISO22301 のリスクマネジメントを行う際の指針として、ISO31000「リスクマネジメントー原則および指針」、ISO/IEC31010「リスクマネジメントーリスクアセスメント技法」が策定されており、リスク分析を行う際の参考になります。

7. ISO22301 認証取得のための 15 ポイント

1	BCMS に影響を与える内部要因、外部要因を特定し文書化する。
2	BCMS の適用範囲について明確な定義をし、適用範囲外に関する説明を行い文書化する。
3	BCMS の適用範囲決定の際に、境界、適用性を明確にして、外部及び内部の利害関係者とのコミュニケーションについて考慮する。
4	BCMS の目標に関して、目標を達成するために組織が許容できる最低レベルの製品及びサービスを考慮する。
5	委託先管理として、外部委託されたプロセスを管理することが必要。その際、外部委託先の事業継続の実現能力を評価する。
6	リスクアセスメントは、地震だけでなく、様々なリスク分析を行う。
7	事業影響分析の際、組織としてぎりぎり受容可能なレベルで再開させる目標時間（枠）を設定。
8	事業影響分析の際、事業活動の依存関係及び活動を支えるリソースを特定することが必要。
9	戦略を実行するために必要なリソース要件を決定する際、次のリソースを考慮すること。 （人員、情報とデータ、建物や仕事環境、関連ユーティリティ、設備、ICT システム、交通、財務、パートナーやサプライヤ）
10	対応が必要となるリスクに対して、次の備えを検討する。 （中断の可能性を軽減する、中断時間の短縮を図る、主要製品・サービスの中断の影響を限定する）
11	組織内の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手段の確立と可用性の保証。
12	演習及び試験に関して、明確な目標の下で、適切なシナリオで実施する。
13	様々な演習を実施し、事業継続の取り組みの妥当性を確認する。
14	インシデント（事業を中断させる事象）対応として、利害関係者や当局、メディアとのコミュニケーションを図る。
15	インシデント対応体制として、適切な責任、権限および力量を持った人員を起用する。

付録 1：よくある BCMS、BCP の失敗の原因

BCMS が周知できていない

- ・社員のセキュリティ意識が低い
- ・BCMS 文書が手に負えないほど膨大だ
- ・管理のためだけの BCMS になっている

BCMS は構築作業が膨大だ

- ・最初から高すぎるビジネス影響分析の精度を求めている
- ・最初から高水準の BCP を求めている
- ・最初から広すぎる適用範囲にしている

BCP 対策の実効性が乏しい

- ・不必要な BCP 対策を実施している
- ・過剰な水準の BCP 対策を実施している
- ・利便性とのバランスが十分確保できていない



弊社では、このようなことがないように、豊富なコンサルティング実績から得られた経験と独自のノウハウに基づき、“無理、無駄”なく最小限の工数で御社にとって最適な BCMS のプロセス構築及び BCMS プロセスの定着を実現します。

付録2 弊社サービスの特長

【1】 マネジメント系構築支援コンサルティングの実績が豊富です

- ・ 製造業、IT 系 Sier、データセンター、地方自治体等、多種多様な業界におけるコンサル実績があります
- ・ 数十人から数百人まで、様々な規模のコンサル実績があります
- ・ ISMS 適合性評価制度のパイロット時代(2001 年～)から蓄積した豊富なノウハウを保有しています

【2】 効率的に BCMS を構築できます

- ・ 豊富な実績とノウハウから導いた BCMS 構築支援ツールをご提供します
- ・ 既存のマネジメントシステム(QMS、EMS、ISMS 等)との整合を考慮した BCMS 構築が可能です
- ・ マネジメント対策、技術対策の双方からのアプローチが可能です
- ・ IT ベンダーとして、NEC の総合力を発揮した具体的な BCMS 対策のご提案が可能です

【3】 BCMS 審査のノウハウが豊富です

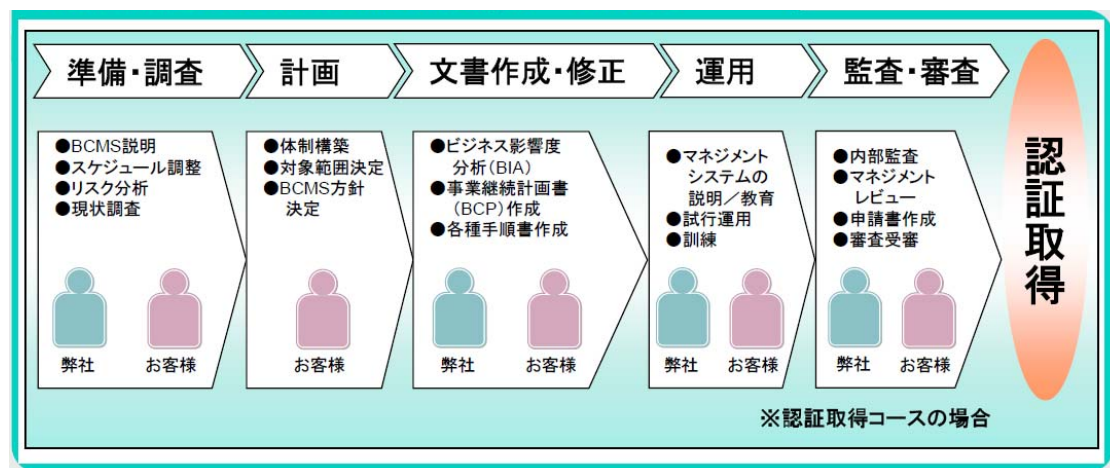
- ・ マネジメント審査員資格を保有するコンサルタントが対応するため、審査員視点でのご支援が可能です
- ・ BCMS 認証機関を問わず対応が可能です
- ・ ISMS 認証機関、及び ISMS 審査員研修コースの立ち上げに携わった実績があります

【4】 認証取得後にご満足いただいております

- ・ 組織内における、BCMS 認証範囲拡大の実績があります
- ・ 内部監査支援、教育支援、訓練支援、審査立会い等、運用開始後のご支援も承っております

付録3 資料

■ 資料1 一般的な認証取得スケジュールです。



既に ISO/IEC27001 等のマネジメント認証を取得済みの場合は、ISMS 等のマネジメント運用体制を活用することで、さらにスムーズな取り組みが可能です。ご相談ください。

■ 資料2 弊社サービスについて簡単にまとめたパンフをご用意しています。



<http://www.nec-solutioninnovators.co.jp/sl/bcp/download/>よりダウンロードいただけます。

本資料の詳細につきましては、下記までお問い合わせください。

NEC ソリューションイノベータ株式会社

プラットフォーム事業本部 第四ソフトウェア事業部

担当者 : 森 徳行、角道 淳平、奥 はる奈

TEL : 044-435-8279

E-Mail : bcp-dl@mls.necst.nec.co.jp

URL : <http://www.nec-solutioninnovators.co.jp/sl/bcp/>

第 2 版 2014 年 4 月 1 日