2012年7月12日
滋賀経済同友会 危機管理研究会

ビジネス継続マネージメント
BCM
Business Continuity Management

立命館大学
情報理工学部
情報コミュニケーション学科
仲谷　善雄

経　歴

- 1981　社会学士（社会心理学専攻）
- 1981　三菱電機（株）入社
  中央研究所　→　産業システム研究所
- 1991-92　米国スタンフォード大学　客員研究員
- 1999-01　（株）ドーシスに出向（高速道路関連コンサル）
- 2001-04　三菱電機　社会情報システム技術部にてSE
  →　社会eソリューション事業所
- 2004　立命館大学　情報理工学部　教授

研究テーマ：4本柱

- 災害対策
  - 観光客防災、企業防災、学校防災、ボランティア支援、防災教育、障害者のための防災、・・・
- ITS（高度道路情報システム）
  - 観光ナビ、観光誘導、車の合流支援、ペーパードライバーの復帰支援、方向音痴支援、・・・
- 思い出工学
  - 災害で思い出の品を失った人の思い出再構築支援
- 感性工学
  - 服との対話によるファッション・コーディネート支援、パーソナルテンポによる生活リズム調整支援、・・・

BCMとは？

- 災害や事故などのリスクを回避するとともに、被害に遭ったときの損害をできるだけ少なくし、復旧・復興を迅速・効果的に行う経営管理手法
  - ビジネスの中断期間が長くなれば信用失墜
    - 物理的な損害や収入の減少
    - 企業イメージの悪化によるビジネスチャンスの喪失
    - 対策の不備による信用の失墜
      ⇒　企業存続基盤の喪失
    - 雇用不安　⇒　地域復興の妨害要因
  - 企業、自治体のBC（Business Continuity）は、地域の復旧・復興に不可欠

リスクとは？

- ISOの定義：目的に対する不確かさの影響
  - 各組織が掲げる目標を脅かしたり、その達成に影響を与えるもの
  - 適切にリスクを管理しないと、組織の目標の達成だけでなく、存続にも大いに影響を与える
  - 反対に、適切にリスクを管理することで、市場優位性や社会の信頼を獲得できる
  - 今日のグローバル社会では、リスクマネジメントの結果は、一組織の事業目的の達成の可否だけでなく、他国や他の組織にも影響を与える

リスクマネジメントの標準化

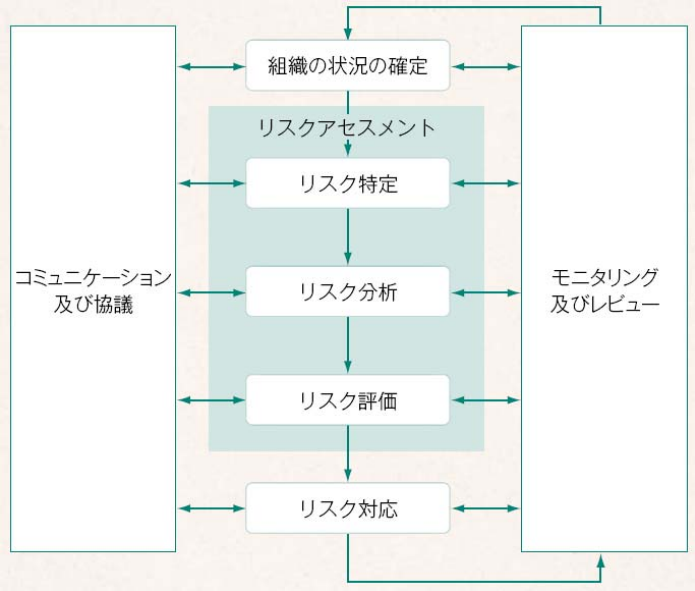
- ISO 31000（2009）
  - リスクマネジメント＝「リスクについて、組織を指揮統制するための調整された活動」
  - 必ずしも「好ましくない影響を管理する手法」ではない
  - リスクには「好ましい方向に目標をはずれること」も含まれる

ISO31000 リスクマネジメントの効果

- 目的達成の可能性を増加させ、事前管理を促す
- 組織全体でリスクを特定し、対応する必要性を認識し、好機と脅威の特定を改善する
- 関連する法律および規制の要求事項、並びに国際的な規範を順守し、義務的・自主的報告を改善する
- 統治を改善し、ステークホルダーの信頼と信用を改善する

ISO31000 リスクマネジメントの効果（続き）

- 意思決定と計画のための信頼できる基盤を確定し、管理策を改善する
- リスク対応のために資源を効果的に割り当てて使用し、業務の有効性と効率を改善する
- 健康や安全のパフォーマンスとともに環境保護を高める
- 損失の予防と事態管理を改善し、損失を最小化する



ISO 31000 のリスクマネジメントプロセス

BCMの対象

- 自然災害：地震、洪水、台風、火災…
- 大規模事故
- 9.11などのテロ
- 政治的混乱、内線などの政治状況の急変
- サイバーテロなどの技術的課題への対応
- サブプライムローン問題などの経済リスク

BCMの歴史

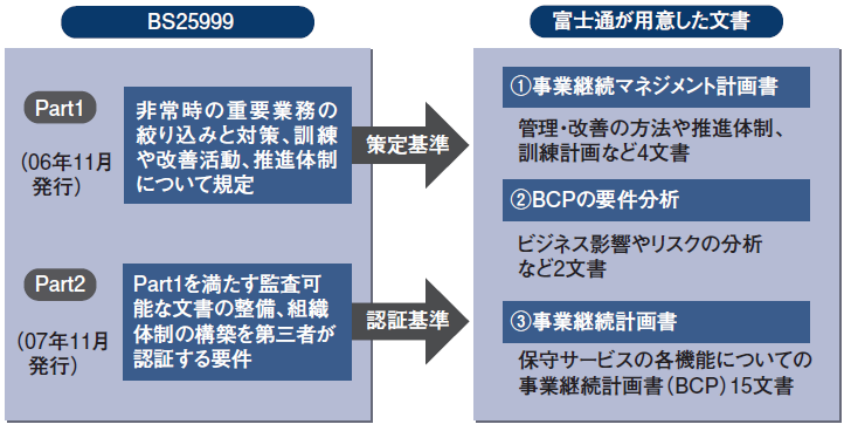
- ファーストインターステートビル火災
  - 1988年5月4日、LA
  - ファーストインターステートバンク
  - 火災発生後30分で、バックアップセンターにディーリング機能を移し、世界中からのディーリングサービス要求に対するビジネスを継続実現
  - 対応の速さが顧客の信頼を獲得し、預金者増加につながった
  - BCMはその最初から「バックアップ」が中心課題

米国におけるBCM

- BCP、COOP、DR
  - COOP：Continuity COperation Plans
  - DR：Disaster Recovery
- 9・11同時多発テロ事件を契機に、BCMの重要性が再認識された
- 経営上起こりうるリスクを開示しないでおいてリスクが現実のものとして発生すると、厳しい法的な罰則が適用される

- 国土安全保障省（U.S. Department of Homeland Security）など連邦政府機関
  - 2003年に、危機対応規格 NFPA 1600（米国規格協会ANSIが作成した国家標準）を取り入れた ”Ready Business” 推奨計画を発表
  - 米国のグローバル企業にとってはリスク管理手法の中心的な基準
- ISO（国際標準化機構）
  - 「自然災害に関するISOイニシアティブ」の理事会決議（5/2005）に従って、IWA（International Workshop Agreement）で国際標準化作業
  - 2012年5月にISO 22301として発行

- BS 25999
  - BSI（英国規格協会）の国際規格（07年11月）
  - 富士通が08年4月に日本初の認証取得
    - 富士通エフサスと共同
    - 顧客の情報インフラ保守サービス事業が対象
  - 被災から最短2時間、最長で1週間の復旧目標
  - 15機能について、特定地域の拠点が被災した場合の代替手段や、機能間の連携について規定
    - コール受付、要員出動管理、部品管理など
    - 災害対策本部：東京、サブ：大阪（可能であれば横浜）
  - 計2400人の社員にeラーニングで教育＋現場訓練



それぞれ50ページにも及ぶ文書

日本での現在の意識

- BCMについての必要性は認めるものの、経営層における認識に歪みがある
  - 既に災害対策には長年取り組んでおり、危機対応マニュアルは策定済みである
  - システムの冗長化などのレジリエンシー（耐故障性）対策には十分投資してきた
  - いつ発生するか不明の災害に投資できない
  - 経済状況が低迷し、それどころではない
  - リスクが顕在化してからでも十分対応できる

BCMへの意識改革の必要性

- 民間においてテロへの危機意識が低くすぎる
  - 内閣から自治体に、テロ対策策定の指示が出ている
  - サイバーテロについて、情報技術について知識の乏しい経営者が多い
- 今後リスク要因は多様化し、日本企業も安全でない
- 世界的に見て、BCP策定やBCM体制構築に投資決定を先送りする経営判断は、株主価値の保護を怠っていると市場から評価される危険性が高い
  - 米国を中心に、取引先企業にBCP策定を要求する動きが出てきている

BCMと災害対策の違い

- 災害対策　・・・　災害ごとに被害を最小限にするための対策を検討し実施するもの
  - 基本的には、「原因」を想定し、それに備える
  - 「想定外」が発生する可能性が常に存在する
- BCM　・・・　「原因」ではなく、「状況」に備える
  - 事業にとって「問題となる状況」を抽出し、それへの対策を具体的に考える
    - 例：20mの津波を想定するのではなく、電源喪失状況への対策を考える

従来の災害対策の問題点

- 「津波に備える」となると、どの程度の高さの津波を想定するかが問題となる
  - まさか20mの津波は来ないだろう
  - 20mの津波が来るか来ないかは人間が決めることではない（現代人の驕り）
  - 「電源が喪失したら困る」「社員が出勤できないと困る」などの状況は、災害以外の原因でも起こりうる
  - そのような困る状況を抽出し、対策を検討すべき

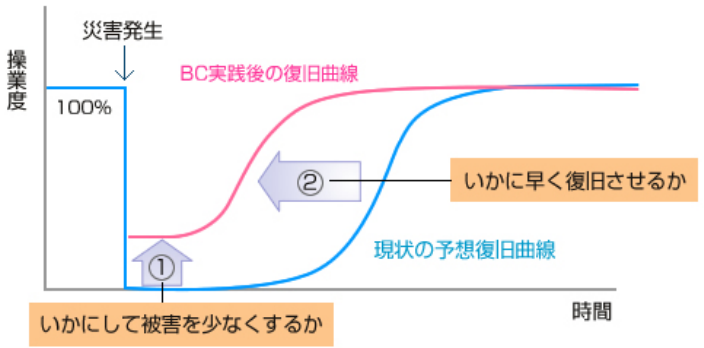
BCMの考え方

- 例:「社員が出勤できない場合」
  - 「そのとき鉄道は動いているのか？」などのように出勤させる方法を考えない
  - とにかく、「出勤できない」状況への対応を考える
  - 例：
    - 「出勤できない」のだから、支社をバックアップオフィスにする
    - クラウド化して各自の家で仕事ができるようにする
  - 「業務を続ける代替案」だけを考える

BCMへの基本的取り組み姿勢

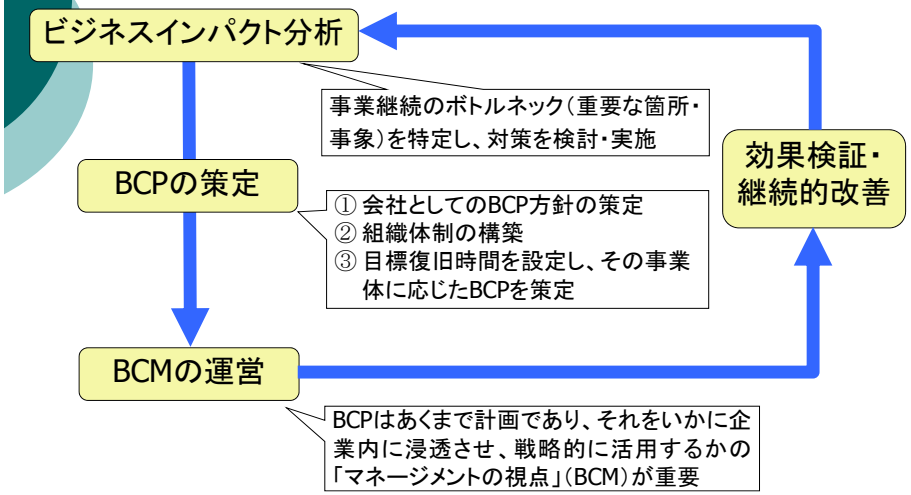
- BPR（Business Process Reengineering）として取り組むべき
  - ビジネス中断による損害予測をでき、客観的に会社の中身を知り、重要なビジネス機能やプロセスを確認できるチャンス
- アウトソーシングするのではなく、社員自らが実施すべき
  - 業務をもっともよく知る社員自らが計画を立て、リハーサルを通して現場の状況を反映し、継続的な見直しを行うことで、より良い（強い）会社を実現する ⇒ これが訓練になる

BCPの概念



＜事業継続のための2つの側面＞
①被害を予防/防止する
・被害や影響を最小限にする事前対策/計画
②重要業務が中断した場合は早期に復旧
・可能な限り早期に再開させる復旧対策
・ブランドスイッチさせない重要業務の目標復旧時間を設定

BCMの実施フロー



- 企業風土
  - BCへの強い意志と、合理的で具体的なBCPを策定・実行できる企業風土を醸成することが必要
  - 経営者や従業員の誠実性・倫理的価値観、経営理念や経営スタイル、経営者が権限や責任を付与する方法、従業員の能力開発の方針、取締役会による監督機能など
  - 株主・顧客・自社社員・業界等・内外の保護対象となる利害関係者に対して、「BCPを策定することにより、何を達成しようとしているのか」について、「意思表明」することが重要
  - 同時に、事前の対策とリカバリー戦略を検討

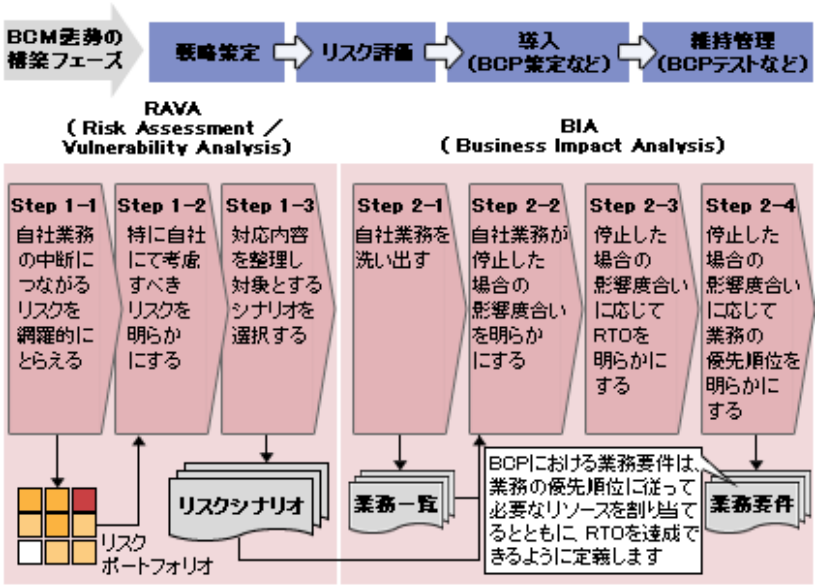
- リスク評価
  - ビジネスを可能な限り継続することにより、ステークホルダーへの影響を最小化し、企業価値の維持と向上を図るという目的の達成を脅かすあらゆる不確実性を評価する（＝BIA）
  - パニック状態下で意思決定するために、あらかじめ対応方針（人命の最優先尊重、利害関係者の優先づけなど）を明確化する
  - 利用可能な経営資源と時間の制約を考慮した対応プランを策定することが必要

ビジネス・インパクト分析：BIA
Business Impact Analysis

- 最悪の事態を想定
- ビジネスが止まった場合の潜在的損失を定量的に（金額ベースに換算して）分析

↓

- 組織のビジネス機能・プロセスの評価・見直し
- ビジネス継続計画作成のために必要な最小限の資源を特定
- 災害時の復旧の優先順位を明確化



BCMの実施フロー

- 脅威・脆弱性分析：RAVA
  - Risk Assessment／Vulnerability Analysis
  - 業務中断につながるリスクを網羅的に洗い出し
  - 特に考慮すべきリスクをリスクシナリオとして検討
  - リスクシナリオが発現した場合に各業務に与える影響度合いを評価
    - 自組織にとって最悪のシナリオを選択することが重要

- 影響度合の把握の仕方
  - 重要視される影響
    - 財務的な影響
    - 評判への影響
    - コンプライアンス（法令遵守）面での影響
  - 時間を考慮した分析
    - 例：発生後15分、1時間、4時間、7時間、24時間、1週間、2週間および1ヶ月

BIAの指標（判断基準）

- 目標復旧時間　RTO
  - Recovery Target Objective
  - 災害発生からシステム復旧までの時間
  - 事業中断によって生じる損失と中断をできるだけ短くするためのコスト等を勘案して決定
- 目標復旧時点　RPO
  - Recovery Point Objective
  - どの時点のデータまで復旧できるか

- RTOとRPOが被災時点に近づくほど、災害対策システムへの投資額は増大する

- 災害復旧までの時間が長期化し、データ復元ポイントが過去にさかのぼるほど、損害は増大する。

- 最適なRTO／RPOを設定するためには、
  - 「投資額＋運用費用」と、設定したRTO／RPOで被災する場合の「被災損害」のバランスの調整が必要

ビジネス継続計画：BCP
Business Continuity Planning

- BIAをベースに策定
- 災害や突発事件に遭遇しても、被災地以外の代替先で重要なビジネス機能やプロセスのみを継続するように事前に取り決めた手順書
  - 従来の形態や固定概念にとらわれず、自らが積極的に変化する戦略を取る必要
  - 必要な最小限の資源を準備
  - 代替先や協力関係先との契約を結ぶ
  - 定期的に社員の教育と訓練を実施
  - 毎年もしくは必要に応じてBIAと計画を更新

企業のリスクマネジメントの対象

- データ／ネットワーク管理
- 施設管理と緊急対応
- サーバ管理＆セキュリティ
- リスク管理と法務
- 健康／安全管理と環境
- イメージ管理と危機広報

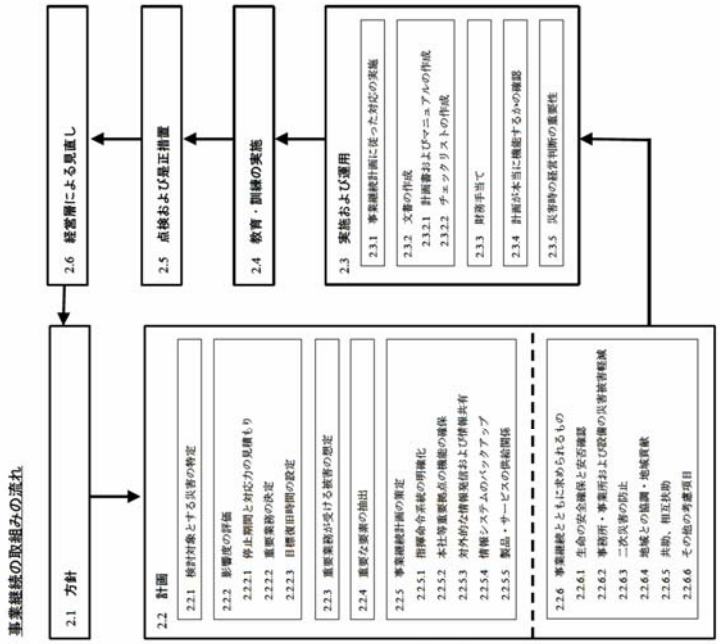
BCPの構成要素

- 基本方針
- 組織体制と役割
- 計画の発動基準
- 上位者/関係者への報告手順（エスカレーション・フロー）
- 緊急事態発生時の対応手順
- リスク評価結果の文書化

http://www.meti.go.jp/report/downloadfiles/g50331d06j.pdf

経産省：事業継続計画策定ガイドライン

- 2005年4月に正式リリース
- 「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」の一環
- 下記のガイドラインと統合的に規定
  - システム管理基準：287項目
  - 情報セキュリティ管理基準
  - ITIL（ITサービスマネジメントのベストプラクティス集）
  - COBIT（ITガバナンスの成熟度を測るフレームワーク）



Availability

- 可用性の確保
- ⇨ ビジネスの停止につながるようなリスクの発生を未然に防ぐ
  - システムやネットワークの二重化・冗長化
  - 施設や関連設備の二重化
  - 社内で管理運用しているサーバのクラウド化

Recoverability

- 復旧可能性の確保
  - 代替オフィスの確保
  - 非常呼集
  - 緊急連絡
  - 担当者の責務・序列
  - 緊急持ち出し
  - 重要記録の保全
  - パックアップなどの方法

BCMの運営

- 必要なリスク情報、コントロール状況等が適切なタイミングで、情報を必要とする人に共有されるために、BCP発動までの流れを示すエスカレーション・フローの策定が重要
- 「被災状況の情報」「緊急事態の判断」「社内調整」のキーマン（およびそのバックアップ）を明確化する
- 最も重要なことは、トップが正しい判断をするために的確な情報が適時に伝わる企業風土をつくりあげること

  ⇒ 従業員のリスクコミュニケーション能力を高める

効果検証・継続的改善

- 各部署における日常業務の中で、BCMが機能しているかを評価する
- 従業員から自発的・継続的な改善が行われる土壌が作られ、企業全体にリスク管理の重要性や「自己の責任において、問題が生じないように考え、行動する」考え方を浸透させる
- CSA：Control Self-Assessment（統制自己評価手法）
  - 1987年石油関連の企業 Gulf Canada の内部監査チームが開発
  - 業務をよく知る管理者と担当者を集めて、特定の問題や業務プロセスについて議論し自己評価

CSAの手法

	ファシリテーション	インタビュー	ディスカッション
メンバー構成	1名あるいは補佐を含めた2名のファシリテータと、複数の参加者	監査人（インタビュアー）と被験者1名あるいは数名	司会と複数の参加者
方法	ファシリテータが、目標とする成果物を作成するために、参加者から意見、経験、認識を導き出す	監査人が事前に提示した依頼書に基づいて、被験者に問いつつ、被験者に1問ずつ確証的に問いただす	あるテーマに対して、比較的自由に話し合う
成果物	ファシリテータが事前に定める成果物（リスクマップ等）を参加者に提示しておく	監査人が作成する ・ヒヤリングメモ ・フロー図	特定の成果物を求めない

BCMとSCM

- SCM
  - 「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
  - サプライチェーンを構成する企業に事故や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
  - 自企業だけでBCP を構築するのではなく、サプライチェーン全体でBCP を構築する必要

資　料

ISOで開発中の規格（2011年5月9日時点）

- ISO 22320　社会セキュリティー緊急事態管理ー指揮調整
  - 効果的な危機対応を実現するための必要最小限の要求事項を規定し、危機対応にかかわる単一の組織における指揮・調整、情報、連携、協力のあり方の基本的な事項を提供
- ISO 22322　社会セキュリティー緊急事態管理ー警報システム
  - 危機事案発生時およびその前後に発する警報の準備および発令の一般原則、並びに警報の開発、管理、実施をするための指針

- ISO 22324 社会セキュリティー緊急事態管理ー色コードによる警報
  - 安全／危険の度合いを表す色コードを規定
    - 色コードは、状況の厳しさに関して、初期対応者および／またはリスクに直面した一般の人々の注意を喚起し、これらの人々がより多くの情報を求めるよう促したり、事前に通知され指示された適切な安全処置を講じさせるよう促すために使用
- ISO/TS 22351 社会セキュリティー災害及び緊急事態管理ー状況認識の共有
  - 災害対応に関わる組織間で、緊急時の情報伝達および指示命令を効果的に行うため、コンピュータで用いられる各種システム間のメッセージ構造を標準化し、確実に情報を解読できる方法で転送することを規定（国際規格でなく技術仕様書）

- ISO 22397 社会セキュリティー官民連携ー協定の構築の指針
  - 危機事案の発生時およびその事前・事後において、危機対応に取り組むために協調・協力が必須とされる公共組織と民間組織の組織間において、連携協定を策定するための指針
- ISO 22398 社会セキュリティー演習と試験の指針
  - 組織の人員の力量を確実にする責任をもつ者、特に組織のリーダーシップ並びに演習・試験プログラムの管理に責任をもつ者に対し、演習・試験の計画策定、実施、管理、査定、報告、改善を行うために必要な手順を規定

事例：NEC

- 事業運営の効率的なオペレーションと連結管理を支える情報システム化を推進
  - NECおよび関係会社を密に連携した一貫システム化
  - IT戦略部／システム運用統括部は、会社の業務主管部門と協力し、全社業務システム、ITインフラを提供するとともに、ビジネスユニットを支援
- 2004年3月：社内システムに関する対策プロジェクトを発足

- 背景
  - 取引先との相互依存の拡大
  - 業務のIT依存度の増大
  - 分散化
  - システム間リアルタイム連携など密結合化
  - 東海地震への対応が切迫化
  - 2003年夏に起こった電力危機
  - 火災等による連鎖的に起こる事業継続性の障害
  - 顧客情報や設計情報の流出リスクの顕在化

- 2004年4月：ビジネスユニット制を採用、スタッフの中にプロセス改革推進本部を設置
  - IT戦略部
  - システム運用統括部
  - 開発プロセス推進部
  - 生産プロセス推進部
  - 業務プロセス推進部
- IT戦略部：IT面からの経営課題解決を役割とし、NECグループのITの統括および情報セキュリティ、関係会社・海外のIT推進を担当

- 社内体制
  - 関連会社を含め、国内イントラネットに接続されているコンピュータは
    - WindowsPC約16万台
    - UNIX、Linux、ACOSなど計8千台
  - 基幹系
    - 全社的に運用するコーポレートガバナンスシステムとしての経理、連結決算システム
  - 業務系
    - 営業、資材、間接資材、人事、特許などのシステム
- これらのシステムがダウンすると、ビジネスは成り立たない

- 大規模災害対策初動対応マニュアル
  - 想定災害：南関東地域を中心とする震度5以上の地震、台風などの自然現象による災害、事故など人為的原因による災害など
  - 公共機関やライフラインに相当規模の被害が生じ、事業運営に大きな影響が生じた場合に適用
  - 社長を本部長とする「災害対策本部」が設置され、その下に11のチームを設置
  - 情報通信チーム
    - 即時対応としての連絡網、緊急連絡手段の確保
    - 初動についての状況掌握から統制体制の確立
    - 復旧指示までの指示系統の規定

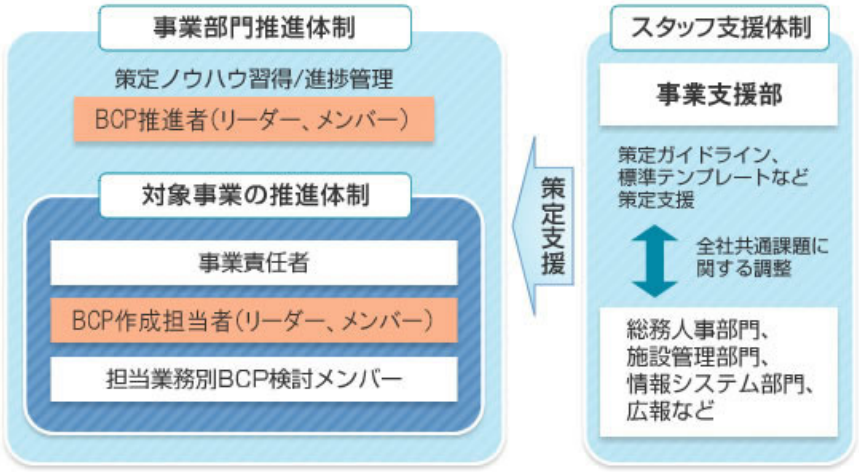
- 大規模災害対策は、初動の状況確認など、即時対応の範囲内
- その後のDR（災害復旧）は、ビジネスと連動することなくシステムサイドが独立に計画
  - 中期活動計画のひとつとして、BCとの連携という観点で『ディザスタ・リカバリ』として見直し
    - BCP（事業継続計画）の策定
    - 現行の初動マニュアルの早期刷新と、現行システムの脆弱性への対応
    - 教育・訓練の定期的実施

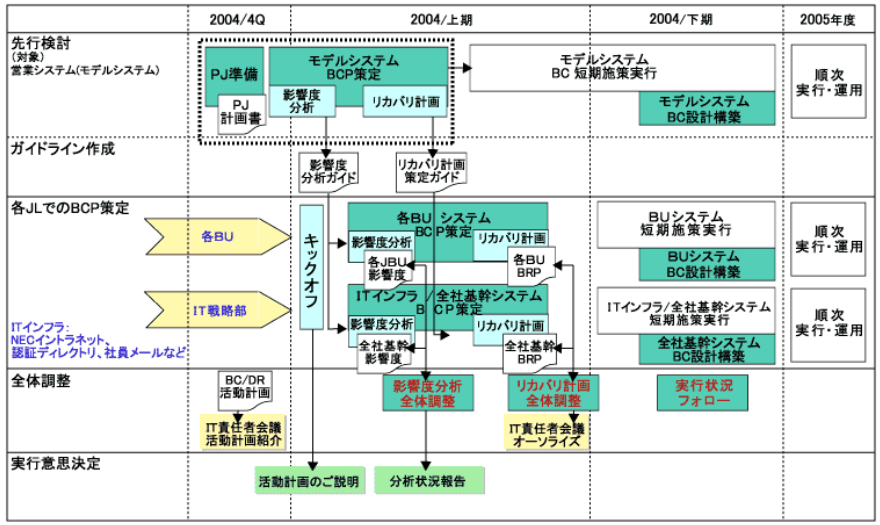
○ 活動の基本方針

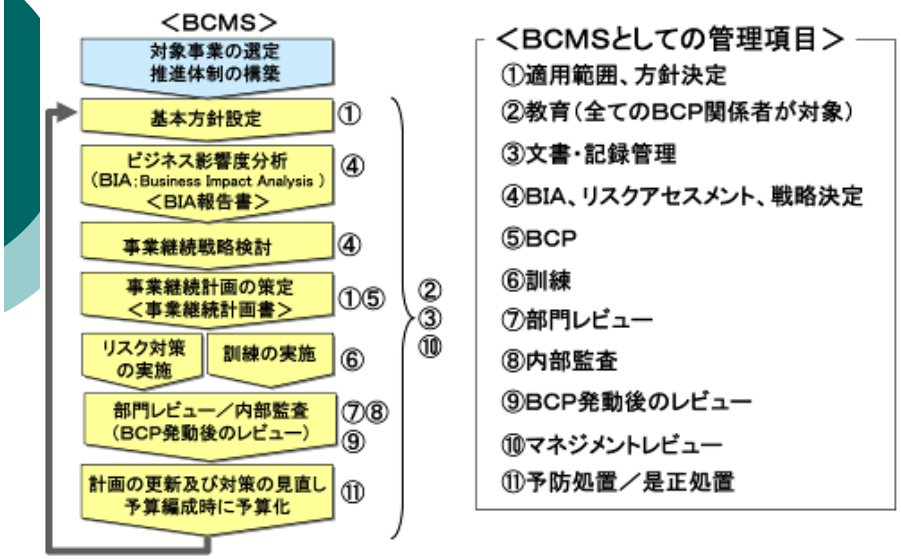
- ビジネス側を巻き込み、災害のビジネス継続への影響とシステムサイドとの整合性を図る
- システムインフラとビジネスユニットのBCPとの相互依存関連を明らかにして、インフラ側の対応を促進する
- マニュアル処理、保険を含めた総合的リスク対策を明確にする
- コスト削減施策の中から資源を捻出し、対策の費用にあてる。

○ NECグループのBCPの基本方針

- 従業員など（構内作業者、来訪者含む）の生命・安全の確保
- NECとして求められる社会的責務の遂行
  - 通信、公共インフラ、交通、防衛、金融など基幹システムの維持・復興
- 事業停止から生じる経営ダメージのミニマム化







- BIA（Business Impact Analysis：事業影響度分析）策定活動
  - 目的：CIOおよび経営層が、リカバリ計画開発の方向性の判断をするための情報を提供
  - 活動プロセス
    - プロジェクト準備
    - 重要業務領域の確定
    - 事業インパクト評価
      復旧レベル設定（最小IT資源の特定と復旧レベル設定）
    - 復旧手順と課題
    - 報告

- BIA策定活動で分かったこと
  - 事業継続性の視点で 、現状のシステム復旧計画では不十分であること
  - 重要IT資源に対する脆弱性と残余リスクの認識が不十分であること
  - リスクへのインパクトを最小にするための予防手段など、リスク管理が継続的に組み込まれていないこと
  - 事業がIT依存度を高めていること
  - 一部の重要IT資源が一ヵ所に集中していること
  - 連携する重要IT資源の安全レベルが合っていないこと。

- ITの復旧計画：ITRP（IT Recovery Plan）
  - BRP（Business Recovery Plan）策定活動の一環
  - プロジェクト準備
  - リスクパターン(災害シナリオ)の定義
  - 緊急事態管理（連絡網や体制）
  - 復旧方針策定・ITRP策定
  - 投資概算策定

○ BRP策定活動で分かったこと

- ビジネスからの復旧目標と想定システム災害からの復旧レベルとにギャップがかなりあること
- ギャップ改善には、各ビジネスユニットの意思決定で進められる施策と、全社的な意思決定が必要とされる施策があること
- 全社インフラに対して短時間の復旧が求められている
- 全社インフラの下位層から上位の業務アプリケーション層への対応と、復旧計画を整合していく必要があること
- 全社の重要インフラの一部にシングルポイントがある
- コンピュータセンターの設置場所がビジネス拠点と地域的に隣接し、共倒れになる恐れのあること

日立の取り組み

○ 07年度からグループ全体でBCP策定を開始

- 様々な業態の事業会社があり、それぞれの会社が抱える課題は異なる。
  - グループ全体で1000社以上
  - 合計38万5000人もの従業員
- 日立本体でBCPを策定して押しつけるのではなく、日立グループとしてBCPガイドラインを作った（07年2月）
- まずは規模の大きな145社（20万人）を対象

- 試算では、ガイドラインがある場合とない場合でBCPの策定コストにおよそ1200万円の差があった
  - 通常は1カ所当たり2500万円かかるが、ガイドラインを使うと1300万円ぐらいに収まる
- 取引先に対しても、取引の量や重要度に応じてBCPの策定と実行を依頼

○ 重要業務を早期に再開するのが目的

- 災害時には、トップに情報が的確かつ速やかに上がっていくシンプルな組織が必要

  ⇒ 権限の委譲や相互の支援体制が必要不可欠
- 代替となる通信手段や支援スタッフの確保

BCMに関係するICT技術

フェーズ	分　類	技術・ツールの例
防災・減災	セキュリティ	認証、アクセス管理
	高可用性	冗長構成、OMCS*、クラウド
	予知・予防	地震予知、アクセス兆候監視
危機的状況発生時	監視・情報収集	遠隔監視用通信、センサ技術
	システム復旧	復旧支援ガイド作成支援
	バックアップ	遠隔バックアップシステム
	業務復旧支援	緊急時指揮支援システム
	安否確認	安否確認システム
	安全確保支援	情報提供伝言板システム
BC運営	業務分析	業務プロセス可視化ツール
	BCP策定	災害シナリオ作成支援ツール
	教育・訓練	BC検定教育システム
	評価・監査	BCP実施状況評価ツール

＊OMCS：Open Mission Critical System