事業継続マネジメントにおける情報通信システムについて

The Point of the Telecommunications System Design Which Should be Taken into Consideration for Business Continuity Management

古本（ふるもと）　勉（つとむ）*

キーワード：事業継続マネジメント，情報通信システム，RTO（目標復旧時間），SLA（サービス品質保証制度），CIRM

1．はじめに

企業を取り巻くリスク環境は，東京湾北部・東南海・南海・東海地震などの大規模地震や水害といった自然災害，火災・事故・テロなどの人的災害，急激な感染拡大が懸念される鳥インフルエンザなど，その種類及び発生時に企業に与えるインパクトとともに拡大の一途をたどっている。これらは，いつ起きるか分からない事象ではなく，必ず起きる事象として認識すべきである。

本稿では，事業継続計画及び事業継続マネジメントに欠かせない重要リソースである「人」，「ファシリティ」，「情報通信システム」のうち，情報通信システムにフォーカスして，現状や必要機能について述べる。

2．BCP策定手法

関連省庁から発表されているBCP策定のためのガイドラインは，下記の三つに代表される。

①経済産業省情報セキュリティ政策室「事業継続計画策定ガイドライン」(2005年3月)

②内閣府中央防災会議企業評価・業務継続ワーキンググループ「事業継続ガイドライン」(2005年8月)

③中小企業庁経営安定対策室「中小企業BCP策定運用指針」(2006年2月)

弊社では，事業継続マネジメント(BCM)は，プロジェクトの立ち上げから，ビジネス影響度分析/リスク分析による必要な対策戦略の抽出と，戦略決定を前提とした計画書作成・対策実施・教育訓練・評価改善の実施運用の各フェーズをPDCAサイクルにより実施するプロセスとに大別し，「FBCMM (Fujitsu Business Continuity Management Model)」として標準化している。これは，BCP策定に当たって網羅することが必要要件となる，米国DRII (Disaster Recovery Institute International) と英国BCI (The Business Continuity Institute) で合意されている10要素を含んでいる(図-1)。

3．情報通信システム部門とBCM

不測の事態発生時にも事業を中断させない取組みは，コンピュータの2000年問題の際に様々なシナリオに応じた対策が執られ，模擬テストが実施されたことが大きなトリガーとなっている。各企業は，アウトソーシングや分業化を進め，最も効率的で無駄（むだ）のないサプライチェーンを目指しており，それが災害時の脆弱（ぜいじゃく）性の高まり及び影響範囲の拡大を招く結果となっている。

近年，情報通信システムは，個々の業務を補助的にサポートするツールではなく，企業経営を支える重要な要素となっていることは自明の理である。情報通信システム部門における事業継続計画策定は，各業務部門に提供するITサービスの継続性を保証する位置付けとなり，業務BCPにより明確化された事業継続業務要件(RTO：Recovery Time Objective)は，情報通信システムに対するサービス品質保証制度(SLA：Service Level Agreement)の位置付けとなる(図-2)。

2006年6月に設立されたNPO法人事業継続推進機構(BCAO)においても，情報通信システムの重要性の認識から，BC基本事項委員会の配下に情報システム分科会が設けられ，共通認識の形成，ガイドラインの制定などの議論が活発に行われている。また，情報セキュリティガバナン

＊富士通㈱コンサルティング事業本部プロセス改革事業推進室
1959年6月生まれ，大阪府出身。1984年富士通㈱入社。コンサルティング事業本部プロセス改革事業推進室プロジェクト部長。認定ファシリティマネジャー(CFMJ)。米国PMI認定PMP (Project Management Professional)。プロジェクトマネジメント学会正会員。

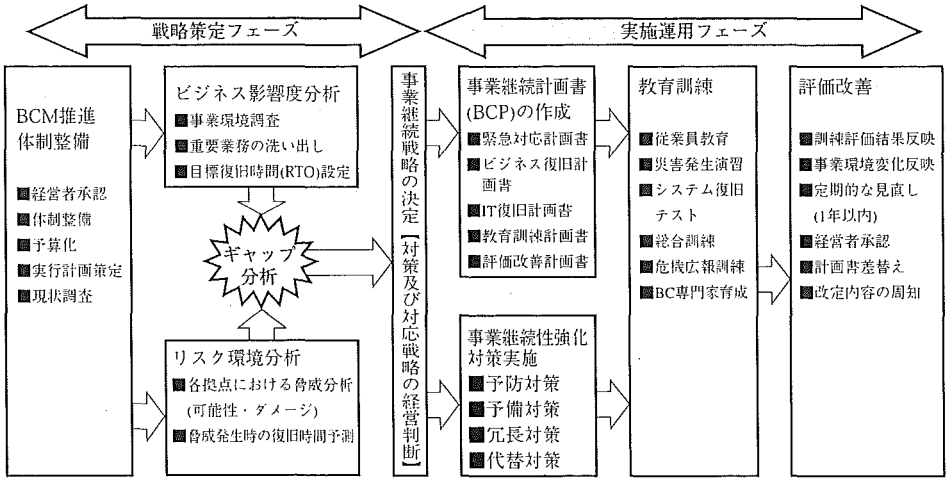


図-1　FBCMM

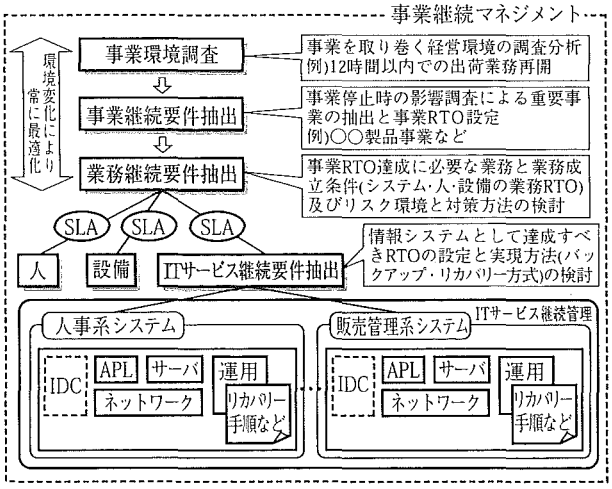


図-2　BC と IT サービス管理の構造

スの面では，2005 年 3 月に経済産業省商務情報政策局情報セキュリティ政策室が公表した「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」報告書で，「事業継続計画策定ガイドライン」以外に，情報セキュリティガバナンスの推進を支援する「情報セキュリティ対策ベンチマーク」及び「情報セキュリティ報告書モデル」を提供している。これらのツールを活用することで，企業は自身の情報セキュリティ対策の有効性と効率性を分かりやすく伝えることができる。企業は情報セキュリティガバナンスを確立する上で，マネジメントシステムを構築し，ステークホルダーに対して，これらの取組みを継続的に説明することが必要となっており，これも BCM の浸透の一因である。

情報通信システム部門における事業継続計画の取組みに当たっては，情報通信システムの運用管理の観点から，下記のような四つの課題があり，業務 BCP をふまえた対策計画の立案のためには，まずこれらの課題解決が最初のステップとなる。

①課題 1「構成管理ができてない」：情報通信システム関連のインフラ（建物・設備・ネットワーク・ハードウエア・アプリケーション・運用人員）と業務との関係性が整理できておらず，情報通信システムインフラに何らかの被害が生じた場合，どの業務範囲が影響を受けるのかが明確になっていない。

②課題 2「リスク分析がされていない」：情報通信システムがさらされているリスク環境，例えば，拠点ごとの地震・水害の発生確率，自社センターの地震による被害想定，被災時の周辺アクセス，要員の居住地分布から見て参集計画，委託先ベンダの事業継続能力の把握，データのバックアップ実施状況，データの保管場所の明確化などが明確になっていない。

③課題 3「現状復旧能力（RTC：Recovery Time Capability）が分からない」：災害時の情報通信システム復旧にかかる時間，具体的には，情報システム復旧にかかる時間，システム起動時間，データ復旧にかかる時間，システム復旧時点でのデータの同期確認などが明確になっていない。

④課題 4「投資対効果が明確になっていない」：目標復旧時間内に復旧させるための費用は幾らかといった，対策にかかる投資と対策効果が明確になっていない。

これらの課題をふまえ，情報通信システムの事業継続能力向上のためには，目標とすべき復旧時間（RTO）と，様々なリスクが発生した場合の実際の停止予想時間（RTC）のギャップを分析した上で，ギャップ解消の対策を実施することが必要となる。

情報通信システム部門向けの BCP 策定手法は，先に述べた「FBCMM（Fujitsu Business Continuity Management Model）」に準じた手順で，現状分析フェーズと対策実施・運用フェーズから構成される（図-3）。

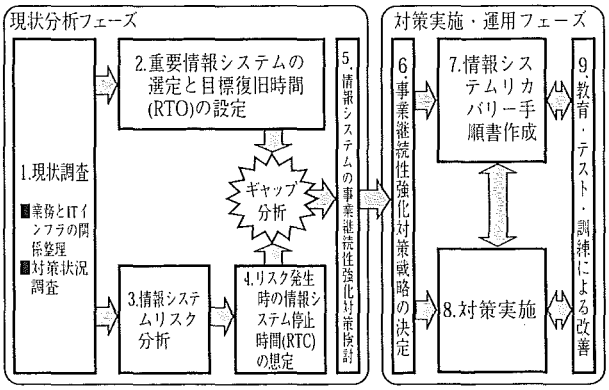


図-3　情報通信システム部門向け BCP 策定フロー

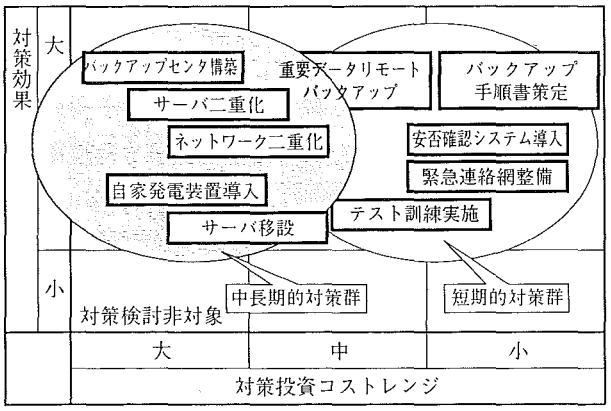


図-4　対策検討の考え方(例)

①現状調査：重要システムの情報通信インフラの利用状況を調査し，重要なシステムの提供に必要な情報通信インフラ(ソフトウエア，ハードウエア，ネットワーク，設備，建物など)の範囲を明確化する。これにより，災害発生時に情報通信インフラがダメージを受けた場合の重要システムの影響範囲及び対策対象範囲を特定することが可能となる。

②重要な情報通信システムの選定と目標復旧時間(RTO)の設定：情報通信システムの復旧順位の検討，その重要度に応じて，重要な情報通信システムの目標復旧時間(RTO)を，停止時間ごとの影響度分析により設定する。

③情報通信システムのリスク分析：拠点ごとに発生する可能性のあるリスクシナリオ(被害の状況)を抽出し，各拠点において検討対象とすべきシナリオを抽出する。

④リスク発生時の情報通信システム停止時間(RTC)の想定：不測の事態による情報通信システム停止時の復旧に要する時間を想定するためには，情報通信システムの復旧プロセスを明らかにする必要がある。リスクシナリオが発生した場合の情報通信システム復旧にかかる時間(RTC)は，建物や電力などの情報通信システム復旧の前提となるインフラ復旧時間と，システムそのものの復旧時間の合計となる。この時間は，現在の対策状況により異なる。

⑤情報通信システムの事業継続性強化対策検討：情報通信システムの事業継続性強化対策を抽出し，投資対効果の観点から整理する。

⑥事業継続性強化対策戦略の決定：投資対効果のマトリクスから，必要な対策及び実施時期を選択する(図-4)。

⑦情報システムリカバリー手順書作成：災害検知から初動・緊急対応・システム回復・システム正常復旧までの全体プロセスを設計し，必要なリカバリー手順書を作成する。

⑧対策実施：投資対効果のマトリクスから選択された対策を実施予定時期に実施する。

⑨教育・テスト・訓練による改善：BCP の必要性や取組み方法に関する気付きの醸成，策定した BCP の内容に関する周知徹底，策定した BCP の有効性や実施した対策の機能確認及び策定した BCP の改善点や変更点の抽出を行う。

4.　災害時に要求される想定機能

KPMG ビジネスアシュアランスが 2005 年に米国 791 社に行ったアンケートでは，事業継続への脅威として，ハードウエア，ネットワーク，ソフトウエア障害が，それぞれ 47.29 %，38.47 %，38.34 %と高い数値を示している。(http：//www.kpmg.or.jp/resources/research/r_ba200601_1.html)。

災害時に情報通信システムに対して要求される機能としては，可用性や冗長性がある。

(1)　可用性(Availability)

システムの壊れ難さを指し，障害の発生し難さ，障害発生時の修復速度などによって計られる。重要なシステムを 24 時間 365 日安定稼働を実現するために様々なデータバックアップ方式も検討されている(図-5)。

(2)　冗長性(Redundancy)

事業継続の観点から，情報通信システムに不測の事態が発生した際に平時の業務処理を継続するためには，情報通信システムの冗長性が重要となる。例えば，サーバやストレージの想定リスクを回避するための分散設置，ネットワーク環境の脆弱性チェックなどを検討する必要がある。また，災害時に有効なサービスには，以下のようなものがある。ただし，事業継続の観点での最適化は途上である。

①安否確認サービス：携帯電話の e-mail が災害時の輻輳や通信制限の影響を受け難いことを利用したサービスが多数提供されている。

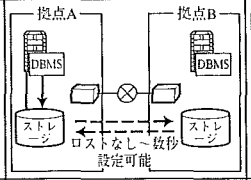
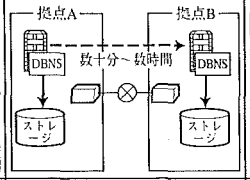
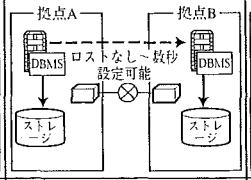
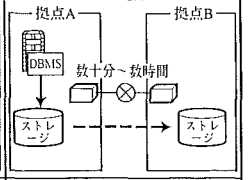
パターン	A ストレージミラー	B ソフトミラー	C DBMSミラー	D リモートバックアップ(ストレージ)
構成図				
特徴	ストレージ間でデータ同期処理を行う方式。非同期でも数秒以内で同期することが可能。 復旧の際は，DBMSの起動が必要。	サーバ上にミラーリングソフトを導入してミラーリングする方式。導入するソフトにより同期性が異なる。 復旧の際は，DBMSの起動が必要。	DBMS独自のプロトコルでログを送信してサーバ間データ同期を行う。 DBMSが提供する方式によりデータ保証範囲が異なる。 復旧の際は，プライマリDBサーバとしての再起動が必要。	ネットワークバックアップ製品を導入して，データ転送を行う方式。Snapshotにて一定期間の更新を反映する方式のため，データの同期は取れない。 復旧の際は，サーバ構築やデータのリストア作業が必要。
メリット	データリストア時間がほとんどない。 サーバへの影響が少ない。	データリストア時間がほとんどない。 ストレージミラーに比べ安価である。	データリストア時間がほとんどない。 比較的狭いネットワーク帯域領域での構築が可能。	ハイエンドなストレージでなくてもストレージ間のバックアップが可能である。
デメリット	広いネットワーク帯域領域(専用線)が必要。 ハイエンドなストレージが必要。	データロストの可能性が高い。 サーバへの負荷が大きい。 TCP層を活用しているため，転送能力がA，Cに比べ遅い。	未更新ログを手動で適用する必要がある。	データのリストアが必要。 ある一定の間隔でDBへの更新を行うため，間隔が長くなるとロストするデータが多くなる。

図-5　データバックアップ方式例

②重要データバックアップ：NAS(Network Attached Storage：ファイルシステムによりアクセスされるストレージの総称)やSAN(Storage Area Network：サーバとストレージ間を接続する専用のネットワーク)といった基本的なストレージサービスに加え，電子メールの管理サービス，リアルタイムでの遠隔地データ保管サービスといった様々な形態のサービスが提供されている。

③共同バックアップ：災害時のバックアップ体制として，一社単独でバックアップ施設を保有することは投資もかさむため，共同バックアップ施設を利用する。バックアップ施設の稼働に必要な設備(センター，ハードウエア，基本ソフトウエア，回線など)をバックアップ施設に用意し，データベースを持ち込むことでバックアップシステムを構築するホットサイト方式などがある。

④ASP (Application Service Provider)：インターネットを通じて利用者にビジネス用アプリケーションをレンタルするサービス。サービス提供者がアプリケーションをデータセンターで稼働させておき，利用者はインターネットでデータセンターに接続することで，アプリケーションの利用が可能になる。利用するアプリケーションの購入や導入作業，日常運用にかかる手間やコストを抑えることができるだけでなく，不測の事態発生時，自社内にサーバなどの設備を抱えて壊滅的なインパクトを受けたり，ダメージ回避のための対策を多額の投資に伴って講じるよりも効果があり，安全で速やかに重要業務を再開するために有効なサービスと考えられる。

5．外部インフラとの連携

不測の事態発生時にも外部との連携を維持するべくネットワークの信頼性や品質を高めるに当たり，事業継続の観点から講ずるべき対策を以下に述べる。

(1)　ネットワークの可溶性・安全性

通信回線の冗長化やバックアップといった通信手段の高信頼化を行うことで，災害発生時に平時の通信手段が使えなくなった場合，別の通信手段で情報へのアクセスを継続可能とする。ここでは，マルチキャリア接続，機器や通信経路の二重化といった冗長化対策をとる必要がある。また，インターネットのように不特定多数の利用者が存在するネットワークの安全性を維持する技術として，仮想専用線(VPN：Virtual Private Network)がある。VPNは，二つの通信ノード間で仮想的に専用線と同等なセキュリティレベルを確保する。

(2)　機密性の確保

不測の事態発生時において，代替の通信手段を採用した際にも，情報コンテンツの機密性は確保されなければならない。そのためには，情報の暗号化技術が必要で，各種暗号処理，例えば認証や通信暗号化に使用する鍵(かぎ)情報の安全な保管機能をハードウエアで高速処理するものもある。

6．機能達成のためのハードウエア仕様

これまで述べてきたように，経営と情報通信システムが一体化したビジネス環境では，情報通信システム基盤の不具合がビジネスに甚大なインパクトを与える可能性がある。㈱電子情報技術産業協会が行った「中堅・中小企業におけるBCP策定状況調査」(2006年度)においても，システムの二重化/冗長化，電源/UPS強化，アタック/ウイルス攻撃対策強化，バックアップ及びメディアの遠隔地保管といった取組みが報告されている。

事業継続に必要な情報通信システムの仕様としては，高信頼であることはいうまでもなく，更に変化に強く柔軟な

情報通信システム基盤であることや，運用面での拡張性・保守性・耐災害性をもつことが求められる。情報通信基盤の構築ポイントを以下に述べる。

（1） アーキテクチャ

改変のサイクルが異なる業務層と情報通信基盤層とをそれぞれ柔軟に拡張できるよう独立させる。

（2） テンプレート

情報通信基盤のライフサイクルを支えるため，運用・保守を容易にするコンポーネントの実装，セキュリティ考慮，トラブル発生リスク低減などの仕組みをテンプレートに組み込む。

（3） フレームワーク

グローバルスタンダードであるITIL(IT Infrastructure Library)を用いてインフラサービスをマネジメントする。

7. BCM定着化に向けたツール活用

事業継続マネジメント(BCM)は，戦略策定フェーズ(プロジェクトの立ち上げから，ビジネス影響度分析/リスク分析による必要な対策戦略の抽出)と，実施運用フェーズ(戦略策定を前提とした計画書作成・対策実施・教育訓練・評価改善)の各フェーズをPDCAサイクルにより実施するプロセスであることは先に述べた。このBCP策定作業及び更新作業の標準化，効率化を支援するツールが必要との認識から国内でもBCP策定の計画段階から，更新の運用段階までの標準的なプロセスをカバーするソフトウエアツールが開発されている。ここには，戦略策定フェーズの中で使用する様々なシミュレーション作業を支援するツールや，各種のドキュメントテンプレート群はもちろん，実施運用フェーズでも有用なBCPの変更管理機能も盛り込まれている。

8. 今後の課題

事業継続計画及び事業継続マネジメントに欠かせない重要リソースのうち，「情報通信システム」にフォーカスして，現状や必要機能について述べた。日本におけるBCP・BCMは，まだ緒に就いたばかりであるといえ，取り組むべきテーマも多い。

①成熟度の測定技術整備：情報通信システム関連の整備状況や完成度などを可視化する手段として，様々な診断ツールが存在している。全体，業種，地域，企業規模などでカテゴライズし，その中で自社/自組織がどの辺りに位置するのか，ベストプラクティスと比べてどの評価軸が劣るのかといったことを診るだけでなく，自社の事業継続に対する経年変化を知る上でも重要である。

②レジリエンス強化の手法確立：レジリエンスとは，事業継続を議論する上でしばしば用いられ，“復元力”や“回復力”といった意味をもつ。重要業務の継続に必要な情報通信システムインフラ(ソフト，ハード，ネットワーク，設備，建物など)の範囲を明確化し，それらが機能し続けるためのグリッドコンピューティングやストレージ仮想化といった先進技術の実用化に向けた手法の確立が必要である。

③組織/制度/ツールのバランシング：BCMが“不測の事態が起きることを前提とした経営管理手法”であることから，本稿で述べた「情報通信システム」についてのみマネジメントするだけでは不十分である。経営に必要な人や組織(ヒューマンリソースマネジメント)，建物や設備(ファシリティマネジメント)がバランスされて進化し続けることが肝要である。

9. おわりに

BCPを策定すること，BCMを企業活動に定着化させることは，もし不測の事態が発生しないとしたら無駄な活動なのか。

情報通信システムだけでなく，人・ファシリティ・財務などの現状を可視化し，企業がもつリソースデータベース(CIRM：Corporate Infrastructure Resource Management)の整備を推進することは，企業が保有するリソースを最高のパフォーマンスが発揮できるように最適配置すること及び企業経営そのものが目指すことであり，その特殊ケースをBCP策定時に検討しているにすぎない。BCP策定時に行った，事業環境を整理して重要事業を可視化，ビジネスやサプライチェーンのプロセスを可視化，情報通信システム/人/ファシリティなどのリソースを可視化，プロセスとリソースの関係性の可視化を行うことは，経営戦略策定時に経営判断できる材料を揃(そろ)え，経営品質向上に寄与することと確信し，日本企業全体が強靭(きょうじん)になることを期待したい。

参考文献

1) 経済産業省商務情報政策局情報セキュリティ政策室：「事業継続計画(BCP)策定ガイドライン」，経済産業調査会，2005年8月
2) 原田：「情報セキュリティで企業は守れるのか」，NTT出版，2005年3月
3) 伊藤：「富士通におけるBCP(事業継続計画)策定」，雑誌FUJITSU，Vol.57，No.5，2006年9月
4) 山際：「安心・安全を支えるIT基盤」，雑誌FUJITSU，Vol.57，No.5，2006年9月