１８－Ｈ００６

事業継続管理（BCM）に関する調査報告書
－BCM(BS25999)と関連領域の整理－

関連領域：RM,内部統制,CSR,IT ガバナンス,情報セキュリティ

平成 19 年 3 月

財団法人　日本情報処理開発協会

この事業は、競輪の補助金を受けて実施したものです。
http://keirin.jp

はじめに

この報告書は、財団法人日本情報処理開発協会が日本自転車振興会の補助金を受けて実施した平成１８年度情報化の進展に関する補助事業「情報セキュリティ基盤の強化に関する調査研究」事業の一環として取りまとめたものである。

企業などの組織活動において、IT依存度はかつてないほど高くかつ重要になっている。そのような状況下、「情報」の処理・流通・保管の形態については紙の文書やソフトウェアなどさまざまな形態があり、情報セキュリティへの取組みがますます重要となる。

情報資産の保護という情報セキュリティマネジメントの目的を達成するには、多様化するリスクについて、顕在化させないための予防策と同様に、顕在化した場合にできるだけ損失を小さくする事故対応策を考えておく必要である。特に事故対応策の中でも事業のサステナビリティへの影響を考慮し、事前に事業の継続計画を策定しておく「BCP（事業継続計画）」及びそれをマネジメントにおいて実践するBCM（事業継続管理や事業継続経営と訳される）に焦点を当て、適切な情報保護資産の保護のあり方について調査研究することは重要であり、情報セキュリティマネジメントの中でBCMの位置付けは非常に大きい。

2006年11月に、BCMに関する英国規格（BS25999-1）が英国規格協会から発行された。英国規格・国際標準に携わる者やリスクマネジメントの専門家、実務者、さらには経営者のBCMに対する関心が益々高まるであろう。BS25999-1は、BCMに取り組み始めた企業がガイドラインとして活用したり、既存のBCMの仕組みが有効であるかを検証するのに有効である。

本調査研究では、BS25999-1の概要を取り纏めるとともに、BCMと「リスクマネジメントや内部統制、CSR（企業の社会的責任）、ITガバナンス、情報セキュリティ」の関係性を整理し、今後のBCMの取り組みに関する知見についてまとめた。さらに、BCMと上記に挙げた他領域の取り組みにおいて、共通事項を明確にすることができた。

我が国における企業など組織におけるBCMの取組を推進させ、そして他領域との総合的かつ統合的な取り組みについてシナジーを出せるよう、今後の諸活動の一助となれば幸いである。

本報告書の作成にあたり、ご協力を頂いた委員の皆様をはじめ関係各位に対し厚く御礼申し上げる。

平成19年3月

情報セキュリティ専門部会
財団法人日本情報処理開発協会

目　次

Ⅰ部　各領域の整理

第１章　ＢＣＭ（事業継続経営）

１.１　はじめに

現在、欧米・アジアなど世界的に多くの企業がBCM(Business Continuity Management；事業継続経営、事業継続マネジメントなどと訳す)の重要性を認識して、取組みを進めている。

BCMに取り組む理由は、以下のようなことが考えられる。

- 企業・組織の存続を守ること（リスクマネジメントの一環）
- 取引先からの要請（現在はBCMを取引先選別基準として活用、また他社との差別化に変貌）
- 政府・官公庁からの要請
- コーポレートガバナンスやSR（社会的責任）の一環
- 企業価値の向上　　など

様々な理由のもとに企業や政府・官公庁はBCMに取り組んできたが、取り組み方について、これまで世界的に統一されたガイドライン・規格は存在しておらず、企業は独自にガイドラインを選択し、若しくはいくつかのガイドラインを取り込んでBCMを構築していた。

このような中で注目したいのが、2006年11月に発行されたBCMの英国規格BS25999-1(British Standard, Business Continuity management - Code of practice)である。英国でも本規格に対する関心は高く、テレビ、各種ホームページなどで取り上げられている。現在、日本でもBS25999-1に関心が高まりつつあり、同規格の取得に動く企業も現れると考えられる。

また、一方でISO（国際標準）化の動きもあるが、BS25999-1は、国際標準の有力な候補でもある。

１.２　英国における国家規格化の流れ　～BS25999-1発行の経緯～

英国では、BCMの国家規格(British Standards)化の取り組みが早くから行われてきた。その推進役を果たしているのが、英国規格協会(British Standards Institution;以下BSI)である。1901年に設立されたBSIは、英国におけるビジネスや社会の要望を満たす規格の開発を行っている組織で、その活動は英国規格の開発のみならず、欧州規格及びISOといった国際規格の開発にまで影響を与えています。BSIはこれまでに、品質マネジメント規格ISO9001のベースとなったBS5750や、環境マネジメントシステム規格ISO14001のベースとなったBS7750等の規格を作成している。実にBSI発行の規格の95%が国際規格／ISOの原案として採用されている。従い、BSIで発行された規格が常にISOの最有力候補であると言われる所以である。

英国規格協会から発行されたBS25999は２つのパートに分かれる。BS25999-1(Code of Practice)はBCMの実践規範であり、BS25999-2は、認証のための規格になる見込みである。BS25999-1は2006年11月28日に発行され、BCMの定義やBCM取り組みのフレームワーク、及び取組み方法を示した。BS25999-2については現在英国内で議論が始まっており、2007年7月に発行され、企業監査条件、チェックポイントが規定される予定だ。BS25999-2が認証のための規格となれば、英国企業は、他のマネジメントシステムの取得同様にこぞって認証を取得すること及び他国の取引企業に認証取得を要求することが想定される。

また、ITの継続性に特化した規格についても、2006年8月に英国規格協会から、PAS77（IT Service Continuity）を発表するなど、IT分野でも具体的なアプローチが展開されている。

さて、BS25999-1のベースになったのは、BCI(The Business Continuity Institute；事業継続協会)が発行したBCI Good Practice Guidelines（実践的なガイドライン)、米国のガイドラインNFPA1600、シンガポールの規格など世界で発行されているガイドラインである。これまでの経緯を以下の通り整理する。

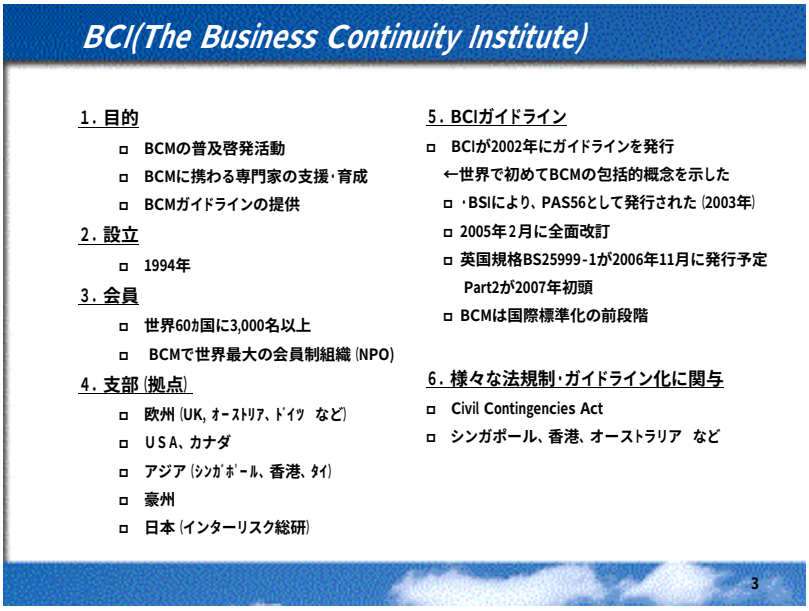
２００２年	BCIがGood Practice Guidelines（実践的なガイドライン）を発行。世界で始めてBCMに関する包括的な概念・考え方を示した。
２００３年	英国規格協会（BSI）がBCIのGood Practice GuidelinesをベースにPAS56を発表。（英国では、実質BCMが英国規格前であることを世界に示した。 PAS56は欧州で「規格のベストセラー」と言われ、日本でもは日本規格協会から日本語版が発行された）
２００５年	BCIのGood Practice Guidelinesを政府・官公庁、主要産業界に活用してもらい、そのフィードバックを受け、BCIが同ガイドラインを全面改訂。 BCMのノウハウの集大成と言われる。
２００６年 ６月～８月	英国規格協会が、BS25999-1のドラフトを作成し、パブリックコメントにかける。
２００６年 １１月	英国規格協会からBS25999-1が正式発行される。本規格をISOに国際標準として活用するよう提案。

BS25999-1のドラフト作成から正式な発行までは、BSIのもと委員会が立ち上がり、英国政府（DTI、FSA)、BCI、AIRMIC（欧州のリスクマネジメント団体)、主要な産業界のメンバー約35名で幾度も議論が行われた。

また､BS25999-1とは直接関係ないが､英国では､2004年11月に｢Civil Contingencies Act｣が施行された。これは、BCMを観点として、地方行政が如何に国民に対し、サービス・業務の提供を継続していくかという有事法制である。ユーティリティ企業や病院、防災に関する企業などはBCPを予め策定する必要がある。

なお、参考までにBS25999-1のベースとなるガイドラインを策定したBCIの概要を以下に記す。

BCIは、BCMに特化した世界最大のNPOであり、全世界でその活動を展開している。



今後、BSIとBCIは、BCMの教育・資格の分野で提携することになっており、この動きも世界的に展開されるであろうから動向を注目したいところである。

１.３　ＢＳ２５９９９の内容

BS25999-1の目的は、「組織内におけるBCMの理解、発展、及び実施の基礎となること」及び「企業間取引及び顧客と企業間の取引を確かなものにする」ことである。本BS規格は、その上で組織は共通認識のもとに同一の手法によってBCMの実効性について推し量ることが可能となるとしている。規格の適用範囲については、最高責任者や取締役会を構成する経営層から、現場レベルの業務担当者まで全てのレベルを対象としている。また、組織の規模も、巨大なグローバル企業から中堅・中小企業、個人事業主まであらゆるレベルのものを対象としている。つまり、あらゆる階層、あらゆる組織が対象である。

１.３.１　ＢＣＭの定義

BCP・BCM は世界的に様々な定義が唱えられているが、英国規格協会 BS25999-1 による定義は、以下の通りである。

ＢＣ	事前に定義されたレベルで事業を継続するために、事故や事業停止に対して計画を立て対応するための、組織の戦略的および戦術的な能力。
ＢＣＰ (Business Continuity Plan)	組織が重要な製品やサービスを供給できるよう、事故時の使用に備えて開発、維持され文書化された一連の手順や情報。
ＢＣＰ (Business Continuity Management Programme)	潜在的な損失による影響を評価し、実行可能な復旧戦略や計画を維持し、トレーニング、演習、維持、保証を通して製品／サービスを継続できるために必要な方策を確実に講じられるようリソースが提供され、トップマネジメントによってサポートされる継続的な管理および統制のプロセス。
ＢＣＭ (Business Continuity Management)	組織を脅かす潜在的なインパクトを認識し、その脅威が現実となった場合に引き起こされる事業運営への影響を特定する包括的なマネジメント・プロセス。このプロセスにより、組織の主要な利害関係者の利益や、組織の名声、ブランド、および価値を創造する活動を守るために効果的に対処できるようになり、組織の回復力を構築するためのフレームワークが提供される。 注：　BCM には、事故が起きた場合の復旧または継続の管理や、事業継続計画を最新の状態に保てるようにする、トレーニング、リハーサル、およびレビューを通しての全体的なプログラムの管理も含まれる

BCP と BCM の違いを整理したい。BCP は Business Continuity Plan の略であり、事業継続計画と訳され、「計画」自体を指す。一方、BCM は BCP を活用して、如何に BCM を企業内に浸透させていくか、戦略的に活用していくかというマネジメント自体を指す。

つまり、BCM は、事故や災害などが発生した際に、「如何に事業を継続させるか」若しくは「如何に事業を目標として設定した時間内に再開させるか」についてあらゆる観点から対策を講じることである。このためには、マネジメントシステムの構築や組織への BCM 文化の構築や浸透が非常に重要となる。

１.３.２　ＢＳ２５９９９－１の構成

ＢＳ２５９９９－１の構成は以下の通りである。

BCM の構築、展開などについて、整然と分り易く記載されているのが特徴である。

２章、３章では、BCM を「組織を脅かす潜在的なインパクトを認識し、利害関係者の利益、名声、ブランド、及び価値創造活動を守るため、復旧力及び対応力を構築するための有効な対応を行うフレームワーク、包括的なマネジメントプロセス」と定義している。4～6章では､PDCAサイクルに基づくマネジメントシステムとしてのBCMが説明されている。また、責任の明確化、プロジェクトマネジメントの進め方、既存のマネジメントプロセスとの関係、BCM 関連文書などの管理などについても記載されている。

章	項　目	内　容
１	スコープと適用性	BS25999-1 は、組織内で BCM を構築・展開・実装するための一貫した手法を提供し、BCM の能力を高めることを目的としていることを記載。
２	用語の定義	BCM や BCP、リスクマネジメントなどが定義
３	BCM の概観	BCM と組織戦略の関係、BCM とリスクマネジメントとの関係、BCM の成果物、BCM のライフサイクル
４	BCM の方針	本方針は、BCM に関する活動が確実に実施されることを示す文書である。
５	BCM プログラムマネジメント	BCM を推進するにあたってのプログラムマネジメント－責任の明確化、ステークホールダーとの連携　などが記載
６	組織の理解	ビジネスインパクト分析、重要なアクティビティ、事業継続にあたっての要求事項、リスク評価　などが記載
７	事業継続戦略の決定	戦略的なオプション－キーパーソン、サイト、技術、情報、取引先、ステークホールダー
８	BCM を実現する手法の開発と実装	組織体制、BCP など計画に含めるべき項目
９	BCM への取組みに関する訓練、継続的改善、及びレビュー	訓練プログラム、維持管理、レビューの手法　など
１０	BCM の組織文化への導入	アウェアネス、スタッフのスキル向上

１.３.３　BCM 構築・確立のためのプログラムマネジメント

BCM を構築・維持に関するマネジメントプロセスは、以下の通りである。以下プロセスの特徴は、全産業界、政府・官公庁などすべての種類に対応できるものであり、フレキシビリティを保たせながら、BCM の構築ができると考えられる。

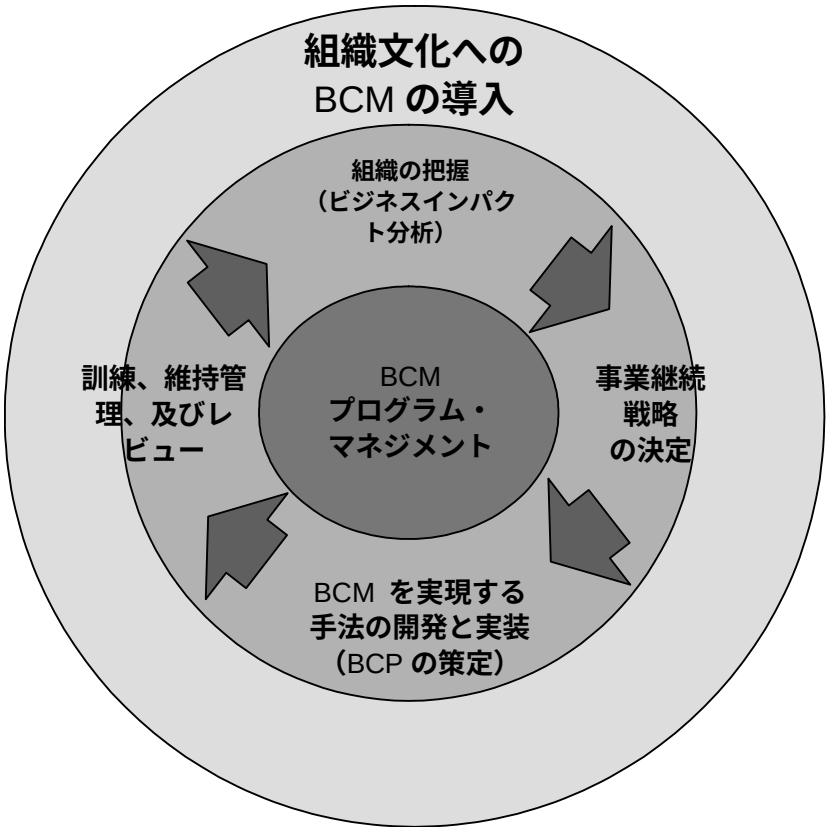


図 1-3　BCM プログラムマネジメント

プログラムマネジメントは、BCM の能力を、組織の大きさと複雑さに適した方法で、構築および維持することであり、具体的には、以下に述べるステージ１～４を継続的に実施することである。

記各フェーズの説明は以下の通りである。

	項　目	目的・結果
ステージ１	組織の理解 （ビジネスインパクト分析を中心に）	組織の重要な製品やサービス、およびそうした製品やサービスを提供するのに必要な活動とリソースについて説明する情報が得られる。
ステージ２	事業継続戦略の決定	一連の戦略や戦術的オプションを評価できる。そのため、重要な製品やサービスそれぞれに対して適切な対応を選択でき、組織が、混乱時および混乱後にも可能な運営レベルで、そうした製品とサービスを提供し続けることができる。組織内部にすでに存在しているレジリエンシーと対策のオプションが考慮される。
ステージ３	BCM を実現する手法の開発と実装	業務を復旧させるためにインシデント時およびインシデント後に取るべき手順を詳述した事業継続計画およびインシデントマネジメント計画を作成する。BCM の事前対策は、脅威による影響や脅威の可能性を排除または低減する。
ステージ４	訓練、維持管理、及びレビュー	BCM のトレーニング・継続的改善を行うことで、組織は、その戦略と計画が効果的で信頼でき目的に適っているものであることを示すことができる。
全ステージを通して	BCM の組織文化への導入	組織の文化に BCM を導入することで、BCM は組織の中心的価値の一部となり、すべてのステークホールダー（利害関係者）に自組織は大きな混乱に対処できるという確信・自身を与えることができる。

（１）プログラムマネジメント

BCM に関するプログラム・マネジメントは、以下事項から構成される。

① 責任の割り当て

- 経営層における責任者の任命
- BCM プログラムを推進する担当者の任命

② インプリメンテーション

- ステークホールダーとの連携
- トレーニングなどの実施

③ 継続的なマネジメントの実施

定期的なレビューや確認を実施。特に、事業環境の大きな変更やキーパーソン、新技術の開発などあった場合。

＜BCM関連文書例＞

a．BCMの方針
- ■　スコープステートメント（BCM適用範囲の宣言書）
- ■　BCM関連用語の定義

b．ビジネスインパクト分析
c．リスク評価分析
d．BCMに関する戦略
e．組織に所属する人間に対する意識向上プログラム
f．トレーニングプログラム
g．インシデントマネジメント計画
h．事業継続計画（Business Continuity Plan）
i．事業復旧計画（Business Recovery Plan）
j．演習計画
k．サービスレベルアグリーメント（SLA）

（２）組織の理解

① ビジネスインパクト分析

a）事業が停止した場合の影響を評価する。

b）次の項目を評価することで、各活動の最大許容停止時間を確立する。

■ 事業の継続ができなくなった後にその活動を再開する必要があるまでの最大許容停止時間

■ 事業の再開時における事業活動の最低レベル

■　事業を通常レベルまでに復旧させる時間

また、最大許容停止時間をベースにしながら、組織の戦略でもある目標復旧時間を設定していく。

② 重要なアクティビティの特定

組織は、事業復旧の優先順位に応じて活動する。ビジネスインパクト分析で特定されるとおり、損失によって短時間に最も大きな影響を与え、即座に復旧する必要がある活動（アクティビティ）を「重要なアクティビティ」とする。優先度の高い業務と依存関係にある他の業務の復旧についても事前に検討する必要がある。

③ 事業継続のためのリソースの確保

以下項目ごとに、事業継続のためにリソース確保を行う。

People	人数、スキル、知識
Premises	ワークサイト、設備を配備する場所
Technology	技術、機械設備　など
Information	システム、データ　など
Supplies	外部機関、取引先

④ リスク分析・評価

「重要なアクティビティ」に対してリスク評価の実施を行う。

参考までに、リスクマネジメントとBCMの違いを以下に示す。

	リスクマネジメント	ＢＣＭ
主な分析手法	リスク分析	ビジネスインパクト分析
主なパラメータ	影響度および可能性	影響度および時間
対象リスク	全てのリスク	重大な事業崩壊の原因となるリスク 若しくは、結果事象としてリスクに拘らない
リスクの規模	あらゆる規模	生存に脅威となるリスクのみ

（出典：BCIの「Good Practice Guidelines」）

（３）事業継続の戦略

事業継続に関する戦略は、「People」、「Premises」、「Technology」、「Information」、「Supplies」、「Stakeholders」について、以下を勘案しながら策定する。

- 重要業務の最大許容停止時間
- 費用
- 事業継続に対するアクションを何ら行わない場合の想定される結果

＜観点＞

リソース	戦略上の観点
People（キーパーソン）	組織のコアスキル、ノウハウを維持することが必要。対象は従業員だけでなく、関連会社、ステークホールダーにまで広げる。ドキュメントの管理、スタッフや関連会社などのスキル、ノウハウの分散、外部リソースの活用　など
Premises（サイト）	社内外の代替場所の活用
Technology （ITなどの技術）	事業復旧の目標復旧時間－事業の復旧にはITの復旧が必要であり、この依存度分析が必要 技術の地理的分散、リスク低減策の実施
Information（情報）	バイタルマネジメント（重要な情報の管理手法） 守秘性、利用可能性　など
Supplies（取引先）	中核事業を継続するために必要な重要な取引先の特定・対策実施で以下を含む。 ・　他場所における在庫の管理 ・　代替取引先のリストアップ－災害時などの対応の交渉 ・　倉庫や出荷場所の確保 ・　取引先の多様化 ・　取引先へのBCP策定要請 ・　SLAの締結　など
Stakeholders （ステークホールダー）	社会的責任を念頭に置いたステークホールダーの利益を守る

（４）ＢＣＭを実現する手法の開発と実装

① 組織体制の構築

② 計画の内容（前記「BCM関連文書例」参照）

a．全ての計画に共通するもの

- 目的とスコープ
- 役割と責任
- 計画の発動
- 計画の管理者
- 連絡先

b．インシデントマネジメント計画

内容は以下の通り。

- 災害など発生直後のタスクとアクションリスト
- 緊急時の連絡先
- メディア対応
- ステークホールダーへの対応　など

c．ＢＣＰ（事業継続計画）

- タスクとアクションリスト
- リソース（「People」、「Premises」、「Technology」、「Information」、「Supplies」、「Stakeholders」への対応）の特定と配分
- 責任者　など

（５）ＢＣＭへの取組みに関する訓練、維持管理、及びレビュー

① 訓練に関するプログラムの策定

② 机上訓練、ウォークスルー、シミュレーション、フルのBCPの訓練

③ 監査や自己評価に関する方法

（６）ＢＣＭの組織文化への導入

BCM 文化を組織内において構築、推進、および導入すると、その文化が組織の中心的価値および効果的なマネジメントの一部となる。

BCM 文化により、組織が次のことを行うことができる。

- BCM プログラムをより効率的に開発・運営できる。
- 混乱に対処する能力に関して、ステークホールダー（利害関係者）（特にスタッフと顧客）に自信を植えつける。
- すべてのレベルでの判断で BCM が検討され、時間の経過とともに組織のレジリエンシー（脅威に対する対応・復旧力）が増加する。
- 混乱による影響と混乱の発生可能性を最小限に抑える。

手法としては、アウェアネスプログラム、トレーニングなどが挙げられる。

１.３.４　ＢＣＭ監査と自己監査

BCM 監査の目的は、組織の BCM の力量と能力をレビューし、それらを規格および基準と照らし合わせて検証することである。監査には主に次の 2 つの機能がある。

(1) 組織の BCM 方針を順守することで、適用する法律、規格、戦略、フレームワーク、および優良実践例ガイドラインについても順守が保証されることを検証する。

(2) 主な欠点や課題を明らかにし、その解決を保証する。

監査活動の頻度とタイミングは、組織の大きさ、性質、および法的状況に応じて、法律および規定の影響を受けることがある。また、ステークホールダー（利害関係者）からの要求にも影響を受ける場合がある。

組織は、実際の欠点および潜在的な欠点を特定するために BCM の独立監査を提供すべきである。また、そうした欠点に対処するための手順も構築、実装、および保守すべきである。

組織の BCM プログラムの監査では、次のことを検証すべきである。

- すべての重要な生産物とサービス、それらが依存する活動、およびサポート・リソースが、組織の BCM 戦略に特定され記載されていること。
- 組織の BCM 方針、戦略、フレームワーク、および計画がその優先順位と要件を正確に反映し続けていること。
- 組織の BCM の力量と BCM 能力が効果的で目的に適っており、そうした力量や能力によって BCM インシデントの管理、統御、統制、および調整が可能になること。
- 組織の BCM ソリューションが有効、最新、かつ目的に適っており、組織が直面してい

るリスク・レベルに適していること。

- **組織の BCM 保守および演習プログラムが効果的に実装されていること。**
- **BCM 戦略と計画には、演習後の報告書に記載されているとおり、演習により学習した教訓と、保守プログラムから発生した修正が組み込まれていること。**
- **組織には、BCM のトレーニングを行ったり BCM を認識するための継続的なプログラムがあること。**
- **変更管理プロセスが配置されており、効果的に動作していること。**

１.４　日本と世界の動向

（１）ＩＳＯ化への動向

国際標準（ISO）化へ目を向ける。

国際標準化機構では、企業や自治体などの緊急時対応（Emergency Preparedness）について、国際標準化されることが決定し、2006 年４月に米国で第一回の国際会議が開催され 13 カ国からの出席者により様々な観点で議論が行われた。この会議に先立ち、英国（当初 PAS56、現在は BS25999 を提案）、米国・カナダ(NFPA1600)、オーストラリア(HB221)、イスラエル、日本が ISO のドラフトを掲示した。中でも英国の BS25999 は、ISO へ大きな影響力を持っていると考えられており、その意味でも、今後の動向には注視する必要がある。

現在、ISO では，BCM の ISO 化について議論するため、正式に TC（技術委員会）２２３委員会を立ち上げている。図１-4 が ISO における体制である。TC223 では、Society Security（社会セキュリティ）を所管し、同分野における国際標準を議論する。TC223 は、「技術的、人的、組織的かつ機能的な相互運用性を向上させ、状況を関係者全員が共通して認識することで、危機管理能力及び事業継続能力を向上させること」を目的とし、BCM はこの社会セキュリティの一環で議論をされている。特に WG１（ワーキンググループ１）の傘下におかれる TG１（タスク・グループ１）では上記 5 ヶ国から提出された原案を統合したものをベースに最終原案を策定，2006 年 11 月の委員会で審議される。現在のスケジュールでは、2008 年～2009 年頃に BCM の ISO 化が実現すると言われている。

図 1-4　ISO/TC223 の構成

なお、現状として、ISOでは、公的機関にはBusinessという言葉が馴染まないとして、表現は、「Incident Preparedness and Operational Continuity Management」と呼称されている。

（２）日本の動き

日本の動向としては、経済産業省が 2005 年３月に「事業継続策定ガイドライン」を発表

した。また、内閣府・中央防災会議の「民間と市場の力を活かした防災力向上に関する専門委員会」の中で「企業評価・業務継続ワーキンググループ」を設置し、2005 年８月に事業継続ガイドラインを発表、現在、同ガイドラインの解説書を策定している。中小企業庁でも、BCP に関する委員会を設置し、2006 年２月に中小企業を対象とした BCM 構築の指針を発表した。日本政府・官公庁では日本のあらゆる規模の全産業に BCM に取組んでもらう環境・インフラ作りにつとめている。金融機関においては、日本銀行が 2003 年 7 月に民間金融機関を対象にして「金融機関における業務継続体制の整備」についての報告書を取りまとめている。これは民間金融機関にも業務継続体制を整えるよう求める内容である。日本規格協会でも 2004 年 6 月に「事業継続管理のための指針」と題して、PAS56 を翻訳・発行し、日本で初めて BCM に関するガイドラインを発行した。

このように日本では、BCM に関するガイドラインが政府・官公庁を中心に発行されるなど、今後日本で BCM に関する動きがさらに活発化してくると考えられる。

＜参考：日本の政府・官公庁等におけるBCM関係委員会＞

機　関	委員会等
経済産業省	企業における情報セキュリティガバナンスのあり方に関する研究会　事業継続計画策定ガイドライン　ワーキンググループ
経済産業省	BCP 国際標準化委員会
中小企業庁	BCP 有識者会議
内閣府中央防災会議	民間と市場の力を活かした防災力向上に関する専門調査会　企業評価・業務継続ワーキンググループ
内閣府中央防災会議	企業等の事業継続・防災評価検討委員会
(財)情報処理相互運用技術協会	高可用性システム技術委員会（旧ビジネス継続性技術委員会）
(財)日本情報処理開発協会	マネジメントシステム評価検討委員会
(財)日本情報処理開発協会	情報セキュリティ専門部会

１.５　まとめ

以下の図は、BCMと企業価値の関係を示したものである。世界で発生した25の大事故・災害・事件における企業の株価を分析した結果である。横軸に時間、縦軸に株価を示し、25企業の株価を「事業継続が迅速にできた企業」と「事業継続が迅速にできなかった企業」の２種類にグルーピング化して、株価を調査した（分析の過程では、純粋な市場の変動要因は除外している)。共通することは、「事業継続が迅速にできた企業」と「事業継続が迅速にできなかった企業」共に、大事故・災害・事件発生後５日間は株価が下がっている。その後、「事業継続が迅速にできた企業」は、株価は上昇に転じ、最大で25%増、また250日後でも10%増の株価上昇を得ている。一方、「事業継続が迅速にできなかった企業」の場合、株価は下落を続け、250日後も15%減少した。ここで、判明していることは、株価に最も影響を与えるバリュードライバーは、経営者の発言であり、行動であった。

事業継続を妨げるリスクは様々であり、かつ鳥インフルエンザやノロウィルスに代表

されるような事業を停止させ得る新たなリスクが出現することが考えられる。以下の図に示す分析では、経営者自ら、先頭に立ちBCMに取り組まなければならないことを示している。事業継続上、何が脆弱(ボトルネック)であり、それが機能しなくなった場合に、「どう対策を打つべきか」、「事業継続が困難になった場合にどう行動すべきかというBCP策定」を日頃から検討・対策を進めておく必要がある。これらＢＣＭを体系的に戦略的に、そして総合的に進めることを示した規格がBS25999 といえよう。

図1-5　事業継続の分析例

現在、世界各国でガイドライン・規格化が進められ、加えISOによる国際標準化が進められている。企業などの関心は益々高まることが予想される。企業は、ISO化を待たずして、可能な範囲で早期にマネジメントシステムとしてBCMの取組みに着手し、ステップバイステップで構築していくことが求められよう。そして自主的にBCMを経営戦略として捉え、従業員含めたBCM企業文化の構築し、また災害・事故・事件に強い企業文化を育てることができるかどうかが、企業価値の向上を大きく左右することになる。

第２章　リスクマネジメントについて

２.１　リスクマネジメントの定義

(1) リスクマネジメントの概念

リスクマネジメントに関する概念は、今日の日本において、必ずしも画一的に確立されたものではない。そもそもの発祥の地である欧米においても、立場によって、その範囲を広く解釈したり、狭く解釈したりすることがある。

「マネジメント」と言うからには、様々な形態や方式があってもおかしくはない訳であるし、企業の経営方法が変化すれば、「リスクをどう管理するか」に対する考え方が変化するのも当然である。

一方、対象とするリスクの範囲、組織や職務分担などは、マネジメントを行う主体（企業や団体、あるいは個人）によって異なっても、これらの主体が安定して事業（生活）を継続・発展させていくためには、損失を発生させる様々なリスクに対して適切に対処する必要がある。企業にしても個人にしても、その活動を狂わせるものはリスクであり、リスクへの対処が不適切であれば、思い切った行動を阻害したり、過大なコストがかかったり、無防備から破綻をきたすことも十分にあり得る。この様な障害を完全に無くすことは不可能であるが、よりよい対処方法を考え、経営（生活設計）に生かすことが当然に求められる。そのための管理が「リスクマネジメント」である。また、管理をするということは、当然にコストも管理しなければならない。所要コストの比較により、最も効果的な対策を講じていくことが重要になる。

以上より、「リスクマネジメント」は次のように説明できる。

> リスクに対して、最小かつ経常化されたコストで、適切な処理を行い、 安定した経営を行うための管理手法

(2)リスクマネジメントの定義

上記(1)にてリスクマネジメントの概念を説明したが、ではリスクマネジメントはどのように定義できるのであろうか。ここでも、いろいろな学者、コンサルティング会社、リスクマネジメント機関等が独自の「定義」を披露しているが、ここでは以下の通り定義付ける。

> 企業を取り巻く様々なリスクを予見し、そのリスクがもたらす損失を予防するための対策や不幸にして損失が発生した場合の事故処理対策などを効果的・効率的に講じることによって、事業の継続と安定的発展を確保していく企業経営上の手法

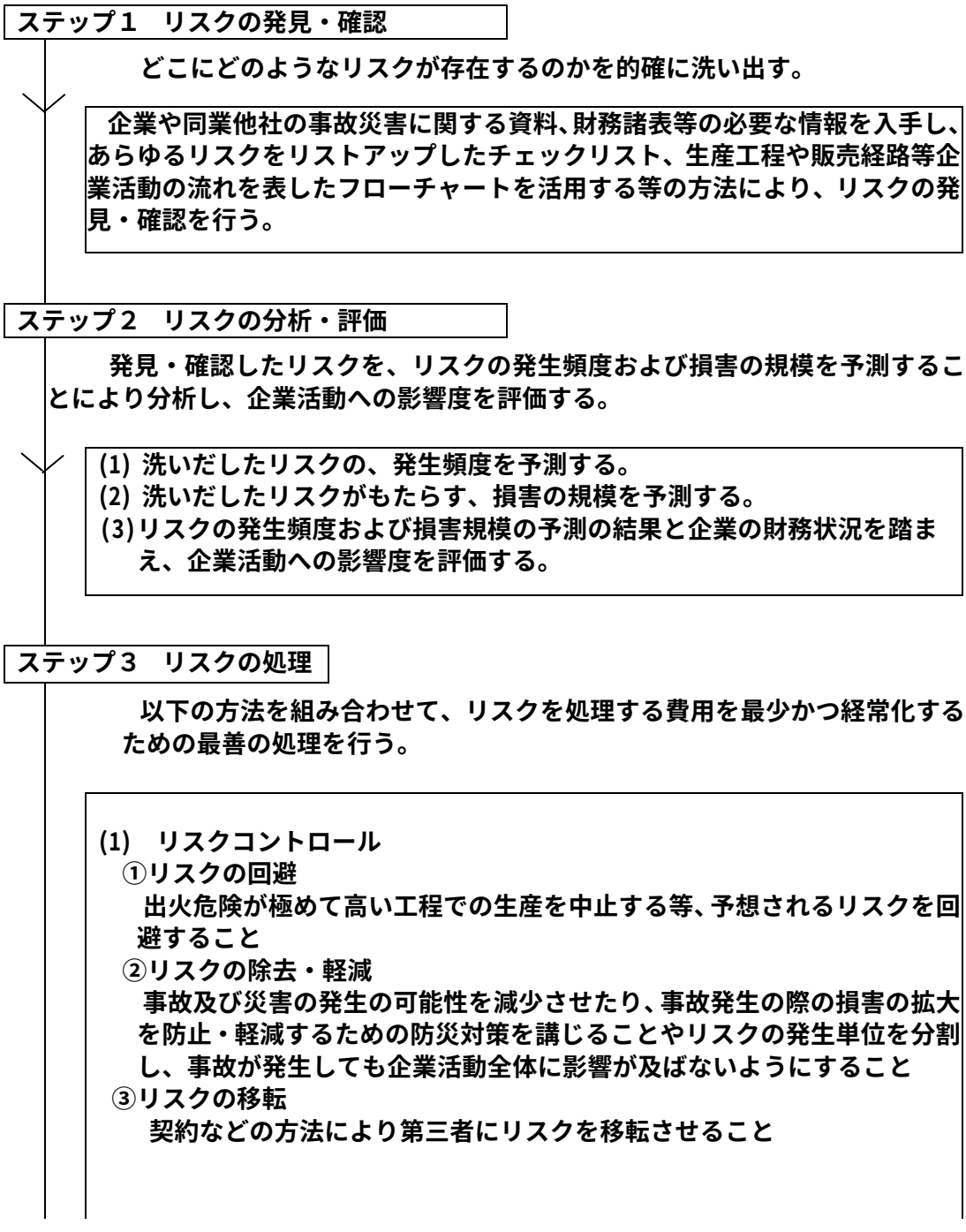
多くの場合、「事業の継続」と「安定的発展」が企業目的であることは論を待たないであろう。この企業目的を達成するために様々な「予防策」と「事後処理対策」を講じていくことがリスクマネジメントであり、見方を変えれば、リスクマネジメントは企業

経営そのものに他ならない。

２.２　リスクマネジメントのプロセス

(1) ４つのステップ

リスクマネジメントの基本的なプロセスは、以下のとおりである。(「リスクの処理」を「リスク処理方法の選択」と「リスク処理方法の実施」に分け、全体を５つのステップに整理するやり方もありうる。)



(2)　リスクファイナンシング
①リスクの保有
各種準備金の積立、自家保険等、損害が発生した場合、企業自身で負担すること
②リスクの転嫁（保険等の利用）
保険等を利用し、第三者に損害を転嫁すること

ステップ４　結果の検証

事故データ、保険データ、安全防災対策の実施状況を検証し、リスクの処理手段の見直し、安全防災対策の見直しを行う。

(2)リスクの発見・確認（洗い出し）

リスクの発見・確認をする上で重要なことは、自社の業務内容を正確に把握した上で存在するリスクを漏れなく探し出し、見逃さないようにすることである。

近年、技術革新や企業活動のグローバル化等に伴い、企業をとりまくリスクは、複雑化・多様化しており、従来予想されなかったリスクが発生することも想定される。当然のことながら見逃されたリスクに対応する手段がとられなかった場合には、発生する損害のすべては企業が負担することになる。リスクの洗い出しを行う際には、災害に関する資料や同業他社の事故事例などを参考にし、考えられうるリスクをリストアップしたチェックリストを活用したり、生産工程・販売・流通経路等の企業活動の流れを表したフローチャートや財務諸表、各種契約書等から必要な情報を入手する方法が一般的である。留意すべき事項としては、

a.チェックリストを活用する場合、企業をとりまくリスクには、多様なものがあるので、実態に応じてチェック項目の追加・訂正を行う必要がある。

b.一つの事故で多様な損害が発生することがあるので、見落とさないよう確認する必要がある。

例.

火災の発生 ➡ 建物・機械設備の損害
休業による利益損害
従業員のケガ
第三者への賠償責任　など

労働災害の発生 ➡ 従業員の傷害・死亡
災害補償責任
使用者の賠償責任
刑事責任
社会的責任の追求、信用の失墜　など

(3)リスクの分析・評価

リスクの分析・評価とは、確認したリスクについて、そのリスクによる損害の発生頻度と強度（大きさ）を推定することである。

① リスクの分析

a.損害の発生頻度

損害の発生頻度は、自社および同業他社の事故記録、官公庁等から提供される各種事故統計、災害事例報告書等から推定する。

b.損害の強度（大きさ）

損害の発生強度とは、発生しうる損害の規模のことで、損害が発生した場合に企業がその損害に耐えられるかどうか、経常利益、純資産、売上高、流動性資産等、企業の財務面に与える影響度合いから判断することになる。

② リスクの評価例

上記、損害の発生頻度および発生強度を２段階に格付けして、リスクの影響度の評価した例を以下に示す。リスクの影響度は、後述するリスクの処理・制御手段を選択する上での目安となる。

		損害の発生頻度	
損害の程度		高	低
	大	A	B
	小	C	D

A評価のリスク：リスクコントロールを徹底に実施し、B またはC 評価へ転換する。

B評価のリスク：リスク強度の軽減を図りD 評価への転換を図るとともに、保険を中心としたリスク処理を実施する。

C評価のリスク：リスク頻度の軽減を図りD 評価への転換を図るとともに、リスクの保有を基本的な処理手法としつつ、必要に応じ保険との組み合わせを検討する。

D評価のリスク：基本的にはリスクを保有する。

なお、リスクの洗い出しから分析・評価まで実施する際に、以下のようなチェックリストを使うと有効である。

リスク分類（例）

事業リスク		リスクの有無	発生頻度	損失規模
財物リスク	自然災害（地震、台風等）			
	火災・爆発			
	電気的・機械的事故			
	輸送中の事故			
人的リスク	役員・従業員の就業中の事故			
	雇用（人手不足等）			
	キーパーソンの喪失			
	テロ			
	誘拐			
	ストレス・ノイローゼ			
情報リスク	情報システム障害			
	コンピュータウィルス			
	情報漏えい			
	サイバーテロ			
財務リスク	不正な財務処理、入力ミス			
	虚偽の表示			
	流動性損失			
コンプライアンス（法令等の遵守）	証券取引法への抵触			
	個人情報保護法への抵触			
風評リスク（直接的）	うわさ			
市場リスク	金利リスク			
	為替リスク			
信用リスク	貸し倒れリスク			
賠償責任リスク	施設に関わる賠償責任			
	業務・作業に関わる賠償責任			
	製品の欠陥			
	知的財産に関わる賠償責任			
	環境汚染に関わる賠償責任			
	会社役員の賠償責任			

(4)リスクの処理

リスクの処理の手段としては、前述の通り、リスクコントロールとリスクファイナンシングがある。ある１つのリスクに対してリスクコントロールとリスクファイナンシングの双方から最低１つずつの手段を講じるのがリスクマネジメントの大原則である。

a．リスクコントロール

リスクコントロールとは、予想されるリスクに関し、企業が被るかもしれない損害を緩和･軽減したり､排除･消滅させたりする事前のリスクの処理手段のことを言う。具体的には以下のような処理手法がある。

ア．リスクの回避

予想されるリスクを回避するため､例えば出火危険が極めて高い工程での生産を中止する等、逃避的な危険処理手段である。この方法を用いれば完全なリスク

の遮断を行うことができるが、一方でリスクを回避しなければ、享受できる便益や利益を失うことにもなる。

例示すると以下の通り。

・製造物責任リスクの発生頻度が高い製品の製造を中止する。

・地震や風水災のリスクの発生頻度が高い地域への工場の進出を断念する。

イ．リスクの除去・軽減

以下のような手法が存在する。

損害の予防・低減

損害の発生頻度と強度に影響する各種の人的および、物的な予防軽減手段のことで、一般的に「安全対策」「防災対策」と言われているものである。

例示すると以下の通り。

・労働災害を防止するため、機械設備に安全装置を設置したり、安全な作業手順を定める。

・スプリンクラーを設置して火災による損害を最小限にくい止める。

リスクの分離

リスクの発生単位を分割し、事故が発生しても企業活動全体に影響が及ばないようにすることである。

例示すると以下の通り。

・工場を防火区画する。

・工場を地域的に離れた２つの場所に設置する。

・部品の仕入れ先を複数確保する。

ウ．リスクの移転

契約などの方法によりリスクそのものを第三者に移転する手法である。例えば、コンピュータ・リース契約を利用することにより、コンピュータ自体の物的損害に関わるリスクをリース業者に転嫁するやり方などがある。

b.リスクファイナンシング

リスクファイナンシングとは、損害が発生した場合の資金手当のことである。

ア．リスクの保有

損害が発生した場合、それを補填するのに必要な資金を、借り入れも含めて企業自身で調達することをリスクの保有と言う。

リスクの保有には、積極的保有と消極的保有がある。

積極的保有

積極的保有には、以下のような方法がある。

○経常費処理

小規模な損害に対しては、発生の都度、経常費として処理する。

▼例．機械・設備・自動車の修繕費など

○準備金の設定

将来発生しうると想定される損害に対し準備金を設定し、企業内に資金を留保しておくことを言う。損害が発生した場合には準備金を取り崩してその補填にあてられることになる。

例．リコール費用の一部、貸倒引当金、海外投資損失準備金

○自家保険

自家保険は、厳密に言うと準備金の一形態であるが、自家保険による引き当て金は、損金とならないため、利益処分による積立金の形を取らざるを得なくなる。

<u>消極的保有</u>

消極的保有とは、企業がリスクの存在に気がつかずに、何の処理手段も講じていないことを言う。（リスク転嫁の手段がないため保有を余儀なくされているケースも含む。）

実際には、人的リスク、物的リスク、責任リスク等すべてのリスクの存在を完全に確認し、処理手段を講じることは容易ではないので、一般的には多くの企業が多かれ少なかれリスクを消極的に保有していると言える。

イ．リスクの転嫁

リスクの転嫁とは、リスクが発生した場合の損害を第三者に転嫁する手段のことであり、主に保険もしくはこれに類似した保証、共済、基金制度等により行われる。

保険以外の転嫁の方法としては、契約による転嫁、例えば、工事請負契約において、工事に起因する発注者の損害賠償責任を全て請負業者に転嫁する方法などがある。

(5) リスク処理手段の選択

リスクの処理手段は、その効果適合性（損害を最小化すること）とともに費用適合性（費用を最小にし、経常化すること）に配慮して選択されることになる。

リスク処理手段を選択するにあたっては、以下の点に考慮する必要がある。

①リスクの回避

リスクを回避することにより、企業が被るかもしれない損害を確実に回避できるという長所があるが、実施するにあたっては、以下の点を考慮する必要がある。

ａ．リスクの回避は、不可能な場合があること。例えば、法律上の損害賠償責任のリスクを完全に回避するには、企業は活動をやめることしか方法はない。

ｂ．リスクを回避することにより、企業が回避しなければ享受することのできた利益

を得られなくなること。
ｃ．リスクを回避することにより、新たなリスクを生じることがあること。例えば、空輸による輸送手段を回避しトラック輸送に切り替えることにより､新たにトラック輸送に関するリスクが生じることとなる。

②リスクの除去・軽減
リスクの除去・軽減を実施するにあたっては、以下の点を考慮する必要がある。
ａ．すべての損失を防止もしくは軽減することは、技術的あるいは経済的に可能であるとは限らないこと。よってリスクの除去・軽減の手段は、リスクの保有もしくは転嫁の手段と組み合わせ検討する必要がある。
ｂ．リスクの除去・軽減にかかる関連経費（消防火設備、安全設備等に関する資本的支出と減価償却・警備員・安全管理者・消防隊員等安全防災に関わる人の人件費等）とそこから得られる潜在的な利益（リスクの頻度および損害の強度の軽減、保険料コストの軽減、社会的責任、顧客に対する責任、労使関係の改善等）を比較する必要があること。利益が経費と等しいかそれ以上でないと、除去・軽減を実施する意味はないことになる。

③リスクの保有
　リスクの保有にあたっては、十分なリスク分析を行い、保険市場の構造、リスク保有に対する税法上の取扱い、企業の財務力、過去の損害データ等を検討する必要がある。
　一般的には、以下のような条件が存在する時は、リスクの積極的保有を検討する必要がある。
ａ．リスクの除去・軽減およびリスクの転嫁（保険の利用等）が困難な場合で、リスクを回避した場合、享受できなくなる利益の損害が無視できない場合
ｂ．発生可能最高損害額が低いために、企業の経常費もしくはわずかな準備金の範囲で　処理ができる場合
ｃ．リスクの発生頻度が極めて低いため、無視できる場合
ｄ．リスクの発生頻度が高いため、保険会社等に転嫁した場合予想最高損害額と同じ程度かそれ以上の費用がかかる場合
ｅ．企業が同質の危険を数多く保有しているため、リスクの発生頻度や損害の規模がかなり正確に予測できる場合

④リスクの転嫁
　リスクの転嫁は、リスクコントロールの実施にもかかわらず発生し、保有するには規模が大きすぎるリスクの処理手段として有効な方法である。リスクの転嫁を行うに当たっては、以下の点に留意する必要がある。
ａ．保険によるリスクの転嫁
　保険は、リスクの転嫁という処理手段を考慮する上で、中心となる手段である。

なぜならば一般的に保険は安価であり、費用の合理性（最小化、経常化）の点からみて優れた危険処理効果を持っているからである。

保険によるリスクの転嫁をするにあたっては以下の点に留意する必要がある。

・すべてのリスクが保険に転嫁できるわけではない。

・リスクの頻度が大きい場合など予想最高損害額と同じ程度かそれ以上費用がかかることがある。

・保有、除去・軽減との組み合わせを検討する必要がある

ｂ．契約によるリスクの転嫁

・契約により第三者に移転したと考えていたリスクの全部もしくは一部しか移転していないことがある。

・公序良俗に反する、もしくは著しく公平を欠くという理由でリスクの転嫁が無効であると判断されることがある。

(6)結果の検証

事故データ、保険データ、安全対策の実施状況などを検証し、リスク処理手段の見直しおよび安全防災対策の見直しを行う。ポイントとしては以下の通り。

①予定したリスクマネジメント手法を実施できたか。

例えば､社員教育などこの種のリスクマネジメントに関する様々なフランを計画していたが､予算あるいはスケジュールの都合でその全てを実施することができなかったといった事態も往々にしてある｡計画と実行のギヤッフについて検証し､より実効性の高いリスクマネジメント手法とするよう工夫する必要がある。

②期待通りのリスクマネジメント効果がえられたか。

例えば、労災リスクに関して、従業員の教育を実施し、より安全な設備を導入し、作業行程も見直したにもかかわらず､期待したほど労災事故が減少しなかったようなケースにおいて、その原因・問題点の所在を明らかにし、今後のリスクマネジメント手法に反映していく必要がある。

③リスク処理基準を見直すべきような事態は発生していないか。

例えば、企業の業容が急成長したり、あるいはマーケットの環境が大きく様変わりした場合には、当該企業を取り巻くリスクの大きさに変化が生じたり、また新たなリスクが発生することもある。常に客観的な目で自社のリスクを分析し、必要に応じてリスクマネジメント手法の軌道修正を行う必要がある。

④リスクコストを削減できたか

リスクマネジメントとは「リスク・コスト（リスクマネジメントに要するコスト）をいかに削減するか」という側面も有している。よって、保険料や事故予防のために要したコストなど都度検証し、効果的なリスクマネジメントが実行できているかチェックすることも重要である。

本来であれば、リスクマネジメントは、事業戦略に連動させ、取り組まれるものであり、米国を中心に関心が高まっている。リスクの洗い出し、分析・評価、そのマネージだけでなく、事業戦略に密着した形で、リスクマネジメントを解決していくのは、ERMとなる。

第３章　エンタープライズ・リスクマネジメント

３.１　エンタープライズ・リスクマネジメントの定義

リスクマネジメントについてはこれまでも様々な議論が行われてきたが、多くの経営者が共有しうる考え方が求められてきた。ERM はこれまで企業内の各部門でバラバラにリスク管理されていたものを、企業として総合的、包括的に捉えてリスク・ポートフォリオを管理する新しいパラダイムの導入により、企業全体の経営課題とする方法である。企業経営全体をスコープにいれ、全社的にプロセスに従い、リスクマネジメントを行うものである。90 年台前半にリスクマネジメントの新概念として提示されたが、Enterprise-wide Risk Management, Integrated Risk Management, Comprehensive Risk Management とも呼ばれ、特に金融工学の発展により、リスクの計量化が進んだ 90 年代後半から現在に至るまで様々なアプローチで論議されてきた。ERM についてはさまざまな定義があるが、一般的に取り組んでいる内容は共通している。

＜ERM定義例1＞米国カジュアルティ数理人協会‘Enterprise Risk Management概観’での定義（2003.5）

“ERMは、すべての産業の組織において、株主への短期的長期的価値増大のため、
すべてのリスク源泉について、
評価、コントロール、活用、財務対応、モニタリングを実施するプロセスである。”

ＥＲＭでの一般的な取り組み事項

①リスク管理担当役員（ＣＲＯ）任命と推進セクションの明確化
②企業を取り巻くすべてのリスクの確定
③業務リスクと戦略的リスクの計量化
④リスクの統合的な評価
⑤リスクへの対応方法の決定
⑥ＥＲＭプロセス管理
⑦企業文化へのＥＲＭの浸透

３.２　COSOレポート 2004の登場とその影響

近年米国で会計がらみの不祥事が続いたことから、ＥＲＭについても会計監査の視点の重視が出てきており、2004 年９月に米国トレッドウエイ委員会組織委員会（COSO）が発表したＥＲＭモデルの枠組みに関するレポートは、こうした要請に基づいてまとめられたもので、その後会社のリスクマネジメントのあり方に大きな影響を与えた。このレポートは従来から公表されて内部統制概念の事実上の標準として各国に広まっていた COSO 内部統制概念をさらに発展させたものであり、そのタイトルは‘Enterprise Risk

Management-Integrated Framework’（邦訳「全的リスクマネジメント」）となっている。この枠組みは COSO ERM とも呼ばれていますが、３つの基礎概念（８構成要素、４目的カテゴリー、事業組織）で整理され、以下の立方体イメージ（図 3-2）で表現されている。前述の米国カジュアルティ数理人協会の定義では企業価値創造の側面を強調されていたが、この COSO　ERM の定義では、リスクコントロールに焦点が当てられている。

＜ERM定義例2＞COSO‘ Enterprise Risk Management-Integrated Framework ’での定義

“ERMは、事業目的の達成について合理的な保証を提供するために、
取締役会、経営者その他従業員によって実行される。
戦略の策定はもとより、事業体のあらゆる領域に適用され、
事業体に影響を及ぼす「潜在的な事象」を認識するよう設計されて、
「リスク」をその事業体の「リスク欲求」の範囲に治めるプロセスの事である。”

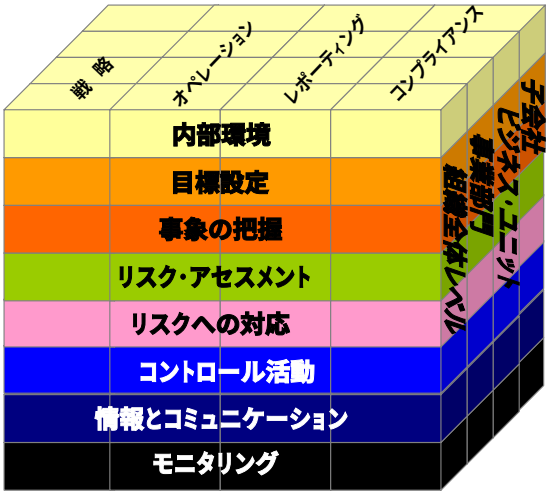


図 3-2：COSO キューブ

この COSO ERM をベースとして ERM を欧米で導入した企業が増加しているが、COSO はあくまでも枠組みを示したもので、具体的にどのようにリスクマネジメントとして実行していくのか、細説してあるわけではなく、実際の運用については個別会社が独自性を発揮して実施することになる。また、COSO ERM では会計不振を背景に監査の専門家が中心になって立案されたため、ダイナミックな企業活動のリスクを会社経営として捕らえるという視点が弱いという批判がありますが、これをどう生かしていくかはそれぞれの会社次第といえる。

BASEL II の議論でもＥＲＭの考え方が取り入れており、特に金融関係、多国籍企業では導入が進んでいるとされています。以下にその概要と実際にどのように企業で導入されているか、について過去の調査・研究から紹介する。

３.３　従来のＲＭとＥＲＭの違い

現在でも多くの企業が、全社的なリスクマネジメントシステムを導入しているが、多くの企業において次のような課題が浮き彫りとなっている。

＊事業戦略や業績評価の仕組みと連動していないため「ボランティア」的意識が強くモチベーションが上がらない

＊経営レベルで網羅的に事業リスクを把握する仕組みとなっていない
＊仕組みだけが先行し現場に根付いたものとなっていない
＊全社ベースでの課題が明確化されていない／全社的ＰＤＣＡサイクルが未構築
＊管理対象リスクが限定されている
＊その他にも様々なマネジメントシステムが存在し整合性がとれていない／重複感がある

ERM は、このような課題を解決するためのフレームワークを提供するものと位置付けることができる。

従来のリスクマネジメントシステムは、経営戦略や事業戦略から独立したシステムとして運用されるケースが大半であった。ERM はそれらを一体的に運用することを志向し、経営レベルでは戦略上の意思決定の場においてリスクマネジメントを有効に機能させること（事業の裏に潜むリスクを認識した上での意思決定を行うこと）を、また事業現場では『本業』としてリスクマネジメントに取り組ませる仕組みの構築を実現させることが主たる目標となる。

このように、リスクマネジメントを経営管理システムと連動させ、一体のマネジメントシステムとしての運用を実現することこそが、ERM の目指すべき姿であると言える。

３.４　企業がＥＲＭを導入する理由

ＥＲＭの実施状況について調査研究が本格的に始まったのは比較的最近だが、ERM を導入済みの企業とそうでない企業との相違について調査した例＊がある。2003 年にジョージア大学の研究者により行われた調査では、米国企業による ERM の採用と企業財務・企業所有形態の相違については、相関が認められず、同業種・同規模の企業でも財務的に自己資金以外に依存している企業では CRO（Chief Risk Officer）を指名している会社が多いという傾向を見出している。

2005 年の別の研究でも、ERM を導入済みの企業とそうでない企業との相違を見出そうとして調査した例＊がある。この研究ではなぜ企業が ERM を導入したのか、23 の組織のデータから実証分析を行い、その結果、ERM がどういう風に展開されているかは、CRO の存在、取締役会の独立性、CEO と CFO による ERM 推進の意向、四大監査法人の存在、組織規模、銀行・保険会社の選択、によるところが大きいということが要因であることを明らかにしている。ERM によるリスクマネジメントが進みつつあるものの、企業によってその進展度はまちまちであるのが実態であり、米国内の企業は国際的に展開している企業よりもＥＲＭの実施が遅れているとしている。

＊ Mark S. Beasley, Richard Clune,Dana R.Hermanson. 'Enterprise risk management: An empirical analysis of factors associated with the extent of implementation'(Journal of Accounting and Public Policy 24　2005)

３．５　日本の動き

国内でも経済産業省において、以下資料を発行した。

- 平成 16 年 3 月に、「事業リスク評価・管理人材育成システム開発事業」が、「事業リスクマネジメント」を発行。
- 平成 17 年 3 月に同事業が、「先進企業から学ぶ事業リスクマネジメント実践テキスト」

これらテキストの中では、企業価値を向上させる事業リスクマネジメントとしてＥＲＭを取り上げ、次の点を強調している。

① 経営の安定性と効率を高め、企業価値を高めるツール

② 個々の事業に存在するリスクの量に対して、その事業が適切なリターンを得ているか把握できるようになるため、企業全体としてリスクとリターンのバランスの評価ができるようになる。この結果株主から見たコーポレート・ガバナンスを高めることができる。

経済産業省は、上記資料を通して、「収益性とリスクを見据えた企業の絶えざる投資こそ、新しいイノベーションの道を開拓し、不確実性・リスクが増大・巨大化するグローバル化する中で、経営は企業全体を見渡したリスクマネジメントが必要」、と述べている。

第４章 内部統制について

４.１　内部統制の定義

内部統制は、一般に企業などの内部において、違法行為や不正、ミスやエラーなどが行われることなく、組織が健全かつ有効・効率的に運営されるよう各業務で所定の基準や手続きを定め、それに基づいて管理・監視・保証を行うことをいう。

従来の内部統制は、財務会計分野からの視点でのみ語られ、財務報告の適正性確保を目的とする活動として捉えられていた。しかし、1990年代になると会計統制以外に、コンプライアンスや経営方針・業務ルールの遵守、経営および業務の有効性・効率性の向上、リスクマネジメントなどにより広い範囲が対象となり、コーポレート・ガバナンスのための機能・役割という側面を強めている。

そのきっかけとなったのが、米国トレッドウェイ委員会組織委員会（COSO）が1992～94年に公表した報告書「Internal Control – Integrated Framework（内部統制－統合的枠組み：COSOレポートのこと）」で、この中で新しい内部統制のフレームワーク（COSOフレームワーク）が提唱された。

米国では、エンロンやワールド・コムの粉飾決算／破綻を受けて、2002年に成立したサーベンス・オクスリー法で内部統制システムの構築・運用を経営者の義務、その監査・監査意見表明を外部監査人の義務としている。

日本においても、2006年5月から施行となった会社法では、取締役／取締役会に内部統制システム構築の義務を課している。2005年8月には、経済産業省が、「コーポレートガバナンス及びリスク管理・内部統制に関する開示・評価の枠組みについての指針」を公表。企業が自主的に内部統制システムの構築に取り組むための指針で、リスク管理の概念を盛り込んでいる。

さらに、金融庁が主導して、証券取引法の抜本改正となる金融商品取引法（日本版SOX法）が2006年に成立。2009年3月期の決算から、上場企業に内部統制報告書の提出・公認会計士によるチェックが義務付けられた。

日本の企業会計審議会では、内部統制を以下の通り定義している。

内部統制とは、
（１）事業経営の有効性・効率性を高め、
（２）企業の財務報告の信頼性を確保し、
（３）事業経営に関わる法規の遵守を促す
（４）そして資産の保全を確保する
ことを目的として、企業内部に設けられて運用される仕組みを指す。

項　目	内　容
事業経営の有効性・効率性向上	日常の業務が事業活動の目的を達成するために、効果的で効率的な仕組みで行われていることを目指す
財務報告の信頼性確保	財務諸表、あるいは財務諸表に重大な影響を及ぼす可能性のある情報について、信頼性を確保すること
事業経営に関わる法規の遵守	事業活動にかかわる法令や規範などの遵守を促進すること
資産の保全	資産の取得や使用、処分が正当な手続きや承認のもとで適切に行われていること

内部統制を構成する要素は以下の通りで、経営管理の仕組みに組み込まれて
一体となって機能することで、上記の目的が達成される。

（１）統制環境
（２）リスク評価
（３）統制活動
（４）情報とコミュニケーション
（５）モニタリング
（６）IT（情報技術）への対応

項　目	内　容
統制環境	①誠実性及び倫理観 ②経営者の意向及び姿勢 ③経営方針及び経営戦略 ④取締役会及び監査役又は監査委員会の有する機能 ⑤組織構造及び慣行 ⑥権限及び職責 ⑦人的資源に対する方針と管理
リスクの評価と対応	①リスクの評価 ②リスクへの対応
統制活動	
情報と伝達	①情報 ②伝達（内部伝達、外部伝達）
モニタリング	①日常的モニタリング ②独立的評価 ③評価プロセス ④内部統制上の問題についての報告
ITへの対応	①IT環境への対応 ②ITへの利用及び統制

４.２　日本版SOX法

日本版SOX法は、相次ぐ会計不祥事やコンプライアンスの欠如などを防止するため、米国のサーベンス・オクスリー法（SOX法）に倣って、会計監査制度の充実と企業の内部統制強化を求める日本の法規制である。

具体的には、証券取引法の抜本改正である「金融商品取引法」がこれに該当する。同胞では、第24条で「有価証券報告書を提出しなければならない会社のうち、金融商品取引所に上場している有価証券の発行者である会社その他の政令で定めるものは、事業年度ごとに、当該会社の属する企業集団及び当該会社の関わる財務会計に係る財務計算に関する書類その他の情報の適正性を確保するために必要な体制について評価した報告書（内部統制報告書）を有価証券報告書と併せて内閣総理大臣に提出しなければならないこととする。また、内部統制報告書には、公認会計士又は監査法人の監査証明を受けなければならないこととする」と定めている。

金融商品取引法（実際には「証券取引法等の一部を改正する法律」およびその整備法）は、2006年3月に国会へ提出され、6月に成立した。同法は、緊急性の高い条項から順次段階的に施行される。内部統制報告書の提出・監査に関しては、附則第15条で「平成20年4月1日以後に開始する事業年度から適用する」と定めており、2009年（平成21年）3月期の本決算から上々企業およびその連結子会社を対象に適用となる。

2005 年の７月に金融庁の企業会計監査院から、ディスクロージャーの信頼性を確保するため、開示企業における内部統制の充実を図る方策として、「財務報告に係る内部統制の評価及び監査の基準（公開草案）」が公表された。

本草案は、日本版 SOX 法の公開草案とも言われており、今後、パブリックコメントの手続きを経た上で確定され、金融審議会において導入時期などの具体的な法制度化に向けた議論が行われることとなっている。米国の SOX 法は 2002 年に制定された法律で、企業に財務の透明性と正確性の確保を厳しく求め、違反すると経営幹部は最長 20 年の禁固刑といった厳しい罰則が課せられている。その日本版が正式に法制度化されれば、企業経営者に対してそれを遵守すべく社内体制を構築する義務が化せられることとなる。今や企業は法制度化を見据えて日本版 SOX 法への体制構築にむけた準備が求められている。

公開草案では、企業等の４つの目的（①業務の有効性及び効率性、②財務報告の信頼性、③事業活動に関わる法令等の遵守、④資産の保全）の達成のために企業全体で取り組むべきプロセスとして「内部統制」を位置付けている。その上で、内部統制の基本的な枠組として６つの基本的要素（①統制環境、②リスクの評価と対応、③統制活動、④情報と伝達、⑤モニタリング、⑥IT の利用）を明確化し、経営者にその基本要素がプロセスとして組み込まれた内部統制システム構築を求めている。なお、公開草案中では、企業内における内部統制システムの構築・運用は財務報告における記載内容の適正性の確保以外に、業務の有効性及び効率性の確保による情報処理コストの削減、さらには市場における資金調達機会の拡大、資金調達コスト削減といったメリットの享受が期待できるとも言っている。

この公開草案の特徴としては、米国の SOX 法をベースとしつつ、「内部統制推進の為に IT の利用が明記され、財務報告に関するシステムでの不正防止はもちろん、内部統制が有効機能しているか否かを監視する手段としてもシステムを活用する事が求められている」ことが強調されている点が挙げられる。

公開草案における「IT の利用」とは、内部統制の基本６要素が有効かつ効率的に機能す

るように業務に組み込まれている一連の IT を活用することと位置付けられている。その上で、IT を利用した内部統制を全般統制（ハードウェアやネットワークの運用管理、ソフトウェアの開発・変更・運用等に対する統制、例：企業内全体にわたる情報処理システムが財務報告に係るデータを適切に収集し処理するプロセスとなっていることを確保する）と業務処理統制（各業務アプリケーションプログラムに組み込まれた統制、例：各業務領域において利用されるコンピューター等のデータが適切に収集、処理され、財務報告に反映されるプロセスとなっていることを確保する）の２つに大別して定義し、相互が補完しあう形で内部統制システムを機能させる必要があるとしている。

　また、様々な局面でのIT利用のうち、特に監査におけるIT利用の背景には、効率的な財務報告に係る内部統制の有効性評価にはシステム的な業務フローの標準化が必要であるとの認識があることが伺える。業務フローの標準化の促進は業務の効率化を推し進め、その結果、同一の評価・監査手続きの適用が可能となる。

II部　各領域の関係

第１章 組織戦略とＢＣＭ

規模の大小に関わらず、すべての組織には、成長、多様化、他の事業の買収といった目的や目標がある。こうした目的や目標は、通常、組織の短期、中期、および長期の戦略的な計画によって達成される。目的や目標を達成するためには、事業の継続が必要不可欠であり、BCM は組織にとってますます中心的で極めて重要な戦略課題となってきた。組織の最高レベルで BCM が認識され管理されることで、新しい事業機会に関連するどんな事業中断リスクに対しても、対応が可能になる。インシデントの結果はさまざまであり、広範囲に及ぶ可能性がある。これら結果には、人命の喪失、資産や収益の損失、または組織のブランド・評判や生き残りがかかっている重要な活動の失敗などがあげられる。従い、BCM はこれらの対策を含め、組織が取り組まなければならない課題である。BCM では、ステークホールダー（利害関係者）の戦略における重要性も認識する必要がある。ステークホールダー（利害関係者）の例としては、社内および「外注」の被雇用者、顧客、供給業者、販売業者、投資家、株主などがあげられる。

結果は、組織に対するものだけではないこともある。インシデントの一例として、次のようなものがある。

- 物的損害、利益損害
- 電気、水道、運輸、電話といった公共施設におけるサービス中断
- 組織の運営に関わる法律、規制、および政治環境に変化を及ぼす事象
- 取引先がインシデント等により影響を受け、製品やサービスの提供に失敗することにより、当該組織自体の製品やサービスの提供に重大な影響を及ぼす障害（サプライチェーン全体の観点）

こうしたすべての課題は組織の戦略的な懸念事項であるため、リスクの影響を効果的に管理するための仕組み作りが重要である。各事業におけるプロセスが、組織の大きさ、構造、および責任に応じて変化する一方、基礎的な考え方は、民間または公共の組織にとって、その大きさ、範囲、または複雑さに関わらず同じである。

上述の通り、組織戦略を達成するためにも、そしてステークホールダーとの戦略的関係を向上させるうえでも、BCM は今後、組織戦略の中心的、そしてインフラ的役割を益々強めていくと考えられる。

第２章　各領域とＢＣＭの関係

以下にBCMとリスクマネジメント、内部統制、CSR、ITガバナンス、情報セキュリティ等の領域との関係を整理する。

２．１　リスクマネジメントとＢＣＭ

BCM は、事業に対するリスクと、そうしたリスクの結果を把握するために評価されるより広範囲のリスクマネジメント・フレームワークに対し互いに補完するものである。

リスクマネジメントでは、組織が生き残れるようにするための重要な活動に関するリスクを管理する必要がある。BCM では、組織がその生き残りのために依存している製品とサービスが特定されリスクマネジメントが行われるが、そうした製品やサービスは、組織が信用を維持し常に責任を果たせるようにするため必要である。BCM を行うことで、組織は、組織の人々、名声、資産、システム、および情報を常に安全に保つために、インシデントが起きる前に何を行う必要があるのかを認識することができる。

このような認識があれば、組織は、事業が継続できなくなった際に、必要な対応について現実的な見解を持つことができ、製品やサービスの提供を容認できないほど遅らせることなく、どんな結果であっても徹底的にマネージすることができる。

BCM とリスクマネジメントの具体的相違を説明する。

BCM の分析手法は、ビジネスインパクト分析と呼ばれ、「事業や業務などが機能しなくなった場合の影響度を時間軸を基軸に検討する」。この事業や業務の継続を支えるボトルネックを特定していきながら、対策を講じていく。なお、経済産業省の事業継続策定ガイドラインでは、このボトルネックを「組織の存続上、必ず必要な事象（事業を構成する業務・工程・部門、物流、キーパーソン、データ・システム、資金など)」と定義している。

ビジネスインパクト分析では、原因事象のリスクを観点でなく、重要な事業や業務、そしてボトルネックを対象に分析を進めていく業務プロセス分析といえる。

一方、リスクマネジメントの分析手法は、リスク分析と言われ、リスクの洗い出しを行った後で、そのリスクの発生確率とリスクによって生じる損害額を検討する。リスクが与える影響が大きいリスクに対し優先順位を付けていきながら、リスクへの対応方法を検討することになる。大きな考え方の相違は以下の通りである。

	リスクマネジメント	ＢＣＭ
主な分析手法	リスク分析	ビジネスインパクト分析
主なパラメータ	影響度および可能性	影響度および時間
対象リスク	全てのリスク	重大な事業崩壊の原因となるリスク若しくは、結果事象としてリスク毎に細分化する
リスクの規模	あらゆる規模	生存に脅威となるリスク

また、ビジネスインパクト分析とリスク分析の違いを以下の通りまとめる（BS25999-1から)。

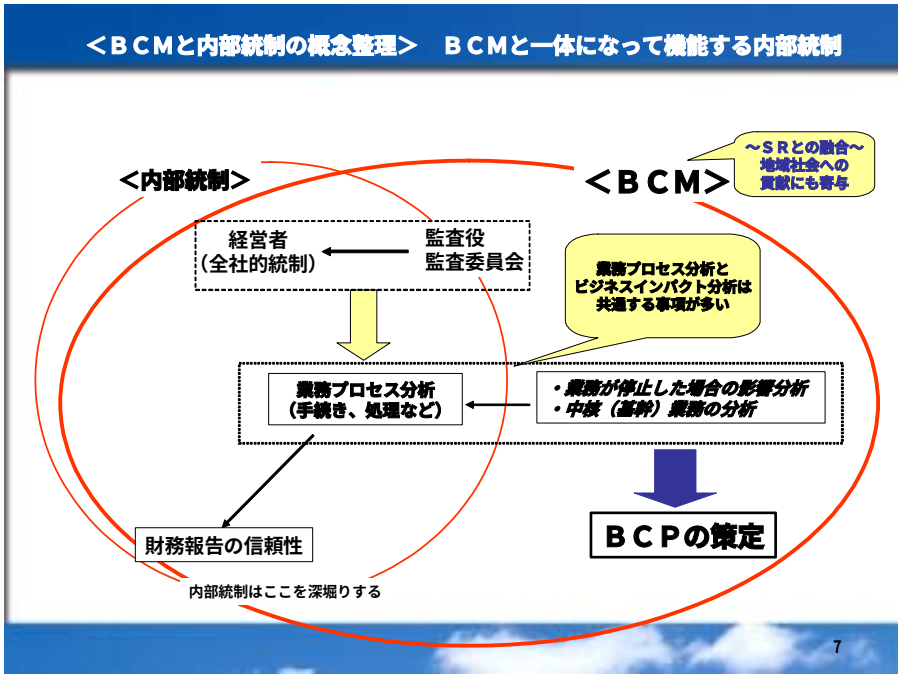
＜ビジネスインパクト分析の切り口＞

項　目	内　容
結果事象か原因事象か	結果事象
分析・評価手順・方法	業務の停止が与える影響（インパクト）を分析する。観点は例えば以下の通り。 ・組織の目的とステークホールダーの社会的責任 ・製品・サービスの提供をサポートする活動、資産、およびリソースの特定 ・これら活動の停止による長期による影響と結果の評価 ・組織の活動を混乱させる可能性があると認識された脅威を特定し評価
重要業務・サービスの特定、 優先順位付け	「重要な活動の特定」という項目がある。 組織は、復旧のための優先順位に応じて活動行う。BIA 実施時に評価されるとおり、事業停止によって短時間に最も大きな影響を与え、即座に復旧する必要がある活動を「重要な活動」と呼ぶ。最大許容停止時間内に確実に復旧できるよう事前に手配しておかなければならない他の活動にも配慮する必要がある。組織は、重要業務復旧の計画に活動に集中させたいと考えるかもしれないが、他の業務もそれぞれの最大許容停止時間内に復旧する必要があることを認識すべき。
復旧にあたってのリソースの特定	復旧時の各活動が必要なリソース（復旧要件）について評価・見積もる。例えば以下事項が含まれる。 ・「People（キーパーソン）」 ・「Premises（サイト）」 ・「Technology（IT などの技術）」 ・「Information（情報）」 ・「Supplies（取引先）」
時間軸（RTO、MTO など）	各活動について、以下を評価する。 ・事業停止に陥った後にその活動を再開する必要がある最大期間 ・事業の再開時の事業活動レベル ・通常の事業活動レベルにまで到達させるまでの時間
業務継続にあたっての相互依存性（取引先、社内の機能　など）	「各活動の相互依存性」及び「外部機関・場所にある組織のレジリエンシー」に関する事項について理解する必要がある。
定性／定量どちらを求めるか	組織の判断。ただし、上記時間軸は定量的。
経営層の承認の有無	定期的にレビュー、更新されるべきである。加えて、事業環境や人事や技術の変更などあれば実施されるべきである。
特記事項	特になし

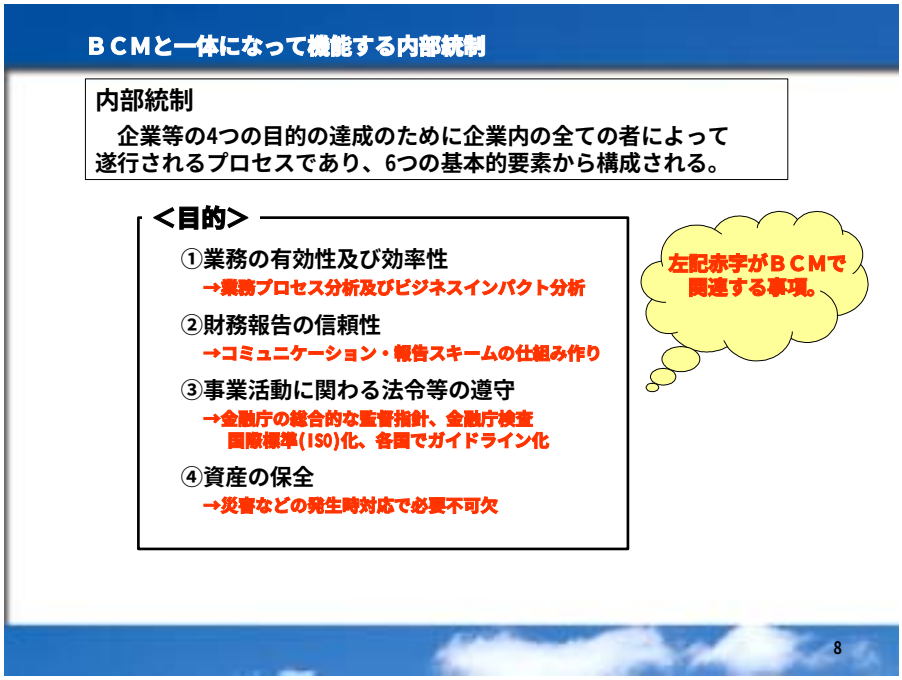
＜リスク分析の切り口＞

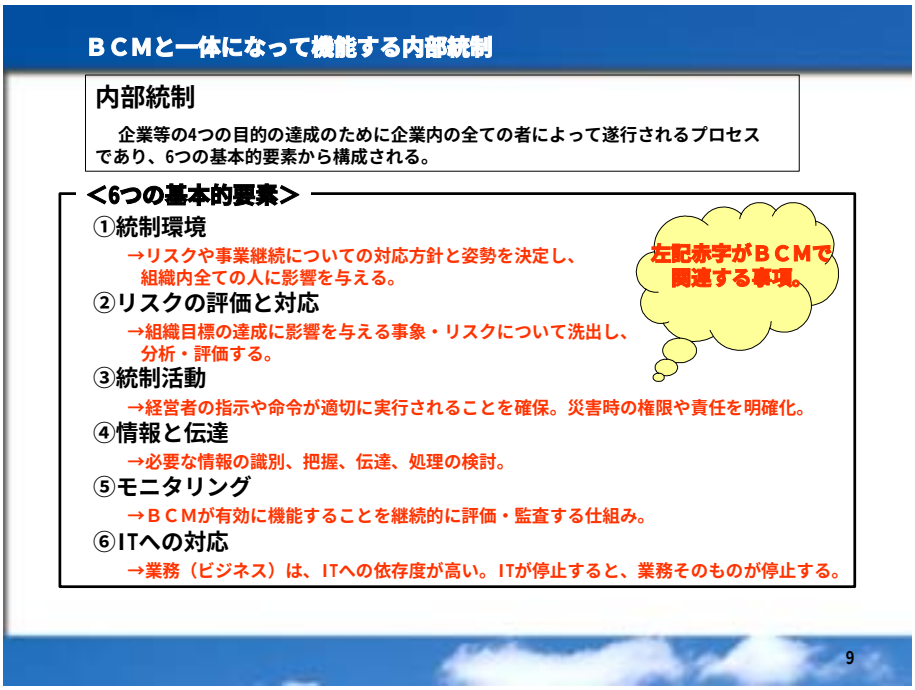
項　目	内　容
リスクの洗い出し	・リスクレジスター（リスクリスト）の作成について言及されている。 ・特定のリスク（火災、洪水、停電、キーパーソンの喪失、コンピュータウイルスなど）については、特定されることも想定。
対象リスク	事業の継続を妨げるリスクを対象とするが、リスクの選択は、組織の判断に委ねる。
分析・評価手順・方法	重要な活動（アクティビティ）に対してリスク分析・評価を行う。 以下リソース毎に脆弱性、及び脅威が発生した場合のインパクトを分析する。 ・「People（キーパーソン）」 ・「Premises（サイト）」 ・「Technology（IT などの技術）」 ・「Information（情報）」 ・「Supplies（取引先）」 リスク評価については、例えば以下に挙げる事項などについてフレームワークを持つこと推奨。 ・リスクの保有（如何なるリスク評価手法を選択しようが） ・リスク分析 脆弱性（例えば、ボトルネック、防火、IT セキュリティなど）の機能不全の可能性について検討する。
確率分析	「混乱（事業停止）の可能性」について言及
特記事項	BIA の結果を踏まえ、以下を踏まえ実施する。 ・混乱（事業停止）の可能性 ・混乱（事業停止）期間の短縮化 ・組織の主製品・サービス提供の混乱の影響を極小化する

２．２　内部統制とＢＣＭ



内部統制とBCMで共通しているのは、先ずは「業務プロセス分析」であろう。本業務プロセス分析は両領域での基礎分析であり、実施のための前提ともいえる。ともに、業務プロセスを見える形にする必要がある。内部統制でいえば、財務報告の信頼性を確保するために分析を進める。一方BCMでは、中核業務やそれを支えるためのボトルネックの特定など業務継続を観点にして分析を進める。これら２つの分析を個々に進める必要があるかどうかについては、今後議論が深まるであろう。また、両領域では、以下観点で共通項目多いため、また企業として考え方にブレを生じさせないようにするため、一体で検討・運営することを勧めたい。





また、内部統制とBCM双方経営の観点で評価・承認する必要がある。

内部統制では、経営者に主として以下事項が求められている。

１.内部統制の基本的要素が組み込まれたプロセスを構築し､それを適切に機能させる。

２．内部統制を整備・運用する役割と責任を有する。財務報告に係る内部統制については、その有効性を自ら評価し、その結果を外部に向けて報告する。同報告に係る評価では、以下を行う。

- 全社的な内部統制の評価
- 業務プロセスに係る評価
- 内部統制の有効性の判断
- 内部統制の重要な欠陥の是正
- 評価範囲の制約
- 評価手続き等の記録及び保存

さらには、経営者に財務報告に係る内部統制の有効性の評価に関する報告書の作成も求めている。

上記事項は､BCMでも求められているところでもある｡BCMもマネジメントシステム(PDCA)の中で、常に経営による承認が求められている。

これら共通・関連する項目の一体となった運営の検討が今後求められよう。

２．３　ＣＳＲとＢＣＭ

２．３．１　定義と国際的動向

CSR （corporate social responsibility：企業の社会的責任）は、一般的に「企業は社会的存在として、最低限の法令遵守や利益貢献といった責任を果たすだけではなく、市民や地域、社会の顕在的・潜在的な要請に応え、より高次の社会貢献や配慮、情報公開や対話を自主的に行うべきであるという考え」とされている。

国際的には、ＳＲ-Social Responsibility（社会的責任）※に関する国際規格ＩＳＯ26000 策定のワーキンググループ第３回総会が 2006 年 5 月にポルトガルのリスボンで開催、WD1（第１次作業文書）が検討され、定義と領域については以下の内容で合意された。

定義：

「社会および環境に対する活動の影響に責任を果たす組織の行動。それらの行動は、社会の関心と持続的発展整合のとれたものであり、倫理行動、遵法性および政府間文書に基礎をおいたものであり、かつ組織の既存活動と一体化したものであるとする」

領域：

① 環境
② 人権
③ 労働慣行
④ 組織のガバナンス
⑤ 公正な商習慣
⑥ コミュニティ参画・社会開発
⑦ 消費者課題

今後の動向だが、2007 年 1 月または 2 月にオーストラリアのシドニーでワーキンググループの第 4 回総会が開催され WD２（第 2 次作業文書）の検討および委員会原案（CD）の作成に向け準備が行われる。ＩＳＯ26000 の発行は 2008 年 10 月の予定であったが、2009 年の初めにずれ込む見込みである。

先進国では社会が豊かになるに従い、経済的成長以外のさまざまな価値観が育まれ、企業評価の指標として、法律や制度で決められた範囲を超えて“よりよい行動”をすることを望ましいとする傾向が生まれている。そこで企業がこうした社会的要請に応えることは、社会的行動の不足や欠落が招くリスクを回避するとともに、社会的評価や信頼性の向上を通じて経済的価値を高めることができると認識されるようになってきている。

実際の活動内容はさまざまで、従来的な「関連法規の遵守やコンプライアンス」「よい製品・サービスの提供」「雇用創出・維持」「税金の納付」「メセナ活動」などを含める向きもあるが、典型的な CSR 活動としては「地球環境への配慮」「適切な企業統治と情報開示」「誠実な消費者対応」「環境や個人情報保護」「ボランティア活動

支援などの社会貢献」「地域社会参加などの地域貢献」「安全や健康に配慮した職場環境と従業員支援」などがある。

その普及の直接的な要因としては、株式市場や格付機関が企業評価の尺度としてCSRの視点を取り入れるようになってきていることが挙げられる。英、仏、独などでは年金の投資先評価の際に、環境・社会・倫理面の評価を法律で義務付けている。CSRの視点を取り入れた投資のあり方を「社会的責任投資（SRI：socially responsible investment）」というが、環境対策や法令遵守、企業統治などを基準に投資先を選定した投資信託商品も発売されている。

国連においては1999年に「グローバル・コンパクト」が提唱され、OECD（世界労働組合会議）の「OECD多国籍企業ガイドライン」が2000年に更新されるなど、企業のグローバルな活動に対して、より高い倫理観による規制・ガバナンスを要請する動きも急で、ISO（国際標準化機構）では2008年～2009年をめどに国際規格化が進められている。

英、仏ではCSR担当大臣が置かれているが、日本においては企業や経済団体が主導的に活動しており、日本経団連「企業行動憲章」／経済同友会「自己評価ツール」などが提示されている。日本規格協会には「CSR標準委員会」が設置され、ISOの動きに対応した形で日本規格作りが進められている。

※ISOでは、SR（social responsibility）という呼称が用いられている。

内部統制とCSRの関連についても簡単に触れておくと、CSRを推進している企業では並行して内部統制システム構築にも取り組んでいる企業が多い。内部統制は、5月に施行された会社法や今般成立した金融商品取引法（日本版SOX法）でその体制整備が求められていることからも、企業にとって重要な課題である。

CSRと内部統制を同時に進めることは企業にとって大きな負担に思えるが、以下の共通点、効果が期待できる点では双方に取り組むことが効果的な推進活動を行うにあたり、必要不可欠ともいえる。

[CSRと内部統制の共通点]：

①企業の全事業領域を対象としている

②ステークホルダーの期待に応え､信頼を獲得する上で必要不可欠な前提条件である。

③企業のビジョンの実現や企業ひいては社会の持続的な発展を目的としている。

[内部統制システム構築の効果]：

①ステークホルダーとの関係をプラス・マイナス双方に変動させる要素が網羅的に把握できる。

②企業が目指す姿・ビジョンがを全役職員に共有、浸透させることが容易になる。

③ステークホルダーとの関係・優先順位、社会環境の変化に対して速やかに反応し、的確な対応が可能となる。

２．３．２　ＣＳＲとＢＣＭ

CSR の考え方は日本でも古くから「企業は人なり、社会の公器」という言葉があるように何も新しいものではない。CSR の活動については米国ではエンロンやワールドコムなどの企業不祥事や SRI（社会的責任投資）の残高増加に後押しされたり、日本では環境リスクマネジメントの延長に活動の基盤を置いたりとその取り組みに明確な方向性が見えていないのが現状である。

また、定義においても明確なものがあるわけではなく「コーポレートガバナンス＝企業経営」という立場からすれば各企業独自に経営の立場から定義されるべきである。CSR 推進の主体者は組織構成員個人であるので各個人の倫理ある行動がその根底になければ CSR は当然機能しない。CSR を標榜する企業はまさに倫理観ある行動に向けての体制作りが求められる。

リスクマネジメントおよび BCM との関係についてだが、最近日本では BCM はリスクマネジメントの一環、リスクマネジメントは CSR の一環という枠組みで取り組む企業が増えている。

企業のリスクが多様化、複雑化するなか自身を取り巻くリスクを効率的にマネジメントすることは各種のステークホルダーの期待に応えるのに必要不可欠であることは言うまでもない。

CSR の観点から行う BCM とは経済的、環境的、社会的利益（トリプルボトムライン）を目標とする BCM であり、認識されるべきリスクは企業の目的や目標のみを基準とするのではなく、社会的要請やステークホルダーからの期待や要求を踏まえたものでなければならない。

例えば BCM においては自らの資産の保全のみならず地域住民の安全、地域経済、雇用問題、製品やサービスの安定供給などを視野に入れて取り組む必要がある。

２．４　ITガバナンスとBCM

IT ガバナンスは一般的に「組織が、IT を導入・活用するにあたり、目的と戦略を適切に設定し、その効果やリスクを測定・評価して、理想とする IT 活用を実現するメカニズムをその組織の中に確立すること」とされる。

1999 年ごろ、通商産業省（現 経済産業省）と日本情報処理開発協会は、IT ガバナンスを「企業が競争優位性構築を目的に、IT 戦略の策定・実行をコントロールし、あるべき方向へ導く組織能力」と説明した。

IT 戦略の策定においては、ビジネス（ビジネスレビュー）、IT 技術（技術レビューとオプション）、導入戦略（ハイレベル導入戦略）の３つのエリアに対して明確に定義することから進めていくことになる。

ビジネスレビュー

- 組織ベースおよびユーザ必要条件の特定と識別
  ここで言う組織ベースとは企業の事業所や活動拠点を表し、ユーザとは組織を構成するメンバーを言う。これら両方の観点から企業がビジネスを遂行するために必要な要求事項の抽出を行う。
- 競合他社より優位に立つための IT コミュニケーション環境をどう活用するかについての特定と識別
- ステークホルダーの利益の特定と識別
- ビジネスベネフィット（利益）のマッピング
  生産、流通、経理、営業、マーケティング、情報システム、ビジネスサービスといった各部門で要求される IT 技術、機能とサービス（ニーズ）、それが提供された場合の求められる価値のマップ化を行う。マッピングを行う目的は、“ ニーズ分析を業務要求に転換 ”し、“ 必要不可欠な要求事項をクリアに認識 ” し、現時点から将来に渡る IT 投資の重み付けと優先順位付けの基礎とするところにある。
- 導入プログラムの立案

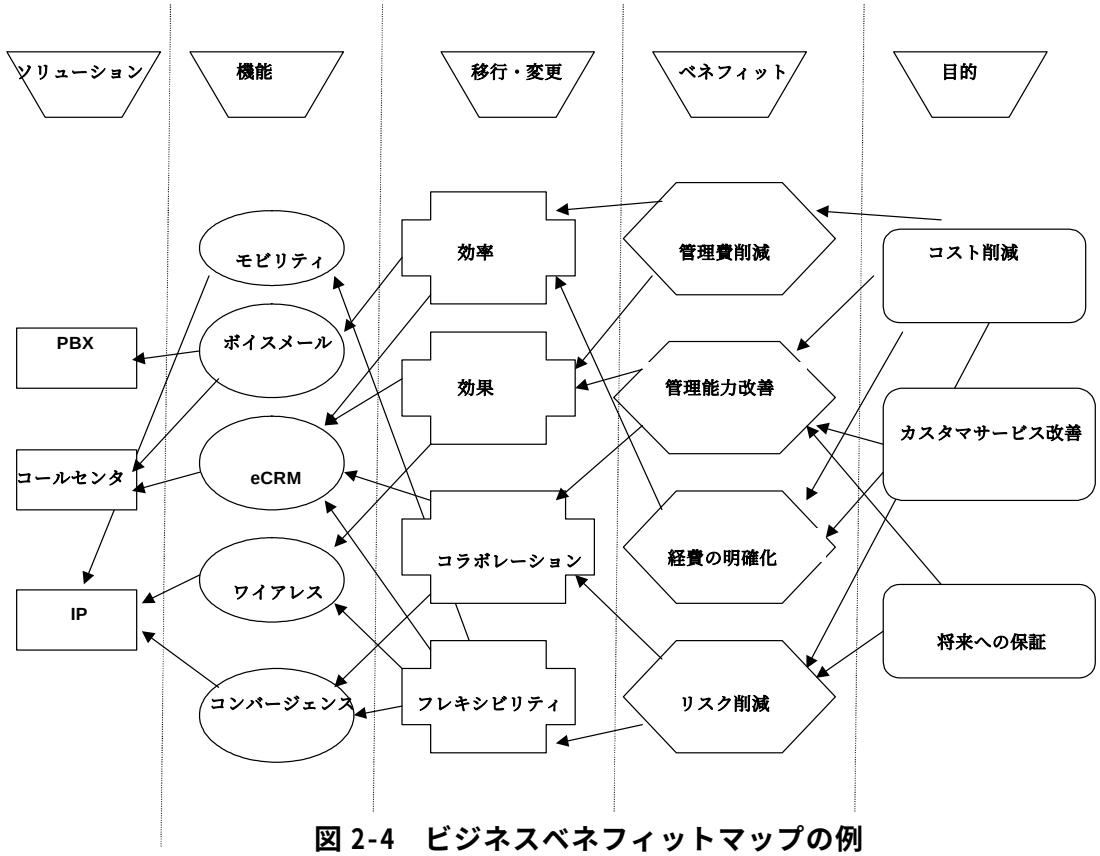


図 2-4　ビジネスベネフィットマップの例

上記例ではビジネス目的（右側）がベネフィット（達成利益）に分解され、必要とされる機能（IT 技術）とそれらを実現する IT ソリューションへと結び付けされているのを示している。　効率、効果、コラボレーション(例えば電話、Web、e-メールの統合された協調動作、eCRM で言えば電話だけではなくマルチチャネルで受付可能なコールセンター、コンタクトセンター)、フレキシビリティ４つの観点から必要とされる機能を導き出すのが移行･変更フェーズである。例えばビジネス目的である”カスタマサービス改善“を達成することによるベネフィットは”管理能力改善“、と”リスク削減“であり、これらを実現するためには、効率、効果の観点からは eCRM 機能（技術）が利用可能なコールセンターがソリューションとして結び付けされる。

技術レビューとオプション　(例)　（オプションとは選択肢のこと）

- **電子メールサーバーの現在の配置と、最適化のための分析を含む、電子メールシステムのインテグレーション検討**
- **導入する国内・国際ネットワークへの音声およびデータサービスの統合**
- **IT およびコミュニケーション管理方法の最適化**
- **ネットワークと IT セキュリティ**
  - **IT 資産を幾つかの特定した脅威から守るためのソリューション導入の検討**
  - **故意あるいは計画的に発生する電子的脅威に特化した対策**

- 現在と将来の運用上のニーズ、帯域、速度といったキャパシティーおよびコストにフォーカスした個々の IT サービスとソリューションの評価。さらに、それらがビジネス・プロセス改良計画の一部として関連付けできるかの評価
- 追加が必要なサービスとソリューションの特定
- プライオリティを、選択した技術におくか、または商業価値におくかを考慮した調達戦略の策定（優れた技術であっても調達できなければ意味がない）
- 導入ソリューションのリスク分析
  現行サービスデリバリに関する SLA（サービスレベル同意書）と新たなソリューションが現行サービスにもたらす影響の分析

ハイレベル導入戦略　(例)

- キーとなるコミュニケーション･サービスおよび IT システム稼動状況の把握
- 新ネットワークへの音声およびデータサービスの統合のアウトライン･スケジュールの確立
- キーIT プロジェクトの特定と、これらプロジェクトの導入計画への反映・統合
- 業務、サービスのアウトソーシング可否判断
- リスク分析
  ここで言うリスク分析は幾つかのソリューションについて自社で行うのか、アウトソースするのか、ソリューション構築を一社窓口で調達するのか複数サプライアと行うのかなど様々である。どのソリューションをどのような形態で導入するかについての強みと弱みのインパクトに対する分析となる。
- 業務・事業継続の活動低下・停止に対する防御と対応
  バックアップ・リストアプロシージャ
  ディザスターリカバリプラン

IT ガバナンスの実践

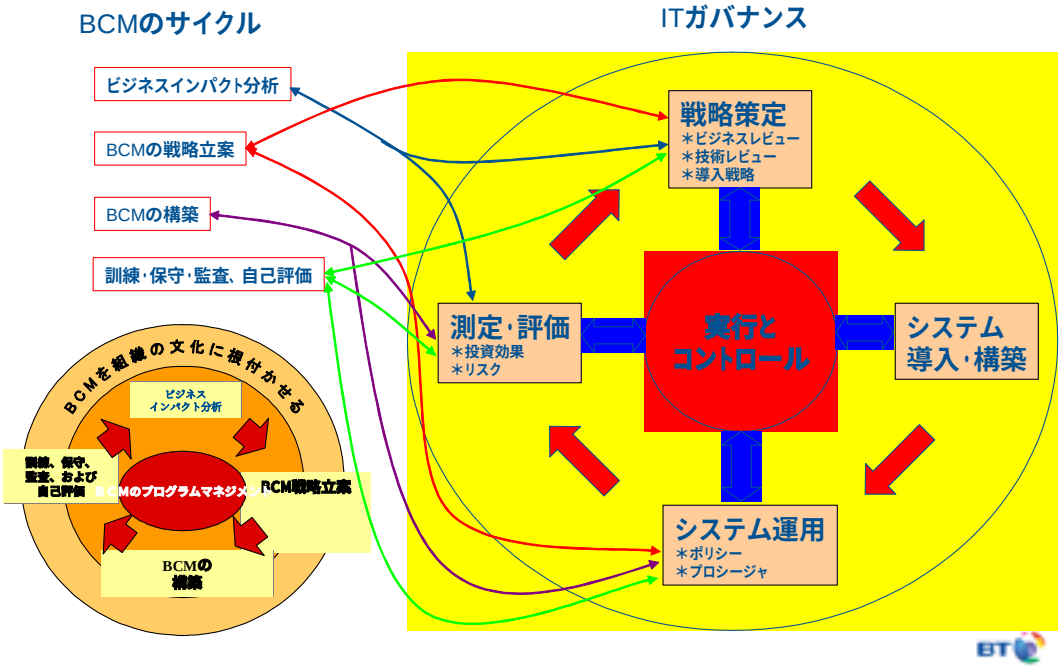
IT ガバナンスは企業の経営戦略と密接にリンクして実践されなければならない。経営戦略目標を達成するために必要な IT システムの構築・導入目的を明らかにし、投資効果とリスクを評価し、IT の運用と利用に関するポリシーとプロシージャをマネージメントするメカニズムを構築することで IT ガバナンスは確立される。

IT ガバナンス、IT システム構築から見た BCM との関連性

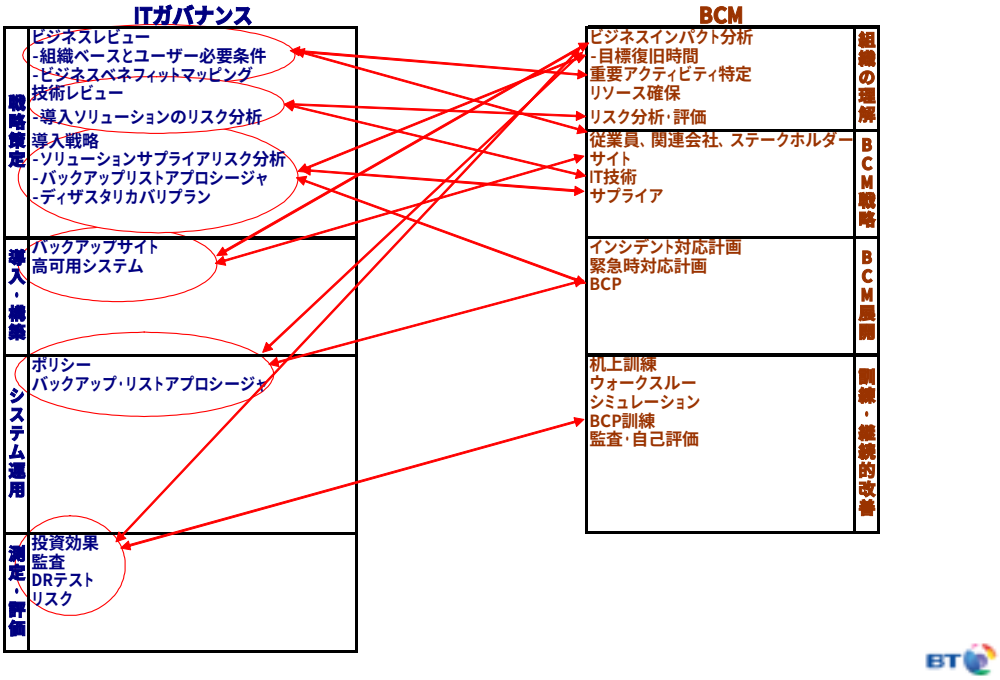
IT ガバナンスは BC･セキュリティにもフォーカスをあてて実践されなければならない。IT ガバナンスにおける実行とコントロールサイクルは BCM のサイクルと関連付けされるべきである。BCM のビジネスインパクト分析（BIA）は組織の理解を行い、業務やリソースの特定を行うことから、IT 戦略策定におけるビジネスレビュー、導入戦略と結び付けされる。例えば導入戦略で掲げるディザスターリカバリプランの実行は BIA で設定される目標復旧時間を達成するものとしなければならない。BCM 戦略立案は技術レビューと導入戦略、システム運用プロシージャに反映されなければならない。

例えば導入 IT 技術のひとつであるネットワークは高可用性、レジリエンシを持ったもの（拠点接続における通信事業者の二重化など）を選択する必要がある。BCM 構築におけるリスクマネジメントの推進は IT システムにおけるリスクの測定、評価を活用し脅威の低減を目指さなければならない。

ITガバナンスから見たBCMとの関連性



ITガバナンスから見たBCMとの関連性（詳細）



IT システム構築においては復旧を前提としたインフラ技術の選択や高可用性、レジリエンシシステムの設計、どのような状況であれ電話通信は継続利用ができるようなオプションを導入したりする必要があるであろう。昨今発生した通信事業者による IP 電話利用の低下や停止が企業に与えた不安はひとつの教訓である。IT システム構築から見た BCM は、業務・事業の活動低下・停止に対する防御と対応が重要なポイントとなる。

セキュリティに関しては、IT 環境上の問題にフォーカスをあてた IT セキュリティと企業ビジネスの観点から見た情報セキュリティをしっかりと認識しておく必要がある。

情報セキュリティについては企業のビジネス領域（つまりコアビジネス）と密接に関連することから社内にチームを組織して十分に戦略と体制を練る必要がある。

IT セキュリティについては IT サービスの一部として戦略の方向性と分解点（つまりノンコアビジネス）を見極め、アウトソーシングの可能性を探る必要があるであろう。

実際、欧米企業の間では、IT セキュリティ管理を社内で行うべきかアウトソーシングすべきかという問題が取締役会の重要議題となっている。効果的なセキュリティ管理を行うためには、最先端の製品と技術を使わなければならないことはもちろんのこと、優秀なセキュリティ・スタッフが綿密に準備された手順によってセキュリティ管理ソリューションの作成、統合、保守を行う必要がある。不足する部分が少しでもあれば、不十分なセキュリティしか得られず、事業に破滅的な損害が発生することも考えられる。セキュリティ・インフラの運用保守に多大な時間と予算を投入してきた企業にとって、このように重要な問題を第三者と共有すること、ましてやアウトソーシングすることなど、つい最近までは考えられないことだったに違いないが、より高度なハッキング・ツールが簡単に入手できるようになったことから、専門家の支援を受けずに各企業レベルでどこまで効果的な対処ができるのかを再検討をしなければならない状況が発生している。

以下に IT システム構築から見た BC・セキュリティに関する IT 各領域の検討事項を掲げる。

ITシステム構築から見たBC･セキュリティ

分野	1.アウトソーシング	2.コンタクトセンター/CRM	3.IPインフラストラクチャー	4.モバイル通信
対象	マネージドサービス ネットワークアウトソーシング ビジネスプロセスアウトソーシング IT アウトソーシング	コンタクトセンター コンタクトセンターのセルフ／アウトソース運用 マネージドプロフェッショナルサービス CRMアプリケーション	WAN IPテレフォニー LAN オプティカル SAN	接続性 複合ソリューション
セキュリティ	セキュリティギャップ分析（ISMS監査） ベンダー選定/評価 ポリシー、スタンダード、プロシージャ策定	コンタクトセンターセキュリティアーキテクチャ ポリシー、スタンダード、プロシージャ	ポリシー、スタンダード、プロシージャ策定 セキュリティアーキテクチャ セキュアネットワーキング ファイアウォール ISMS監査	ポリシー、スタンダード、プロシージャ策定 ワイヤレスLANのセキュリティ モバイルセキュリティポリシー リモート通信のセキュリティ
事業継続（BC）	BCアウトソーシング戦略策定 ベンダー向けRFQ策定 DRベンダー選定 遵守状況の評価	コールセンターリスク評価 コールセンタービジネスインパクト分析 DRプロセスおよび計画 DRテスト BCP監査 金融業界規制の準拠	復旧を前提としたインフラ技術の選択 高可用性、高回復力システムの構築 電話通信の継続	事業継続における俊敏性 モバイルに対するリスク評価

ITシステム構築から見たBCM･セキュリティ

分野	5.デスクトップ管理	6.アプリケーション管理およびホスティング	7.サーバ/プラットフォーム
対象	パッケージソリューション	メッセージング インターネット Eコマース（ビジネスアプリケーション） ホスティング	システムハードウェア、ソフトウェア（OS、ミドルウェア） サーバシステム設計 サーバ実装 サーバシステムアウトソース
セキュリティ	ポリシー、スタンダード、プロシー策定 デスクトップセキュリティ ウイルス対策アーキテクチャ	ポリシー、スタンダード、プロシージャ策定 ペネトレーションテスト PKI等認証ソリューション セキュアポータルサイトの構築 セキュリティリスク評価 ウイルス対策	ポリシー、スタンダード、プロシージャの策定 セキュアOSによる強化 ペネトレーションテスト 脆弱性分析 セキュリティペリメタ検査 ネットワークとサーバー間のセキュリティ
事業継続計画	リカバリー要求度合いの決定 バックアップ･リストアプロシージャ	バックアップ･リストアプロシージャ バックアップサイト構築 危機管理チームの構築	バックアップ･リストアプロシージャ バックアップサイト構築 デザスターリカバリプランの策定

2.5　情報セキュリティとＢＣＭ

組織の経営に不可欠である情報を適切に保護する認識は年々高まっている。情報が適切に保護されていないことが原因で漏洩したり、内容が不正確であったり、必要な時に使えない等、業務の遂行に支障をきたすといったリスクが高まったためである。「情報セキュリティ」とは、重要な情報をこうしたリスクから守ることをいう。

2.5.1　情報セキュリティとは

ISO/IEC 27001:2005(JIS Q 27001:2006)（以下、「本認証基準」という。）では、情報セキュリティを以下のように定義している

> 3. 情報セキュリティ(information security)
> 情報の機密性，完全性及び可用性を維持すること。さらに，真正性，責任追跡性，否認防止及び信頼性のような特性を維持することを含めてもよい。
> (JIS Q 27001:2006 3 用語及び定義　より)

つまり、情報セキュリティとは、情報に関連する資産に関わるリスクを明確にするために、情報セキュリティの主たる３要素である「機密性」、「完全性」、「可用性」のそれぞれの観点から分析し、必要な対策を確実に実行することをいう。その他、真正性、責任追跡性、否認防止、信頼性の４つの特性は、通常上記３つの要素から導くことができると考えられる。

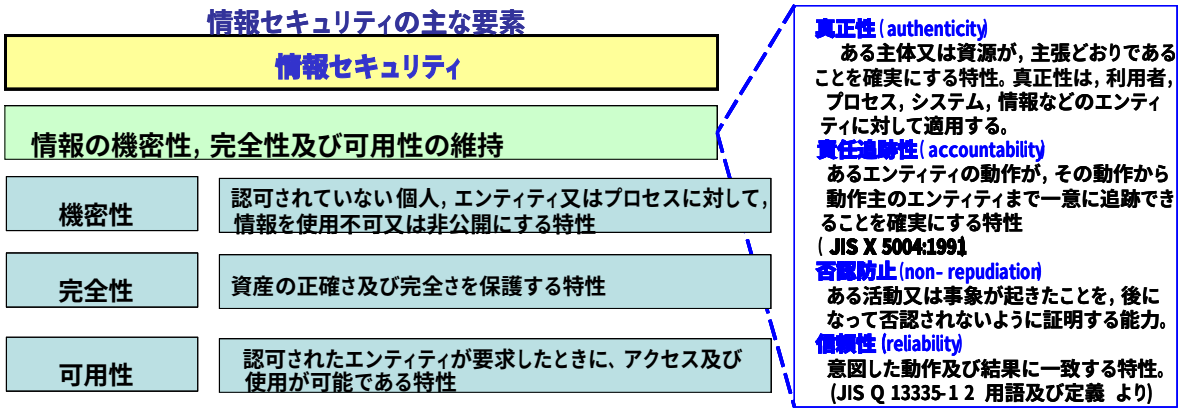


図 2-5-1　情報セキュリティの主な要素

「機密性」、「完全性」、「可用性」は、1992 年に発行された「OECD 情報セキュリティガイドラインに関する委員会勧告」[1]の附属文書「情報システムのセキュリティガイドライン」[2]（以下、「OECD ガイドライン」という。）において定義されて以来使われてきた。

[1] Recommendation of the Council concerning Guidelines for the Security of Information Systems(adopted by the Council at its 793rd Session of 26-27 November 1992)

[2] Guidelines for the Security of Information Systems,26 November 1992

情報システムの機密性、完全性及び可用性を阻害する危害（harm）から情報システムを保護すること

（OECD ガイドライン:1992　より引用）

この 3 つの「～性」は、その頭文字をとって「情報セキュリティの C.I.A」と言われることがある。

本認証基準では、機密性、完全性、可用性を以下の様に定義している。

2.機密性(confidentiality)
認可されていない個人，エンティティ又はプロセスに対して，情報を使用不可又は非公開にする特性。

（JIS Q13335-1:2006 2 用語及び定義　より）

情報の機密性は、「情報漏洩しないようにする」ことに関連する。

5.完全性(integrity)
資産の正確さ及び完全さを保護する特性。

（JIS Q13335-1:2006 2 用語及び定義　より）

完全性には二つの意味がある。一つは情報そのものの完全性を確保することをいう。これは「情報が改ざんされないようにする」ことに関連する。

もう一つは情報処理の方法の完全性をいう。これは、「情報システムが勝手に変更されないようにする」ことや「情報の取扱いが手順化されていて、その手順が確実に順守されるようにする」こと等に関連する。

1.可用性(availability)
認可されたエンティティが要求したときに，アクセス及び使用が可能である特性。

(JIS Q13335-1:2006 2 用語及び定義　より)

可用性は、「自然災害やシステムダウンなどにより、情報が使えなくなること」に関連し、BCM との関連性が高い。

情報に関連する資産には，次のような多くの種類がある。

a) 情報：データベース及びデータファイル，契約書及び同意書，システムに関する文書，調査情報，利用者マニュアル，訓練資料，運用手順又はサポート手順，事業継続計画，代替手順の取決め，監査証跡，保存情報
b) ソフトウェア資産：業務用ソフトウェア，システムソフトウェア，開発用ツール，ユーティリティソフトウェア
c) 物理的資産：コンピュータ装置，通信装置，取外し可能な媒体，その他の装置
d) サービス：計算処理サービス，通信サービス，一般ユーティリティ（例えば，暖房，照明，電源，空調）
e) 人，保有する資格・技能・経験
f) 無形資産（例えば，組織の評判・イメージ）

（JIS Q 27002:2006 より引用）

これらは、組織に対しての価値，法的要求事項，取扱いに慎重を要する度合い及び重要性の観点から分類することが望ましい。

（JIS Q 27002:2006 より引用）

２.５.２　情報セキュリティから見た BCM との関連性

ここまで、情報セキュリティの定義について記載した。次に、情報セキュリティマネジメントシステム（ISMS）と事業継続管理について、説明する。

２.５.２.１　事業継続管理における情報セキュリティの側面

ISMS において、事業継続管理については、特に情報および情報処理施設に関連する資産の損失からの防御ならびに復旧について触れている。

JIS Q 27002:2006(ISO/IEC17799: 2005)では、以下のように事業継続管理について記載している。

> 目的:情報システムの重大な故障または災害の影からの事業活動の中断に対処するとともに、それらから重要な業務プロセスを保護し、また、事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。
>
> 組織への影響を最小に抑えるため、及び予防的管理策と回復のための管理策との組み合わせによって、情報及び情報処理施設に関連する資産の損失（例えば、自然災害、事故、装置の故障及び悪意による行為の結果の場合がある。）を受容可能なレベルにまで回復するために、事業継続管理手続を実施することが望ましい。この手続では、重要な業務プロセスを識別すること、並びに運用、要員配置、資材、配送及び設備といった点で関連する。情報セキュリティ管理面以外の事業継続の要求事項と情報セキュリティ管理面の事業継続の要求事項とを統合することが望ましい。
>
> 災害、セキュリティ不具合及びサービス停止の結果、並びにサービスの可用性を、事業の影響分析の対象とすることが望ましい。必要不可欠な運用の時機を失しない再開を確実にするために、事業継続計画を策定し、実施することが望ましい。情報セキュリティは、組織の包括的な事業継続手続き及びその他の管理策手続の、必要不可欠な部分であることが望ましい。
>
> 事業継続管理には、リスクを特定して低減するための管理策のほか、リスクアセスメントの手続に加え、損害を与えるインシデントの影響から抑制するための管理策、及び業務プロセスに必要な情報が常に利用可能であることを確実にするための管理策を含むことが望ましい。
>
> （JIS Q 27002:2006　14.1　事業継続管理における情報セキュリティの側面　より引用）

上記の内容について、事業継続管理における P-D-C-A でまとめると、以下のようになる。

- P（計画）：手続きの策定、BIA,リスクアセスメント、BCP の策定と実施
- D（実行）：BCP の実施
- C（点検）・A(改善）：事業継続計画の試験、維持及び再評価

具体的な取組みとして、以下のような5項目に関して記載している。

2.5.2.1.1 事業継続管理手続への情報セキュリティの組込み

事業継続のために、組織の事業継続に必要な情報セキュリティの要求事項を取り扱う管理された手続きを、策定し、維持するためのコントロールが紹介されている。

ここで、手続きとして推奨されるものには、

- 重要な業務プロセスの識別と優先順位付けのための手続き
- 直面しているリスクを可用性および影響面から理解するための（測定するため）手続き
- 重要な業務プロセスにかかわるすべての資産を識別するための手続き
- 業務プロセスの中断が事業に及ぼすと思われる影響を理解し、情報処理施設の事業目的を確立するための手続き
- 適切な保険への加入のための手続き
- 予防、緩和のための追加策の特定及び実施のための手続き
- 情報セキュリティの要求事項を取り扱うために十分な、財政上、組織上、技術及び環境上の経営資源を特定するための手続き

などをあげている。

2.5.2.1.2 事業継続及びリスクアセスメント

業務プロセスの中断を引き起し得る事象、そのような中断の発生確率及び影響、並びに中断が情報セキュリティに及ぼす結果等を特定するためのコントロールが紹介されている。

ここでは、以下の事項の実施が推奨されている。

- 業務プロセスの中断を引き起こし得る事象（又は一連の事象。例えば、装置の故障、人による誤り、盗難、火災、自然災害、テロ行為）を特定する
- 業務プロセスの中断の発生確率及び影響を時間、損傷規模及び回復期間の面から判断するために、リスクアセスメントを行う。
- リスクアセスメントは、事業資源及び業務プロセスの管理者の全面的な関与の下で実施すること。
- リスクアセスメントは、すべての業務を検討し、情報処理施設に限定しないことが望ましいが、情報セキュリティ特有の結果を含むこと。
- リスクアセスメントでは、組織の事業管理に関する要求事項の全容を把握するために実施する。
- リスクアセスメントでは、組織に関連した基準及び目的（目標）に対して、リスクの特定、定量化及び優先順位付けをする。
- 組織に関連した基準及び目的（目標）には、重要な資源、中断の影響、受容可能な停止時間及び回復の優先順位を含むこと。
- リスクアセスメントの結果に応じて、事業継続に対する包括的な取組方法を決定するために事業継続戦略を策定し、経営陣から承認を得ること。

- 戦略を実施に移すために計画を立て、承認を得ること。

2.5.2.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施

重要な業務プロセスの中断又は不具合発生の後、運用を維持又は復旧するために、また、要求されたレベル及び時間内での情報の可用性を確実にすうために、計画を策定し、実施するためのコントロールが紹介されている。

ここでは、事業継続計画の策定プロセスで、以下の事項を考慮することが推奨されている。

- すべての責任及び事業継続手順の特定及び合意。
- 受容可能な情報の損失及びサービス停止の特定。
- 業務の運用、並びに情報の可用性の回復及び復旧を、要求された時間内で可能にする手順の実施。このとき、内部の事業間及び外部の事業との事業上の依存関係、並びに締結済みの契約を評価すること。
- 損傷を受けたプロセスが回復及び復旧するまでの、損傷を受けなかったプロセスにおける運用手順。
- 合意された手順及び手続きの文書化
- 危機管理を含む、合意された手順及び手続きについての、適切な要員教育
- 計画の試験及び更新

また、事業継続計画の策定プロセスでは、要求される事業目的（例えば、顧客向けサービスを受容可能な時間内に復旧すること）に重点を置き、事業継続計画の実行を支持するサービス及び経営資源を特定することを重要視している。

2.5.2.1.4 事業継続計画策定の枠組み

すべての計画が整合したものになることを確実にするため、情報セキュリティ上の要求事項を矛盾なく取扱うため、また試験及び保守の優先順位を特定するために、一つの事業継続計画の枠組みを維持するためのコントロールが紹介されている。

ここでは、事業継続計画に記載されるべく項目や考慮すべく関連事項について推奨している。

- 各事業継続計画では、事業継続の取組み方（例えば、情報又は情報システムの可用性及びセキュリティを確実にするための取組み方）を記述する。
- 各計画では、計画の各要素の実行について責任を負う各個人だけではなく、その段階的計画及びその発動条件をも定める。
- 新しい要求事項が明確になった場合、既存のいかなる緊急時手順（例えば、非難計画、代替手段利用計画）を適切に改訂する。
- 事業継続上の問題を常に適切に取扱うことを確実にするための手順を。変更管理プログラムに組み込む。
- 各計画にそれぞれの管理者を置き、緊急時手段、手動による代替手段利用計画及び再開計画は、該当する事業資源又は関連するプロセスの管理者の責任の範囲とする。

2.5.2.1.5 事業継続計画の試験、維持及び再評価

事業継続計画が最新で効果的なものであることを確実にするために、多だめに従って試験・更新するためのコントロールが紹介されている。

事業継続計画の試験において、関連要員が次の事項を認識することを推奨している。

- 事業継続計画、並びに事業継続及び情報セキュリティに対する自身の責任
- 計画が発動された場合の自身の役割

また、計画が実際に役立つことを保証するために、以下のような手法を用いることを推奨している。

- 様々な状況の机上試験
- 模擬試験
- 技術的回復試験
- 代替の事業場所における回復試験
- 供給者の設備及び供給サービスの試験
- 全体的な模擬試験回復

加えて、上記のような試験の結果を記録し、それらを評価した上で、必要に応じて計画を改善することは重要である。そのためには、各事業継続計画の手順に従ったレビューに対する責任を割り当てておくことも重要である。

2.5.2.2 情報セキュリティにおけるBCMの取組み

上記のように、情報セキュリティにおけるBCMの取組みは、前述のBCMの取組みと整合が取れているといえる。

一方、情報セキュリティが取扱う資産（対象とする資産）は、BCM全般から見ると、その範囲が限定されるため、BCMが対象とするリスクと情報セキュリティが対象とするリスクが異なる場合がある。

以下に前述のBCMにおけるリスク表例を基に、情報セキュリティの範疇であるリスクについてまとめる。記号は、深く関与するが○、ある程度関与するが△、関与しないを×とした。

但し、下表はあくまでも一例であり、情報セキュリティマネジメントシステムの限界を示しているものではない。

リスク分類（例）

事業リスク		情報セキュリティの範疇
財物リスク	自然災害（地震、台風等）	○
	火災・爆発	○
	電気的・機械的事故	○
	輸送中の事故	○
人的リスク	役員・従業員の就業中の事故	○
	雇用（人手不足等）	○
	キーパーソンの喪失	○
	テロ	△

	誘拐	△
	ストレス・ノイローゼ	×
情報リスク	情報システム障害	○
	コンピュータウィルス	○
	情報漏えい	○
	サイバーテロ	○
財務リスク	不正な財務処理、入力ミス	○
	虚偽の表示	×
	流動性損失	×
コンプライアンス（法令等の遵守）	証券取引法への抵触	×
	個人情報保護法への抵触	○
風評リスク（直接的）	うわさ	△
市場リスク	金利リスク	×
	為替リスク	×
信用リスク	貸し倒れリスク	×
賠償責任リスク	施設に関わる賠償責任	△
	業務・作業に関わる賠償責任	△
	製品の欠陥	×
	知的財産に関わる賠償責任	○
	環境汚染に関わる賠償責任	×
	会社役員の賠償責任	△

III部　参考資料（BS25999-1 と各領域との整理）

ISO 標準の有力候補

１．BCM 規格 「BS25999-1」

「日経コンピュータ」2007 年 2 月 5 日号 p57-p59 から転載

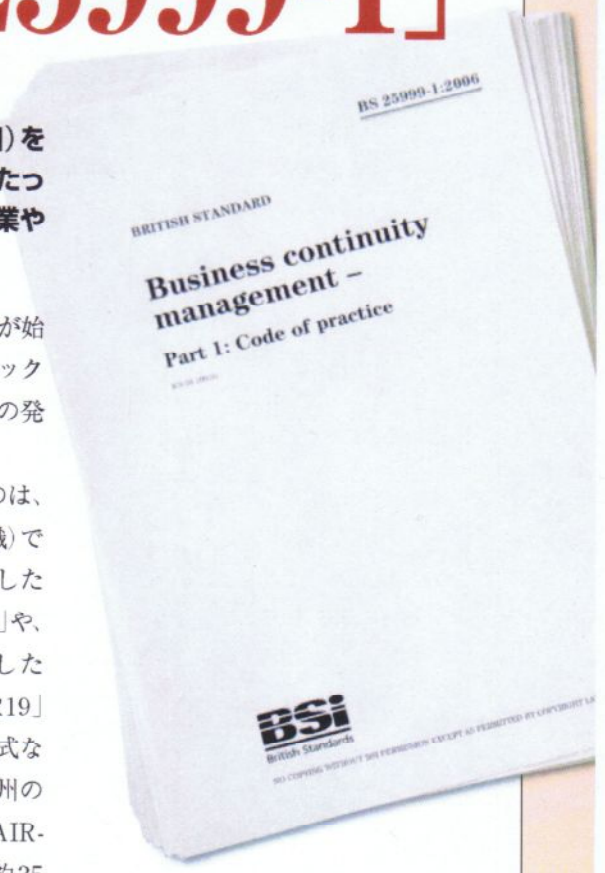
寄稿

ISO標準の有力候補
BCM規格「BS25999-1」

昨年11月28日、BSI（英国規格協会）が事業継続マネジメント（BCM）を実現するための規格「BS25999-1」を発行した。A4判42ページにわたって、BCM導入・改善の指針を示している。BCMに取り組み始めた企業や自社の仕組みが有効であるかを確認したい企業にとって有用だ。

BCI（事業継続協会）日本支部代表
篠原 雅道（Masamichi Shinohara）

リスク・マネジメント専門会社インターリスク総研 BCM室で主任研究員を務める。03年12月にBCIの日本支部代表に就任したほか、経済産業省BCP国際標準化委員会委員、内閣府委員、NPO事業継続推進機構の副理事長なども務める



BS25999-1の正式名称は、「British Standard, Business Continuity management-Part1：Code of practice」。発行の目的は、「組織内におけるBCMの理解、発展および実施の基礎となること」と、「企業間取引および顧客と企業間の取引を確かなものにすること」である。そのために必要な、BCMの定義やBCM取り組みのフレームワーク、取り組み方法などを示している。すでにBCMを導入している組織であれば、その実効性を推し量る"ものさし"として使うこともできる。

実はBS25999-1とは別に同-2が存在する。今回の「-1」は自己認証のための規格。昨年6月にBSIがドラフトを公表してパブリック・コメントを募集し、11月に正式版を発行した。現在は国際標準化機構（ISO）に対して、国際標準として活用するように提案している段階だ。一方の「-2」は第三者認証の規格になる見込みである。すでに議論が始まっており、企業監査条件やチェックポイントなどを規定して今年7月の発行を予定している。

BS25999-1のベースとなったのは、BCMに特化したNPO（非営利組織）であるBCI（事業継続協会）が発行した「BCI Good Practice Guidelines」や、ANSI（米国規格協会）が作成した「NFPA1600」、シンガポールの「TR19」などである。ドラフト作成から正式な発行までは、英国政府、BCI、欧州のリスクマネジメント団体であるAIRMICや主要な産業界のメンバー約35人で構成した委員会が担当した。

最初のステージは組織の理解

BS25999-1は10章で構成する（次ページの**表5**）。1章では、前述した目的のほか、適用対象を示す。具体的には適用対象として、経営層から現場の業務担当者まで、巨大企業から個人事業主までと、あらゆる階層、組織で利用できる。

2章で用語を定義しており、3章と合わせてBCMの全体像を明らかにする。実際のBCPやBCMの定義は、次ページに示した**表6**の通り。BCPは事業継続のための"計画"であり、その活用を含めて、事故や災害などが発生したときに事業を継続させ、継続に向けた活動を企業内に根付かせることを戦略的にマネジメントするのがBCMである。

そうしたBCMを実現するには、PDCAサイクルに基づいたマネジメント・システムの構築や、BCM文化を組織に浸透させることが必要不可欠だ。最終的には59ページの**図13**にあるようなBCMのライフサイクルを確立する。そのために何をすべきかを、5章以下で説明している。

まず5章のプログラム・マネジメントは、全体の進め方だ。組織の大きさや複雑さに合わせて、どのように考えればよいかを示している。具体的には、責任者をどう割り当てるか、ステークホルダー(利害関係者)との連携やトレーニングの実施といった実装法、継続的なマネジメント実施の重要性を説く。

プロセス確立の最初のステージである「組織の理解」を説明するのが、6章だ。組織の重要な製品やサービス、それらを提供するのに必要な活動とリソースについて説明する。

特に重要な作業が、ビジネス・インパクト分析である。事業が停止した場合の影響を洗い出し、事業が継続できなくなった後にその活動を再開する必要があるまでの最大許容停止時間を確立する。その際には、事業の再開時における事業活動の最低レベルや、事業を通常レベルまでに復旧させる時間も考慮する。最大許容停止時間を勘案しながら、企業としての戦略でもある目標復旧時間を定める。

災害発生時などには、優先順位に応じて活動する必要がある。ビジネス・インパクト分析の結果から、即座に復旧すべき活動(アクティビティ)を「重要なアクティビティ」として特定する。目標復旧時間内に確実に復旧できるよう事前に手配しておかなければならない活動も、「重要」だ。

こうした活動を支えるため、リソースを確保する必要がある。人(People)、サイト(Premises)、技術(Technology)、情報(Information)、外部機関・取引先(Supplies)が、リソースである。例えば「人」であれば、人数のほか、必要なスキルや知識も考慮に入れなければならない。

最後に、重要なアクティビティに対するリスク評価を実施する。

「BCMの展開」でBCPを作成する

次のステージとして7章が示しているのが、「事業継続に関する戦略」である。上記のリソースにステークホルダー(Stakeholders)を加えた六つの観点で、戦略を策定する。

「人」では、組織のコアスキル、ノウハウを維持することが必要だ。対象は従業員だけでなく、関連会社、ステークホルダーにまで広げる。「サイト」では社内外の代替場所の活用を考える。「技術」としては、事業復旧にはシステムの復旧が必要なケースが多く、その依存度分析が重要だ。技術の地理的な分散やリスク低減策の実施も考えなければならない。「情報」は守秘性などに注意。「外部機関・取引先」では、事業継続に必要かつ重要な取引先を特定し、その対策を考える。取引先を多様化したり、取引先に対してBCPの策定を要請したりする。「ステークホルダー」には、社会的責任を念頭に置きながら利益を守ることを考える。

こうした一連の戦略や、戦術的オプ

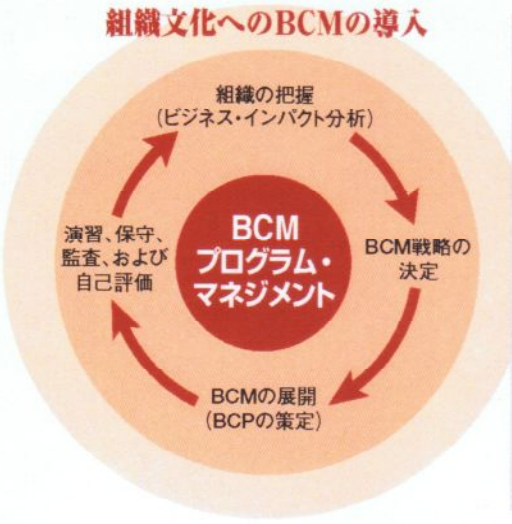
表5◉BS25999-1の章構成

項目	内容
1章 スコープと適用性	BS25999-1の目的。具体的には、「組織内でBCMを構築・展開・実装するための一貫した手法を提供し、BCMの能力を高めること」と記載
2章 定義	BCMやBCP、リスク・マネジメントなどの定義
3章 BCMの概観	BCMと組織戦略の関係、BCMとリスク・マネジメントとの関係、BCMの成果物、BCMのライフサイクル
4章 BCMの方針	BCMに関する活動が確実に実施されることを示す文書の作成
5章 BCMのプログラムマネジメント	BCMを推進するにあたってのプログラム・マネジメント。責任の明確化や、ステークホルダーとの連携などを記載
6章 組織の理解	ビジネス・インパクト分析、重要なアクティビティ、事業継続にあたっての要求事項、リスク評価の仕方など
7章 事業継続に関する戦略	キーパーソン、サイト、技術、情報、取引先、ステークホルダーなどに関する戦略的なオプション
8章 BCMの展開	組織体制、BCPの策定
9章 訓練、継続的改善	訓練プログラムなど
10章 BCM文化の構築・浸透	BCMの意識付けや、スタッフのスキル向上など

表6◉BS25999で定めているBCP、BCMの定義

BC (Business Continuity)	事故や災害などによって引き起こされる事業停止に対して、事前に定義した"許容可能なレベル"で事業運営を継続するための戦略的・戦術的な組織機能。経営者によって承認されていることが前提
BCP (Business Continuity Plan)	事業停止に際して、重要な製品やサービスが供給できるように策定・維持されている一連の手順や情報
BCM (Business Continuity Management)	組織を脅かす潜在的なインパクトを認識し、その脅威が現実となった場合に引き起こされる事業運営への影響を特定する包括的なマネジメント・プロセス。このプロセスにより、組織の主要な利害関係者の利益や、組織の名声、ブランド、および価値を創造する活動を守るために効果的に対処できるようになり、組織の回復力を構築するためのフレームワークが提供される

図13◉BCM構築・確立のためのプログラム・マネジメント



BCM関連文書の例□

a. BCMの方針
- スコープ・ステートメント
- BCM関連用語の定義

b. ビジネス・インパクト分析
c. リスク評価分析
d. BCMに関する戦略
e. 組織に所属する人間に対する意識向上プログラム
f. トレーニング・プログラム
g. インシデント対応計画
h. 事業継続計画 (Business Continuity Plan)
i. 事業復旧計画 (Business Recovery Plan)
j. 演習計画
k. サービス・レベル・アグリーメント (SLA)

ションをきちんと立てられれば、混乱時にも混乱後にも、重要な製品やサービスを提供し続けることができる。

8章で説明するのが、BCMの展開である。必要な組織体制を構築した上で、各種の計画を作成する。業務を復旧させるために取るべき手順を詳述した事業継続計画(BCP)や、インシデント対応計画などだ(図13右)。

これらすべての計画には、目的とスコープ、役割と責任、計画の発動条件、管理者、連絡先を記す。BCPでは、災害など発生直後のタスクとアクション・リスト、リソースの特定と配分、責任者などが必須項目だ。さらにインシデント対応計画には、メディア対応やステークホルダーへの対応などを記載する。

残るは、9章で説明している訓練と継続的改善である。訓練に関するプログラムを策定するが、机上訓練やシミュレーション、実地訓練などを行う。さらに、監査や自己評価に関する方法についても定めておく必要がある。こうした訓練や継続的改善を行うことで、組織は、その戦略と計画が効果的で目的にかなっていることを証明できる。

こうしたステージを経て、図13で示したBCMのライフサイクルを確立するわけだが、すべてのステージを通して考えなければならないことがある。それが、10章で解説している「BCM文化の構築・発展」である。

組織の文化としてBCMを根付かせることができれば、BCMは組織の"価値"の一部となる。具体的には、下記のような効果を生む。

- BCMプログラムを、より効率的に開発・運営できる。
- 混乱に対処する能力に関して、ステークホルダー(特にスタッフと顧客)に自信を植え付ける。
- すべての行動においてBCMが検討され、時間の経過とともに組織のレジリエンシ(脅威に対する対応・復旧力)が増加する。
- 混乱による影響と混乱の発生可能性を最小限に抑える。

08～09年予定のISO化に提案

以上が、BS25999-1で示されている内容の概略である。冒頭でも説明したようにBS25999-1は、自社の達成状況を把握するための規格である。第三者機関による認証があるわけではないが、BCMの導入を検討している企業にとっては有用なひな型になる。

BS25999-1はBSIのWebサイト(http://www.bsi-global.com/Risk/BusinessContinuity/bs25999.xalter)から購入できる。価格は、90ポンドである。

最後に、BCMに関する国際標準化について触れておきたい。

ISOでは、企業や自治体などの緊急時対応について国際標準化することを決めており、昨年4月に米国で第1回の国際会議を開催。13カ国からの出席者により様々な観点で議論が行われた。

この会議に先立ち、英国がPAS56(現在はBS25999)、米国・カナダがNFPA1600、オーストラリアがHB221をISOのドラフトとして提示したほか、イスラエルや日本も独自のドラフト案を示した。現在ISOでは、正式にTC(技術委員会)223が立ち上がり、議論している。2008～09年頃にBCMのISO化が実現する予定だ。

【参考文献】

- *Business Continuity management-Part 1: Code of practices*, British Standards, 2006年
- *Business Continuity Management Good Practice Guidelines*, The Business Continuity Institute, 2005年
- 小林誠 監修、『事業継続マネジメント(BCM)構築の実際』、日本規格協会、2006年
- 江尻明隆 著、『リサーチビュー 事業継続マネジメント(BCM)の国際規格化の潮流』、インターリスク総研ニュースレター、2006年

２．BCM と各領域の関係

- BCM 構築の必要性
- BCM 英国規格(BS25999-1:2006)の概要
- BCM と他領域との関係整理

  (内部統制、リスクマネジメント、ＣＳＲ、情報セキュリティ、
  ＩＴガバナンス)

内容

Ⅰ．BCM構築の必要性

Ⅱ．BCM英国規格(BS25999-1:2006)の概要

Ⅲ．BCMと他領域との関係整理

＊内部統制、リスクマネジメント、
ＣＳＲ、情報セキュリティ、ＩＴガバナンス

Ⅰ．ＢＣＭ構築の必要性

事業継続を脅かした災害・事故・事例

１９９５年：	阪神淡路大震災
２０００年：	西暦２０００年問題
２００１年：	米国同時多発テロ
	ー多数の企業が事業継続の観点から影響を受け明暗を分ける
２００３年：	ＳＡＲＳが発生。 宮城県沖地震。 北米大地震
２００４年：	台風２３号。新潟県中越大震災。需要逼迫による原料不足
２００５年：	福岡県西方沖地震。関東でも震度５強の地震発生。 ロンドンシティでテロ。 東証システム障害
２００６年：	東京で送電ケーブル損傷 台湾南部地震で国際海底ケーブル切断
２００７年：	千島沖でＭ７．８の地震発生 鳥インフルエンザが流行

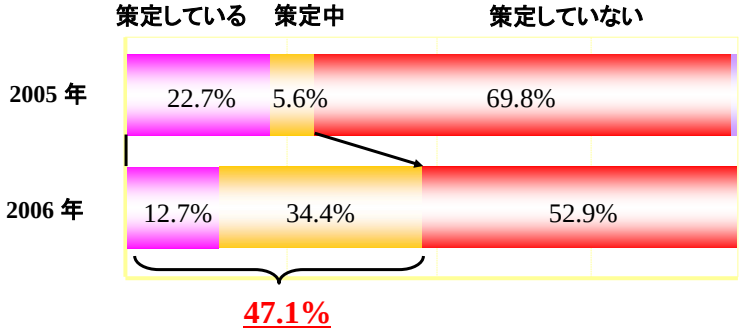
ＢＣＭ構築の必要性

- 事業継続性
- BCMとCSR（社会的責任）
- BCMとサプライチェーン
- BCMと企業価値
- ISO/IEC27001、ISO/IEC20000
- 関連法規等
  - 内閣府／事業継続ガイドライン
  - 経済産業省／事業継続計画策定ガイドライン
  - 中小企業庁／BCP策定運用指針
  - JISQ2001リスクマネジメント
  - 災害対策基本法
  - 個人情報保護法
  - 金融商品取引法（J-SOX）
  - その他各種事業法

BCPへの取り組み状況

＜日本企業の取り組み＞

海外企業のBCP策定率
全体：４７％
売上高20億円以上：６９％



BCP策定済みの企業が増えたとは言えないが、
BCPへの取り組みが増加傾向にある

（インターリスク総研調査から）

Ⅱ．BCM英国規格(BS25999)の概要

BS25999の構成

BS25999の構成

- BS25999-1：事業継続マネジメントのための実践規範
  2006年発行
- BS25999-2：事業継続マネジメント　ー要求事項
  2007年8月発行予定

BS25999-1：2006

■ 概観

1. Scope and applicability　スコープ及び適用性
2. Terms and definitions 用語の定義
3. Overview of BCM　BCMの概要
4. The business continuity management policy　BCMの方針
5. BCM Program management　BCMプログラム・マネジメント
6. Understanding the organization　組織の理解
7. Determining the business continuity strategies　事業継続戦略の決定
8. Developing and implementing a BCM response
   BCMを実現するための手法の開発と実践
9. Exercising, maintenance, and reviewing of BCM arrangements
   BCMへの取り組みに関する訓練、維持管理、見直し
10. Embedding BCM in the organization's culture　BCMの企業文化への導入

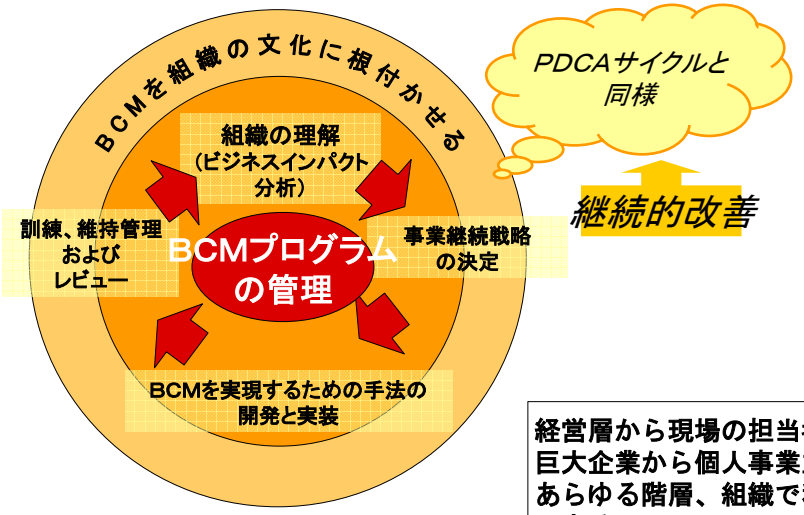
BS25999-1:2006

- BCMのための実践規範（Code of practice）
  - BCMのプロセス、原則、用語の確立

組織を脅かす潜在的なインパクトを認識し、
ステークホールダーの利益、評判、ブランド及び
価値創造活動を守るため、復旧力及び対応力を
構築するための有効な対応を行なうフレームワーク、
包括的なマネジメントプロセス。

・組織内のBCMの理解、発展および実施の基礎を提供
・企業間取引や組織間取引を確かなものにする

BS25999-1:2006　プログラムマネジメント



（図は BS 25999-1 より引用し、インターリスク総研にて仮訳）

経営層から現場の担当者、
巨大企業から個人事業主、
あらゆる階層、組織で利用
できる

BS25999-1:2006

■ **組織の理解（ビジネスインパクト分析）**

以下が特定されることを目指す

- 組織の主要な製品・サービス
- それを支える重要な活動とリソース
- これらへの脅威／リスク
- それらの製品・サービスの最大許容停止時間と、事業中断時の目標復旧時間（RTO）

BS25999-1:2006

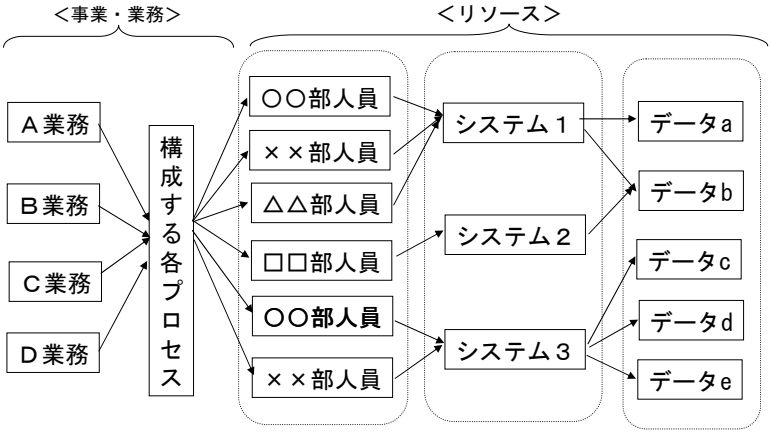
■ **組織の理解（ビジネスインパクト分析）**

復旧時に各活動で必要なリソース（復旧要件）について、
評価・見積もる。観点（例）は、以下事項について。

- **People（人員）**
- **Premises（サイト）**
- **Technology（ITなどの技術）**
- **Information（情報）**
- **Supplies（物資）**
- **Stakeholders（ステークホールダー）**

BS25999-1:2006の概要

業務を支えるリソース＜BIAの結果例＞



＜業務と復旧要件の関係を洗出し、依存関係を明確にする＞

BS25999-1:2006の概要

- **事業継続戦略の決定**

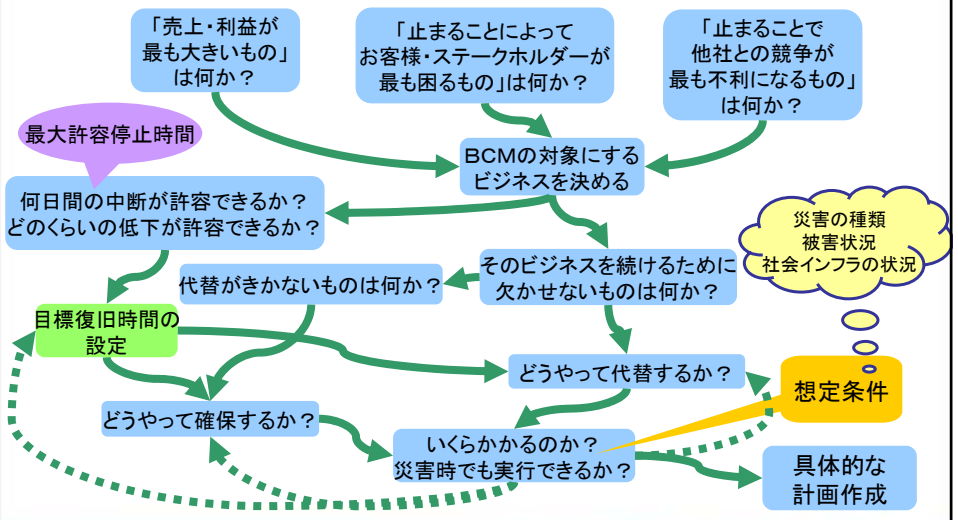
「戦略」とは何か?

BCMの中での「戦略」とは、インシデント発生時に、組織のレジリエンシーを維持するために必要なリソースの「選択」と「決定」に関すること（時間軸、コストなどの要素にも依存）。また併せリスク低減策に関すること。

＜ポイント＞

・People（人員）
・Premises（サイト）
・Technology（ITなどの技術）
・Information（情報）
・Supplies（物資）
・Stakeholders（ステークホールダー）

事業継続の戦略を決めるプロセス(例)



BS25999-1:2006

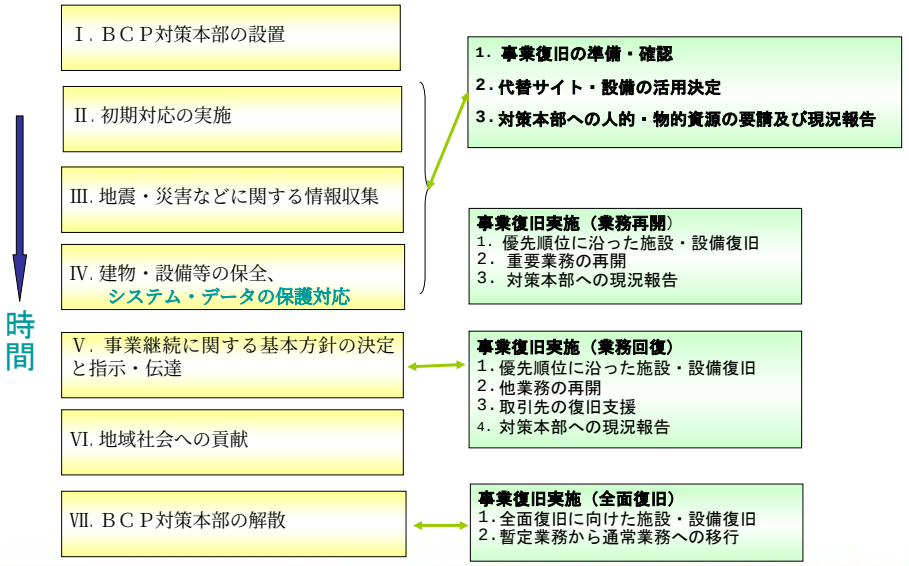
- BCMを実現するための手法の開発と実装(BCPの策定)

プランは以下を含む;

- 適用範囲
- 役割・責任
- 計画の発動
- 詳細連絡先
- タスクとアクションリスト
- リソース要件
- フォームと付属書

BCPは
各部署が自己責任で策定するもの！
BCPの成功は、
経営者と部署の真剣度！

＜ＢＣＰ対策本部（会社の意思決定機関）と事業部署間の連携＞



BS25999-1:2006の概要

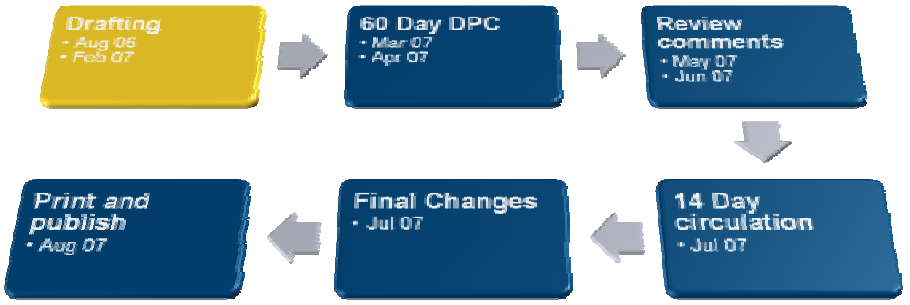
- **BCMの訓練、維持管理、見直し**
  - ・BCMの有効性を確認し、最新の状態に維持されて初めて信頼される
  - ・訓練は不可欠
- **BCMの組織文化への導入**
  - ・シニアーレベルのリーダーシップ
  - ・責任の割り当て
  - ・意識向上
  - ・演習　など

BS25999-1:2006の概要

- まとめ　ーBCM導入のポイントー
  - 適用範囲の決定
  - トップレベルからのサポート
  - 責任の割当
  - 主要製品・サービスの特定
  - 支援プロセスにおける単一障害点の特定
  - 適切な戦略の決定
  - 現実的かつ有効なプランの策定
  - 訓練、維持、レビュー
  - 全員参画

今後の展望(BS25999-2)

- BS25999-2の開発スケジュール(現時点の見込み)



今後の展望

- **事業継続性への対応は組織の必要不可欠な課題**
  - トップマネジメントにはより多くのコーポレートガバナンスに対する責任がある
  - 変化するビジネスリスクを把握し、対応可能な状態を維持しなければならない
  - ベストプラクティスとして規格を活用する
- **BS 25999-1の活用:**
  - BCMを確立し、管理し、改善する
  - BCMを企業文化に定着させる
- **BS 25999-2は:**
  - BS25999-1をスタートラインとして、組織の中に事業継続マネジメントシステムのフレームを提供する
  - 第三者による監査、認証のための最低限の要求事項が用意される
    - 規格要求事項への適合性の決定
    - BCMへの対応の度合いを第三者へ証明

企業価値向上へのステップ

Ⅲ．ＢＣＭと他領域の関係整理

※内部統制、リスクマネジメント、ＣＳＲ
情報セキュリティ、ＩＴガバナンス

１．ＢＣＭと内部統制の関係

ＢＣＭと一体になって機能する内部統制

内部統制
　企業等の4つの目的の達成のために企業内の全ての者によって遂行されるプロセスであり、6つの基本的要素から構成される。

＜目的＞

①業務の有効性及び効率性
→業務プロセス分析及びビジネスインパクト分析

②財務報告の信頼性
→コミュニケーション・報告スキームの仕組み作り

③事業活動に関わる法令等の遵守
→金融庁の総合的な監督指針、金融庁検査
　国際標準(ISO)化、各国でガイドライン化

④資産の保全
→災害などの発生時対応で必要不可欠

ＢＣＭで
関連する事項

ＢＣＭと一体になって機能する内部統制

内部統制

企業等の4つの目的の達成のために企業内の全ての者によって遂行されるプロセスであり、6つの基本的要素から構成される。

＜6つの基本的要素＞

①統制環境
→リスクや事業継続についての対応方針と姿勢を決定し、組織内全ての人に影響を与える。

②リスクの評価と対応
→組織目標の達成に影響を与える事象・リスクについて洗出し、分析・評価する。

③統制活動
→経営者の指示や命令が適切に実行されることを確保。災害時の権限や責任を明確化。

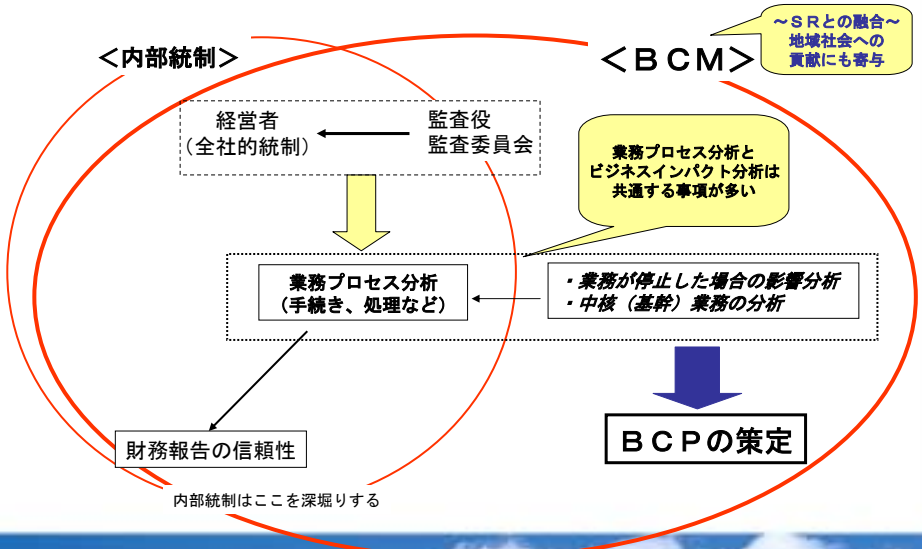
④情報と伝達
→必要な情報の識別、把握、伝達、処理の検討。

⑤モニタリング
→ＢＣＭが有効に機能することを継続的に評価・監査する仕組み。

⑥ITへの対応
→業務（ビジネス）は、ITへの依存度が高い。ITが停止すると、業務そのものが停止する。

ＢＣＭで関連する事項

＜ＢＣＭと内部統制の概念整理＞　ＢＣＭと一体になって機能する内部統制



２．ＢＣＭと
リスクマネジメント、ＣＳＲとの関係

リスクマネジメントについて

（１）ＲＭ（リスクマネジメント）

組織を取り巻く様々なリスクを予見し、そのリスクがもたらす損失を予防するための対策や不幸にして損失が発生した場合の事故処理対策などを効果的・効率的に講じることによって、組織の事業の継続と安定的発展を確保する手法

（２）ＥＲＭ（エンタープライズリスクマネジメント）

企業など組織体が、その目的達成のために行なう意志決定や業務遂行などにおける全てのリスクに関して、組織全体の視点から統合的・包括的・戦略的に把握・評価・最適化し、価値最大化を図るリスクマネジメントのアプローチ。上記（１）と比較して、より密接に事業戦略や事業展開に連携した手法である。

ＢＣＭとＲＭの相異

	ＲＭ	ＢＣＭ
手　法	リスク分析	ビジネスインパクト分析
分析パラメータ	確率（可能性）と損害額	時間と損害額
想定するリスク	基本的には全てのリスク	事業の継続／企業の存続を妨げるリスク
分析の切り口・観点	リスク 自然災害、火災、ＩＴ事故　など	ビジネスプロセスの脆弱性 脆弱性・ボトルネックとは、その ビジネスを構成する以下事項など。 *業務・工程、物流、キーパーソン、* *システム・データ、資金など*

ＢＣＭの考え方は、全てのリスクを対象にするのではなく、事業の停止・崩壊を事象にする。また、「主要な事業の継続」に焦点を絞った考え方である。

ＣＳＲの定義

ＣＳＲ-Corporate Social Responsibility（企業の社会的責任）

企業は社会的存在として、最低限の法令遵守や利益貢献といった責任を果たすだけではなく、市民や地域、社会の顕在的・潜在的な要請に応え、より高次の社会貢献や配慮、情報公開や対話を自主的に行うべきであるという考え。

但し、定義においては明確なものがあるわけではなく「ＣＳＲおよびコーポレートガバナンス＝企業経営」という立場からすれば各企業独自に経営の立場から定義されるべきである。また、ＣＳＲとして何をするのかではなく上記の観点から企業として行った活動の結果がＣＳＲと言うこともできる。

典型的な活動としては「地球環境への配慮」「企業統治と情報開示」「ボランティア活動支援」「地域社会参加」「社員の安全と健康」などがあげられる。

ＢＣＭとＣＳＲ

社会的要請・ステークホルダーからの期待・要求

最近では**ＢＣＭをＣＳＲの一環と位置づけている企業が増えて**いるが、
ＣＳＲの観点から行う**ＢＣＭにおいて認識されるべきリスクは企業の目的や目標のみを基準とするのではなく、社会的要請やステークホルダーからの期待や要求を踏まえたものとなる**。

例えば自らの資産の保全のみならず地域住民の安全、地域経済、雇用問題、製品やサービスの安定供給などを視野に入れる必要がある。
また、電気、ガス、水道、電話、コンピュータネットワークなど社会インフラの構築を担っている企業では社会的貢献より一歩進んだ**「社会的使命」といった考え方の下にＢＣＭ構築を目指すべきであろう。**

３．ＢＣＭと
情報セキュリティとの関係

情報セキュリティとは

情報セキュリティの主な要素

情報セキュリティ

情報の機密性，完全性及び可用性の維持

機密性	認可されていない個人，エンティティ又はプロセスに対して，情報を使用不可又は非公開にする特性
完全性	資産の正確さ及び完全さを保護する特性
可用性	認可されたエンティティが要求したときに、アクセス及び使用が可能である特性

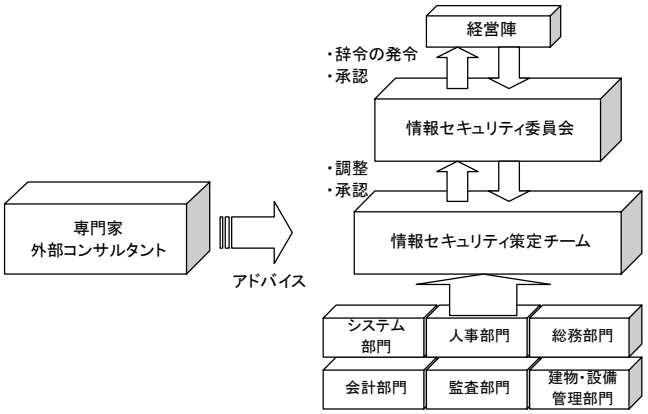
真正性（authenticity）
ある主体又は資源が，主張どおりであることを確実にする特性。真正性は，利用者，プロセス，システム，情報などのエンティティに対して適用する。

責任追跡性（accountability）
あるエンティティの動作が，その動作から動作主のエンティティまで一意に追跡できることを確実にする特性
（JIS X 5004:1997）

否認防止（non-repudiation）
ある活動又は事象が起きたことを，後になって否認されないように証明する能力。

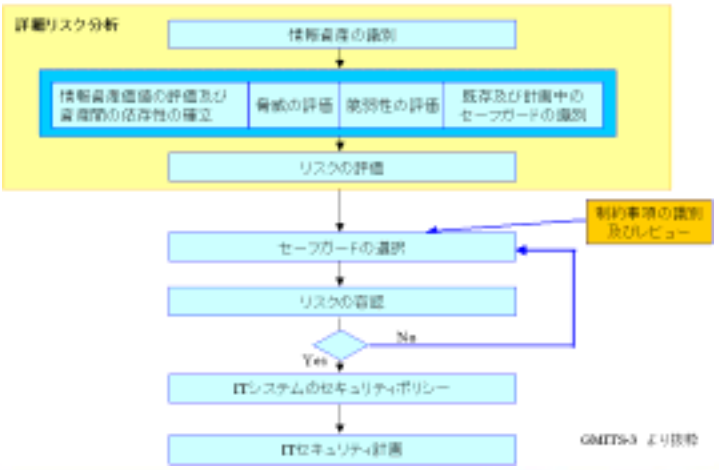
信頼性（reliability）
意図した動作及び結果に一致する特性。
（JIS Q 13335-1 2 用語及び定義 より）

情報セキュリティ体制の例

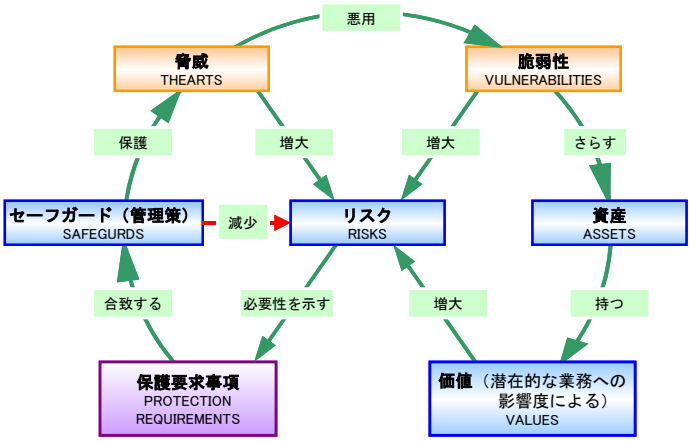


情報セキュリティにおけるリスクマネジメント

詳細リスク分析を含むリスクマネジメント



リスクアセスメントの考え方



情報セキュリティが対象とする資産例

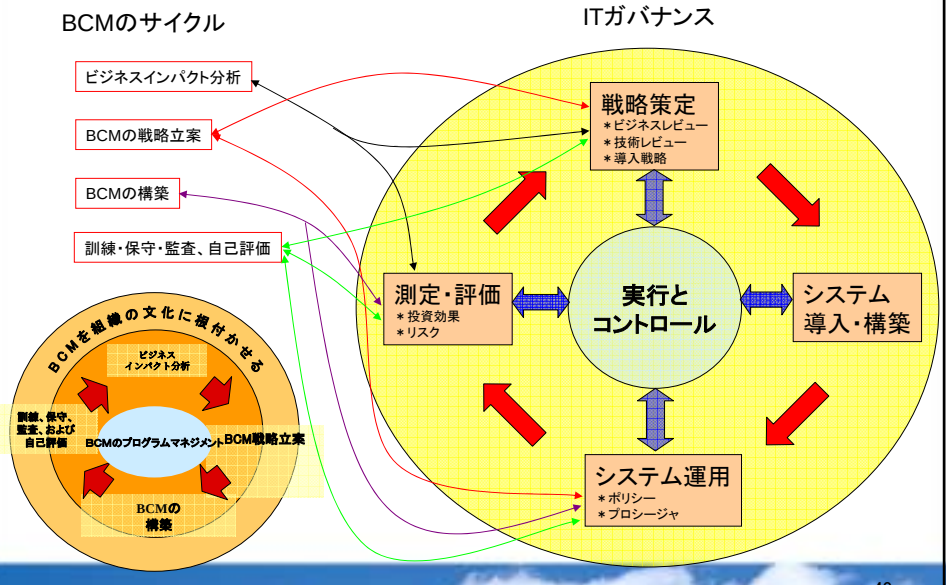
資産の種類	例示
情報	データベース及びデータファイル、契約書及び同意書、システムに関する文書、調査情報、利用者マニュアル、訓練資料、運用手順又はサポート手順、事業継続計画、代替手段の取決め、監査証跡、保存情報
ソフトウェア資産	業務用ソフトウェア、システムソフトウェア、開発用ツール、ユーティリティソフトウェア
物理的資産	コンピュータ装置、通信装置、取外し可能な媒体、その他の装置
サービス	計算処理サービス、通信サービス、一般ユーティリティ（例えば、暖房、照明、電源、空調）
人	保有する資格、技能、経験
無形資産	例えば、組織の評判、イメージ

情報セキュリティとBCM （例）

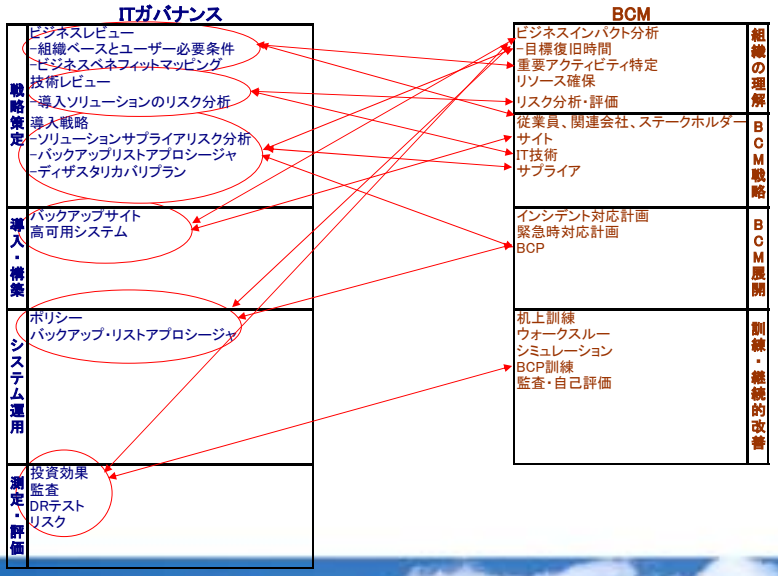
事業リスク		情報セキュリティの範疇
財物リスク	自然災害（地震、台風等）	○
	火災・爆発	○
	電気的・機械的事故	○
	輸送中の事故	○
人的リスク	役員・従業員の就業中の事故	○
	雇用（人手不足等）	○
	キーパーソンの喪失	○
	テロ	△
	誘拐	△
	ストレス・ノイローゼ	×
情報リスク	情報システム障害	○
	コンピュータウィルス	○
	情報漏えい	○
	サイバーテロ	○
財務リスク	不正な財務処理、入力ミス	○
	虚偽の表示	×
	流動性損失	×
コンプライアンス（法令等の遵守）	証券取引法への抵触	×
	個人情報保護法への抵触	○
風評リスク（直接的）	うわさ	△
市場リスク	金利リスク	×
	為替リスク	×
信用リスク	貸し倒れリスク	×
賠償責任リスク	施設に関わる賠償責任	△
	業務・作業に関わる賠償責任	△
	製品の欠陥	×
	知的財産に関わる賠償責任	○
	環境汚染に関わる賠償責任	×
	会社役員の賠償責任	△

４．ＢＣＭと
ＩＴガバナンスとの関係

ITガバナンスから見たBCMとの関連性



ITガバナンスから見たBCMとの関連性（詳細）



ITシステム構築から見たBC・セキュリティ

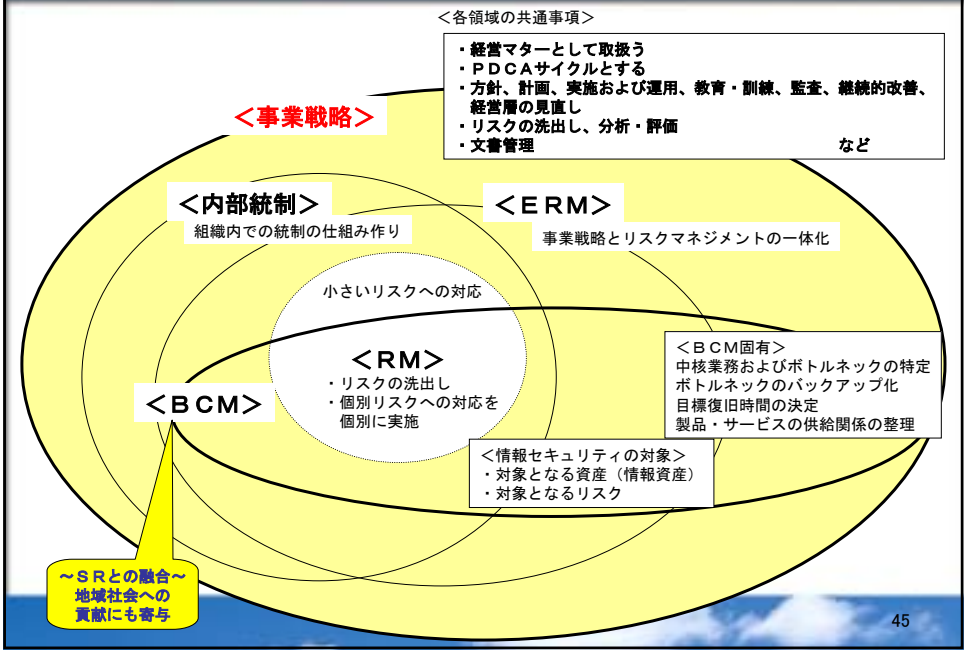
分野	1.アウトソーシング	2.コンタクトセンター/CRM	3.IPインフラストラクチャー	4.モバイル通信
対象	マネージドサービス ネットワークアウトソーシング ビジネスプロセスアウトソーシング IT アウトソーシング	コンタクトセンター コンタクトセンターのセルフ/アウトソース運用 マネージドプロフェッショナルサービス CRMアプリケーション	WAN IPテレフォニー LAN オプティカル SAN	接続性 複合ソリューション
セキュリティ	セキュリティギャップ分析（ISMS監査） ベンダー選定/評価 ポリシー、スタンダード、プロシージャ策定	コンタクトセンターセキュリティアーキテクチャ ポリシー、スタンダード、プロシージャ	ポリシー、スタンダード、プロシージャ策定 セキュリティアーキテクチャ セキュアネットワーキング ファイアウォール ISMS監査	ポリシー、スタンダード、プロシージャ策定 ワイヤレスLANのセキュリティ モバイルセキュリティポリシー リモート通信のセキュリティ
事業継続（BC）	BCアウトソーシング戦略策定 ベンダー向けRFQ策定 DRベンダー選定 遵守状況の評価	コールセンターリスク評価 コールセンタービジネスインパクト分析 DRプロセスおよび計画 DRテスト BCP監査 金融業界規制の準拠	復旧を前提としたインフラ技術の選択 高可用性、高回復力システムの構築 電話通信の継続	事業継続における脆弱性 モバイルに対するリスク評価

ITシステム構築から見たBCM・セキュリティ

分野	5.デスクトップ管理	6.アプリケーション管理 およびホスティング	7.サーバ/プラットフォーム
対象	パッケージソリューション	メッセージング インターネット Eコマース（ビジネスアプリケーション） ホスティング	システムハードウェア、ソフトウェア（OS、ミドルウェア） サーバシステム設計 サーバ実装 サーバシステムアウトソース
セキュリティ	ポリシー、スタンダード、プロシージャ策定 デスクトップセキュリティ ウイルス対策アーキテクチャ	ポリシー、スタンダード、プロシージャ策定 ペネトレーションテスト PKI等認証ソリューション セキュアポータルサイトの構築 セキュリティリスク評価 ウイルス対策	ポリシー、スタンダード、プロシージャの策定 セキュアOSによる強化 ペネトレーションテスト 脆弱性分析 セキュリティベリメタ検査 ネットワークとサーバー間のセキュリティ
事業継続計画	リカバリー要求度合いの決定 バックアップ・リストアプロシージャ	バックアップ・リストアプロシージャ バックアップサイト構築 危機管理チームの構築	バックアップ・リストアプロシージャ バックアップサイト構築 デザスターリカバリプランの策定

５．ＢＣＭ、ＲＭ、内部統制、情報セキュリティの関係整理

各領域の関係整理



課題とヒント

【課題】
企業として、リスクや統制などに対する考え方・行動にブレが生じないようにするには何がベストか。

【ヒント】
BCM、リスクマネジメント、内部統制、ＣＳＲ、情報セキュリティなどでは、共通となる領域が存在する。
★組織体制、進め方、経営の関与などについて、統合的に進められると判断される領域については、効率的にシナジーを出しながら推進する。

最後に（事業継続から企業価値、そして）

迅速な復旧ができた場合とそうでない場合、どのような軌跡をたどるか。危機はチャンスにも本当の危機にも変えることができる。

（英国Oxford Metrica社提供）

【引用・参考文献】

【引用・参考文献】

- British Standards, Business Continuity management (BS 25999) - Part 1: Code of practices
- The Business Continuity Institute, Business Continuity Management Good Practice Guidelines (2005)
- 小林誠［監修］　事業継続マネジメント（ＢＣＭ）構築の実際、日本規格協会、2006年
- 江尻明隆　リサーチビュー　事業継続マネジメント（ＢＣＭ）の国際規格化の潮流、2006年
- Rory F Knight , Reputation & Value - the case of corporate catastrophes

- 中央青山監査法人編　ＣＳＲ実践ガイド　中央経済社　2004
- 野田健太郎　ＢＣＭを理解する本　日刊工業新聞社　2006
- ＠ＩＴ情報マネジメント用語辞典
  http://www.atmarkit.co.jp/im/terminology/index.html
- インターリスク総研　CSR Topics　2006
- インターリスク総研編著　実践リスクマネジメント　事例に学ぶ企業リスクの全て、
  経済法令研究所　2006

おわりに

BS25999 はそのパブリックコメント中に BSI（英国規格協会）のウェブサイトから 5,000 を超えるダウンロードが各国からあったと言われるように、BCM に対する関心が世界中で高まっている。ちなみに通常の規格の場合、ダウンロードは 250 程度だそうなので、単純に言えば他の規格の 20 倍の関心度である。

それだけ各団体、個人が BCM に関心を持つと同時に規格の必要性を感じていることの表れである。

BCM に関する法規としては災害対策基本法、個人情報保護法、金融商品取引法（J-SOX）、各省庁のガイドライン、各種事業法などがあげられるが、いわゆる規格には法的な強制力はない。しかし、BCM に先進的に取り組みたい関係者にとっては法規はもとより BCM 構築に対する包括的なアプローチを示してくれる規格への需要が高いことは当然のことと言える。

本調査報告書は BS25999 の概要に加えて BCM とリスクマネジメント、内部統制、CSR、IT ガバナンス、情報セキュリティとの関係性、個々の定義についても整理を試みた。全てを相互的に体系化するまでには至っていないが、BCM との関連については現時点でのひとつの見解として参考にしていただけるものと思う。

各々対象とするビジネス、目的、組織、経営の関与、ステークホルダーとの関係など共通の領域が少なからずあるので、平行して行うことは負担に感じるかもしれないが、統合的に推進することでリソース（人・物・お金・情報）の効率化、相乗効果などのメリットも得られる。

本調査報告書が BCM とその関連領域の整理、推進の一助となれば幸いである。

平成 19 年 3 月
情報セキュリティ専門部会

情報セキュリティ専門部会メンバー

委員長	篠原　雅道	ＢＣＩ日本支部／株式会社インターリスク総研
委員	駒瀬　彰彦	株式会社アズジェント
委員	斎藤　俊治	株式会社ＫＤＤＩ＆ＢＴグローバルソリューションズ
委員	原田　薫	日本ヒューレット・パッカード株式会社