参考⑥

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　報告書

参考資料

事業継続計画策定ガイドライン

目　　次

第Ⅰ章　基本的考え方 1
1.1. BCP(Business Continuity Plan)の必要性 1
1.2. BCP が求められる背景 2
1.3. BCP の特性 6
1.4. 世界と日本の動向 9

第Ⅱ章　総論（フレームワーク） 10
2.1. BCP 策定に当たっての考慮事項 10
2.2. 組織体制について 11
2.3. ビジネスインパクト分析から BCP 策定までの流れ 12
2.4. BCP の導入と教育・訓練 15
2.5. BCP の維持・管理 16

第Ⅲ章　BCP 策定に当たっての検討項目 17
3.1. 検討項目の全体像とポイント 17
3.2. BCP の実施体制 18
3.3. BCP 発動フェーズにおける対応のポイント 19
3.4. 業務再開フェーズにおける対応のポイント 22
3.5. 業務回復フェーズにおける対応のポイント 24
3.6. 全面復旧フェーズにおける対応のポイント 25
3.7. リスクコミュニケーションの重要性 26

第Ⅳ章　個別計画（ケーススタディ） 28
4.1. 大規模なシステム障害への対応 28
4.2. セキュリティインシデントへの対応 33
4.3. 情報漏えい、データ改ざんへの対応 37

事業継続計画（BCP）策定ガイドライン参考資料集 41
参考１　各フェーズにおける実施項目
参考２　対策本部室に備えるべき設備・備品類チェックリスト
参考３　フェーズ毎の対策本部の役割
参考４　フェーズ毎の各チームの役割
参考５　システム関連 BCP 一覧表の項目
参考６　代替手段の検討項目事例
参考７　総括の項目（システム関連）
参考８　ベストプラクティス：BCP 構築事例

第Ⅰ章　基本的考え方

＜本章の位置付け＞

本章では、事業継続計画（BCP）の必要性や定義、一般的な構築の流れなどの概要を記載するとともに、BCP が求められる社会的背景やその特性、国内外の関連動向など、BCP の理解を深めるための基本的な説明を行う。

1.1. BCP(Business Continuity Plan)の必要性

（1）序　論

日本では、地震、火災・爆発、大規模なシステム障害[1]などが相次いでおり、その結果、基幹となる事業の停止に追いこまれるケースが見られる。この場合、財物への直接の被害や、基幹事業が停止している間の利益を損なうばかりでなく、取引先や顧客を失う大きな原因となり、ひいては事業からの撤退を余儀なくされることになりかねない。

また、近年発生している基幹事業の停止は、自社の損失にとどまることなく、取引先や顧客の事業停止へと影響が連鎖している。思わぬところから企業存続の危機に立たされるケースも見られる。そのためすでに、取引先や顧客をはじめとする利害関係者（ステークホルダー）は、自社の基幹事業を停止させるリスクやボトルネック[2]に対して、どのような対策を講じているのかの説明を求めている。

危機が発生したときに、企業に対して問われるのは、その企業が危機に直面した時であったとしても事業を遂行（継続）するという社会的使命を果たせるかどうか、である。これは、マニュアル化という次元で解決できる問題ではなく、危機に直面したときの「企業経営のあり方」そのものなのである。企業は、自身の被害の局限化という観点に留まらず、コンプライアンスの確保や社会的責任という観点から対策を講じなければならない。

企業経営者は、個々の事業形態・特性などを考えた上で、企業存続の生命線である「事業継続」を死守するための行動計画である「BCP（Business Continuity Plan）」及び、その運用、見直しまでのマネジメントシステム全体である「BCM（Business Continuity Management）」を構築することが望まれる。

（2）BCP・BCM の定義

現時点で BCP・BCM には様々な定義が唱えられているが、英国規格協会(BSI)[3]が策定したPAS56「事業継続管理のための指針（Guide to Business Continuity Management）」では以下の様に記述されている。

BCP	**潜在的損失によるインパクトの認識を行い実行可能な継続戦略の策定と実施、事故発生時の事業継続を確実にする継続計画。事故発生時に備えて開発、編成、維持されている手順及び情報を文書化した事業継続の成果物。**
BCM	**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。**

[1] システムのハード障害、アプリケーション障害、通信回線障害等により、当該企業の情報システムが利用不能となった場合のこと。

[2] 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）。

[3] BSI(British Standards Institution):http://www.bsi-global.com/index.xalter

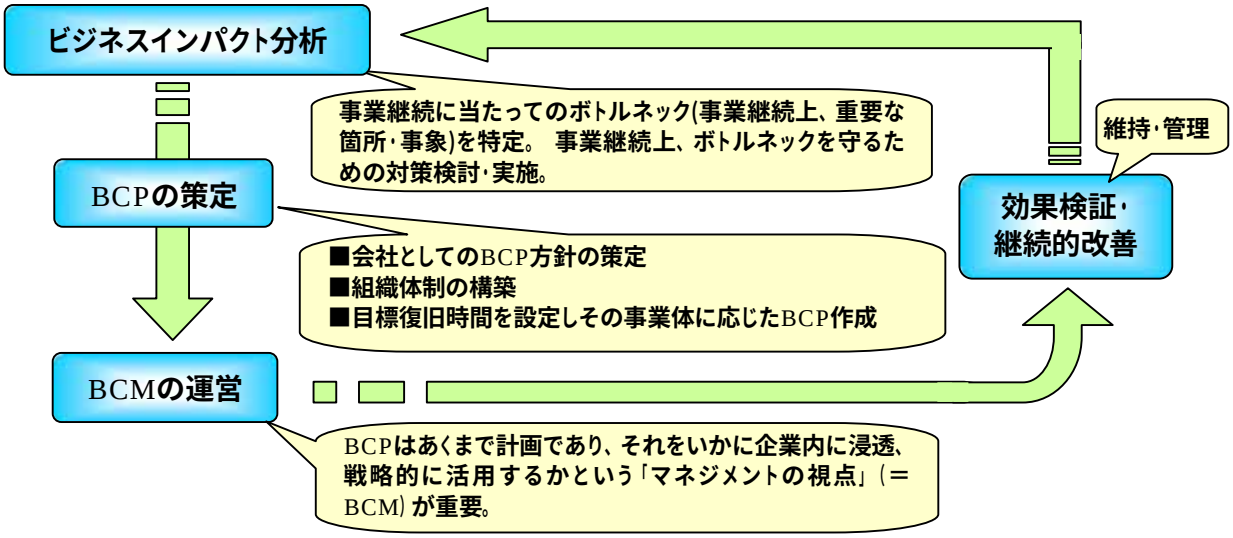
BCP・BCM は、事故や災害などが発生した際に、「如何に事業を継続させるか」若しくは「如何に事業を目標として設定した時間内に再開させるか」について様々な観点から対策を講じることである。BCP は、そのための計画自体を指し、BCM は、BCP の策定から運用、見直しまでのマネジメントシステム全体を指すのである。

したがって、企業にとって重要な視点は、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ことである。具体的には、BCP の重要性を企業内で普及啓発・周知させることによりリスク管理能力を向上させたり、また取引先や監督当局に対し、BCM の取組みをアピールしたりすることなどである。

（3） BCM 構築の一般的な流れ

BCM では通常次のような PDCA[4]サイクルを実施することとなる。

【図表１　BCM 構築の一般的な流れ】



BCP は、BCM 上重要な要素であることは間違いないが、一方で先に述べた通り BCP はあくまで計画であり、それをいかに企業内に浸透、戦略的に活用するかという「マネジメントの視点」を欠かしてはならない。

1.2. BCP が求められる背景

（1）事業活動の変化

企業は、現在、効率化を追求し徹底的なコスト削減を行うため、生産拠点や物流拠点、取引先等を集約せざるを得ない状況に追い込まれている。このことは一方で、その拠点や取引先に障害が発生した場合、代替拠点や取引先の手配を困難にし、基幹事業の停止に直結する確率が格段に増加していることを意味する。自動車部品メーカーの部品供給が停止したために自動車メーカーの操業が停止してしまったなどという事象は記憶に新しいところである。

[4] 事業活動を「計画（Plan）」「実施（Do）」「監視（Check）」「改善（Action）」のマネジメントサイクルとして捉え、組織運営を通じて継続的な改善を図る取組み。

＜BCP と SCM（サプライチェーンマネジメント）＞

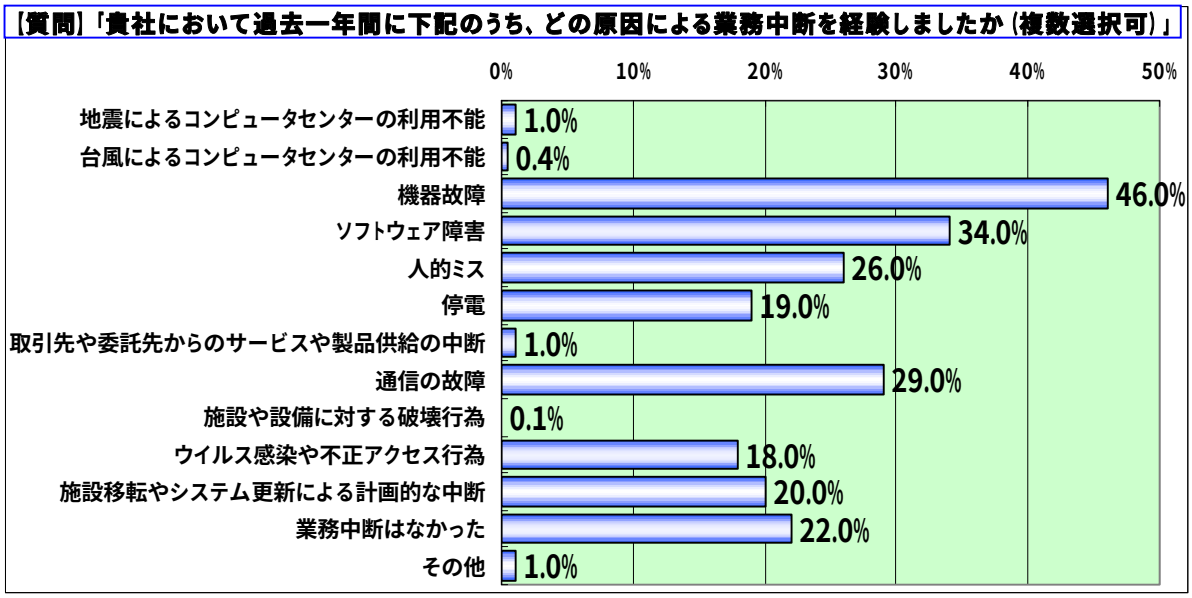
SCM は、サプライチェーンを構成する企業全体で経営効率を追求する経営管理手法である。「在庫や仕掛品の削減」、「生産や供給のリードタイムの削減」などの実現につながるものと考えられている。一方で、SCM の導入は、サプライチェーンを構成する一企業にボトルネックがあれば、構成企業全体に影響を与える可能性を有する。つまり、サプライチェーンを構成する一企業の事業中断が、他の企業の事業中断へと波及することになる。

それゆえに自企業だけで BCP を構築するのではなく、サプライチェーンを構成する全企業で BCP を構築する必要があり、こうした考え方の浸透する欧米のグローバル企業から、サプライチェーンを構築する企業に対して BCP の策定や適用を求められるケースも見られる。

（2）情報システムへの依存増大

重要インフラである金融サービスや通信サービスを提供する企業はもちろん、在庫管理や受発注管理、顧客管理等、ほとんどすべての企業において、事業は情報システムやネットワークの稼動を前提に構築されている。情報システムに障害が発生した、あるいはネットワークが中断した場合に、BCP の準備がない企業は、工場を稼動させることも、顧客にサービスを提供することも不可能な状況に追い込まれる可能性がある。2002 年夏に KPMG ビジネスアシュアランスによって実施されたビジネス継続マネジメントサーベイにおいても「ビジネスの中断の原因というと真っ先に地震などの自然災害が思い浮かぶかもしれないが、実際には情報システムの障害によるケースが非常に目立つ」と報告されている。過去１年間に経験した事業中断の原因として，最も多かったのは「機器故障」で 46%，次いで「ソフトウェア障害」が 34%だった。「ウイルス感染や不正アクセス行為」の 18%という数字が注目される。

【図表２　業務中断の原因】（KPMG ビジネスアシュアランス ビジネス継続マネジメントサーベイ 2002）



ただし、上記統計は過去一定期間の業務中断をもとにしているのであって、地震がもたらす事業継続への影響が小さいことを意味するのではない。地震国である日本においては、地震リスクの大きさを盛り込んだ BCP を構築する必要がある。

また、世界の企業にとってもBCP上のITの重要性については大きく認識されている。BCIが2004年に世界企業を対象にした調査結果によると、企業のBCP責任者が、BCM上事業の混乱に関して最も留意している事項は、「テレコミュニケーションの喪失(62%)」、「IT 能力の喪失(60%)」、「火災(53%)」、「事業拠点の喪失(51%)」となっている。

＜コンピュータ西暦2000年問題への対応＞

年号を二桁で管理しているコンピュータが西暦2000年を1900年と誤認してしまい、処理できなくなるというコンピュータ西暦2000年問題（Y2K問題）は、システムリスクが経営に及ぼす影響の大きさを認識させるとともに、未知のリスクがシステム部門だけでは解決できず、経営者としての対応が必要となることを認識させた。また、2000年問題への対応が遅れている企業に対して取引停止を勧告するなど、サプライチェーンを構成する企業すべてに対応が求められた点も特筆すべきポイントである。

ただし、2000年問題は「2000年問題が発生しないこと」のみを目的とした危機管理対応であったことに留意する必要がある。

（3）予測困難なリスクの頻発

2001年9月11日に発生した米国同時多発テロは、世界中に衝撃を与えた。BCPにとっても様々な課題を浮き彫りにした。米国では、BCPに取り組んでいる企業が多かったものの、これほどまで突然でかつ広範囲に影響を及ぼす想定はしていなかった。複数の企業が同一のバックアップサイトを対象に契約を結んでいたため、実際にバックアップサイトを利用することのできた企業はごくわずかであった事例等、様々な課題が浮き彫りになった。

また重症急性呼吸器症候群（SARS）の蔓延は、自然災害だけではなく、予想し得ないリスクによって事業停止に追い込まれることを改めて認識させられる事象となった。

＜2001年9月11日 同時多発テロの対応＞

世界貿易センター地域に所在していた金融系会社が、最重要拠点を失ったにもかかわらず危機的状態を見事なまでにくぐり抜け、9,000人以上の従業員を無事に避難させたばかりか、その翌日からその拠点にあった事業の一部を他の場所で再開した。

この会社は、自社の業務状況・リスク状況を分析（ビジネスプロセスの脆弱性分析）に沿ってBCPを策定し、BCPのトレーニングを効果的に実施してきた。このBCMの過程では、あらかじめ、どの業務を国内外のどこの拠点に移すことができるか、さらにどの従業員をどの拠点に移すかについて検討をしていた。また、経営層のBCMに対する理解が会社内でのBCM推進に大きな役割を果たしたことは言うまでもない。

（4）地震等自然災害リスク

日本は他の地域にくらべはるかに自然災害が多い国である。特に、地震については、過去にも巨大地震に見舞われ大きな損害を被っている。従来は工場などを分散することで地震リスクに対応した企業も、海外企業とのグローバルな競争環境の中で、拠点を集約化せざるを得ない状況に追い込まれている。これが、自然災害の経営に与える影響をより一層深刻なものとしているのである。海外の取引先にとって、日本の企業がサプライチェーン上の重要な要素となっている場合には、今後地震をはじめとする様々なリスクに対するBCPを求められることが想定される。

＜震災など自然災害の経験＞

1995 年1月の阪神･淡路大震災以前の地震対策は、従業員の安全対策、資産の保全と避難訓練という視点でのみ取り組まれており、事業の継続を視野に入れて考えられることは少なかった。自社の安全だけを考えていた従来の地震防災計画は、その枠組みの根本的な見直しを迫られることになった。地震対策は経営の根幹をなす重要な危機管理対策であり、事業を継続するためのマネジメントが不可欠であることを思い知らされる結果となった。

2004 年 10 月の新潟県中越地震では都市直下型地震であった阪神･淡路大震災と比べ、企業の本社や重要な拠点の直接的な被災は少なかったものの、被災地に製造拠点を置く取引先や子会社などが被災し、サプライチェーン上で問題が生じ、事業活動に影響が生じた企業もあった。代替拠点の確保など、SCM の観点からも BCM を構築する必要が改めて認識された。

また、新潟県中越地震は大きな余震が続いたことが特徴に挙げられる。これにより復旧に向けた施設や設備の総点検を何回も繰り返さなければならず、復旧作業に大幅な支障を来した。計画通りに復旧ができない場合には、被災地外で事業を早期に再開する対策が必要となるが、こうした企業の早期再開･早期復旧･全面復旧など事業継続に関する総合戦略を柱とした BCM が重要となることを学んだ。

（5）BCP の取組みに関する情報開示

2003 年 3 月に「企業内容等の開示に関する内閣府令」等が改正され、有価証券報告書において「事業等のリスクに関する情報」の記載が義務付けられた。単にリスクを開示するのみならず BCP の取組みについて触れる報告書も多く、この流れは今後加速することが予想される。

また、金融業界では金融庁が危機管理体制の構築を求めているほか、BCP やコンティンジェンシープランなどに関する取り組みについての情報開示を自主的に行っている先もある。

＜日本銀行「災害発生時における日本銀行の業務継続体制の整備状況について」より抜粋＞

『取引先金融機関等からは、自社の業務継続計画をより実効性のあるものとするためにも、災害発生時における日本銀行の業務継続体制のフレームワークを示して欲しいとの要望を数多く頂きました。私どもでも、業務継続体制の整備についてはなお検討を要する点が残されていますが、現時点で体制整備が進んでいる部分について、その概要をセキュリティ等の面で支障のない範囲で公表することとしました。』（http://www.boj.or.jp/about/03/sai0307a.htm）

＜東京証券取引所「危機管理への取り組み」より抜粋＞

『当取引所は、我が国証券市場全体の業務継続体制の整備のために、BCP について取引参加者をはじめとする関係機関にもできる限り広く知っていただくことが有効であると考えており、この度、セキュリティ等の面で問題とならない範囲で公表することといたしました。』

（http://www.boj.or.jp/set/03/fsk0307a.htm）

（6）従業者との関係

BCP を運用していく上で重要な要素として人的資源の側面がある。特に広域災害が発生した場合は、人員確保の必要性が高く、緊急時の復旧作業に動員すべき従業員のモチベーションを維持しておく必要がある。併せて、災害時の福利厚生確保も人員を確保する重要な要素と言える。

また事業が継続できなくなると、従業員の雇用問題にまで発展することがあり、工場閉鎖などにより大量の失業者を生み出すことになれば、地域社会への影響は甚大である。雇用確保を含めた地域社会への貢献など、企業の社会的責任の観点からも BCP への取組みは重要である。

1.3. BCP の特性

（1）経営戦略としての位置づけ

海外では BCP を他社と差別化するための経営戦略と位置づける企業が数多く見受けられる。つまり、BCP の水準を利害関係者である株主や取引先にアピールすることにより企業価値を向上させようとしているのである。大規模な事故・災害・事件などが発生しても短期間に事業を復旧できる企業であるか否かは消費者や企業が今後取引先を選別する上での重要な要素になるということを先取りした取組みといえる。

また、BCP の大きな特性は、「目標復旧時間(RTO; Required Time Objective)」を定めることである。この目標復旧時間は、事故・災害・事件などが発生した場合に、その発生時から基幹事業の再開までの企業が設定する「目標とする復旧時間」である。テロなどの大災害が発生しても、BCP を導入している企業は、目標復旧時間内に製品・サービスの提供を再開することにより、他社より圧倒的優位に立つことができる。事実、大規模な災害が発生した際の BCP の有無がマーケットシェアを大きく変化させた事例もあり、その意味でも BCP は経営戦略として位置づけなければならないのである。

なお、BCI の調査（2004 年実施）によると、世界企業が BCP を導入した理由は、「既存顧客からの要望(30%)」、「コーポレートガバナンスの一貫(24%)」、「保険会社からの要望(22%)」、「見込み顧客からの要望(21%)」と続いており、企業の事業及び経営戦略上にとって、BCP は重要な役割を果たしているといっても過言ではない。

＜携帯端末メーカーの事例＞

2000 年に発生した他企業での火災事故により、携帯端末用のコンピュータチップの供給が停止。A 社は事故後直ちに BCP を発動させ、代替のコンピュータチップメーカーの確保に努め、生産を継続、マーケットシェアを維持することができた。ライバル会社である Z 社は、対応が後手となってしまったため、代替のコンピュータチップメーカーの大多数を A 社に押さえられ、生産を継続することが不可能となり、結果としてマーケットシェアを大きく落とすこととなった。現在 A 社と Z 社のマーケットシェアには大きな差が見られるが、BCP の有無もその一因となっているといわれている。

（2）経営者のトップマネジメント

策定される BCP はあくまでも緊急時・復旧時・回復時の「計画」である。その実効性を確保するためにも、あらゆる事業の停止リスクに対応できるわけではない。様々なリスクの中から事業停止の影響の範囲を想定し、事業継続・復旧の優先順位を付け、真に必要なものを選別し、対応することが不可欠となる。これはひとえに重要な経営判断であると言え、経営者の強いリーダーシップ、トップマネジメントが求められる。

（3）結果事象による対応方針の整理

財団法人 情報処理相互運用技術協会の調査[5]によると、9.11 世界同時多発テロ発生の際、BCP

[5] INTAP「平成 15 年度ビジネス継続性技術調査報告書」
http://www.net.intap.or.jp/INTAP/information/report/15-business-report.pdf

の詳細なプランはかえって効果が少なかったことが報告されている。リスク毎に BCP を作成すれば、企業として危機発生後、対策の漏れは少なくできる。しかしながら、全てのリスクについて BCP を作成すれば、そのコストは多大なものになり、また企業内に浸透させる場合も効率的に実施できなくなる。

様々な想定に基づくビジネス影響度分析を実施すれば、基幹事業に対する脅威を各々評価することが可能となるが、むしろ、施設も従業員のアクセスもシステムの稼動もすべて失われたという最悪のシナリオを想定することによって洞察に満ちた評価を得ることができる。

東京証券取引所が公表している BCP によると、同取引所では結果事象を下記のように分類しそれぞれの対応手順を定めている。

＜.結果事象の分類定義＞ （東京証券取引所「危機管理への取り組み」より）

①局所被害	**テロ（予告、破壊行為）等により当取引所は被害をうけているものの、外部関係機関には特段の影響がない場合**
②広域災害	**大規模地震、風水害等により、当取引所及び外部機関がともに被害を受けている場合**
③システム障害	**システムのハード障害、アプリケーション障害、通信回線障害等により、当取引所の情報システムが利用不能となった場合**

（4）BCM とリスクファイナンシング

リスクファイナンシングとは、リスクが具現化し、損害が生じてしまう場合に必要な資金繰りをあらかじめ計画して準備しておく手法である。企業の利益を守ること、そして事業を継続するための各種費用を確保することを考えても、BCM 上、リスクファイナンシングの機能は非常に重要である。リスクファイナンシングの手法としては、保険、災害時発動型融資予約契約、保険デリバティブ、リスクの証券化などが挙げられる。ただし企業は、事業の停止による顕在化する損失（利益の減少、財務的なインパクト、事業を継続するために必要となる費用）と、潜在的な損失（顧客や取引先の離反、マーケットシェアや株価の低下、ブランド価値低下）を整理して考える必要がある。

リスクファイナンシングの機能は顕在化する損失をカバーするものであり、潜在的な損失をカバーできるわけではない。潜在的な損失は、BCP の構築・運用以外に軽減する方法はないのである。また、リスクファイナンシングの機能には、BCP における発動時（緊急時対応）に要するコストや当面の財務インパクトを軽減する効果があるが、これらも的確な BCP の運営・管理が前提である。

（5）周辺領域・関連法規制

①BCP と関連法規

BCP を運用していく上で、関連法規及び関係官公庁等との関係も生じてくる。例えば、災害対策基本法や都道府県の防災計画等に基づく国や自治体との情報共有、連携も場合によっては必要になってくる。個人情報保護法では、各省から公開されているガイドラインに個人情報が漏えいした場合の対処方法などが記載されている場合もあるので、確認の必要がある（**第Ⅳ章 4.3** 参照）。また各種事業法がある業界（金融、通信、交通、エネルギー等）では、それぞれの法令に従って関係部局に対する報告を行う義務なども生じてくるため、法令に従った内容を盛り込まなければならない。こうした各種関連法規は、コンプライアンス確保の視点からも留意する必要があり、BCP を構築する際には参照すべきである。

②BCM と CSR[6]

BCM は、企業にとって「最も重要な事業の継続性」という具体的な事象に焦点をあてたマネジメント手法である。企業が事業継続性を確保することは、上記のように関連法規を遵守することであり、顧客や取引先にとっては製品・サービスを継続的に受けることを可能とするものであり、地域社会にとっては継続的な雇用につながるものである。BCM と企業の社会的責任（CSR）は互いに密接に関連するものであり、企業は双方を推進していく必要がある。

③BCP とコンティンジェンシープラン（CP、緊急時対応計画）

企業によっては危機管理対策として、これまでコンティンジェンシープラン（緊急時対応計画）を構築してきたところもある。BCP と CP との違いは、想定できるインシデントに対して、発生した場合の対応計画をあらかじめ策定しておくことは同様であるものの、BCP は事業の継続性の観点から事項、手順、体制、資源等の計画を具体化したものであると言える。

また、CPは緊急事態発生直後の行動を中心とした計画であるのに対し、BCPは事前にビジネスプロセスの脆弱性を分析（ビジネスインパクト分析）した上で、それに基づいた計画を実施することに特徴がある。

④BCM と JISQ2001 リスクマネジメント

阪神淡路大震災の教訓を生かすために「リスクマネジメントシステム構築のための指針」としてJISQ2001が2001年に制定された。ここで示すリスク対策は時系列で「事前対策」、「緊急時対策」、「復旧対策」の３つに分けられている。総論的なリスクマネジメントに関するJISQ2001に対し、BCMはあくまでも事業継続に焦点を絞った上で、事業継続にとって非常に重要な事象を洗出し、対策を立て、計画・システム化していくものである。したがって、BCMはJISQ2001を適用しようとする組織が「事業継続」を目的とした対策をリスク対策のひとつとして具体的に立案・実施・推進する場合の具体的方法論である。

⑤BCM と情報セキュリティマネジメントシステム（ISMS）

ISMS の国際規格である ISO/IEC17799 では、技術的な対策だけでなく、物理的な対策、コンプライアンスの確保など、経営管理上のあらゆる側面における情報セキュリティ対策が網羅的に示されている。この中で BCM について記載されており、詳細管理策として「事業継続管理手続」、「事業継続及び影響分析」、「継続計画の作成及び実施」、「事業継続計画作成のための枠組み」、「事業継続計画の試験、維持及び再評価」が記されている。ISMS 構築に当たっては、BCM が重要な要素の一つと言える。

⑥BCP とサービスレベルアグリーメント（SLA）[7]

情報システムの構築、運用や保守、データ保存などを外部に委託している事業者が、BCP を策定し、「目標復旧時間」を定める場合は、外部のサービス事業者とサービス内容について協議しなければならない。SLA の項目の一つとして、障害などが発生した場合に備えて、どの程度システム停止が許容できるのかを取り決め、そのレベルを保証するために二重化等の措置を取ることになる。

---

[6] 企業の責任を，従来からの経済的・法的責任に加えて，企業のステークホルダー（社内外の利害関係者。従業員や株主、消費者、取引先に加え、地域社会まで含める場合が多い）にまで広げる考え方。

[7] SLA(Service Level Agreement): 製品・サービスの提供者が、利用者にサービスの品質を保証する制度（契約）。

例えばIT関係であれば、レスポンスタイム、セキュリティレベル、保守体制、緊急時体制、許容停止時間、料金体系などの項目について規定し、サービス提供側はそのサービスレベルを保証する義務を負うことになる。

1.4. 世界と日本の動向

（1）各国の状況

欧米では多くの企業がBCPの重要性を認識して取組みを進めている。英国ではBCIが2002年に策定した「Good Practice Guidelines（実践的な指針）」をもとに英国規格協会（BSI）がPAS56（一般仕様書）を策定した。米国ではDRII(Disaster Recovery Institute International)がBCMの普及啓発活動を行い、NFPA(National Fire Protection Association)でも2004年にNFPA1600「Standard on Disaster/Emergency Management and Business Continuity Programs」[8]を発行し、BCMの導入を促進している。両国ではそれぞれPAS56、NFPA1600をベースに国際基準化の提案を準備している。

アジアでも、BCMの規格化・規制化の動きが出てきている。例えば、シンガポールでは、金融当局が実質的にBCMの強制化しており、これを現在全産業に広げる動きがある。また香港やマレーシアでも規制化される見込みであるという。

（2）日本の状況

これら活発化している海外の動きに対して、日本では、経済産業省の本研究会以外に、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」[9]に「企業評価・業務継続ワーキンググループ」が設置され、BCPについて議論されている。

また前述のように金融機関においては、金融検査マニュアルに危機管理体制の重要性が指摘されていることから、BCPやコンティンジェンシープランに関する対応がすすめられている。（財）金融情報システムセンター（FISC）[10]が「金融機関等におけるコンティンジェンシープラン策定のための手引書」を発刊しているほか、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」[11]についての報告書を取りまとめており、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となっている。

[8] http://www.nfpa.org/PDF/nfpa1600.pdf
[9] http://www.bousai.go.jp/MinkanToShijyou/
[10] http://www.fisc.or.jp/
[11] http://www.boj.or.jp/set/02/fsk0203a.htm

第Ⅱ章　総論（フレームワーク）

＜本章の位置付け＞

本章では、BCM 構築の一般的な流れについて、ステップ･バイ･ステップで説明し、BCP 策定プロジェクトの開始に当たって考慮すべき事項に言及する。

2.1. BCP 策定に当たっての考慮事項

○対象事業･業務は原則全てであるが、重要度･緊急度に応じて優先度付けが必要な場合もある。

○リスク分析は網羅的に行う必要があるが、これに時間をかけ過ぎてはいけない。なぜなら、事業継続を脅かすリスクは常に変化しているので、検討に時間をかけている間に対策が陳腐化してしまう危険があるからである。

○BCP 発動時においては、行政の目的との整合性が求められる場合もあるので、遵守すべき法令のチェックが必要である。

（1）対象範囲

BCP は、組織において事故や災害などが発生した場合に、「いかに事業を継続させるか」あるいは「いかに事業を目標として設定した時間（目標復旧時間）内に再開させるか」について、様々な観点から対策を講じることが目的であるので、対象範囲は原則として、全ての事業・業務、施設、人員になる。しかしながら、組織によっては、対象範囲をまずは基幹事業・業務[12]に特定したり、また、人員の安全確保や公平な取引の観点から事業・業務を停止することなど、優先度に応じて復旧させる施設（設備）を限定したりする場合も考えられるので、BCP においても、対象とする業務、対象施設、対象となる人員を定義することは必要である。また、段階的にその範囲を拡大していくことも考慮されるべきである。

経営者は、企業の社会的責任の観点から事業継続の基本方針を決定し、いくつもの事業が継続できなくなるような状況に陥った場合には、事業継続の観点から事業・業務の優先順位付けをすることが重要である。

対象範囲	記述の例
対象事業・業務	全ての事業・業務、基幹事業・業務など。
対象施設	対象施設が被災した場合に、事業・業務の継続が困難となる可能性のある本社・他の拠点ならびにコンピュータセンターとする。
対象となる人員	対象施設に常勤の正社員、契約社員、派遣社員ならびに協力会社社員等。その他、対象施設に来訪している顧客等については、必要に応じて対象に準じた扱いをする。

（2）BCP と他規程との関係

BCP は、平時のリスク管理を主な目的として規定された『情報セキュリティポリシー』、『プライバシーポリシー』、『コンプライアンス規程』などにおいて、それぞれで想定されているリスクが発現した場合かつ事業継続が脅かされる可能性がある場合に発動される計画として位置付ける

[12] 基幹事業・業務：企業の存続に関わる最も重要度・緊急度の高い事業・業務。重要度・緊急度の高い事業・業務とは、それを失うと企業の財務状態に大きな影響を与える事業・業務をさす場合が多いが、ブランドイメージ失墜（例として、創業以来の商品の供給不能など）や顧客との関係悪化などの影響を加味する場合もある。

ことが考えられる。

また、危機管理規程（あるいは緊急事態管理規程等）と相まって、事業・業務を継続できない不測事態における基本計画、あるいは「2.1(1) 対象範囲」において人員の具体的な行動指針として位置付けられる場合もある。

（3）遵守すべき法令・関連法規

BCP が発動される事態においては、自社が取ろうとしている対策が行政の目的と整合性をもっているかどうかを確認する必要があり、日頃から行政との連携について調整をしておくことが重要になる。また、法令において事故報告に関する規定が定められている場合がある。遵守すべき法令として、どのようなものが存在するかを列挙し、法令違反が起こらないようにすることが必要である。例として、災害対策基本法、個人情報保護法、各種事業法などがある。

2.2. 組織体制について

（1）BCP 責任者（BC マネージャー）の任命

BCP 策定には、多数の組織や要員が関与するが、最終的には BCP 責任者がその取りまとめについて責任を負う必要がある。BCP 責任者は BC マネージャーとも呼ばれ、次のような役割を担う。また、組織として最終的な責任の所在を明確化するために、組織の経営陣の役割・責務を明記することが望まれる。

＜BCP 責任者の役割＞

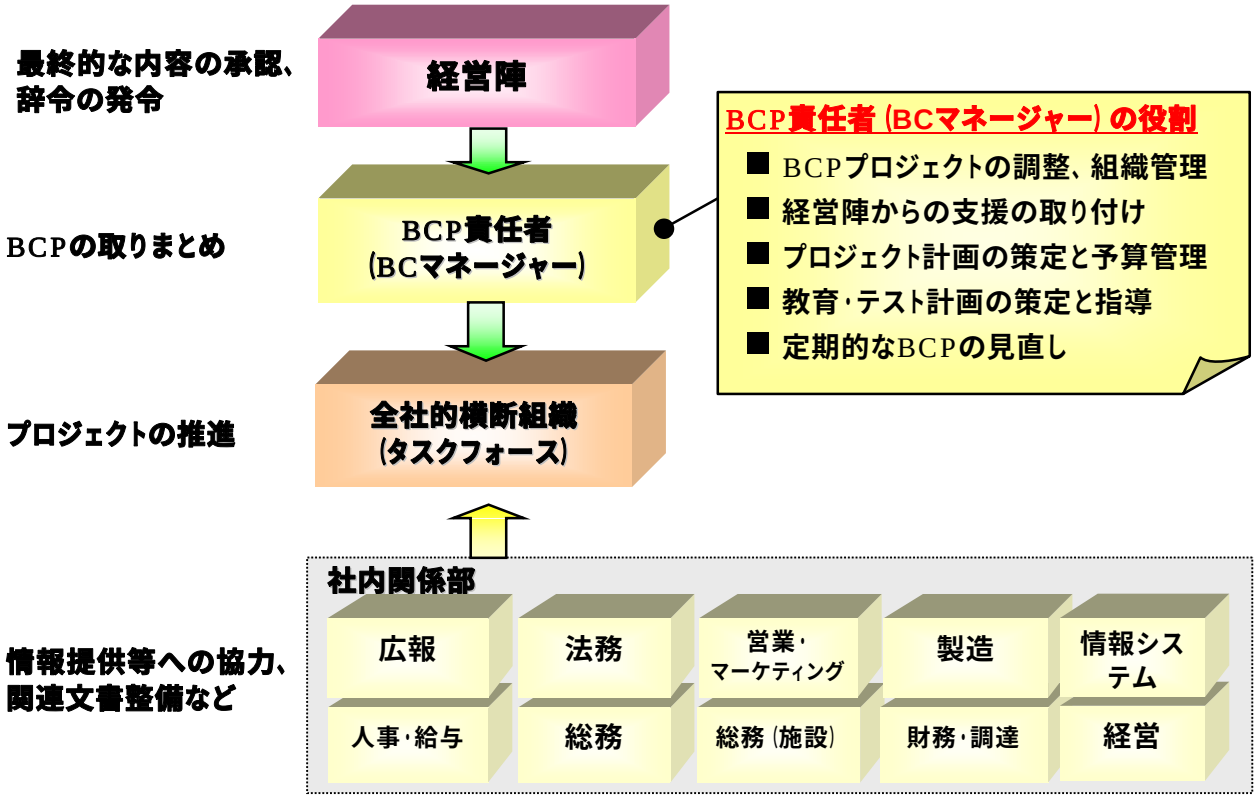
- ○BCP プロジェクトの調整、組織管理
- ○経営陣からの支援の取り付け
- ○プロジェクト計画の策定と予算管理
- ○教育・テスト計画の策定と指導
- ○定期的な BCP の見直し

（2）全社的横断組織（タスクフォース）の設立

BCP では、事業継続に係る組織内の様々な問題を取り扱うことから、原則すべての部署等の関係者がこれに関わることが必要となる。したがって、全社的横断組織（タスクフォース）を設けて対応することが有効である。中心的な構成メンバーとしては、人事・給与、総務（総務・施設関連）、財務・調達、経営、広報、法務、営業・マーケティング、製造、情報システムなどの関係者を含むことが考えられる。

なお、BCP 策定には、経営陣の関与・承認は必須であるので、タスクフォースのメンバーの中に経営陣を含めることもできるが、上位組織として経営陣等で構成する組織（例えば、リスク管理委員会、BCP 委員会等）を設ける場合もある。これにより、組織全体による支援が約束されることとなる。

【図表３　BCP プロジェクトの組織体制の例】



2.3. ビジネスインパクト分析から BCP 策定までの流れ

ステップ１:ビジネスインパクト分析
　①事業継続、復旧の優先順位付け
　②ボトルネックの特定
　③目標復旧時間の設定
ステップ２：リスク分析
ステップ３：発動基準の明確化
ステップ４：BCP 策定

（1）ビジネスインパクト分析

ビジネスインパクト分析とリスク分析は、発動基準の明確化につながる一連のプロセスである。ビジネスインパクト分析の目的は以下の通りである。

①事業継続・復旧の優先順位付け
②ボトルネックの特定
③目標復旧時間（RTO）の設定

ビジネスインパクト分析では、組織における重要な事業・業務（基幹事業・業務）・プロセス、それに関連するリソースを特定し、事業継続に及ぼす影響の分析を行う。この分析で、ボトルネックの特定やそのボトルネックの機能を如何に継続させていくかという方策を検討する。分析の手法としては、社内外でのビジネスの流れや取引先などとの相互依存関係分析、リスク管理関係の資料の確認、関係者によるインタビューやアンケートによって行われるのが一般的である。時間軸に沿った業務への影響を明らかにすることで、目標復旧時間（RTO）を設定し、事業継続の優先順位付けや BCP 関係者の行動指針を設定・明確化することができる。

【図表４　ビジネスインパクト分析結果のイメージ】

業務名			主管部署	関連部署	業務遂行上必要となるリソース				影響度分析結果			復旧優先度	RTO
区分	業務名	業務概要			業務遂行場所	利用システム名	必要人員数	その他必要資源	顧客影響度	収益資産影響度	社会的影響度		
管理	経営企画業務	経営計画の策定	経営企画部	－	本社	社内 LAN システム（PC5台）	5名		3	3	1	低い	1W
管理	法務関連業務	監督官庁対応	総務部	－	総務別棟	－	3名	電話、FAX	2	3	1	中位	24H
システム	顧客照会業務	顧客情報の照会、DBメンテナンス	情報システム部	営業部	コンピュータセンター	顧客照会システム、顧客情報 DB	本社2名、センター2名	－	5	4	5	高い	2H
：	：	：	：	：	：	：	：	：	：	：	：	：	：

①事業継続・復旧の優先順位付け

特定した事業・業務やそれに関連するリソースのうち、その影響度を総合的に勘案した上で、事業継続及び早期の事業再開の観点から、それぞれに優先順位を付ける。これに基づき資源配分や事業・業務停止時の再開順序を決定する。企業にとってどの事業を優先するかは、正に経営判断であると言え、経営層による了承が必要である。

②ボトルネックの特定

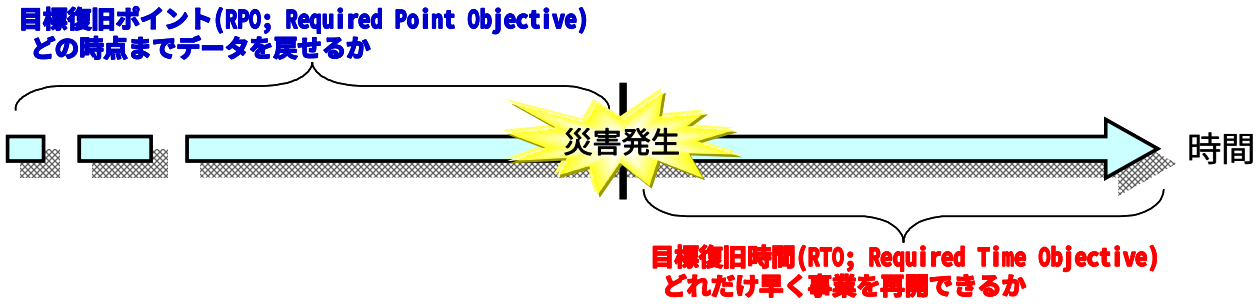
通常、ひとつの事態から複数の結果（シナリオ）が考えられる存在することになるが、企業にとって最悪のシナリオ事態から優先して検討することにより、他のシナリオを包含することが可能な場合もある。リスクが発生する事態（原因）だけに目を奪われず、事業を継続する上でのボトルネック[13]になるリソースの喪失を想定するとよい。

③目標復旧時間の設定

目標復旧時間（RTO）とは事業・業務の中断が発生した場合に、事業に重大な影響を及ぼさないうちに事業活動を復旧・再開させるための目標時間である。言い換えれば、どの程度まで中断が許容されるかの指標ともいえる。目標復旧時間を設定することは、ビジネスインパクト分析における主な成果物である。目標復旧時間は、図表４に例示するように、事業・業務と、それに関連するリソースを特定した上で、影響度を分析する。加えて、顧客からの要請、社会的要請、さらには関係当局からの要請など影響度を総合的に勘案した上で、ビジネス部門側の役員の承認も得て組織として最終決定する必要がある。また、IT 部門においては、データ・システムの喪失をどれだけ許容できるかを示す目標復旧ポイント（RPO；Recovery Point Objective）を設定し、これに応じたバックアップシステムを構築することが重要になる。このように、BCP のビジネスインパクト分析においては、時間枠で考えることが非常に重要である。

13 ボトルネック：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）。

【図表5　目標復旧時間と目標復旧ポイントの概念】



（2）リスク分析

ビジネスインパクト分析の過程において、並行的に組織に存在するリスクの洗出しと、そのリスクを低減させるための方策を検討するリスク分析・評価も実施する。リスク分析・評価では、組織における重要な業務（基幹業務）、プロセス、関連するリソースを対象に関係するリスクを洗い出すことから始まる。洗い出されたリスクの脅威と発生可能性に関して、統計データ、新聞の記事、過去のトラブル報告書など利用可能なデータをできる限り収集し、それらのデータを参考にして、BCP の発動にいたる可能性のある事態（リスク）を関係者で検討する必要がある。これにより、組織の事業継続に関わる重要な事態（シナリオ）が明らかになる。

（3）発動基準の明確化

ビジネスインパクト分析において、事業・業務への影響度と目標復旧時間を明らかにした後、組織としての対応レベルに従った発動基準を定めることが必要である。地震などのリスクについては、発動基準を自動立上げとすることも有り得る。これにより、組織として対応するレベルに応じた対応手順を策定することが可能になる。また、各組織は、目標復旧時間を達成するために、必要なリソースを準備することも重要である。ここでのリソースには、要員のほかに、バックアップデータの確保や通信手段の確保なども含まれる。

（4）BCP 策定

ビジネスインパクト分析終了後、その結果に応じた BCP を策定する。組織として合意の取れた目標復旧時間を達成するために必要な投資額の予算化を行うことも、ここでの重要な作業である。全社に関わる基本対応手順と部署毎に異なる対応が必要な個別計画があるので、相互の依存関係を明確にしたり、うまく分割したりすることで、重複を避け効率化することが重要である。

なお、情報システムの復旧に当たっては、複数の選択肢があり、一般的には次のような対策が考えられる。

＜情報システム･データの維持･復旧のための方法＞

○ホットスタンバイ、ホットサイト（同等の機器やシステムを準備し、同じ動作を行わすもの）
○ウォームサイト（同等の機器を準備しておくこと）
○コールドサイト（機器のスペースを予め準備しておくこと）
○内部分散システムおよびネットワーク
○相互援助協定（災害時における要員や機器等のリソース共有）
○上記の組み合わせ

2.4. BCP の導入と教育・訓練

（1）導入作業の概要

不測の事態において、BCP を有効に機能させるためには、組織の構成メンバーに BCP を周知徹底し、確実に実行できるようにしておく必要がある。BCP の教育・訓練とテストは、BCP についての知識と理解を深めるために重要なものであり、計画的に実施する必要がある。

（2）年間計画

①教育・訓練

教育・訓練の計画は、BCP 責任者の指導のもとに行い、組織全体および各部署にて行う。教育・訓練の主催者は年間の「教育・訓練計画書」を作成し、実施状況は「教育・訓練実施記録」として保存する必要がある。全社的に実施する場合は、集合教育として実施する例が多いと考えられるが、BCP の配付や説明会を行い、不測事態発生時の報告・連絡体制およびシステム障害時に確認すべき事項等を確認する。各部署で実施する教育・訓練では、より具体的な緊急連絡網やシステム障害時の代替・復旧手順の確認を行う。

＜教育・訓練の実施方法＞

教育・訓練受講対象者	実施時期・回数	実施の必要度合い
新入社員	採用時	必ず実施
対策本部メンバー	少なくとも一年に 1 回	必ず実施
上記以外のメンバー	少なくとも一年に 1 回	必要に応じて実施

②テスト

テストは、BCP の有効性を検証するために必要なものであり、実際に対応手順を経験することで対応力の強化にもつながる。しかしながら、BCP のテストはそれ自体リスクを伴うものであるため、実際には、机上テストと実践テストを組み合わせて行うのが一般的である。テスト計画を作成するに当たっては、テストの目的にあった検証項目、テスト実施範囲、テスト方法、実施対象部署および頻度などを検討し、「テスト計画書」として文書化する必要がある。

＜BCP のテスト検証項目＞

検証項目	種　別	実施方法
体制の確立	BCP のテストとして実施	机上（文書レビュー）
緊急連絡網・安否確認	BCP のテストとして実施	実践
消防・避難訓練	防災訓練として実施	実践
システム障害訓練	BCP のテストとして実施 個別システムの障害訓練として実施	実践・机上
BCP 総合訓練	関係部署を対象とした総合訓練	実践

③結果の記録、評価

教育・訓練の結果は、「教育・訓練実施記録」として、また、テストの結果は、「テスト結果報告書」として、記録し保存する。これらは BCP 導入の状況を知る重要な指標となる。「教育・訓練実施記録」は、BCP の周知徹底の浸透度を調査するために、また、「テスト結果報告書」は、テストの成功・失敗に関わらず BCP の見直しの必要性を検討するために重要なものである。

④経営陣への結果報告

教育･テストの結果もまた､経営陣への報告が必要である｡BCP は時々の事業環境に適応させ、常に見直しをする必要があるため、教育・テストから得られた結果に基づいて、改善が必要な事項があれば、経営陣の指示に従って、見直しを行う必要がある。

2.5. BCP の維持・管理

（1）BCP の管理方法と配付

BCP を関係者に周知するための、BCP の配付や説明会を行う。なお、BCP の配付先は「BCP 配付先一覧」に規定された部署・メンバーに限定し、外部に漏えいしないよう、厳重に取り扱うことを徹底する必要がある。配付された BCP は、最新版のものを不測事態発生時に直ちに取り出せるように保管しなければならない。また、BCP の発動時に重要な役割を担当する者については、自宅保管者として、最新版のコピーを自宅にも保管しておく必要がある。

（2）見直し

BCP は､情報システムの変更､新たな脅威等を踏まえ､見直しを適切に行うことが必要である。見直しの結果、BCP の見直しが必要な場合には変更を行わなければならない。

＜BCP 見直しの契機の例＞

- ○テスト結果による BCP 自体の見直し
- ○定期的な見直し
- ○BCP の前提条件の変更による見直し
- ○人事異動や組織の大幅な変更による見直し
- ○システム構成の大幅な変更による見直し
- ○新たな脅威の発生 (リスク環境の変化) による見直し
- ○監査の指摘事項による見直し
- ○準拠すべき法令等の改正による見直し

（3）BCP の監査

BCP は時々の事業環境に適応させ、常に見直しをする必要があるため、必要な変更が適切に行われている必要がある。このために、BCP の監査を適切に実施することが重要である。BCP の監査では、最新性および実効性の観点から実施することが必要である。BCP が適切に維持・管理されているかどうかの確認は、次のような事項により行うことが考えられる。

＜BCP の適切な維持･管理のための確認事項例＞

- ○BCP の最新版が定められた場所に保管されているか
- ○BCP のテスト結果に沿って、見直しが行われているか
- ○緊急連絡網を含む各種リストが最新版に更新されているか
- ○BCP において想定されている脅威等が評価され、その結果で見直しがされているか
- ○経営陣の承認が得られているか

（4）変更・承認手順

BCP の内容に変更もしくは改定が必要であると判断した場合には、BCP 責任者の指示に従って改定案を作成する必要がある。改定案は、全社的横断組織（タスクフォース）において検討された後、最終的には経営陣の承認を得て発効する。改定に伴う発効日付、バージョン等の履歴管理は組織のルール（文書管理規程など）に基づいて行う必要がある。BCP が変更・改定された場合、各種リスト等の関連文書も見直しを行い、速やかに必要な変更を行う必要がある。また、改訂された BCP は、BCP 配付先一覧に基づき速やかに配付する必要がある。

第III章　BCP 策定に当たっての検討項目

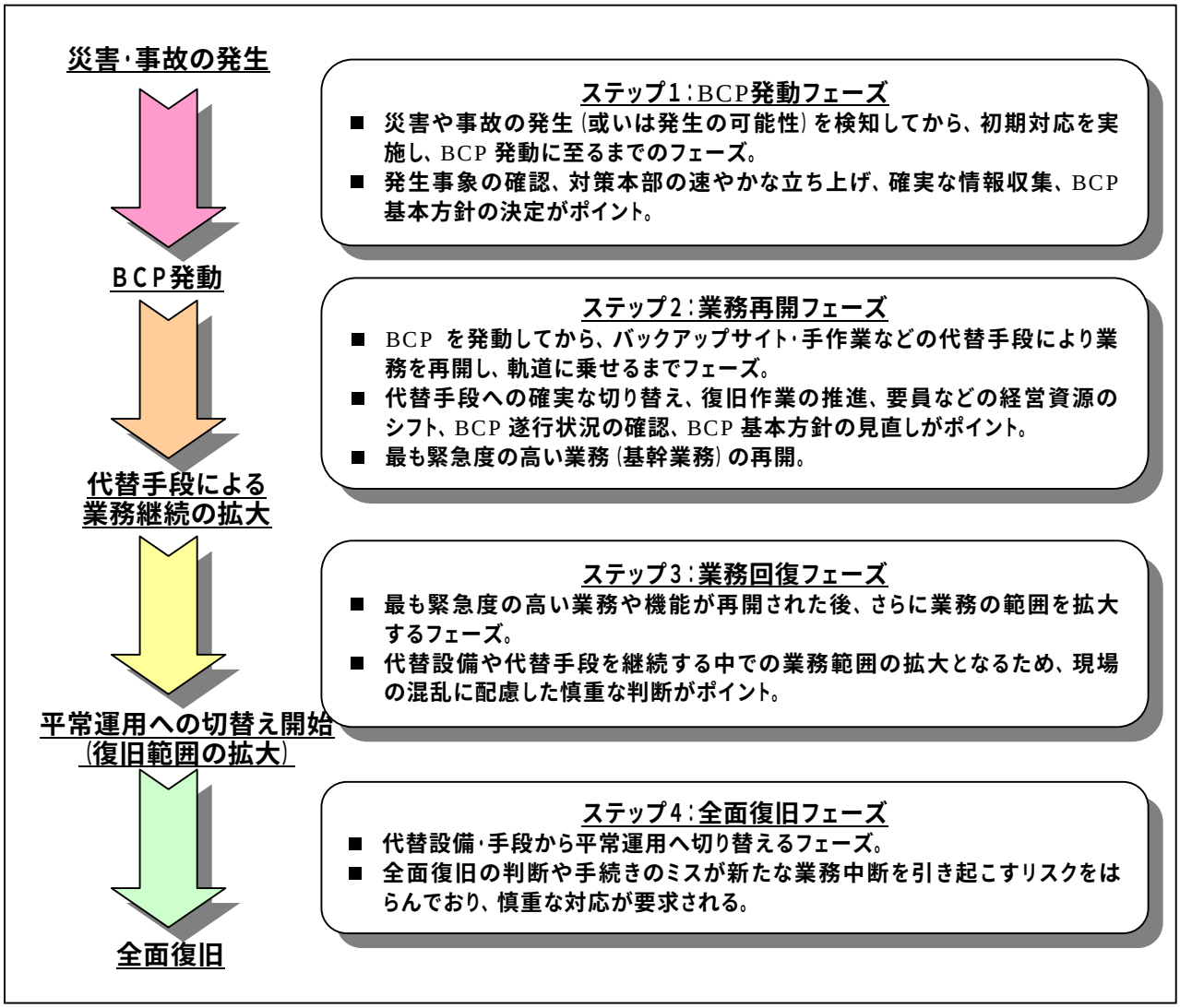
＜本章の位置付け＞

前章「II 総論（フレームワーク）」のビジネスインパクト分析やリスク分析の結果を踏まえて構築される BCP について、BCP の発動から全面復旧に至るまでの各フェーズにおける基本的な検討項目のポイントを例示的に記載している。

3.1. 検討項目の全体像とポイント

BCP の発動から全面回復に至るまでは、①BCP 発動時、②業務再開フェーズ、③業務回復フェーズ、④全面復旧フェーズの大きく４つのフェーズに分けることができる。各フェーズにおいては、BCP 発動から回復後の事後処理まで、経営層の的確な意思決定が求められる。緊急時の対策本部や対策チームはその意思決定をサポートするとともに、決定事項を遂行する役割を担う。（各フェーズにおける詳細な実施項目については参考１を参照）。

【図表６　検討項目の全体像とポイント】



3.2. BCP の実施体制

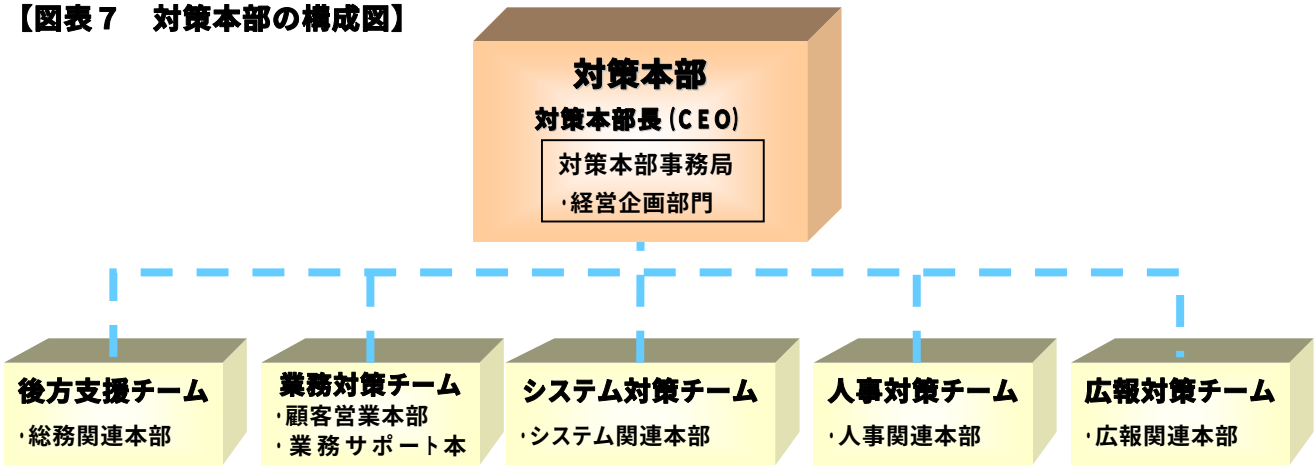
（1）対策本部の概要

対策本部は、非常時における最高意思決定機関として BCP の指揮を行う。具体的には、BCP の各フェーズにおける意思決定、BCP に関する行動の指示、BCP の実行状況の監督等の役割を担う。

対策本部の構成については図表７のような例がある。本社に経営層をトップとする対策本部を設置し、それ以外については平時の組織機構にて対応することも考えられるが、非常時においては平時とは業務の内容もボリュームも異なってくる。例えば、総務業務についてみると、通常はコスト削減のためアウトソーシングなどを活用して要員を削減していたとしても、非常時においては施設復旧・物資確保などが一度に集中するため平時の要員では機能しない場合がある。システム部門においても、企画・開発部隊ではなく運用・連絡部隊への要員シフトが必要となる。したがって、あらかじめこれを想定した機能別のチーム体制としておくことが望ましい。

以下に組織体制の例を示す。以降本章においては、この例を前提に記載する。

【図表７　対策本部の構成図】



（2）対策本部の設置基準

対策本部の設置については経営トップや対策本部長が発生事象及び影響範囲を勘案した上で判断することを原則とするが、大規模な災害や事故発生時において意思決定に手間取ったり判断に迷ったりしないように、あらかじめ発生事象を想定して設置基準を策定しておくとよい。設置基準の例は以下の通りであるが、不意の災害や事故発生時のみならず、かつての Y2K 問題や大規模なシステム統合・更改など将来予定されている事項についても、リスク日（Ｘデー）における事故発生に備えて対策本部を設置しておくことが望ましい。

＜対策本部設置基準の例＞

- ○ 東海地震に関する注意情報（あるいは予知情報、警戒宣言など）の発表
- ○ 本店、主要拠点、システムセンターの設置地域における震度○以上の地震発生
- ○ 緊急度レベル○の障害が発生し、回復の見込みがない
- ○ 大規模な情報漏えい事故の発生、もしくはその恐れの検知
- ○ 大規模なシステム統合・更改の○日前

（3）対策本部の設置場所

対策本部についてはあらかじめ設置場所を定めておく。その際、第１設置場所（例えば本店など）が被災した場合に備えて、第１設置場所と地理的に遠隔地にある拠点を第２設置場所とするなど、対策本部についてもバックアップ体制を取っておくことが望ましい。

対策本部の構成要員は、本部長、各対策チームの長、事務局要員で構成する。対策本部においては情報統括機能及び収集した情報を基にした経営判断機能が最も重要となる。

＜対策本部設置のポイント＞

①情報の発信担当者、収集担当者を定める。この場合、対策チーム別に担当を分けるなど、連絡先が集中しないよう配慮する。

②対策本部の設置候補地として、地理的に離れた複数の拠点を挙げておく。

③情報連絡のための設備面を整えておく。

（対策本部を設置する部屋に備えておくべき設備・備品類については参考２参照）

（4）対策本部の役割及び対策チームの設置

対策本部及び対策チームの基本的な機能は前述したとおりであるが、BCP の展開に対応して果たすべき役割が変化する。BCP において両者は緊密に連携しつつ、対策本部は迅速な意思決定及び各対策チームへの指示を行い、各対策チームは収集した情報や把握した状況について逐一対策本部への報告を行い、本部の意思決定を支援する。現場などの関係部署からの情報収集を継続し、業務継続上の支障や問題の発生についてモニタリングを行う。各対策チーム内で解決できない場合は、対策本部に判断を仰ぐ必要がある。また、各対策チームにおいても BCP の展開に対応して果たすべき役割が変化する。

（対策本部及び各対策チームのフェーズごとの役割は参考３，４を参照）

＜各対策チームの機能＞

チーム	統括部門	機能
後方支援チーム	総務関連本部	施設の復旧・保全、物資調達、物流
業務対策チーム	顧客営業本部 業務サポート本部	顧客対応、業務継続（対顧客）
システム対策チーム	システム関連本部	システム復旧・保全、業務継続（システム）
人事対策チーム	人事関連本部	安否確認、要員配置、労務
広報対応チーム	広報関連本部	社外広報・IR[14]、社内広報

3.3. BCP 発動フェーズにおける対応のポイント

（1）発生事象の確認

①発生事象の検知及び連絡

緊急事態が発生した場合に、最初に行うべきことは事実関係の把握である。発生事象の早期検知が遅れた場合、対策が後手となって事態の深刻化を招き、異常事態の長期化や顧客などの利害関係者への影響も大きくなる恐れがあるほか、場合によっては企業の存続に関わる恐れもある。したがって、できるだけ早いタイミングでリスクを統括する部署や経営トップ層に対し、一報を入れることが重要となる。

大地震など自然災害の発生については外部ニュースなどにより発生の事実を知ることが比較的

[14] IR(Investor Relations): 資金調達などのために、株式・社債等の発行体が株主・社債保有者等投資家に対し行う広報活動

容易であるが、システム障害や通信インフラ事故などは事態の把握が遅れることもあるほか、情報漏えいなどについては、内部からは発生の事実を把握しにくい面がある。また、危機につながる事象が検知されたとしても、第一発見者が事象を看過した結果対応が遅れ、その後事態が悪化し、大事故に発展するというケースもありうる。

したがって、あらかじめどのような事態が発生した場合に連絡を行うかを決めておくことが望ましい。その場合、重大な事態については経営層に直ちに伝達されるよう、緊急度を階層別に定義し、検知した事象と最終連絡先を区分しておくことも有効である。

＜緊急連絡ルール（システム障害関連）＞

緊急度	発生事象	説明	連絡先		
			システム部長	CIO[15]	CEO[16]
レベル４	基幹システム、基幹ネットワークの停止、重障害	広汎な範囲で業務遂行が困難。対外的に多大な影響が発生。	●	●	●
レベル３	基幹システム、基幹ネットワークの中障害 一般システム、一般ネットワークの停止、重障害	複数の業務において支障が発生。対外的な影響が発生。	●	●	
レベル２	一般システム、一般ネットワークの中障害	一部業務に支障が発生。対外的な影響は軽微。	●	●	
レベル１	一般システム、一般ネットワークの軽障害	対外的な影響はなし。	●		

また、連絡ルートについても責任者や担当部署に確実に伝わるようにあらかじめ緊急連絡網を定めておくとよい。その際、主担当のほか副担当を定め、不在時にも対応できるようにしておくべきである。事態を検知した場合には、発生時に確認できる事項を簡潔に連絡する。緊急性を要するため、まずは電話（口頭）で連絡を行い、その後、メールや FAX を用いて、書面で確実に内容の伝達を行うことが望ましい。

②連絡すべき項目

緊急時において必要な事項を漏れなく連絡できるよう、連絡すべき項目をあらかじめ定めて周知しておくことが望ましい。連絡すべき項目は以下に例示する。

＜緊急時の連絡項目の例＞

- ○対象システム
- ○発生場所
- ○発生事象
- ○レベル判定
- ○原因
- ○復旧見込み
- ○応援体制の要否
- ○業務への影響範囲

（２）安全確保、安否確認

緊急事態が発生した場合に、まず要員の安全確保を行う。対象となるのは、役員・社員のほか、協力会社の社員、スタッフ等である。役員・従業員の家族の安否確認の支援や、場合によっては施設内の顧客の安全確保を行う。安否確認については、あらかじめ社内での確認方法を定め、周知徹底しておくことが望ましい。

[15] CIO(Chief Information Officer): 最高情報責任者
[16] CEO(Chief Executive Officer): 最高経営責任者

＜安否情報の確認方法例＞

NTT171番号等の利用、安否確認情報の連絡先共有　等

（3）要員の配置

緊急時当初に安否確認ができた要員で、緊急対策本部および各対策チームの設置を行う。計画で予定された要員が召集できない場合に備えて副要員を定めておくとよい。正副の要員が不足する場合には、召集できた要員で改めて役割分担を決める必要がある。

（4）被害状況の確認

被害状況の確認を行う。その際、対策チーム毎に確認項目、確認責任者、確認情報の連絡先をあらかじめ定め、一覧表にしておくとよい。

＜被害状況の確認項目（システム対策チームの例）＞

	社員	協力会社	建物	電力	ネットワーク	交通インフラ	物流
本店							
システムセンター							
事務センター							
バックアップセンター							
倉庫（データ保管倉庫）							

※各システムの稼動状況についての確認を並行して行い、対策チームで被害状況をまとめる。

（5）業務影響の確認

事故や災害が業務にもたらす影響について確認する。そのために、事前にシステムセンター（ネットワーク）や事務センターのサポートが停止することにより影響を受ける業務についてまとめておくとよい。実務的には、個別システムレベルにおける前後の業務フローやインターフェース、冗長化構成などについて調査しておき BCP 一覧表としてとりまとめておくと、事故や被害の発生場所による影響が把握しやすい。（参考５参照）

（6）基本方針の決定

対策本部は、各対策チームから収集した被害の状況、業務影響を勘案し、BCP の選択と、復旧目標の策定を行う。生産設備やシステムの被害の程度によっては、代替生産やバックアップへの切替えが必ずしも得策とは言えない状況も考えられることから、十分に情報を収集した上で判断を行う。

＜基本方針決定の際に必要な情報＞

○要員配置や物流シフトの実現性

○処理能力及び業務範囲の制限

○切替えに要する時間、本番復帰に要する時間　等

これらの条件によっては、BCP の発動範囲を制限し、部分的に業務を停止することについても判断しなければならない。以上をとりまとめ、BCP についての基本方針を決定する。基本方針には以下のような項目が含まれる。

＜BCP 基本方針の項目＞

○業務優先順位
○BCP 発動範囲、発動タイミング
○業務の復旧目標と復旧計画
○要員等の経営資源の配置計画
○顧客対応計画
○広報計画　等

（7）対応の優先順位の決定

ビジネスインパクト分析によりあらかじめ決定している業務優先順位を基準に、設備の被害状況、要員体制、回復見込みなどを総合的に考慮して、BCP における業務優先順位を決定する。この優先順位に従って、要員や物資等の経営資源の配備計画を策定する。

（8）復旧目標の決定

BCP と合わせて、被害を受けた施設・設備・システムの復旧目標を決定する。その際、基本方針に則って配備された要員や資源を条件として、あらかじめ定めている目標復旧時間（RTO）の見直しを行う。その結果、優先順位の低い業務の事業継続範囲を制限したり、業務そのものを中断したりすることにより、優先順位の高い業務の早期復旧を目指すなどの判断を行う必要がある。

その際、業務継続範囲の拡大と復旧目標の早期化はトレードオフの関係になる場合があるため留意を要する。例えば、システム事故の場合は、システム対策チームが提供する業務継続可能範囲と復旧目標と、業務対策チームによる業務範囲の制限や中断による顧客への影響度合いとについて、対策本部が情報を収集した上で、経営に与えるインパクトを判断し、どちらを優先するかの決定を行う必要がある。

（9）初期対応の実施

災害や事故が発生した場合、被害の拡大を極小化するため初期対応は極めて重要となる。従って、災害や事故が発生した直後から、対策本部が BCP の方針決定と発動を行うまでの間に、各対策チームにおいて初期対応を実施する必要がある。例えば、各対策チームが行うべき役割の中のほとんどは、対策本部からの指示を待たずに着手できるものである。したがって、これらの項目について体制が整い次第順次対処することができるよう、あらかじめ実施担当者や実施手順を定め、チェックリストを作成しておくことが望ましい。

3.4. 業務再開フェーズにおける対応のポイント

（1）人的資源の確保

業務再開時においては、業務の再開・継続と復旧活動を同時に行う必要があることから、人的資源を効果的に配置する必要がある。しかしながら、平常時には存在しない追加的な業務が発生するほか、何らかの制限によって平常時よりも人手を要したりすることがあり、さらには社員や家族の被災などによって、要員が十分に確保できない場合が多い。このため、BCP 基本方針に従って部分的に業務を縮退し、必要な部分に要員を配置するなどの人的資源の確保策が重要となる。

（2）代替オフィスの確保

災害や事故の発生によって本番オフィスが使用不能となった場合には、代替オフィスにて業務継続を行う。代替オフィスについては、本社とは地理的に離れた拠点などをあらかじめ定めておく。代替オフィスは空間の制限がある場合が多いことから、BCP 基本方針に従い優先度の高い業務を行うための人的・物的資源を先行的に配置する。

（3）物的資源の確保

業務再開時において必要な物的資源の確保を行う。物資には、代替施設に持ち込む業務機器、システム、備品類、代替施設を稼動するための非常用電源稼動用燃料、業務処理に必要なバックアップデータ・帳票類[17]などのほか、生活物資なども含まれる。併せて、これらの物的資源を搬送するための物流ルートを確保する。

（4）業務再開とモニタニング

BCP 基本方針によって定めた業務継続の範囲について業務を再開するとともに、問題なく遂行できているかをモニタリングする。特に、代替オフィスやバックアップセンターなどでの運用や、手作業による運用を行う場合は、当初計画通りに業務遂行ができないケースがある。

例えばシステム運用の場合、代替状況について大まかにケース分けすると以下の通りとなり、これらの状況についてモニタリングを行う。

＜システムの代替状況＞

①バックアップシステムへの全面切替えを行っているケース
バックアップシステムにおいて通常範囲と同じレベルで業務を継続しているため、人的資源や物的資源、物流等の制限がなければ、特段の問題は発生しないと想定される。
②部分的に切替えを行っているケース
バックアップシステムの処理能力、或いは本番システムへの部分的な故障でバックアップシステムが準備されていないなどの理由から、業務再開範囲に何らかの制限がある状況。量的な処理能力もしくはサポート範囲の縮小が発生しており、顧客に対する量的制限、サポートができない業務についての抑止、あるいは暫定処理などの判断を行う必要がある。
③バックアップシステムへの切替えが不可能なケース
バックアップシステムへの切替えが不可能であるため、全ての業務の抑止、暫定処理、或いはその組み合わせの判断を行う必要がある。

（5）復旧作業の実施

災害や事故により損傷を受けた施設やシステムなどの復旧作業を実施する。災害や事故により損傷を受けた施設やシステムなどの復旧作業の進捗状況、要員や物的資源の配備状況から、復旧目処を見直す。復旧が当初想定よりも遅れる場合は、代替運用の継続期間が長引くことから、顧客影響、要員配置、物的資源の調達、物流などの計画の見直しが必要となる。

（6）運用上の留意事項

①物流ルートの錯綜

バックアップセンターなどの代替施設を利用する場合には、平常時の物流ルートと異なることを十分考慮する。部分的に本番サイトにおいて業務を継続するなど、バックアップサイトと本番サイトとの併用が発生するような場合は、帳票類やデータテープ類の仕分けや搬送に混乱が発生することも想定されるため留意を要する。

②要員の訓練不足

BCP 運用において、不慣れな代替施設での作業や通常行わない手作業などに熟練していないことによるミスが発生しやすい。これに備えて、非常時用の手順書などを作成しておく必要がある。

---

17 特に、企業の存続に関わる文書や代替情報が他に求められない文書（バイタル・レコードと呼ばれる）が失われると、事業に支障を来すことから、そうした文書の特定、複製化や分散管理など管理方法の検討、緊急時の利用・活用手順の検討などを行うことが望まれる。

ただし、想定外のケースについては応用処理が必要となるため留意を要する。

③特殊な要員の不足

特に熟練した要員が必要な業務の場合は、当該要員が優先して配置されるような計画としておくほか、交通インフラの中断がある場合でも要員が確保できるよう、平時より配慮しておく必要がある。また、不慮の事故に備えて、バックアップ体制を敷いておく。

3.5. 業務回復フェーズにおける対応のポイント

（1）業務拡大範囲の見極め

このフェーズにおいて、対策本部の最も重要な役割は状況を的確に把握し、臨時体制の中で業務拡大がどこまで可能であるか経営として意思決定を行うことにある。自社内の要員や資源等の確認はもちろん、取引先との関係、業績に与える影響等を分析し、判断する必要がある。誤った判断は、緊急性が高く最優先で取り組んでいる業務にも支障をきたす可能性があることを認識しておかなければならない。

また､利害関係者から全面復旧の見込みについての情報提供を求められるのもこの時期であり、マスコミ等を通じた宣言が行えるよう手立てを講じる必要がある。

（2）確実な情報収集

このフェーズにおいては、混乱した中での正確に情報の収集を分析することが要求される。要員や施設・設備の確保はもちろん、物流の確保等、臨時の体制の中で業務を再開するためには、確認漏れは許されない。平時に各業務において必要となる要員や設備、帳票等の物の流れを確認し、どのような確認項目をクリアすれば業務が回復できるのか、シュミレーションしておくことが必要であろう。

また､正確な情報収集を行うためには､収集する情報の種類や収集方法（現場から対策チーム、対策チームから対策本部への報告方法）を確立しておくことが重要である。どのような情報を対策チームに集めなければならないのかが明確にされていなければ、必要な情報を必要な期日までに集めることは困難である。

（3）業務継続の影響確認

業務拡大の判断に際しては、現時点の業務継続状況が、今後の業務運営にどのような影響をもたらすのかを分析する必要がある。競合他社の状況等今後の業務運営への影響予測により、取るべき対応・投入すべき経営資源を判断することになる。

（4）復旧状況の確認

業務範囲を拡大するためには､それまでの復旧状況の確認が不可欠である｡業務内容によって、必要とされる情報は異なるため、あらかじめ確認項目を準備しておくことが必要である。

＜復旧状況の確認項目の例＞

○通信手段（郵便･電話等）、交通手段

○従業員の出勤の可否（被災状況の確認）

○コンピュータセンター運用可否

（5）追加資源投入の検討、実施

復旧状況の確認後、必要機器の手配・搬入、被災した機器の整備、通信機器の確保等の追加資

源投入の検討を行うことになる。各業務について、代替手法で業務を継続する場合、必要な追加資源をあらかじめ検討しておくことが望ましい。（代替手段の検討項目事例は参考６参照）

（６）更なる業務縮退の検討、実施

業務再開フェーズにおける業務の継続が順調に推移しているかを確認し、場合によっては更なる業務縮退を検討しなければならない場面も想定される。業務縮退の判断を誤ると、事業継続そのものが危ぶまれることになる。しかし、一度再開した業務について適切に縮退の判断を下すことを現場に期待するのは困難であるため、経営陣の責務として慎重に対応する必要がある。

（７）継続業務の拡大の検討、実施

想定した BCP に沿って業務が継続されていることを確認できたら、随時業務を拡大することになる。場合によっては、部分的な展開により現場に与える影響度を測定・検証しながら徐々に拡大する等、細心の注意を払う必要がある。

（８）復旧作業の実施、復旧目途の確認

業務範囲を拡大するためには様々な作業を同時並行にすすめる必要がある。システムの復旧であれば、要員や物流の確保を同時に進めることになる。システム復旧の目処を示すことで、その他の作業スケジュールが確定する。

（９）全面復旧のタイミングの決定、資源再配置の計画

業務拡大に一応の目処がついた段階で全面復旧のタイミングを決定することになる。自社の状況、競合他社の状況、経営資源の追加投入額等、戦略的な判断を多分に含むことになる。

全面復旧に向けた準備も並行して進めることが必要となる。代替施設・設備・システムによる業務継続状況を踏まえ、被災した施設・設備・システムを修復するのか、刷新するのか、あるいは当該業務から撤退するのか等、戦略的な対応が求められる。また復旧のための運用手順書の作成等、全面復旧に向けたシナリオ・マニュアルの作成が必要となる。

（１０）復旧後の制限の確認

臨時の対応を行った間の情報やデータは、手作業によるものや代替システムによる対応のために、必要な情報・データを全て満たしていない場合が多い。全面復旧に当たっては、これらの情報・データについてどのように取り扱うかという判断をしなければならない。特に基幹業務を担う重要システムにおいては、データの制限による業務への影響を十分にシミュレーションした上で､場合によってはこの様な事態を想定したシステムの作り込みを事前に行うことが必要である。

3.6. 全面復旧フェーズにおける対応のポイント

（１）切替えの判断

代替設備・手段からの切替えは、要員の配置や物流を大きく変更することになるため、現状の正確な把握・分析と慎重な判断が求められる。各対策チームは全面復旧及び復旧作業の現場指揮者として統括する。トップマネジメントは大抵、全面復旧を急ぐ場合が多い。正確な情報収集と分析により適切な判断を行うことは、むしろ各対策チームの責務といえる。

（２）復旧手順の確認・全面復旧の実施

平常運用へ移行するためのテスト・検証の手続きは事前に明確にしておく必要がある。特にシ

ステムの場合、復旧は全面切替えと同義であり、障害が発生する可能性が非常に高いため、テスト項目や方法を含めて事前に確認項目を準備しておく必要がある。また、要員の配置や帳票等の物の流れも大きく変更されることになるため、事前にチェック項目を準備する必要がある。

（3）資源の再配置

代替設備･システムを､切替えた設備やシステムが安定的に稼働できることを確認できるまで、バックアップとして稼働させることも想定して、全面復旧の実施と同時に要員や物流のシフトを実行しなければならない。また、これを機会に設備の刷新や効率的な資源配置を行うことも可能である。

（4）業務制限への対応

全面復旧においては、代替運用中の業務制限やデータ制限を的確に把握する必要がある。基幹業務に係わるものであれば、それまで制限されていた情報・データを全面復旧のタイミングで遡って修復する作業も必要となる。IT 部門においては、この際バックアップサイトから本番サイトへの全面切替えを実施したとしても、バックアップサイトにおいて制限を受けていた情報・データがそのまま引き継がれると、全ての業務が全面復旧せず、引き続き制限を受けたまま運営される場合がある。したがって、その部分を見極めた上で、新たな業務中断を招かないためにも慎重な対応が求められる。

（5）総括

全面復旧が一段落した段階で、被害状況や利害関係者への影響、今後の業績見込み等を総括する必要がある。特に BCP については、有効に機能したのか、改善点はどこかを整理しなければならない。たとえ小規模の業務中断であったとしても、障害となった事象について様々な角度から想定を行うことにより、より大規模な業務中断リスクに対して有効に機能する BCP を構築することが可能となる。（総括の項目は参考７参照）

3.7. リスクコミュニケーションの重要性

（1）リスクコミュニケーションの概要

リスクコミュニケーションとは、災害や事故が発生した（発生の可能性を検知した）場合などにおいて、情報の収集、分析、連絡、発表などを通じ、リスクに対する認識の程度を揃え、情報の共有を行うための活動のことである。近年、説明責任の高まりから、情報の取扱いや利害関係者に対する説明の方法に関して関心が高まっている。

具体的には以下のような情報活動であり、リスクコミュニケーションの巧拙が BCP 遂行の成否を分けることにつながる場合もあるので、日頃の訓練等を通して周知する必要がある。

＜リスクコミュニケーションにおける情報収集の例＞

①対内的な情報活動

内容	**○現場、各対策チーム、対策本部における情報収集と情報発信による情報共有**
目的	**○情報統制、リスクの発見･特定、目標の共有化、混乱の防止、対外的な説明の一致**

②対外的な情報活動

内容	**○顧客、協力会社、地域住民、マスコミ、投資家、株主などの利害関係者に対する情報提供（記者会見、ホームページ掲載、新聞発表等）** **○国、地方自治体、関係当局、消防･警察･保険所などへの報告･情報収集**
目的	**○正確な情報提供による誤解･憶測･混乱の防止、協力の要請** **○リスクの公表による被害拡大の防止、社会的信頼の維持、社会的責任の遂行（法令遵守）**

（2）各フェーズにおけるリスクコミュニケーションのポイント

フェーズ毎に必要とされる情報や、提供の方法が異なるため、注意が必要である。

①BCP 発動フェーズ	**災害や事故について、発生の事実、影響範囲、回復の見込みなどについての情報共有**
②業務再開フェーズ	**二次災害が発生していないか、発動した BCP が支障なく遂行できているか、顧客への影響が拡大していないか、回復見込みに遅れが生じていないかなどについての情報共有**
③業務回復フェーズ	**業務の再開が順調に推移しているか、代替設備･システムでの業務遂行の留意点、全面復旧の目処などについての情報共有**
④業務回復フェーズ	**全面復旧を安全に果たすための情報共有と、復旧後の業務影響を取りまとめて第三者に示すという情報収集･情報発信** **対外的に発表復旧の時期、全面復旧に伴う業務遂行の留意点、今後の企業活動への影響度などについての情報共有**

＜実効的な BCP にするために＞

BCP ではビジネスインパクト分析を行い、それに応じた事前準備･計画が緊急時の対策に影響を及ぼすのだが、被害を受けた経営資源の範囲や規模、関係先の状況等により、様々な想定が可能であるため、より詳細な計画がより実効性のある計画とは限らない。事業や業務の変更、新たなリスクや法令など外部要因の変化に伴って変更頻度が高くなることも考えられる。

業務回復･復旧に当たって「どのような確認を行わなければならないか」「注意事項は何か」「経営の判断を必要とする項目はなにか」「現場で判断すべきことはなにか」を明確にしておくことが、現場における対応をスムーズにし、誤った対応による混乱を回避することになる。

＜本章の位置付け＞

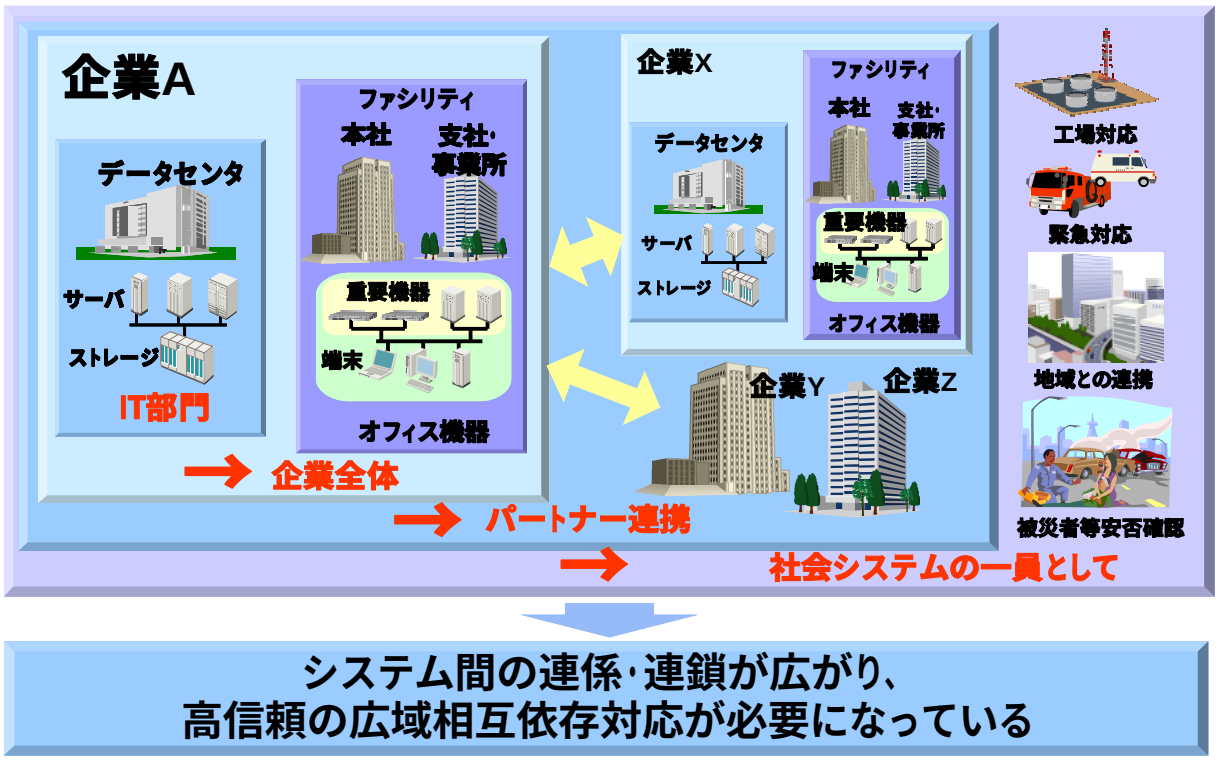
企業が被る災害や障害は多岐にわたり、その対応手順についても各企業で異なるのが自然である。第III章の基本的な対応手順の説明を受けて、3つのケースの対応手順について、具体的な障害の特徴や考慮事項を説明する。

① 大規模なシステム障害への対応
② セキュリティインシデントへの対応
③ 情報漏えい、データ改ざんへの対応

4.1. 大規模なシステム障害への対応

米国は２００１年の米国同時多発テロでは、ニューヨーク市マンハッタン地域での広域災害[18]を経験し、日本は２００４年の新潟県中越地震で、特に新潟県中越地域一体での交通の壊滅的被害を経験した。金融機関での大規模なシステム障害が社会的問題を引き起こしたことが記憶に新しいが、日頃の BCP 対応の優劣により、発生時及び発生後の企業での評価や競争力に差が生じることも考えられる。大規模なシステム障害発生時にも事業継続性確保の観点から、従業員の安全確認、要員確保や移動手段確保、オフィス確保、電源や通信ネットワークのような周囲環境を考慮する必要がある。

【図表７　広域での大規模システム障害と相互依存の関係】



[18] 広域災害とは、大規模地震、風水害等により、当該企業の本社・事業所及び関連外部機関等を含め、ともに被害を受けている場合のこと

（1）広域災害への対応

①通信手段関係

情報システムの通信手段の確保は特に広域災害時の場合、重要な情報の回復等に加え、要員の安否も含めた状況確認と、どのような初動を行うかの判断、その指示伝達において極めて重要な要素と位置づけられる。実際に国内外の事例を見ても、充分な BCP があったにもかかわらず、要員間の通信確保が上手くできなかったために、その再構築も含めた時間の損失となり、被害の増大や業務復旧の期間の長期化につながったケースも見られる。

通信手段の確保は、このような内部コミュニケーションを確保すると同時に、取引先や行政など外部とのコミュニケーションを確保するという観点から、BCP における優先度合いが上がりつつある。なお、通信手段の確保、継続的な利用実現には、「④電源装置、燃料関係」とのバランスを考慮することも大切である。

＜具体的な通信手段の確保方策＞

・通信手段の併用（固定電話、携帯電話、衛星電話、PC 電子メール、携帯電話メール、Web など）

・複数の通信会社やネットワーク・プロバイダーとの契約、通信回線の多重化　など

②ファシリティ関係

広域災害の場合、情報システムのセンターの代替や遠隔地センターとの連携を図ることへの考慮はされるが、ワークエリア全体が物理的に使用不可能となり、たとえデータやコンピュータ・システム、ネットワークが復旧したとしても、物理的に業務を再開する場所が確保できないというケースが発生する。このため、近隣に被災時のバックアップ用のワークエリアを自前あるいは外部ベンダとの契約によりあらかじめ確保したり、あるいは他地域の関係会社や場合によっては他社との相互契約により、広域災害の場合のワークエリアの確保を補完し合うという事例も見られる。また、ハードウェアが損傷する場合も想定して、バックアップ用のワークエリアには、業務用の PC 端末、電話、机、椅子、会議室などをあらかじめ備え付ける企業も見受けられる。

＜宿泊施設確保の教訓＞

業務復旧を確実にし、かつ、効率よく行うため、近隣にホテルなどの宿泊施設を確保する必要がある。2001年の米国同時多発テロの際にアメリカの大手投資銀行が近隣のホテルを借り切ったケースや、2004年の新潟中越地震では温泉旅館を長期間確保したケースなどが見られる。ただし、外部宿泊施設の場合は”first come, first served”（早い者勝ち）であるため、予め複数候補の情報入手、あるいは事前交渉することで、災害時の宿泊施設確保の確実性を上げることが望ましい。

③物流関係

対外的な事業継続性を維持するため、業務に通常必要な物資のみならず、生活用品や食糧なども含む必要な物資の入手を確実にすること、また在庫に基づいた仮業務から業務再開以降の仕入れ・納入に必要な物流の手段を最低限確保することが重要である。特に他社も含めたサプライチェーンに深く組み込まれているビジネスの場合、広域災害時にも物流手段を確保する優先度は極めて高いと思われる。

④電源装置、燃料関係

広域災害時には、広域停電の発生や電力も含めたインフラ関係の復旧が遅延することも考えら

れる。情報システムは機器自体の故障がなくとも電源がなければ作動できないため、電源を確保する必要性が高い。無停電電源装置（UPS）、発電機（ジェネレーター）などにより自家発電体制を構築していることが望ましい。

（2）オペレーション上の課題

①要員の確保、交通手段の確保

特に広域災害においては、職場における被災だけではなく、従業員の住居における被災が本人ならびに家族にも及ぶことが想定される。BCP とはいえども、まず優先すべきは人命の確保であることは言うまでも無いが、次に業務遂行上必要な要員をいかに確実に確保できるかは、業務の早期復旧のための重要なポイントとなる。

新潟県中越地震の際には、工場がパート社員の確保のため、敷地内に臨時の保育エリアを設け、被災により学校に通えない児童を預かることでオペレーション要員を確保したようなケースが見られた。要員確保に併せて、従業員のオフィス間の移動や住居（本来の住居、もしくは近隣のホテルなどの代替住居）からの通勤に係る交通手段を確保する必要もある。

＜ニューヨークにおける BNet※の取組＞

BNet は、在 NY 市の主要企業と NY 市、警察、消防が連携して、広域災害時において業務復旧に不可欠な従業員を予め特定、ID を持たせることで市、警察、消防の警戒下でも優先的にワーク･スペースへのアクセスを確保しようという仕組みである。官民が連携して地域コミュニティとしての取組んでいる点は注目される。

※BNet: Business Network of Emergency Resources, Inc. (http://www.bnetinc.org/home.html)
FEMA(Federal Emergency Management Agency: **米連邦緊急事態管理局)と、ニューヨーク市の共同で設立された** NPO **(非営利団体)。緊急時において、企業活動の復旧に必要な人間の被災サイトへのアクセスを確保する** CEAS **の仕組みを開発、** NY **市に加えてボストン、シアトル、アトランタなどにも導入展開中。**

②外部関係機関との連携・連絡

事業継続には、まず事業活動の基盤となる業務インフラを確保するために、地方自治体や警察・消防への連絡や監督当局への報告が必要であるが、業務復旧後の取引維持を確実にするために取引先への業務復旧状況、業務復帰見込みなどについての連絡も優先されるべきである。特に仕掛かり中の商取引や、受注済みの商品・サービス提供にかかわる情報については、自発的に発信すると同時に、先方からの照会を確実に受けられるコンタクト先を、事前・事後（ホームページ、FAX などで）に取引先に知らせる仕組みが必要となる。サプライチェーンに深く関与している企業の場合、競合他社と供給協力などの交渉を行うことも考えられる。

③リスクコミュニケーション

広域災害の場合、自社の被災状況の把握に時間がかかることも想定されるが、その間に不正確、あるいは憶測に基づいた情報がメディアを通じて流布し、必要以上に不本意な経済的損失や風評被害のリスクが生じる可能性がある。このような状況を回避するためにも、事実をより早く自発的に開示し、業務復旧の途中経過や復旧見込みを都度アップデートすることが重要である。また、統一した対処方針を示し、社会や投資家、金融機関などからの信頼を維持するためには、対応窓口を一元化し、即時に情報がシェアできる規模の特定の部門や要員・チームに集中させる必要がある。

④業務オペレーション上のリスク管理

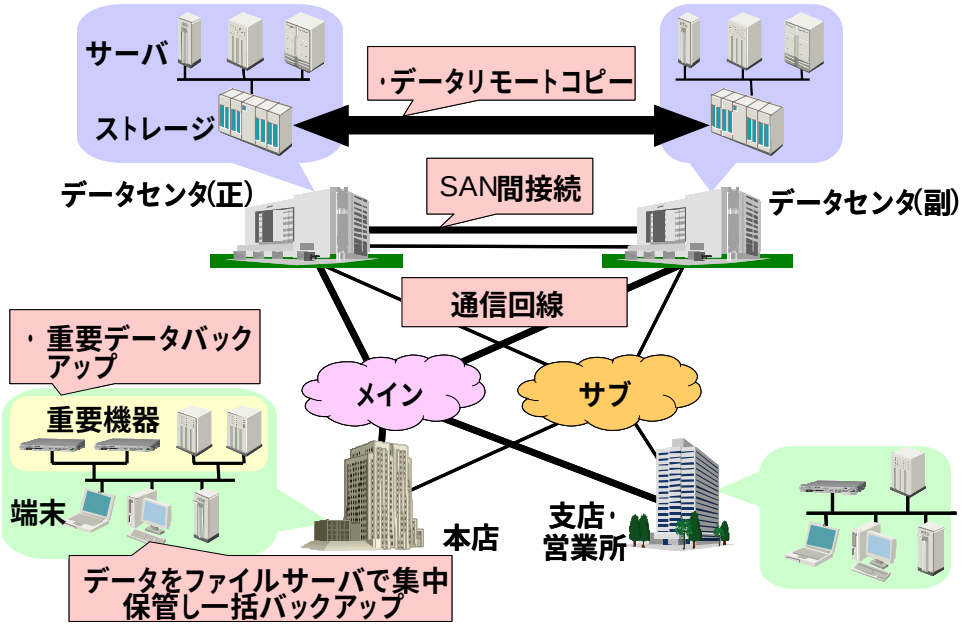
業務復旧時には通常と異なる場所・要員・手続きで業務を行うため、それに伴うセキュリティや商品・サービスの品質確保がより重要となる。特に広域災害の場合には、通常は顔を合わせない要員が出入りしたり、臨時の ID・パスワードなどを用いた運営が行われたりするため、本人確認や情報セキュリティの強化には特に注意する必要がある。また、拙速な業務復旧による業務オペレーション上の障害（事務処理ミス、不履行など）によっては、取引先からの信頼を損ね、災害前の取引が維持できない可能性も出てくるため、業務チェックや検品の頻度・精度を通常以上に上げる必要がある。

（３）技術による耐障害性の確保

①最新・高信頼の IT 環境

災害、特に広域の災害に対して、情報システムの耐障害性を完全にするには莫大な投資が必要になるので、どの業務プロセスを最悪時に継続させるかのポリシーが重要である。米国では重要な情報・データや業務システムの継続性を確保するため、情報、業務アプリケーションを同一ビルや付近地だけでの対応に加え、遠隔地へ分散配置する傾向が見られる。ネットワークの高速化により、複数箇所での情報の同期及び非同期管理や Web サービスを使用した業務の分散化も考慮されている。図表８に示すように、ネットワーク、データ、業務アプリケーション等の IT 環境要素の冗長化が進展してきているので、タイムリーな訓練等の実施により最新・高信頼な IT 環境について適宜検討し、耐障害性を高めていくことが望ましい。

【図表８　システムの冗長化による耐障害性向上】



②技術適用のガイドライン関係

広域災害を想定した事業復旧にかかわるガイドラインの中でも、IT の観点を加えたものとしてアメリカの金融機関の検査を司る FFIEC[19]が公開している”IT Examination Handbook “（IT 検査マニュアル）が有用である。BCM の観点から重要と思われる点を以下に示す。

---

[19] Federal Financial Institution Examination Council（連邦金融検査協議会）、アメリカの金融機関業務の監督を司る FRB（Federal Reserve Board）、SEC（Security Examination Committee）などの機関による検査機能を統括。各編のうち Operations 編（２００４年７月改訂）については INTAP にて仮訳済。

＜IT Examination Handbook より抜粋＞

- ✓ IT 運用上の役割と責任体制の明確化
- ✓ IT 関連のシステム、オペレーションの文書化と最新内容の維持
- ✓ IT 関連資産の詳細リスト作成と最新内容の維持
- ✓ 音声/データ通信にかかわる内部・外部接続にかかわるネットワーク・トポロジーの最新情報維持
- ✓ システム、オペレーション間の相互依存を考慮したデータ・フローとビジネスプロセスの可視化
- ✓ 上記による IT リスク評価実施、リスク軽減策策定とコントロール体制の導入

③訓練における留意点

BCP に関しては、その実効性を上げるための努力が通常時から求められるが、内容の充実もさることながら、訓練を適時に組織を挙げて実施することが重要である。特に広域災害の場合は、異なる地域の関係拠点やサプライチェーンを通じて関係する他企業、また、遠距離のバックアップサイトへの交通機関も含めた形で検討することが極めて有効である。また、訓練の頻度を上げる、業務の繁閑を見ながら特定日に災害時を想定した体制（バックアップサイトや代替オフィスに出勤し、バックアップされたデータに基づき、代替システムや代替ネットワークを利用）で通常業務を行う、といった形で訓練を日常化することも考えられる。

さらに、上記のような訓練で発見された改善点を BCP にフィードバックしたり、社内で共有したりすることで、BCP 自体の実効性を高めると同時に、組織としての耐障害性を企業文化醸成の形で高めてゆくというアプローチが有効である。

4.2. セキュリティインシデント[20]への対応

近年、ソフトウェアの脆弱性[21]を悪用した不正アクセス、コンピュータウイルス感染や Web 改ざんの発生件数が増加しており、それにより業務の停止・低下、個人情報の漏えいや情報の改ざんなどのセキュリティインシデントが多発している。これらの問題は、企業にとって顧客・協力会社や社会から信頼を失うことにつながり、経営に重大な影響を及ぼしうる。本節では不正アクセスやウイルスを主体としたインシデントと BCP の対応を説明する。

セキュリティインシデントへの対応は、24 時間 365 日続く、見えない敵との闘いと言ってもよい。セキュリティインシデントの発生抑止、発生時の拡大防止と被害低減化、早期復旧のためには最新情報の把握や、最適な防護設備の装備、組織や個人の啓発、さらに社外との信頼をベースとした迅速な連携等が必要になる。

（1）インシデント対応体制の整備と外部機関との連携活動

①社内体制整備

可能であれば自社内に、(a) 脆弱性対策並びに(b)インシデント対応の対外的な調整を積極的に実施することを専門に行なうインシデント対応体制（IRT）の整備と、社内組織に対応した専門家・協力者を配置するのが望ましい。

このようなセキュリティ専門家を企業内で維持することが困難である場合には、セキュリティ維持のアウトソーシングサービスを受けることも考慮すべきである。

＜インシデント対応体制の構築事例＞

(a) 脆弱性対策
脆弱性対策では、セキュリティ上の問題を引き起こす脆弱性を除去するための活動を行う。 ・企業のイントラネットや Web サイトについて、問題を引き起こす脆弱性の存在を指摘された場合に、その問題を早急に除去するための内部展開を支援する。 ・具体的な事例として、JPCERT/CC[22]、IPA セキュリティセンター[23]、CERT/CC[24]、NISCC[25]など公的なセキュリティ専門機関やセキュリティ専門ベンダから脆弱性に関する報告を受ける場合などがある。
(b)インシデント対応
インシデント対応では、実際に発生している侵害・障害を回避するための活動を行う。 ・企業のイントラネットや Web サイトに、侵害・障害の要因やそれを悪用する痕跡が発見された場合に、その問題を早急に除去するための内部展開を支援する。 ・企業に対して、侵害・障害の脅威を除去するための協力を依頼された場合に、その協力に関する内部展開を支援する。

[20] コンピュータセキュリティに関係する人為的事象であり、意図的及び偶発的なもの。またその疑いがある場合を含む。例えば、不正アクセス、ウイルスの流布、リソースの不正使用、サービスの妨害行為、データの改ざん、意図しない情報の開示や、さらにそれらに至るための行為（事象）などがある。

[21] ソフトウエア製品、通信プロトコル、インターネットサイトなどにおいてコンピュータ不正アクセスやコンピュータウイルス等の攻撃により、その機能や性能を損なう原因となり得るセキュリティ上の欠陥のこと。

[22] JPCERT/CC(Japan Computer Emergency Response Team/Coordination Center)：日本におけるセキュリティ事故情報の収集機関。（http://www.jpcert.or.jp/）

[23] 独立行政法人情報処理推進機構（IPA）セキュリティセンター（http://www.ipa.go.jp/security/）

[24] CERT/CC (Computer Emergency Response Team/ Co-Ordination Centre)：米国におけるセキュリティ事故情報の収集機関

[25] NISCC (National Infrastructure Security Co-ordination Centre)：英国におけるセキュリティ事故情報の収集機関

②外部機関との連携活動

企業がインシデント関連の対策を進めるとき、問題になるのは企業の機微な情報を社内外の関係者に対してどのように提供し、連携するかである。IRT とは、セキュリティインシデントについてのサポートを提供する機関であり、主な役割は、「インシデント解決のための企業間調整」「インシデントを未然に防ぐための情報の提供／対策」などがある。

IRT を自社組織内に持つことが出来る企業は、外部との連携を考慮した体制を設置することを事前に検討するのが望ましい一方、IRT を自社内に持つことが出来ない企業では、IT ベンダやセキュリティベンダの活用を介して、外部との連携を進めるのがよい。現在、中立的な調整役の IRT として JPCERT/CC, CERT/CC などがある他、製品ベンダやユーザ企業も IRT を組織化するケースも見られる。

一般企業が全て IRT を組織化することはコスト面から見て現実的ではないが、経営者の理解・先導のもと、必要最低限の IRT 機能を担う人・体制を整備し、脆弱性・インシデント関連情報を社内に効率よく流通させると共に、社内外との調整役として機能することが望まれる。

（2）状況把握・インシデント特定と対応

①状況把握

異常の発生を正確かつ迅速に把握し、インシデントを特定することは、困難な場合が多い。日頃の情報システムの状態を常に把握しておくことが基本となるので、自社専門家による監視やセキュリティ監視サービスの活用が選択肢となる。自社の状況把握だけでなく、社外での脅威情報や発生情報の早期入手も傾向把握に必要である。

②インシデント特定と対応発生時

インシデント若しくはその恐れがあると特定された場合、要因により事前に制定されたポリシー（方針、規則、ガイドライン）に沿って対応する。

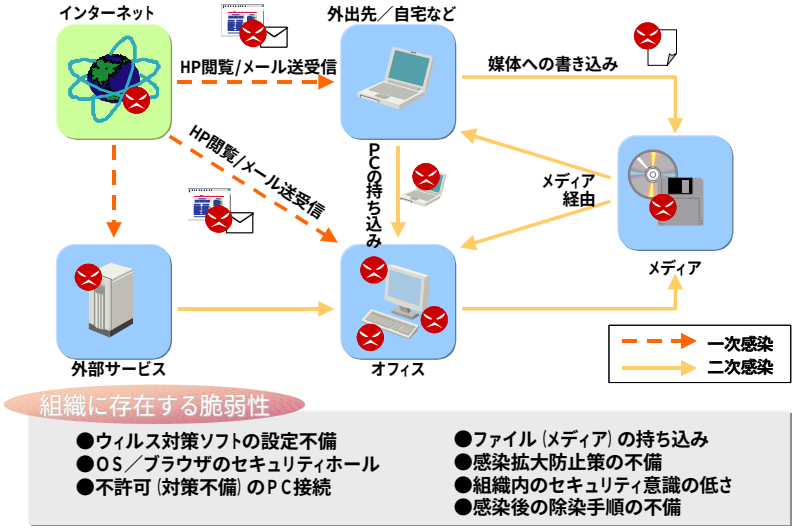
＜インシデント毎の対応ポリシー事例＞

(a)不正パケット発生時
社内で不正パケットが発生した場合、社内のパケットを IDS（Intrusion Detection System）[26]で監視する。不正パケットを受信した場合は、発信元を特定して該当マシン・ネットワークを隔離し、拡大防止を図る。
(b)ウイルスの発生時
アンチウイルスベンダ等からコンピュータウイルスの新種・亜種発生情報を入手した場合は、社内のウイルスパターンファイルを更新する。危険度が高く、未対応の場合、メール受信を一時停止することも検討する。また接続しているだけで感染が広がる Blaster ワームのような強力な感染力を持つウイルスの場合は、ルータにおけるポートの閉塞で対応する。
(c)情報漏えい発生時
情報漏えいが発生した場合は担当部署（例：コンプライアンス担当、情報セキュリティ担当等）へ報告し、迅速な対応を図る（4.3 参照）。
(d)未知ウイルス発生時
アンチウイルスベンダが認識していない新種・亜種ウイルスが社内で発生した場合、検体を入手し、ベンダへ送付して調査を依頼、得られたパターンファイルを社内に展開する。危険度の高いウイルスの発生時には、社内へアナウンスをする。なお、ウイルスの感染ルートの各パターンと脆弱性を理解、分析し、その対策を企業の状況で決めることが望ましい。

[26] コンピュータやネットワークに対する不正行為を検出し、通知するためのシステム。

【図表９　ウイルス感染ルートと脆弱性】

ウィルス感染経路は多岐にわたるため、トータルな対策が必要



③リスクコミュニケーション

社会的に影響の大きいインシデントについては、経済産業省、総務省、警察庁及び IPA、JPCERT/CC 等関係機関と連携し、いたずらに社会を煽ることのないよう、正確かつ適切な形で公表し、被害の局限化と早期解決を図る。

（３）平常時の運用及び教育

平常時のセキュリティ運用は、制定されたポリシー（方針、規則、ガイドライン）に沿って運用し、教育についても計画された教育を、予定に沿って実施するべきである。平常時に実施する重要事項は、セキュリティ関連ログの分析による状況把握と防衛策の策定、セキュリティ関連ソフトウェア/ハードウェアの定期点検とパターン更新、セキュリティ教育計画の策定、見直し、情報セキュリティ監査等が挙げられる。

①運用

セキュリティ運用には、一般的には情報システム部門が責任をもって携わり、セキュリティポリシー（方針、規則、ガイドライン）の作成・見直し、セキュリティ運用機器の点検、セキュリティ関連ログ分析、インシデント発生時の対策・防衛等の検討、インシデント関連情報の発信を行なう。企業によっては、セキュリティ運用の大半をアウトソーシングしているケースもある。

具体的な運用内容としては、以下の項目から自社に適用できるものを選択する。

＜セキュリティ運用内容項目事例＞

①インシデント発生予防（メール、Web、パターンファイル更新）

- **ウイルスチェックサーバによるウイルス侵入防止**
- **従業員による業務目的外の** Web **アクセスの抑止**（Web **コンテンツフィルターシステム**）
- **セキュリティパッチの自動配布**
- **利用者用** PC **のセキュリティチェック**（**パッチ適用、ウイルスチェック、不適切ソフト検出**）
- **情報漏えい防止**（**メールフィルタシステム、**HD **や記憶媒体の暗号化**）
- **情報セキュリティ監査**

②インシデント関連情報発信(従業員への啓発、注意喚起)

- **脆弱性情報をとりまとめ、各事業所、グループ会社へ提供**
- **セキュリティ関連ニュースから情報収集し、各事業所、グループ会社へ提供**
- **長期連休前の注意喚起を各事業所、グループ会社へ提供**
- **e-ラーニング等によるセキュリティ教育の実施**

②教育

自社、グループ会社、派遣会社等の社員教育は必須である。関係者全員のレベル向上と維持が重要であり、教育を計画的に実施する必要がある。セキュリティ教育を効率よく進めるために、e-ラーニング方式を取り入れている企業もある。また、教育計画は定期的に見直し、最新状況に適した教育メニューへの入れ替えが必要になる。

＜教育内容の事例＞

○セキュリティインシデントに関する企業ポリシー教育（方針、規則、ガイドライン）

○セキュリティインシデントに関する啓発教育

（法律、基準、ガイドライン、インシデント対応への取組み、世の中の動き、新技術等）

○ソフトウェア開発者に対するセキュアプログラミング教育

4.3. 情報漏えい、データ改ざんへの対応

近年、情報漏えい事故が多発していることや 2005 年 4 月より個人情報保護法が全面適用になることを受け、各企業・団体等は事故の未然防止のために情報セキュリティ対策の強化を進めている。しかしながら、万全を期した対策を取っていたとしても、なお情報漏えい事故やデータ改ざんなどが発生する可能性をゼロにすることはできない。万一の場合に備え、被害の拡大や二次被害の発生を防ぐ観点から考慮すべき事項についてケーススタディとして解説する。

なお、漏えい事故等への対応段階において講じる措置を検討する際には、各府省庁から出されている個人情報保護ガイドライン[27]のフレームワークに沿って具体化することが望ましい。

（1）BCP 発動

情報漏えい事故やデータ改ざんなどにおいては、最初から原因や影響範囲が明らかな場合は少ない。第一発見者が社内の人間である場合もあるが、報道など外部の情報が先行する場合もあることにも注意が必要である。一本の代表電話への問合せから事件に発展することもありうるので、疑義の段階を含め、どのような場合に BCP を発動するのか、組織としての方針を明確にしておく必要がある。そのためには、自社で発生した過去の情報漏えい事故やデータ改ざんに関する記録、他社事例に関する記事などを参考にして、BCP 発動のシナリオを作成し、発動基準に関する情報を共有できるようにしておくことが重要である。

なお、BCP が発動された際には、情報の一元化を図るため、情報管理を行うことが一般的であるが、事件や事故が発生した場合にだけ過敏な管理を行うと、言論統制と受け止められる可能性があることに注意が必要である。公益通報者の保護（内部通報、ホットライン）について、日頃から周知徹底しておくことにより、こうした問題を防ぐことができると考えられる。

＜情報漏えい発覚時の目標復旧時間＞

個人情報などの情報が漏えいした場合は、個人の財産などに物理的な影響が生じるなど危機的な状況が発生する可能性がある。この場合、漏えいした情報の特定や原因の究明、影響範囲特定のための調査を最優先させ、危機的な状況を脱した後に事業を再開するという選択をする場合もありうる。この際、企業では事業を停止してまでも調査をするのかという判断を問われることになる。

また、情報漏えい事故を起こした企業は、信頼回復のためにも再発防止策を講じた後での事業再開を選択する場合もある。この際にも、どの期間までなら事業を停止できるのかという判断を問われることになる。情報漏えい事故が発生した場合は、被害や問合せ状況、対策の進捗などを考慮して、事態の収束を見極め、事業再開の判断をする必要があり、目標復旧時間を検討する際にはこれらを想定して設定する必要がある。

（2）原因調査

原因調査とは、情報漏えいのルート（経路）や漏えいした情報の項目、量などを分析する作業をいう。なぜ漏えい事故が発生したかという根本原因を探るための調査を含む場合もある。自社に調査のノウハウがない場合や徹底した調査をしたい場合には、社外の専門調査機関を利用する場合もある。根本原因までを調査対象にする際には、組織的問題の検討と技術的問題の検討に分けて、分科会を設置することもある。

調査チームを編成するに当たり、原因が分からない段階では、それ自体多くのリスクをはらん

[27] 内閣府ＨＰより「個人情報の保護に係る関係省庁の検討状況
http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html

でいることに留意し、少人数、極秘を大前提にすることが必要である。組織も被害者という考えは通らないことを認識するとともに、内部調査は慎重に行う必要がある。また、調査は必要かつ十分な時間をかけて行うべきであり、早すぎる事態の終結は適当ではないが、進展のない状況は関係者に不安感などを生むことにもなりかねないので、期限を持って対応し、随時情報を公開することも重要である。

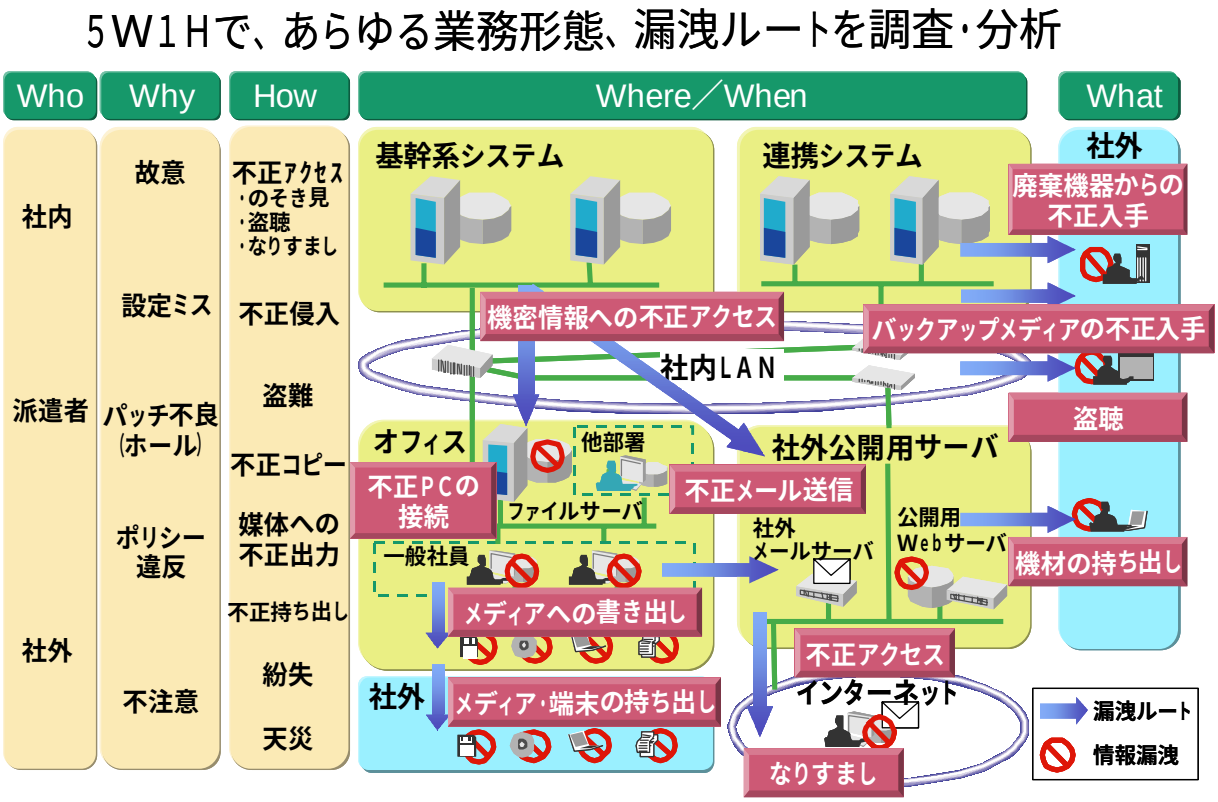
情報漏えいやデータ改ざんのケースでは、調査の正当性を立証する必要があるので、調査を行う場合には、顧問弁護士等の法律の専門家からアドバイスを得られるようにしておくことが必要である。

＜個人データの安全管理措置を講じるための組織体制の整備をする上で望まれる事項＞
（経済産業省個人情報保護ガイドラインより）

○情報漏えい等の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備
○漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備
○漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備

＜事故又は違反への対処をする上で望まれる事項＞（経済産業省個人情報保護ガイドラインより）
○事実調査　　○影響範囲の特定　　○原因の究明

【図表１０　情報システムを介した情報漏えいのルートと対策の分析】



（３）顧客対応

① 事実関係等の公表

事実関係等の公表は、被害の拡大や二次被害の防止、類似事案の抑止等の観点からリスク情報を共有する意味で重要なことであり、組織としてはできる限り公表することが望ましい。公表の方法については、顧客に個別通知する方法も考えられるが、大量情報漏えいの事案など緊急性が

ある場合や個別に通知するのでは確実に連絡がつかないような場合には、緊急記者会見や Web を利用することになる。情報の開示に当たっては、対応の迅速さと平等な対応が重要である。

＜情報漏えい事故やデータ改ざんが発生した場合の顧客対応例＞
○事実関係等の公表　　○顧客問合せ窓口の設置
○緊急記者会見　　○情報開示用 Web の開設

② 緊急記者会見

緊急記者会見は、大量情報漏えいなど緊急性があって影響度の大きい情報漏えいやデータ改ざんの場合や個別に通知するのでは確実に連絡がつかないような場合に行われる。組織としては、記者会見を開く前までに、組織としての統一見解をまとめたポジションペーパーと呼ばれる文書を準備する必要がある。ポジションペーパーには、それまでに判明した事実や経緯、原因、組織としての見解、今後の対応が書かれる。ポジションペーパーで打ち出した方針は、原則変えられないと認識しておく必要がある。

対策本部においては、広報チームが経営陣と連携して対応していくことになる。スポークスパーソンには、事前にコミュニケーション能力の高い人物を選んでおくことが重要である。また、メディアトレーニングを受講するなど､聞き手に誤解を与えないようにしておくことが望ましい。

③ 顧客問合せ窓口の設置

顧客からの問い合わせに関しては、想定問答集の準備やエスカレーション方法を明確にするなどして、個別対応をできるだけなくし、待ち時間の短縮化をする工夫が必要である。

＜顧客問合せ窓口の設置に当たって検討すべきポイント＞
○通常の問合せ窓口と同じにするか別にするか（フリーダイヤル、回線の確保）
○休日、夜間の受付延長をどのようにするか（要員シフト）
○電話以外の受付はどうするか
○いつまでその体制を続けるか

＜情報開示用 Web の開設＞
インターネットの普及に伴い、ホームページは組織の情報発信の重要なチャネルのひとつになっている。情報漏えいやデータ改ざんの事態においても、プレスリリース内容を Web に掲示することは一般的になっているほか、変化する情報を伝達するタイムリーな情報開示のツールとしても利用度は高い。情報開示用 Web を開設する場合の留意点としては、容易にたどり着くことができるような掲示位置にするなどのユーザナビゲーションや保守停止などのメンテナンス計画である。緊急時であっても、リンク先への了承の取付けなどネチケットを忘れないように注意する必要がある。

（4）再発防止策の策定、実施

事態が収束し、業務やサービスを再開するに当たっては、再発防止策の策定と確実な実施が重要である。発生した情報漏えいやデータ改ざんの状況や組織によって、対策は変わってくるのが当然であるが、一般的には次のような対応が考えられる。

＜再発防止策の事例＞

①再発防止策の立案（情報セキュリティ管理体制の見直し、セキュリティ強化のための対策導入、個人データを取り扱う情報システムの使用状況やアクセス状況の監視、情報セキュリティ監査の実施等）

②直後教育（情報セキュリティの重要性の再認識）

③業務およびシステム面での一斉点検

④BCP 発動時における対応の改善（被害の拡大や二次被害の防止の観点から緊急事態の対応として、今後に継承すべき教訓を取りまとめ、BCP 改訂の参考に資する。）

⑤継続的な情報開示（継続的な情報開示によって、対策の進捗状況を明らかにし、信頼を回復していくことが望ましい。）

（5）リスクコミュニケーション

リスクコミュニケーションにおいては、顧客、潜在顧客、株主、関係省庁など誰が聞き手（利害関係者）であるかを明らかにするとともに、聞き手がどのような情報を要請しているのかを理解することが重要である。

個人情報保護法では、個人情報の漏えい等の事案が発生した場合には、所管官庁への情報提供、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表することが要請されていることを念頭に置き、迅速な対応が取れるよう対策を立案しておくことが必要になる。

また、電子メールや Web などインターネットの利用は有効ではあるものの、感情面での対応には限界があることも認識し、対面、電話など他の情報開示手段もあわせて、各開示方法の利点と欠点について検討の上、聞き手や発信するタイミングに適した方法を選択する必要がある。

事業継続計画（BCP）策定ガイドライン
参考資料集

参考１　各フェーズにおける実施項目

参考２　対策本部室に備えるべき設備・備品類チェックリスト

参考３　フェーズ毎の対策本部の役割

参考４　フェーズ毎の各チームの役割

参考５　システム関連 BCP 一覧表の項目

参考６　代替手段の検討項目事例

参考７　総括の項目（システム関連）

参考８　ベストプラクティス：BCP 構築事例

【参考１　各フェーズにおける実施項目】

各フェーズにおける実施項目	
BCP 発動フェーズ	・発生事象の確認 ・対策本部設置 ・各対策チーム（部門）の設置 ・安全確保、安否確認 ・要員の配置 ・被害状況の確認 ・業務影響の確認 ・基本方針の決定 ・対応の優先順位の決定 ・復旧目標の決定 ・初期対応の実施 ・リスクコミュニケーションの実施
業務再開フェーズ	・人的資源の確保 ・物的資源の確保 ・代替オフィスの確保 ・業務再開範囲の確認 ・代替運用の開始 ・復旧作業の実施 ・復旧目処の確認 ・運用上の留意事項 ・リスクコミュニケーションの実施
業務回復フェーズ	・業務継続の影響確認 ・復旧状況の確認 ・追加資源投入の検討、実施 ・更なる業務縮退の検討、実施 ・継続業務の拡大の検討、実施 ・復旧作業の実施 ・復旧目処の確認 ・全面復旧のタイミングの決定 ・復旧に向けた資源再配置の計画 ・復旧後の制限の確認 ・リスクコミュニケーションの実施
全面復旧フェーズ	・復旧手順の確認 ・全面復旧の実施 ・資源の再配置 ・業務制限への対応 ・代替運用の本格的縮退 ・総括（被害状況のまとめ、利害関係者への影響のまとめ、再発防止策の検討、BCP の見直しの実施、サービスレベルアグリーメントの見直し、利害関係者への事後処理の実施、業績への影響の見極め） ・経営計画の見直し ・リスクコミュニケーションの実施

【参考２　対策本部室に備えるべき設備・備品類チェックリスト】

	対策本部室に備えるべき設備・備品類
	会議システム：テレビ会議システム等
	通信設備：一般電話、衛星電話、携帯電話、無線電話、FAX 等（各複数台）
	会議備品：ホワイトボード、PC（社内ネットワーク、インターネットに接続)、 その他筆記用具類
	連絡網：緊急連絡網、組織図等
	資料類：システム構成図、ネットワーク構成図　等
	電源等：非常用電源、電池、燃料等
	非常用の生活物資：食料、飲料水等

【参考３　フェーズ毎の対策本部の役割】

フェーズ	役割
BCP 発動フェーズ	情報収集により状況を把握した上で、BCP の発動範囲、優先順位、復旧目標等の基本方針を決定し、BCP を発動する。 ・緊急対策本部の立ち上げ ・各対策チームの立ち上げ状況確認 ・発生事象の事実確認 ・影響範囲の見極め ・復旧可能タイミングの判断 ・対策本部と各対策チームの役割分担の決定 ・BCP 発動の意思決定のための情報収集 ・BCP の基本方針の決定 ・BCP の発動宣言
業務再開フェーズ	BCP を発動して業務再開を指揮するとともに、業務再開状況をモニタリングし、問題点等の発生に対して適切な処置を取る。 ・業務再開の指揮 ・業務再開状況のモニタリング ・復旧状況のモニタリング ・問題点の把握 ・BCP 基本方針の見直し ・要員等の経営資源の再配置
業務回復フェーズ	臨時体制の中で業務拡大がどこまで可能であるか､経営としての意思決定を行う。 ・業務再開の指揮 ・業務再開状況のモニタリング ・復旧状況のモニタリング ・問題点の把握 ・BCP 基本方針の見直し ・要員等の経営資源の再配置
全面復旧フェーズ	代替設備・手段からの切替えのタイミング、範囲、順序についての方針を決定し、本番への切替えを発動する。また、被害の総括と BCP の見直しを行う。 ・業務回復の進捗把握 ・全面復旧のタイミングの判断 ・要員等経営資源の再配置 ・本番への切替え発動 ・被害総括 ・BCP の見直し

【参考４　フェーズ毎の各チームの役割】

	BCP 発動フェーズ	業務再開フェーズ	業務回復フェーズ	全面復旧フェーズ
後方支援チーム	・対策チームの立ち上げ ・拠点窓口の立ち上げ ・施設の損壊状況の調査 ・電気･交通インフラの被害状況確認 ・初期の施設保全対応･復旧対応指示 ・非常用物資の手配	・施設の損壊状況の調査（継続） ・電気･交通インフラの被害状況確認（継続） ・初期の施設保全対応･復旧対応指示（継続） ・物流ルートの確保 ・物資の供給	・損壊した施設の復旧状況の調査 ・被害を受けた電気交通インフラ等の復旧状況の確認 ・代替施設、代替設備の確保 ・物流ルートの確保（継続） ・物資の供給（継続）	･物流ルートの確保（継続） ･物資の供給（継続） ･被害状況の総括
業務対策チーム	・対策チームの立ち上げ ・拠点窓口の立ち上げ ・顧客影響の確認 ・業務サポート体制の確認 ・顧客への第一報の指示 ・顧客の安全確保の指示	・顧客影響の確認（継続） ・業務サポート体制の確認（継続） ・代替手段による業務サポート（手作業等）指揮 ・顧客からの要望事項や問題点の把握 ・顧客への続報の指示	・顧客影響の確認（継続） ・業務サポート体制の確認（継続） ・代替手段による業務サポート（手作業等）指揮（継続） ・顧客からの要望事項や問題点の把握（継続）	・顧客影響の確認（継続） ・業務サポート体制の確認（継続） ・全面復旧への移行における業務サポート ・顧客からの要望事項や問題点の把握（継続） ・被害状況の総括
システム対策チーム	・対策チームの立ち上げ ・連絡窓口の立ち上げ ・システム被害状況調査 ・復旧目処の確認 ・業務への影響範囲の想定と特定 ・運用体制の確認 ・バックアップ切り替え要否判断のためのその他の情報収集 ・初期のシステム保全対応･復旧対応指示	・代替手段によるシステム運用の指揮 ・問題点の把握、対応、報告 ・システム被害状況調査（継続） ・復旧目処の確認（継続） ・業務への影響範囲の確認（継続） ・運用体制の確認（継続） ・システム保全対応･復旧対応指揮（継続）	・代替運用の状況把握 ・全面復旧時期の設定 ・全面復旧に向けた手順の策定 ・復旧目処の確認（継続） ・業務への影響範囲の確認（継続） ・システム保全対応･復旧対応指揮（継続） ・代替手段によるシステム運用の指揮（継続） ・問題点の把握、対応、報告（継続）	・代替運用の状況把握 ・手作業分データの反映 ・平常運用のテスト･検証 ・本番機への移行対応指揮 ・運用記録の整備･保管 ・代替機縮退対応指揮 ・被害状況の総括 ・業務への影響範囲の確認（継続） ・問題点の把握、対応、報告（継続）
人事対策チーム	・対策チームの立ち上げ ・連絡窓口の立ち上げ ・役員･社員の安否確認情報の収集 ・役員･社員の家族の安否確認支援 ・出張･宿泊･医療等の労務	・役員･社員の安否確認情報の収集（継続） ・役員･社員の家族の安否確認支援（継続） ・出張･宿泊･医療等の労務（継続） ・要員配置上の異例処理の実施	・出張、宿、医療等の労務（継続） ・要員配置上の異例処理の実施（継続）	・出張、宿、医療等の労務（継続） ・要員配置上の異例処理の実施（継続） ・被害状況の総括
広報対策チーム	・対策チームの立ち上げ ・社内広報 ・社外広報の準備、情報収集、実施（第一報） ・マスコミ対応	・社内広報（継続） ・社外広報のための情報収集、実施（続報） ・マスコミ対応（継続）	・社内広報（継続） ・社外広報のための情報収集、実施（続報） ・マスコミ対応（継続）	・社外広報のための情報収集、実施（続報） ・被害状況の総括 ・社内広報（継続） ・マスコミ対応（継続）

【参考５　システム関連 BCP 一覧表の項目】

システム関連 BCP 一覧表	
システム名	
設置場所（設置センター）	
利用事務センター	
利用ネットワーク	
サポート業務、ユーザ部署	
上流システム、下流システム	
利用形態・頻度 （オンライン、バッチ（日次、月次等））	
冗長化構成 （完全二系統化、ホット／コールドスタンバイ等）	
復旧サービスレベル （無停止、○時間、当日内等）	
許容停止期間	
開発会社	
運用会社	

【参考６　代替手段の検討項目事例】

区分	検討事項
(1)手作業による代替の場合の検討事項	① 手作業対応のために必要な応援要員数 ② 手作業処理手順書や伝票、白紙帳票の整備・保管 ③ 可視元帳、台帳の作成、保管または臨時可視元帳、台帳（ダンプリスト等）の緊急作成体制 ④ 公印、事務用品等の品目、必要量 ⑤ 事務機器（パソコン、集計ソフト等、ワープロ、電卓、複写機、ファクシミリ等）の機種、台数等
(2)バックアップシステムによる代替の場合の検討事項	① バックアップシステム収容建物 ② CPU 機種、記憶装置、ディスク台数等 ③ 通信回線の種類・回線数 ④ 周辺機器、装置（端末、印刷装置等）の種類・台数 ⑤ 分散情報システム（PC、LAN、サーバーシステム等） ⑥ 電力設備、空調、燃料 ⑦ 給排水装置 ⑧ データ、プログラム、OS（及びそのバージョン管理） ⑨ サプライ（磁気メディア、用紙等） ⑩ マニュアル　等
(3)仮店舗・仮事務所の場合の検討事項	① オフィススペース（僚店、関連会社、賃貸等） ② 通信設備（携帯電話、ポケットベル、モデム等） ③ 電力設備 ④ 端末機器 ⑤ 事務用品（伝票、白紙帳票、筆記用具等） ⑥ 諸設備、什器（机、椅子、キャビネット、白板、大型金庫、紙幣／硬貨カウンター、チェックライター、ファクシミリ、シュレッダー、複写機、受付整理票発行機、監視 TV 装置、セキュリティアラーム装置、非常時通報装置）等

出典：金融機関等におけるコンティンジェンシープラン策定のための手引き書（財団法人　金融情報システムセンター）

【参考７　総括の項目（システム関連）】

項目名	内容
被害状況のまとめ	・ 自社が受けた被害についてまとめる。 ・ BCP 発動時「被害状況の確認項目」で使用する一覧表の項目に従ってまとめるとよい。
利害関係者への影響のまとめ	・ 顧客のほか、協力会社等に対する業務影響、損害、追加費用などについてまとめる。 ・ 場合によっては損害賠償に発展する可能性もあるため、契約上の履行責任の範囲かどうかの見極めも行う必要がある。
再発防止策の検討	・ 事故原因を分析し、再発防止策等の是正措置を検討する。 ・ 自社のみでなく、協力会社等に対し、再発防止策の策定を依頼する。
BCP の見直し	・ 被害の実態を総括し、BCP の不備や改善すべき点を洗い出す。 ・ 優先業務の選定、BCP の組織体制・連絡体制、必要な人的資源・物的資源の配備などについての課題を把握し、BCP の見直しを実施する。
サービスレベルアグリーメント（SLA）の見直し	・ SLA には、①システム部門が顧客営業部門等の他部門に提供するサービスについての保証レベルと、②システム部門が協力会社から提供を受けるサービスについて、その保証レベルの両方を含む。 ・ BCP の見直しを反映し、システム部門が他部門から求められるサービスレベルを遂行するために、協力会社との SLA の内容について点検・見直しを実施する。
利害関係者への事後処理の実施	・ 顧客、ベンダ等に対する損害賠償や、追加費用の支払いの交渉、調整を実施する。 ・ その際、関係当事者間の責任があいまいとなっている点については、SLA の見直しに反映し、責任分担を明確にしておく。
業績への影響の見極め	・ 被害状況、損害賠償、追加投資など災害・事故によって受けた損害を総括し、業績に与える影響を見極める。
経営計画の見直し	・ BCP の見直しや SLA の見直しを踏まえ、代替オフィスやバックアップセンターの強化・構築、要員の強化など、必要な投資計画の策定、見直しを実施する。

【参考８　ベストプラクティス：BCP 構築事例】

＜IT 企業のケース＞

1. 概要

企業、各種機関からコンシューマまで、幅広い顧客層を対象に、グローバルに IT サービス事業やコンピュータ関連製品を提供しているこの企業では、業務の IT 依存度も高いため、BCP の策定に早くから取り組んでいた。全社的に BCP の必要性が意識され始めたのは１２年程前のことであるが、組織や部署によっては既に BCP を策定していたところもあった。BCP を役員レベルの危機管理委員会が管轄するリスクマネジメントの一部と位置付けている点が特徴的である。リスクマネジメントの考え方は、Risk Mitigation （リスク緩和）をベースにしている。これは、リスクを 0 にしようとするのではなく、リスクを前提として、リスクが現実化した場合の影響をできるだけ緩和するような仕組みを構築しておくというものである。また、リスクマネジメントツールを活用しながら、PDCA サイクルによる BCP の継続的な改善を実施している。

2. BCP の作成手順について

同社では BCP 作成の具体的な手順として、リスクをどこまで許容するのかを割り切ることと、具体的な事故を想定することがポイントとしている。地震等広い範囲の災害が発生した場合に、競合他社は事業を継続しているのに、自社の事業が中断するわけにはいかない、あるいは、顧客の信用喪失やブランドイメージへの影響は最小限にしたい等､回避したい状況をリストアップし、そのような状況を引き起こすと想定される災害を決める。これらの前提条件が決まれば、非常時にするべきことも決まるので、あとは状況に応じて対応するようにすればよい。同社の場合、震度７クラスの地震を想定しているが、部分的な被害の場合、競合他社は事業を継続させている可能性が十分考えられる。自社の顧客だけに迷惑をかけるような事態は避けるという条件の基で BCP を作成している。

3. 非常時の連絡体制と行動マニュアルについて

非常時に適切な判断を行うためには、現場の人間と事業継続責任者との間での連絡・情報交換が重要である。この企業では、発生確率は小さくとも、発生した場合の損害が大きいリスクが現実化した場合には、上司を経由して、あるいは、本人から直接役員に通報され、役員が判断するようになっている。基幹ネットワークが停止するなど、結果的にはシステムが停止したのと同じ状況になる場合には、障害の影響度に応じた対応方法について細かく取り決めをしている場合もある。一方、役員にまで上げる必要がないような事案については事業部長が指示を出すことができるが、その場合には、例えば 代替配送手段の確保などコストが発生するものについては、指示を出していいのかどうかを判断するための根拠が必要になる。

また、詳細な行動マニュアルよりも、対応する人を明確化し、状況に応じて臨機応変に対応できるようにしておくことが重要であるという考え方から、行動マニュアルには必要最低限の項目のみが記述されている。そして、非常時にはそのときにその場にいる人がリーダになればよいという考え方で、マニュアルのリーダの名前を記入する欄は空欄にされている点が特徴的である。

4. グローバルな BCP への取り組み

同社のような IT 依存度が高い企業では、一つの国のオフィスで発生した IT 事故の影響は全世界に及ぶ可能性が高い。その意味でも同社にとってグローバルな BCP への取組みは重要な課

題である。

同社では、本社から全ての組織に対して、BCP を実施するための組織を作るよう指示が出ているが、それ以外にも、会社の理想を達成するためには BCP が必要であるという認識がグローバルに共有されていることが BCP に取り組む動機付けとなっている。事業が中断することによって、ブランドイメージ、評判、顧客の信用、株主の信頼、株価などにネガティブな影響がでることを想定し、ビジネスユニットごとに BCP コミュニティを設置し、グローバルリスクマネジメントの一部として BCP に取り組んでいる。

また、ヨーロッパ、北米、南米、アジアパシフィックの各地域で BCP のレベルを統一するための議論がコミュニティで行われている。各国における IT の活用状況は、サーバが中心であったり、ネットワークが中心であったり、アプリケーションが中心であったりと様々であることや、特定の地域間での依存性があることから、地域の特性にあった計画が作成されている。

5. BCP 作成上のポイント

同社には、IT セキュリティチーム、BCP チーム、地震対策チーム、環境対策チームなどいくつかのリスクマネジメントチームがあり、チーム間で同期をとりながら活動が行われているが、どのチームも管理部門及び各部署の代表という構成をとり、結果的にメンバーは重複している。これは、BCP 担当者を場当たり的に任命してもうまくいくものではなく、リスクマネジメントの一部として、日常業務を担当するメンバーが BCP のフレームワークの中で行動できるようにしておかなければ、実効的な BCP にはならないという考え方に基づいている。また、リスクマネジメントの対象に経営リスクが入っていることから、BCP を策定するためには情報システムの視点だけでなく、様々な項目に関する全社的な視点が必要であるという認識があることも特徴的である。

6. BCP の実効性確保のための取組

BCP を作成している企業でも普及活動や訓練、メンテナンスまで実施できている企業はまだ少ない。同社では、人事異動などで担当者の変更があった場合に、新たな担当者として実際に行動できる人を任命することにより、BCP の実効性を確保している。現場での混乱が生じないようにするためにも、あまり詳細な設定をせずに臨機応変の対応を求めている。

また、BCP を社内外の状況の変化にあったものとするために、分析、計画、実行、レビューのサイクルを繰り返すことにより改善が行われている。BCP の実効性を高めるための方法として、2001 年以降 BCP の監査を実施していることも特徴的である。監査を実施したことで、社内的に BCP への注目が高まるという効果もあった。

加えて、同社では BCP を検討するに当たって、投資対効果を考慮している。例えば、対策を導入する際には、バックアップテープの外部保管など、投資対効果の観点で適切だと思われるものに絞っている。投資対効果を考えた BCP とするためには、最低限のリスク分析が必要であり、リスク分析に相応のコストと時間をかける必要がある。

7. 今後の取組の課題について

非常時においても顧客へのサービスを継続するためには、事故が発生した時に従業員を確保できなければならないという意識から、そのための取り組みとして社員の安否確認を行う仕組みの検討が始められている。また、事業継続を脅かす事象が発生した際の、BCP の実効性の確保が最大の課題であり、常に試行錯誤を行いながら改善を続けていくこととしている。

8. まとめ

グローバル IT 企業では、IT 事故を原因とする事業中断によるネガティブな影響が大きく、事業継続計画の作成は必須事項であろう。この企業の最大の特徴は、『会社の理想を達成するためには BCP が必要であるという認識がグローバルに共有されている』という点であり、従業員の意識が重要であるということの顕著な例であるといえる。他にも BCP をリスクマネジメントの一部として位置付け、ビジネスユニットごとにグローバルに取り組んでいる点が特徴的であるが、事業の中断が業績にも影響する可能性がある事を考えれば、BCP をリスクマネジメントの一部として考えることは極めて合理的である。BCP を全社的な課題として捉えている企業はまだまだ少ないが、この企業の事例にみられるように、今後は BCP を全社的なリスクマネジメントの一部として考え、経営に直結した課題として取り組むことが求められるといえる。

＜金融機関のケース＞

1．はじめに

近年の銀行におけるシステム障害からもわかるように、銀行は業務が中断した場合に人々の暮らしや企業活動に与える影響が大きい。また、決済業務などの業務の性質上、銀行には、災害が発生した場合やシステムに障害が発生した場合においても業務を継続することが強く求められる。このような厳しい要求条件の下で、BCP に取り組んでいる国内金融機関の事例を紹介する。

2．BCP の考え方

この銀行では、従来から地震等の自然災害およびシステム障害を念頭においたコンティンジェンシープランを準備しており、非常時の意思決定体制や要員確保策などに関するマニュアルも作成していたが、その後、2000 年問題の影響が予見された時にコンティンジェンシープランの見直しと改善を実施し、2000 年問題対応マニュアルを作成している。近年になって、テロなどの新たな脅威が顕在化したため、2000 年問題対応マニュアルを進化させた BCP を作成した。最新の BCP では、危機管理としての BCP という考え方が取り入れられ米国同時多発テロ事件を契機に、より広範化する想定脅威に対応可能な業務継続体制の整備に着手した。

3．事業継続のための連絡体制について

事故発生時の対応を一元的に行うための非常時対応の事務局を設け、リスクコントロールを行いながらの対策の実施や、事故の状況を外部に伝える非常時コミュニケーションといった対応を行うようにしている。実際に事故が発生した場合、影響が一定レベルに達すると、事務局に連絡が入り、連絡を受けた事務局は事故の状況に関する情報収集を行い、上部組織に対して適宜状況の報告を行う。事故発生の初期段階において重要なことは、一定の時間内に判断し、適切な対処を行うということである。判断や対処が遅れた場合、外部からは事故が発生した事実を隠蔽していたと思われてしまう可能性があるので、こうした観点からもリスクコントロールは重要である。

また、銀行業務の特性上、非常時における金融機関同士の連絡手段の確保も重要な課題である。この銀行では、コンタクトリストを交換することにより、非常時においても連絡がとれるようにしている。

4．BCP 作成のポイント

BCP を作成する際に、自然災害、サイバー攻撃、テロ等、個々の原因に対してどのような対応をすべきかを検討するというアプローチでは、想定すべき状況が多岐に渡るため、なかなか検討を進めることができない場合がある。そのような場合には、原因から考えるのではなく、災害が発生した場合の影響を予測し、影響を極小化するための対策を考えるというアプローチが有効である。この銀行では、災害による影響として例えば、以下のような状況を仮定して、バックアップ体制、連絡体制、意思決定方法を決めている。

① 情報システムの機能が停止している状況
② オフィスの機能が停止している状況
③ オフィス、情報システムともに機能が停止している状況

①の場合、システムをバックアップセンターに切り替えるとともに、ネットワーク障害が発生した場合にはデータをFAX等によりバックアップセンターに送信し、システムに入力するようにしている。②の場合には、他のオフィスにおいて必要最低限の業務を継続できるようにしている。③の場合には、①と②の両方の手段により対処するようにしている。

バックアップシステムは正副構成とし、災害発生からバックアップサイトで業務を再開するまでの時間として２時間以内という規定を設けている。業務再開までの時間には、システムの切り替えに要する時間、データの引継ぎに要する時間、システムのオペレータがバックアップサイトに移動するのに要する時間が含まれており、これらの合計が２時間以内ということである。

また、BCP はその性質上、課題を解決することにより得られる効果という観点からの明確な目標を定めることが難しいので、独自に目標を定めてプロジェクト化し、適切なプロジェクト管理の基に進めることが重要である。また、BCP は組織全体に関わるものであり、様々な部署の人が計画に関係することから、プロジェクトをスムースに進める上で、トップのコミットメントは重要である。

5. BCP 作成に際しての課題

近年、BCP に対する関係者の認識は高まっているが、費用対効果が分かりづらいといった理由から、BCP の作成をスムースに進めることができない場合もある。このような費用対効果の問題や、事故はいつ発生するかわからないという理由から BCP の作成を先延ばしにする組織があるかもしれないが、金融機関としての社会的責任や、金融業務が情報システムやネットワークに依存する度合いが高まっていることを考えれば、対策を先延ばしする姿勢は適切ではないといえる。BCP を作成した企業がビジネス上有利になるという社会的な仕組みを構築できれば、BCP 作成が進展するとも指摘している。

6．今後の取組について

金融機関の業務は、例えば、ある取引において決済された資金が別の取引に充当されるといった形で、金融機関相互に依存関係があるという特徴がある。そのため、ある金融機関において業務コンピュータの障害により決済業務を実行できなくなった場合、他の金融機関において、業務コンピュータが稼動していたとしても決済業務ができなくなる可能性がある。したがって、自社だけではなく、当局を含めた金融機関全体の事業継続へ向けた取り組みが進むことが望ましい。

7. まとめ

銀行という業務の性質上、事業の中断は可能な限り避けなければならないが、この銀行では、事故発生時の連絡体制、他の金融機関や顧客との連絡手段の確保、バックアップサイトでの業務再開といった項目に関する詳細な計画が作成されており、BCP において先進的な取り組みを行っている企業であるといえる。BCP が組織全体に関わるものであり、トップのコミットメントが重要であること、業界内の連携が必要不可欠であるという点は、金融業界に限らず全ての企業にとって示唆となるであろう。