

セキュリティ技術国際動向調査研究報告書

平成18年3月



財団法人 日本情報処理開発協会

KEIRIN

00

この事業は、競輪の補助金を受けて実施したものです。

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17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す。

国家戦略である「e-Japan 戦略」が2001年から始まり、その端緒となるネットワークインフラの基盤整備により、我が国の「ブロード・バンドは世界で最も低廉・高速」となるに至った。企業内はもとより企業間でも、電子商取引などブロード・バンドを利用したビジネスが盛んに行われている。

ITの利便性追求の中で、確かにシステムは進化し、社会経済活動は激変した。身近なところでは、インターネット検索や電子メールなど多くの人がITの利便性を享受している。ITは、電気、水道、ガスなどと同様にライフラインの一つとして位置付けられるようになったといえるだろう。そのような環境変化の下で、企業が有する電子データは幾何級数的に増加し続けており、その保管に必要な容量は増大の一途を辿っている。

しかし、現状は、災害などITを脅かす脅威に対応できる磐石な基盤が作られているとはいいがたい。情報システムやネットワークなどが停止することにより、これらが支える社会経済活動は、機能麻痺をおこすところまで来ている。

地震によるサーバー等の損壊、台風や津波などの風水害による記録媒体の冠水、テロや人的ミスによるシステムダウンなど情報資産に影響を及ぼす災害は、いつどこで発生するか予測できない。災害に加えてディスク・トラブルなど日常発生している障害を含めると、情報資産やそれが支える社会経済活動は常にリスクと隣り合わせといえる。特に、情報資産の消失は取り返しがつかない。例えば、社運を賭けた新製品に関する技術資料などの消失は、企業活動にとって大きな影響を及ぼす可能性がある。サーバーやソフトウェアなどは災害に備えて予め用意するか、再度購入することで復旧が可能である。しかし、失われた情報資産を購入することはできない。

事業を継続するためには、重要な情報資産が災害などの事故により喪失したり、破損したりすることを防ぐための手立てが必須なのである。情報量が爆発的に増大した今、どの情報をバックアップするか、優先順位を決めて対策を考えることが喫緊の課題である。しかしながら、いまや企業資産の一つといっても過言ではない情報資産の保護には多くの課題が残されている。

本調査研究では、事業継続のための情報資産管理のあり方に焦点を当て、マネジメントと技術の両方から、近年活発になりつつある国内外の取組みをまとめた。

第1章では、事業継続と情報資産管理、および情報セキュリティの関係について概念整理を行った。

第2章では、事業継続に関する最近の国内外の動向をまとめた。

第3章では、事業継続に関する欧米を中心とした企業の取組みの実際をヒアリングした結果を中心にまとめた。

第4章では、事業継続に必要なスキルと人材について、海外の団体などの動きから考察した。

第5章では、事業継続に関する規格やガイドラインなどをもとに、重要な情報資産保護についてまとめた。

第6章では、事業継続における情報資産保護を支援する最新の技術動向をまとめた。

最後に、第7章で、全体についてまとめ、課題や見解などを述べた。

なお、本調査研究については、株式会社富士ゼロックスに委託した結果を当協会が取り纏めたことを申し添える。

本調査研究が、事業継続に関する取組みの一助となれば幸いである。

平成18年3月

財団法人 日本情報処理開発協会

目次

はじめに

1 事業継続と情報資産管理	1
1.1 事業継続と情報資産管理	1
1.2 情報セキュリティとの関係	2
2 事業継続関連の国内外の動向	4
2.1 米国の現況	5
2.1.1 事業継続の導入状況	5
2.1.2 標準化の動向	6
2.1.3 現地の状況	7
2.2 英国の現況	10
2.2.1 事業継続計画の導入状況	10
2.2.2 標準化の動向	10
2.2.3 現地の状況	13
2.3 日本の現況	13
2.3.1 事業継続計画の導入状況	13
2.3.2 標準化の動向	14
2.4 その他の国の動向	16
2.4.1 シンガポール (TR19)	16
2.4.2 シンガポール (SS507)	17
2.4.3 オーストラリア・ニュージーランド	17
2.5 ISO化動向	18
2.5.1 ISO化の概要とスケジュール	18
2.5.2 日本の対応	19
3 事業継続に関するケーススタディ	20
3.1 金融機関	20
3.1.1 先進金融機関の動向	20

3.1.2 業界としての取組み (欧米・日本・国際)	21
3.2 製造業.....	25
4 事業継続に必要なスキルと人材	28
4.1 人材・プロフェッショナル育成の重要性.....	28
4.2 英国 BCI の資格概要	28
4.3 米国 DRII の資格概要.....	29
4.4 事業継続管理に必要なスキル・セット分野	30
4.5 事業継続に係る職種.....	32
4.6 事業継続に必要なスキルと人材	32
4.6.1 事業継続管理体制構築におけるプロフェッショナル人材育成.....	32
4.6.2 今後の事業継続の課題における人材育成	34
5 重要な情報資産の保護.....	36
5.1 バイタル・レコードの概念.....	36
5.1.1 バイタル・レコードの定義.....	36
5.1.2 記録、文書、および情報、データ	37
5.2 事業継続関連規格等におけるバイタル・レコード	41
5.2.1 NFPA1600.....	41
5.2.2 PAS56 および BCI ガイドライン.....	42
5.2.3 TR19 (シンガポール)	42
5.2.4 米連邦危機管理庁におけるバイタル・レコード.....	43
5.2.5 米国土安全保障省の「重要な記録」	46
5.2.6 経済産業省の事業継続計画策定ガイドライン.....	47
5.2.7 内閣府の事業継続ガイドライン.....	48
5.3 ARMA のバイタル・レコード・マネジメント	48
5.3.1 ANSI/ARMA 5-2003 の全体構成.....	48
5.3.2 リスクアセスメント	49
5.3.3 バイタル・レコードの特定と優先順位付け.....	50
6 事業継続を支援する技術	52
6.1 ストレージ・セントリック	53

6.1.1	ストレージ・セントリックとは.....	54
6.1.2	SAN.....	54
6.1.3	NAS.....	59
6.1.4	NASとSANの相違点.....	61
6.2	事業継続に関連するネットワークの動向.....	62
6.2.1	広域イーサネット.....	62
6.2.2	IP-VPN.....	63
6.2.3	専用線.....	64
6.3	事業継続のためのバックアップとリストア.....	64
6.3.1	バックアップサイト.....	65
6.4.2	バックアップ技術動向.....	69
6.4.3	バックアップ関連の特記事項.....	73
6.4	情報ライフサイクル管理 (ILM).....	75
6.4.1	ILM誕生の背景.....	75
6.4.2	ILMとは.....	75
7	まとめ.....	78
7.1	事業継続に関する全体動向.....	78
7.1.1	事業継続の規格やガイドラインについて.....	78
7.1.2	欧米における取組みの現状から.....	79
7.1.3	事業継続の専門家について.....	80
7.2	事業継続と情報資産保護.....	80
7.2.1	情報管理の変化と事業継続.....	81
7.2.2	コンティンジェンシープランとの関係.....	81
7.2.3	事業継続におけるバイタル・レコード.....	83
7.2.4	支援技術との関連.....	85
7.3	社会的課題.....	86
7.3.1	事業中断リスクの計量化 (含む再構築コスト).....	87
7.3.2	インシデント及びニアミスのデータ収集と分析.....	87
7.3.3	業界内の知識・ノウハウ共有.....	87
7.3.4	経営判断プロセスへの反映.....	87
7.3.5	レジリエンシー文化の定着.....	87
7.4	まとめ.....	88

図表目次

図

図 1 事業継続と ISMS	3
図 2 NPO (BNet) が発行する緊急時アクセスカード	6
図 3 SUNGARD 社が提供する事業継続計画・統合マネジメントツール	8
図 4 英国 BCI が提唱する事業継続のプログラムマネジメント	12
図 5 事業継続計画を巡る行政機関の動向	14
図 6 内閣官房情報セキュリティセンター「第 1 次情報セキュリティ基本計画」より	15
図 7 SS507 の構成概要	17
図 8 事業継続関連基準の ISO 化に向けたスケジュール	19
図 9 事業継続の構成要素(事例)	25
図 10 事業再開 (ビジネス・リザンプション) の各ステップ	26
図 11 BCI の会員資格レベル	29
図 12 DRII の資格階層	30
図 13 プロフェッショナル育成を中心としてアプローチの例示	33
図 14 専門家ネットワークの効用	35
図 15 バイタル・レコードのリスクマネジメント	50
図 16 DAS のイメージ	55
図 17 SAN のイメージ	56
図 18 ストレージ仮想化のイメージ	57
図 19 NAS の例	60
図 20 バックアップサイトとリストア方法の例	67
図 21 サイト間ミラーリングの例	68
図 22 ディスク経由のバックアップとリストアの例	70
図 23 LAN 経由のバックアップ例	71
図 24 スナップショットのイメージ	73
図 25 RAID のイメージ	74
図 26 ILM の例	76
図 27 バイタル・レコード・マネジメントとコンティンジェンシープラン	82
図 28 情報の重要度特定プロセス	85

表

表 1	業界別文書の例.....	1
表 2	BCI が提供する事業継続管理に関わるシラバス（講義要綱）の雛形	12
表 3	TR19 における事業継続管理のフレームワーク	16
表 4	ANSI/ARMA 5-2003 におけるバイタル・レコードの定義.....	36
表 5	付録 G・バイタル・ファイル、レコードおよびデータベースの 11 項目（要約）	44
表 6	バイタル・ファイル、レコードおよびデータベース	45
表 7	ANSI/ARMA 5-2003 の全体構成.....	49
表 8	記録(レコード)の各分類、該当する記録、保護方法の例	51
表 9	文書の法定保存年限（例）	83

1 事業継続と情報資産管理

1.1 事業継続と情報資産管理

企業などの組織において、重要な情報資産は、文書や記録といった有体化された形式で活用され、保管されていることが多い。従来、重要書類という形で管理されてきた情報がこれにあたる。表 1 は、業界別に各事業プロセスで使用されている文書を例示したものである。

表 1 業界別文書の例

業界	経営・管理	人事・組織	企画	営業	技術	取引先
製造	役員会議決議事項 決算関連 予算・財務関連 投資関連・投資先 契約書	人事規定集 組織図 評価情報 組合員名簿 労使関連情報	新製品開発企画 新規事業企画 経営分析資料 調査分析レポート 実行予算指示書	信用調査報告書 契約書 個別取引条件 新製品提案書 販促企画書	機能仕様書 設計書・図面 工程管理表 新製品開発企画書 特許情報 臨床試験結果	取引条件関連 取引契約
建設	市場調査報告書 クレーム情報 会議議事録		プロジェクト予算 クレーム情報 利益予測表	発注実績表 下請管理表	材料管理表 技術ドキュメント 検査仕様書 特許情報	取引契約内容
流通	寄付・加入会関連 承認前諸規定		マーケティング資料 企画資料 運行スケジュール	クレーム情報 事故報告書 原価管理表	材料分析表	顧客名簿
サービス			企画書 外部情報収集 工事指示書	契約書 顧客管理表 不祥事等事件情報	調査手法ツール 調査レポート 特許情報	取引条件関連 新製品情報 外注契約 顧客名簿
金融			新商品企画書 本部通知文 統計表 調査報告書	顧客管理表 信用調査報告書 投資ガイド	新製品マニュアル	個人情報 信用調査報告書 個人取引情報
通信			企画資料 顧客情報	契約書 (電柱/送電線等)		個人情報関連 信用調査関連
大学		職員名簿 行政文書	企画書	産学プロジェクト 文書	研究論文	学生名簿/成績表 受験者名簿 就職活動関連文書

近年、IT の普及により、このような書類も、“データ”という形で、コンピュータ上で作成され、ネットワーク上で流通し、データベースにより共有・保管されることが多くなった。A.M.マクドノウは、「情報とは、特定の状況における価値が評価されたデータ」と定義している¹。この定義に基づいて考えた場合、企業などの組織で取り扱われている“データ”は、特定の目的のもとで集められ、活用されている“情報”であり、その活用目的にもとづいて、分類し管理されているものという考え方が適当であろう。事業継続計画の策定では、保護すべき情報資産を特定しなければならないが、情報の電子化が進んだとしても、この視点は変わらない。企業などの組織では、この情報資産管理のノウハウは、文書管理や記録管理という形で蓄積されてきた。したがって、事業継続と情報資産管理の関係を考える際には、文書管理などにおける分類法や管理手法を、紙の上の情報と電子化された情報が混在する現在の環境において、さらに発展させていく必要があるといえる。

1.2 情報セキュリティとの関係

情報セキュリティマネジメントシステム（ISMS：Information Security Management System）に関する国際規格である「ISO/IEC27001:2005（情報技術—セキュリティ技術—情報セキュリティマネジメントシステム—要求事項）」（2005年10月発行）では、事業継続は、管理すべき項目のひとつとして含まれている。ISMSは、情報資産保護を目的として組織内に構築される管理のためのシステムである。災害や窃盗など、幅広い脅威を対象とし、それらによって事業継続に重大な支障をきたさないようにするために必要な情報資産保護のためのマネジメントシステムの構築と実践を要求している。事業継続は、人命の保護や情報資産以外の資産の保護も対象としているが、ISMSにおける事業継続は情報資産保護のみを対象としている。一方、ISMSは、情報セキュリティ事故の低減など、災害などが発生した場合に、いかにして事業継続を実現するかという視点と異なる要素も含んでいる。その関係を表すと、図1のようになるといえよう。

¹ 経営情報システム、島田達巳・高原康彦、日科技連、2003年

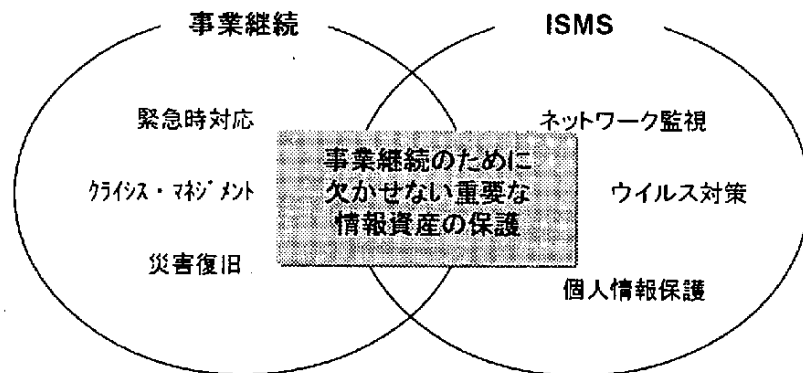


図 1 事業継続と ISMS

事業継続と情報セキュリティの関係について考える際に、別の観点から、注意が必要ことがある。事業継続の視点からは、情報はできるだけ冗長性を持たせるほうがよい。たとえば、重要書類は複製を別の場所においておけば、災害などが発生した場合も、少なくとも情報の中身は失われない。法的に元本性などが要求されていない限り、その複製を使って、支障なく事業は継続できる。しかしながら、情報セキュリティの観点からは、その情報が秘密情報であった場合、複製を作るとは情報漏えいリスクを増大させることになる。事業継続における情報資産保護は、常に秘密情報保護を考えて計画を立て、実践されなければならない。本調査研究においては、この側面に関して深く議論していないが、事業継続における情報資産管理を検討する際には、常に念頭においておかなければならない点である。

2 事業継続関連の国内外の動向

事業継続の分野はこれまで統一的な定義や方法論が不十分であったことから、国、業界、企業、自治体などの組織形態や、担当する個人によって捉え方が様々である。また、既存の防災計画・体制や災害復旧計画（DRP：Disaster Recovery Plan）などとの連関や対象範囲の区分なども明確ではないため、全般的には言葉だけが先行している状況であるといっても過言ではない。その言葉についても、事業継続（BC：Business Continuity）から緊急事態準備（EP：Emergency Preparedness）と内容はほぼ同様にもかかわらず言い換えが始まっていたり、また同じBCPでも事業継続計画（Business Continuity Plan）と事業継続プログラム（Business Continuity Program）と使い分ける場合も出てきている。

このような状況下で、事業継続に関するガイドライン・標準についても、各国・各業界など様々なレベル・範囲で既存のものが存在するが、それぞれ定期的に改訂されたり、他のガイドライン・標準と統合されたりと、常に内容や対象が変化している。これは、事業継続計画が対象とする事象や業務・オペレーションの範囲や深さが、経営環境の変化に順応し続ける必要があることを物語っている。ただ、大きな潮流として観察されたことは、古くはIRAのテロ攻撃によって英国ロンドンのシティー地域で事業中断を余儀なくされた頃から、1993年の米国ニューヨークのワールド・トレード・センター爆破事件で「想定外」の事故・事件が従来から対応してきた自然災害よりも注目され始め、2001年の米国同時多発テロで一気に官民の事業継続の意識や取組みが底上げされたと言える。その後、2003年の北米大停電によって、重要社会インフラの脆弱性が露呈するような事故も経験し、更に2005年のハリケーン・カトリーナによる被害で再度、自然災害対応の重要性も認識され、現段階では、自然災害、事故（意図的・非意図的）・事件といった原因にかかわらず、レジリエンシー（弾力性のある回復力）を確保する事業継続管理体制の構築への取組みが始まっているという状況である。

また、上記期間の大きな出来事としてY2K対応があったが、米国が産官学挙げて情報通信技術（ICT）依存性が高まる現代社会・経済の脆弱性克服のひとつの取組みとして、Y2K以降も視野に入れて対応したことも、大きく事業継続管理や事業継続計画の概念が急速に浸透した大きな要因であるとも言われている。一方、Y2Kを一過性のプログラムミス対応という認識で対応した国々は、普及・啓発や標準化の取組みにおいて米国に大きく水を開けられているとも考えられる。

2.1 米国の現況

米国では従来の災害復旧計画（DRP: Disaster Recovery Plan）から、対象範囲を業務プロセスや人的手配にまで広げ、また災害や障害・事故が起こる前の段階も対象とする事業継続管理が官民間問わず浸透・定着しつつある。この背景にはこれまで米国が経験したテロ攻撃、地震・ハリケーンなどの自然災害、大規模停電での教訓が個別企業のみならず、自治体や政府にまで浸透しているということがある。

2.1.1 事業継続の導入状況

個別企業における事業継続計画インセンティブとして、まずは取引先から要求される場合、次に監督当局などから要求されている場合、そして業界として事業継続計画のガイドラインを制定している場合などに分類できるが、半導体製造業や金融業など業界全体で事業継続管理に関するレベルを向上させないと、ビジネス機会が国外に流出してしまうという危機感から取り組んでいるケースも見られる。

事業継続計画に関わる標準・ガイドラインとして NFPA1600²が公開されているが、実際には上述の、主要取引先が要求してきているガイドラインや、コンサルティング会社が提供する方法論に沿った取り組みを行っており、全般的には NFPA1600 というよりも、米国 DRII³や英国 BCI⁴の方法論やガイドラインを参照している。実際の事業継続性についての認証は、監査法人も高リスクと判断しており、現段階では認証を行う制度やシステムは存在していない。

行政・自治体においては、中でも特にニューヨークを始めとする都市型の自治体における事業継続管理は、行政サービスの事業継続性の維持に対する高い意識と、地元企業との協調という観点から日本の自治体も学ぶべきところは多いと考える。行政として地域のレジリエンスを保持・向上するためには地元企業との連携は不可欠であると位置付け、通常の連絡や訓練・ドリルへの相互参加などを通じて、事業継続計画や事業継続管理の共有化を図ろうとしている。例えばニューヨーク市では、“READY NEW YORK” といった中小企業向けの緊急事態準備計画のハンドブックを公開するといった行政サービスはもちろんのこと、地元

² NFPA : National Fire Protection Association（全米防火協会）。NFPA1600 については 2006 年に改訂予定で、改定案に対するパブリックコメントを募集中。（2006 年 2 月現在）

<http://www.nfpa.org/PDF/nfpa1600.pdf?src=nfpa> で入手可能

³ NFPA1600 の現行版に関与、また金融関係当局検査のマニュアルである FFIEC のハンドブックも DRII の手順を参照している。DRII の詳細は <http://www.drii.org/> 参照。

⁴ 1994 年設立の非営利団体。詳しくは <http://www.thebci.org/> 参照。PAS56 の原案を BSI（British Standard Institute: 英国規格協会）と共同で作成。

産業とも言える金融業と NPO を介して、企業が緊急時に優先的に事業継続に必要な人員や車両を配備できるような仕組み⁵を導入したりするなど、積極的に地域レジリエンシーの強化を図っている（図 2）。

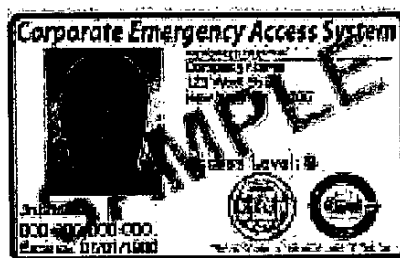


図 2 NPO (BNet) が発行する緊急時アクセスカード

2.1.2 標準化の動向

NFPA1600 を米国規格協会（ANSI : American National Standards Institute）と米国防火協会（NFPA : National Fire Protection Association）が制定。オリジナルは 1995 年の”Recommended Practice for Disaster Management”で、その後 2000 年の改訂を経て、現行”Standards in Disaster/Emergency Management and Business Continuity Programs”が 2004 年に発行された。現在、2007 年の改定に向けてパブリック・コメントを募っている。また、この NFPA1600 は、ISO 化のベースとして持ち込まれようとしている。内容は下記の通り大きく 5 章に分かれるが、全体の構成として別添資料の方が本体部分よりページ数もかなり多い、即ち本体ではフレームワークだけを示して、別添資料で詳細を参考として提示するというアプローチを採用し、NFPA1600 の導入を検討する組織の形態や業態などによって自己判断の部分を多くし、柔軟性を持たせる意図が確認できる。

第 1 章 運営

第 2 章 参考文献

第 3 章 定義

第 4 章 プログラム・マネジメント

第 5 章 プログラム要素（エレメント）

⁵ BNet：予め登録された人員・車両は、緊急時に封鎖された地域にも市の判断で優先的に入ることができる仕組みを提供する NPO。毎月のデータ更新と、緊急車両搭載のバーコードリーダーで読み取れるような専用カードを発行する。ボストン、アトランタといった他都市にも展開中。詳細は、<http://www.bnetinc.org/home.html>

2.1.3 現地の状況

(1) 事例：SUNGARD 社

米国における事業継続関連の商品・サービスのうちデータ・センターやワーク・スペースの提供の約60%をSUNGARD⁶、IBM、HPが占めると言われているが、その中でもSUNGARD社は“information availability services”と自らのサービスを位置付け、顧客企業のビジネスの可用性を上げると同時に、その分野におけるアウトソーシングの投資対効果の向上に努めようとしている。米国と欧州に約60のデータ・センターを保有、従業員用ワーク・スペースも2万シート以上、ネットワークも総計約25,000マイル、また移動式データ・リカバリーセンターも50台以上保有するなど、継続的な投資をしながら積極的にビジネスを展開している。

SUNGARD社はサービス・ラインを

- ① システム・リカバリー
- ② エンド・ユーザー・リカバリー
- ③ モバイル・リカバリー

の3分野に分けてサービスを強化しており、特に②については通常の業務やコールセンターなど、従来のシステム部門やデータ・センター以外の業務や電子メールシステムといった通常業務の継続には欠かせない機能の可用性強化を主眼としている。

また、Paragon という事業継続のプランニング、統合マネジメントツールの販売も行っており、その操作の容易性から顧客が直接購入する場合もあるが、中長期的なメンテナンスの観点から、コンサルティング会社などを通じた販売にも力を入れている（図3）。

⁶ 日本ではNECと業務提携。

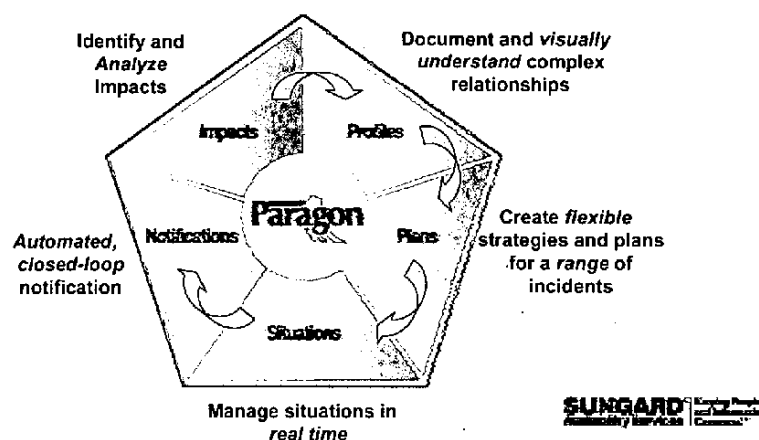


図 3 SUNGARD 社が提供する事業継続計画・統合マネジメントツール

この Paragon がカバーする 5 つの領域の根底に流れる概念は、IA ライフサイクル (IA: Information Availability) と定義され、企業の可用性 (取引先や商品・サービスのユーザーから見た) を確保するためのフレームワークであると位置付けられている。

(2) 事例：Strohl Systems 社

Paragon と同じく事業継続計画策定・運用支援ツールとしては、Strohl Systems 社⁷の製品が良く使われているが、今回の調査でヒアリングを行った米国投資銀行では使用しているものの、かなり内容をカスタマイズしている模様。この銀行はユーザー会のリーダーでもあり、また、事業継続管理のレベルは金融機関の中でもかなり高い位置にあるため、ユーザー側に知識と経験があれば使い勝手が良い、との評価であった。また欧州系グローバル銀行では、Paragon と Strohl System 社製品を比較、更に欧州系の専門ベンダーの製品数種類も検討した結果、できるだけユーザーが使いやすく、メンテナンスが簡単である、という事由で欧州系の専門ベンダーの製品⁸を採択している。

(3) 事例：ARMA (American Record Management Association)

米国規格協会 (ANSI: American National Standard institute) と 2003 年にバイタル・レコード・マネジメント (VRM: Vital Record Management) を公

⁷ <http://www.strohlsystems.com/>

⁸ TwelveCubes/IBM による CPro、Office-Shadow による Shadow-Planner など。

開、企業活動におけるレコードマネジメントに事業継続の観点を盛り込み、更に事業継続計画の中でのバイタル・レコード・マネジメントの位置付けを定義している（詳細は後述）。現時点では、各業界別の個別基準やテンプレートは定義していないものの、ARMA 会員間では業界別にディスカッション・グループを WEB 上で形成し、活発に議論を行っている。

(4) 事例：ニューヨーク大学/INTERCEP

ニューヨーク大学は米国国土安全保障省（DHS : Department of Homeland Security）からの資金援助を受け、企業の緊急事態準備や事業継続に関する調査・研究及び教育を行う目的で INTERCEP（International Center for Enterprise Preparedness）⁹を設立済。現時点では、全米の主要都市を巡回しながら、2 日間で NFPA1600 の解説と組織への導入に関する普及・啓発を行っている¹⁰が、2007 年を目標として修士課程を創設すべく準備を進めている。

現在、INTERCEP が展開しているセミナーの内容は下記の通り、NFPA1600 の内容を中心に据えている。

第 1 日目：エグゼクティブ・フォーラム（この日のみの選択も可能）

NFPA1600 の項目を通じた：

- ・ 緊急事態準備と事業継続プログラムの重要要素の認識。
- ・ プログラム導入あるいは更新に必要なマネジメント体制の定義。
- ・ リスクの優先度決定と経営資源の配賦についての議論。

第 2 日目：監査と評価

NFPA1600 の項目を通じた：

- ・ 効果的な監査の方法についての評価。
- ・ 各要素の正確な解釈と監査の実施。
- ・ 他の監査項目と NFPA1600 に関する項目との統合。
- ・ 事業継続計画改善のための評価結果の経営陣へのコミュニケーション。
- ・ 効果的な NFPA1600 導入評価によるビジネス上の価値認識。

⁹ 詳細は <http://www.nyu.edu/intercep>

¹⁰ 米国内の各都市で行われているセミナーの詳細は、<http://www.nfpa.org/catalog> 中に掲示。

2.2 英国の現況

2.2.1 事業継続計画の導入状況

米国よりも早い時期から IRA などのテロ攻撃を受けてきた経験のある英国でも、やはり 2001 年の米国同時多発テロを機に、各組織の事業継続計画への取り組みは更に促進された。また、これは英国に限ったわけではないものの、英国では特に企業たるものゴーイング・コンサーンとして、成長を続けなければならないという経営者の意識と、企業に投資する投資家や取引を行う取引先や就職する従業員が長期的な継続性をより求めているという背景が強いという観察もある。

事業継続計画の導入状況は官民共に積極的に取り組んでおり、特に民間企業は PAS56 や BCI のガイドライン（共に後述）、自治体は Civil Contingency Act などをベースに事業継続管理体制構築を展開している。

2.2.2 標準化の動向

(1) 英国 PAS56¹¹

英国 BCI（Business Continuity Institute）と英国規格協会（BSI：British Standards Institution）が 2003 年に公開した事業継続管理に関わるガイドライン、パブリック・コメント期間を経て、2006 年中には英国規格（BS：British Standard）化の見込み。現在、主要産業界からのフィードバックを受けながら英国規格化への素案を準備中。対象は行政・自治体といった公的機関と民間企業であることが明記されており、更に下記のような分野と統合的に連関するものであると位置づけられている。

- ① リスク・マネジメント
- ② ディザスター・リカバリー（災害復旧）
- ③ ファシリティ・マネジメント（施設管理）
- ④ サプライ・チェーン・マネジメント（SCM）
- ⑤ 品質マネジメント
- ⑥ 健康と安全
- ⑦ ナレッジ・マネジメント
- ⑧ 緊急時マネジメント
- ⑨ セキュリティ

¹¹ PAS：Publicly Available Specification、一般仕様書。パブリックコメントの期間を経て、英国標準（BS：British Standard）となった段階で、PAS は消滅する。

⑩ 緊急時コミュニケーションと広報

また、内容構成としては下記の通り、事業継続管理体制を構築・運営する手順がとりまとめられている。

- 第1章 スコープ (PAS56 の対象範囲)
 - 第2章 用語の定義
 - 第3章 略語の解説
 - 第4章 概要 (原則、事業継続管理ライフサイクル)
 - 第5章 事業継続管理プログラム・マネジメント (マネジメント、方針、事業継続管理への確信)
 - 第6章 現行ビジネスの認識 (BIA¹²、リスク評価)
 - 第7章 事業継続管理戦略 (組織横断的な戦略、業務レベルの戦略、経営資源再確保のための戦略)
 - 第8章 事業継続管理プランの策定と導入 (事業継続計画、経営資源再確保と手順計画、緊急時マネジメント計画)
 - 第9章 事業継続管理文化の構築と定着 (普及・啓発、トレーニングと組織文化)
 - 第10章 事業継続管理の演習、維持・管理と監査 (演習、メンテナンス、監査)
- 添付資料 A、B

(2) 英国 BCI-Good Practice Guideline

英国 BCI が 2002 年に公開した事業継続計画ガイドラインを 2005 年に改訂したもの。多くの欧米企業が参照している。BCI が提唱するプログラムマネジメントの流れを図 4 に示したが、まず自らの組織の業務やビジネスの可視化から始まり、中長期的にプログラムとして回すことを主張している。

¹² BIA: Business Impact Analysis (ビジネス影響度分析)

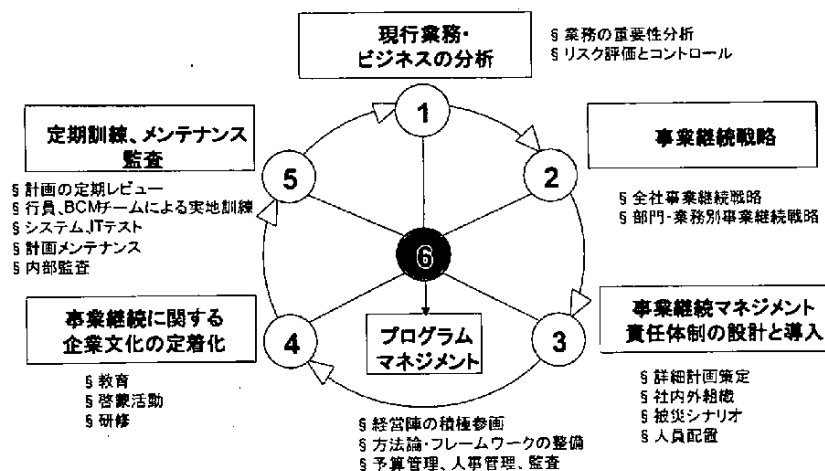


図 4 英国 BCI が提唱する事業継続のプログラムマネジメント

また、BCI の教育部門では、ここに来て急増した大学などの高等教育機関からの要請に応えるべく、事業継続管理に関するシラバス（講義要綱）の雛形を公開している。表 2 はその概要を示しているが、基礎入門レベル（Foundation）、検定レベル（Certificate）と学位レベル（Diploma）の 3 段階で構成され、特に学位レベルでは実際の現場での適用経験が単位として勘案されるなど、実践重視の設計となっている。

表 2 BCI が提供する事業継続管理に関わるシラバス（講義要綱）の雛形

Module title	Foundation	Certificate	Diploma
1 unit = c.6hrs teaching time	6 Units	10 Units	20 Units
Introduction to BCM	1	1	3
1 Initiation and Management	0.5	1	2
2 Business Impact Analysis	0.5	1	2
3 Risk Evaluation and Control	0.5	1	1
4 Developing Business Continuity Management Strategies	1	2	2
5 Emergency Response and Operations	0.5	1	2
6 Developing and Implementing Business Continuity and Crisis Management Plans	0.5	1	2
7 Awareness and Training Programmes	0.5	1	1
8 Maintaining and Exercising Business Continuity and Crisis Management Plans	1	1	2
9 Crisis Communications		0.5	1
10 Coordination with External Agencies		0.5	1
BCM Activity Logbook			2
Assignment			5
UNITS	6	10	20
TEACHING HOURS	36	60	90

The Business Continuity institute, Academic Syllabus 2005

2.2.3 現地の状況

(1) 事例：欧州系グローバル銀行 D 行

オランダに本部を置く D 行は、グローバル事業継続ポリシーを全拠点に展開中。オランダ国内での事業中断は、土地柄、水害系やそれに伴う浸水・停電などが多いようであるが、欧米を中心に自然災害以外の事件・事故も幅広く対象としている。現在、行内の普及・啓発を主に展開中であるが、できるだけシンプルに準備・導入ができ、また、緊急時にも直ぐに実行できるように工夫をしている。あとは訓練、訓練、また、訓練といったスタンスで体力はかかるが、各現場で意識が高まり安定するまでは普及・啓発活動を精力的に継続する予定。

2.3 日本の現況

2.3.1 事業継続計画の導入状況

半導体部品製造業界など、サプライ・チェーンが海外にまで及び、また個々の部品が個別仕様のため、その供給継続が極めて重要となっているような業界では、仕入先からの要請により事業継続計画を既に導入しているケースも散見される。また、金融機関のうち特に銀行においては従来型の災害復旧計画やコンティンジェンシープランを欧米先進金融機関に見習い、また、海外展開している場合には現地当局からの要請により事業継続管理への体制拡張を進めている。政府・自治体においては、まだ事業継続の認識すら浸透していない状況ではあるが、歴史的に自然災害を中心とした広域災害に対応してきた我が国の政府・自治体は、既存の防災計画や体制を活用しながら事業継続計画へと展開させる方法やアプローチを模索し始めている。

2006 年 1 月に全国の主要自治体に対して実施された事業継続管理に関する実態調査¹³によると、事業継続計画を一部でも導入しているのは僅か 3 %にとどまり、検討していない自治体は 86 % (30 自治体) にのぼる。これは、日本企業における導入状況の 10 %と比較しても低い数字となっているが、この背景には、自治体業務の復旧における優先順位の設定が難しいということもある。また、中断することにより影響の高いリスクとして、情報システム障害が高く意識されているにもかかわらず、実際の対策が遅れているという事実も確認されている。

¹³ 三井住友海上火災保険株式会社などによる。プレスリリースについては http://www.ms-ins.com/news/h18/0216_3.html を参照。

2.3.2 標準化の動向

事業継続計画に関するガイドラインや指針が政府から出始めたのは 2005 年に入ってからのことである。図 5 に見られる通り、社会・経済を構成する要素を、地域社会、重要社会インフラ、中小企業、大・中堅企業とした場合、それぞれの領域において、所管省庁が何らかのガイドラインや指針を既に公開したり、現在、策定中といった状況である。

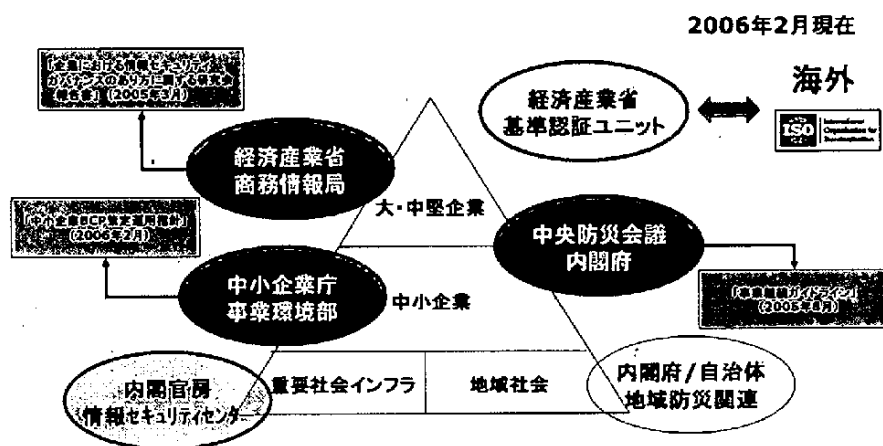


図 5 事業継続計画を巡る行政機関の動向

また、業界で取り組んでいる例としては、半導体製造業の工業会組織である SEMI ジャパン¹⁴でも事業継続のガイドラインを公開したり、また、金融業界でも財団法人金融情報システムセンター¹⁵が、既刊のシステム安全基準と、コンテインジェンシープラン策定の手引書を、事業継続の観点も踏まえて改訂、それぞれ 2006 年 3 月に公開予定である。

(1) 経済産業省

2005 年 3 月に「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」¹⁶にて事業継続策定ガイドラインを公開。IT セキュリティの観点なるも、業務オペレーションや人員の確保といった、幅広い範囲で事業継続を捉えている。

¹⁴ <http://www.bookpark.ne.jp/semi/>

¹⁵ <http://www.fisc.or.jp/>

¹⁶ <http://www.meti.go.jp/report/data/g50331dj.html>

(2) 中央防災会議

2005年8月に「事業継続ガイドライン」¹⁷を公開。あらゆる事象の中から、想定しやすい大規模地震をまず始めの事象として取り上げて構成されている。その他、事業計画に関わる評価項目も定義し、現在、諸意見を集めて改訂を検討中。

(3) 中小企業庁

2006年2月に「中小企業BCP策定運用指針」¹⁸をWEB上で公開。中小企業であっても事業継続を確保できるよう、自己診断や計画策定を支援するようなツールをWEB経由で利用できるように設計されている。

(4) 内閣官房（情報セキュリティセンター）

電気、ガス、水道、金融、通信、運輸といった重要社会インフラの脆弱性を相互依存性も含めて解析、2007年度中にそれぞれの業界における安全基準を策定し、重要社会インフラのレジリエンシー（弾力性のある回復力）確保を目指す¹⁹（図6）。

重要インフラの「安全基準等」の指針

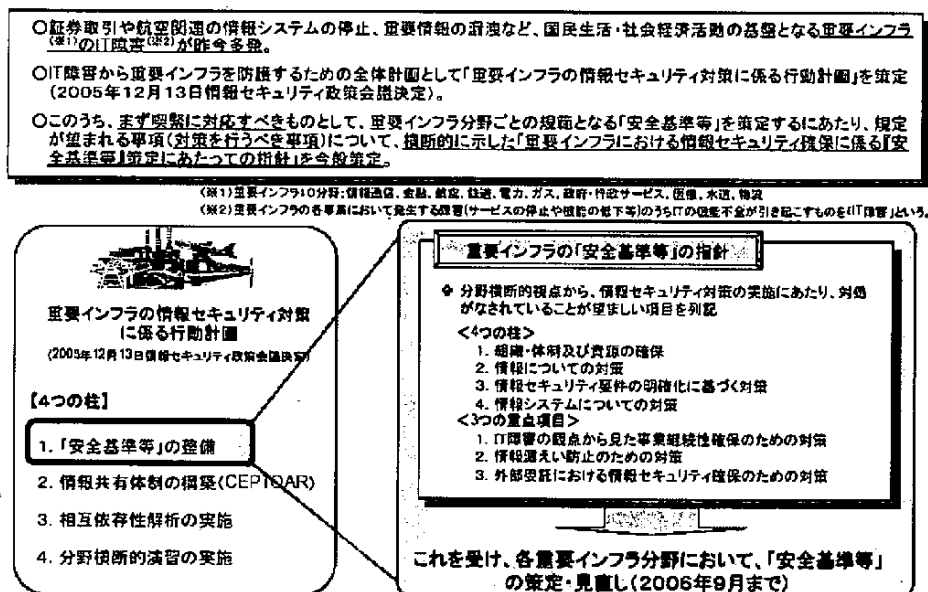


図6 内閣官房情報セキュリティセンター「第1次情報セキュリティ基本計画」より

¹⁷ <http://www.bousai.go.jp/MinkanToShijyou/guideline01.pdf>

¹⁸ <http://www.chusho.meti.go.jp/bcp/>

¹⁹ 詳細は http://www.bits.go.jp/active/kihon/pdf/bpc01_ts.pdf などご参照。

2.4 その他の国の動向

ここでは、米国、英国、日本以外で積極的に事業継続に関する普及・啓発に取り組んでいる、シンガポールとオーストラリア・ニュージーランドの標準化動向を概説する。

2.4.1 シンガポール (TR19)

シンガポール規格協会 (SPRING) が 2005 年 9 月に公開した、事業継続管理に関するガイドライン。約 2 年間のパブリック・コメント期間を経てシンガポール規格 (S S : Singapore Standard) 化を目指す。既存の事業継続に関わるガイドラインや標準を参考しながら、かつ、環境に関わる領域は ISO14000 シリーズを参照させるなど、他の内容と重複しないような方針がとられている。具体的内容は網羅性が重んじられ、表 3 のようなマトリックスの各領域について簡潔にとりまとめられている。

表 3 TR19 における事業継続管理のフレームワーク

BCMのフレームワーク		BCM構成要素			
		方針	プロセス	人員	インフラ
BCMの領域	リスク分析とレビュー				
	BIA(ビジネスインパクト分析)				
	BC戦略策定				
	BC計画策定				
	テストと訓練				
	プログラム・マネジメント				

この中には、リスク・コミュニケーション、サプライチェーン・マネジメント、官民協業といった、最近の事業継続の分野で活発に議論されている諸点も取り込まれており、実効性の高い規格を目指している。また、本調査のひとつの大きなテーマであるバイタル・レコード・マネジメントの概念も重要な要素として触れられている。

表記形式は ISO/IEC の国際規格の草案作成ルールを適用したり²⁰、巻末にはパブリック・コメントをそのまま FAX できるような様式が含まれていたり、広く

²⁰ 細かい言葉遣い、例えば"shall"は厳格に従う必要がある項目、"should"は適切として勧められるが選択的に対応してよい項目、"may"はその規定内で許される項目、そして"can"は可能性や能力を示す項目、といったように、内容に応じて言葉遣いを使い分ける。

産官学などの市中からの意見を取り込み実効性を確保し、最後には国際規格化との整合性も確保することで、シンガポールの国際的市場競争性を向上させようという意向も垣間見ることが出来る。

2.4.2 シンガポール (SS507)

シンガポール情報通信開発庁 (IDA : Infocomm Development Authority of Singapore) が 2004 年に策定した、事業継続や災害復旧に関する業界の標準 (資格制度)。シンガポール政府のバックアップにより国内の事業継続や災害復旧に関する業界の競争優位性の確保を目的とするもの。これまでシンガポールは近隣諸国の企業を相手に、BC/DR 関連のサービスを積極的に展開してきたが、業者間の品質格差が広がり、業界全体の信用力が落ち始めたことを懸念した政府が、産官学で連携した形で規格を制定した。実際にこの規格をクリアした業者は政府系や大手の 7 社程度だが、積極的に政府とタッグを組んでマレーシア、インド・中国・台湾といった近隣諸国に売り込みを展開している (図 7)。

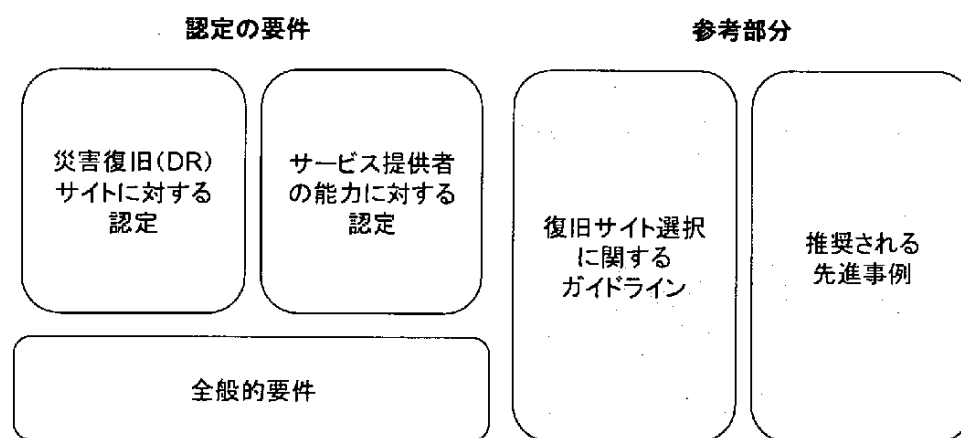


図 7 SS507 の構成概要

2.4.3 オーストラリア・ニュージーランド

2004 年に改訂された HB221:2004 が事業継続管理に特化したハンドブックであるが、これとは別にリスクマネジメントの規格である、AS/NZS4360:2004 でも障害・事故発生直後を対象とした危機・緊急計画 (Crisis and Emergency Plans) の後に続きフェーズ²¹を対象として、事業継続計画を定義している。この

²¹ BCP の後のフェーズについては、復旧計画 (Recovery Plan) の範囲と定義。

AS/NZS4360 は、もともと 1995 年にリスクマネジメントの規格として世界に先駆ける形で制定された。その後 1999 年の改訂を経て、現在の 2004 年版となっている。

また、HB221:2004 は事業継続管理導入を支援するワークブックとして位置づけられ、下記の通り、事業継続管理導入の必要性や位置付けの解説から、ステップを追った説明、更に実際の事業継続管理体制構築に必要な様式が盛り込まれている。

パート 1：事業継続管理とは？

- ・ 事業継続管理の進化
- ・ リスクと事業継続管理の関係
- ・ 事業継続管理とコーポレート・ガバナンスの関係
- ・ 事業継続管理のアプローチ
- ・ リスクの認識と事業継続管理
- ・ 組織活動における重要な相互依存性
- ・ 組織環境の例示
- ・ 事業継続管理の改善

パート 2：事業継続管理マニュアル

- ・ 事業継続管理プログラムの策定と始動（ステップ 1～9）
- ・ 事業継続管理ワークブック（様式 1～11）

添付資料 A,B

2.5 ISO 化動向

2.5.1 ISO 化の概要とスケジュール

企業や自治体などの緊急事態準備（Emergency Preparedness）に関する国際規格化を議論する国際会議を 2006 年 4 月に開催。各国政府はこれに向けて準備中であるが、日本からも既存のガイドライン（経済産業省、内閣府など）を参考にし、また産業界からも意見を取り込み原案を作成、検討体制の準備段階から積極的に参加することとしている。通常の手続きであれば 2008 年夏目処であるが、実際の制定時期については現段階では未定。議長国の米国以外にも欧米諸国などが原案提出、国際ワークショップ協定（IWA: International Workshop

Agreement) にも参加の予定 (図 8)。

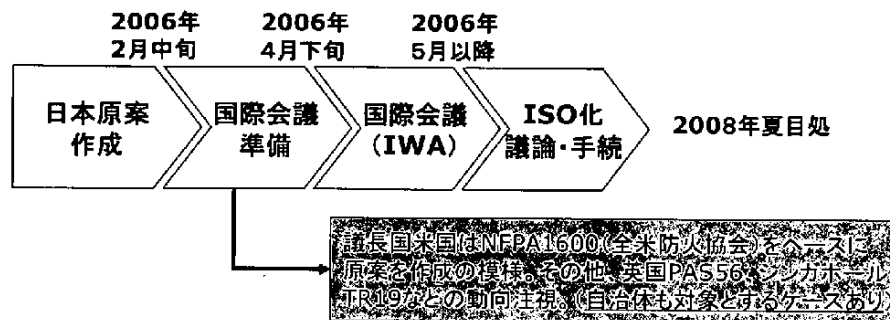


図 8 事業継続関連基準の ISO 化に向けたスケジュール

2.5.2 日本の対応

日本原案の概要と主な論点は以下の通り。

- ① 経済産業省、中央防災会議/内閣府のガイドラインの統合をベースに必要なに応じて内容を補記。
- ② 第三者による認証制度を採用しない。
- ③ 災害発生直後における公的組織が第一義的に行う活動は対象外。
- ④ 対象とするリスクは各組織が合理的な基準に基づき自主的に選択するものとする。
- ⑤ 広域災害においては、被災した地域の復旧計画との連携・調整に留意する。

今後は ISO 化に向けての国際間の議論・調整が始まるが、世界的にサプライ・チェーンを張り巡らす企業群を配し、また、地震などの広域災害の経験を豊富に持つ日本は、その立場・経験に基づき官民間問わず組織や地域がレジリエンスを確立できるよう、また、発展途上国においてもそれが実現できるよう、議論・調整に貢献する。

3 事業継続に関するケーススタディ

本章では、国内外におけるヒアリング調査に基づき、事業継続関連の取組みをまとめる。

3.1 金融機関

3.1.1 先進金融機関の動向

欧米の先進金融機関の動向に関しては、これまでの調査に加え今回は特に米国の投資銀行数行と欧州の銀行及び監督当局の事例に触れることが出来たが、概して欧米の先進金融機関の事業継続管理体制は、もはや標準化・当局対応の域を超えようとしている。もちろん、業界内の個別金融機関の間での温度差や、監督当局との牽制関係におけるバランスなど、一筋縄ではコントロールできない要素はあるものの、少なくとも重要な経営課題のひとつとして位置付け、主体的かつ積極的に（proactive）取り組んでいる。

このような状況を鑑み、本項では他業界への参考にもなるようなポイントを中心に、先進金融機関における動向を紹介する。

(1) 事例：米国系投資銀行 A 行

常に競合他行、当局からの要求の先を行くポリシーを全世界の拠点で貫こうとしている。事業継続の責任者は主要マーケット国の拠点には、グローバルで事業継続体制の一貫性を維持するために頻繁に出張、コーディネーションを行っている。また、取引を始める投資家に対しても、事業継続への取組みを説明する資料を前面に出してアピールしている。（営業部門も事業継続への取組みを顧客に説明できるレベルにまで教育済み。）従業員は緊急時の連絡リストや対応ステップの書かれたカードを常に携帯しており、緊急時にも必要なコンタクトを素早く試みることが出来る。

(2) 事例：欧州系グローバル銀行 D 行

前述の通り、行内における事業継続管理体制の構築に関しては、簡略化することで世界各地の拠点に展開しやすい工夫を凝らしているが、各拠点においては逆に各国の法規制や商習慣に合わせてより詳細レベルでの事業継続管理体制を個別に構築している。また、現在進行中の基幹業務のインドへのアウトソーシング

による移管については、事業継続管理体制の大幅な見直しが必要であることを認識し、積極的かつ慎重にプロジェクトを遂行中である。また、関係する保険会社では、世界の約 50 拠点の拠点長の 2004 年度のパフォーマンス評価のうち 50% を事業継続計画策定としたため、一気に事業継続計画の導入完了、2005 年度からは実際の運用段階に入りつつある。

(3) 事例：米国系投資銀行 E 行

約 50 カ国、9,700 名のオペレーションの ICT インフラを統括する部門では、ビジネス部門を「社内顧客」として位置付け、提供するサービスのレジリエンシーを効率良く確保すべくプログラムを展開中。このプログラムでは、法規制の変化、合併、イン・ソーシングといった多様な経営環境の変化にも対応できることも視野に入れた戦略的な位置付けとなっている。また、RMM (Resiliency Maturity Model: レジリエンシー成熟度モデル) を米国カーネギーメロン大学と共同開発、ICT 分野での事業継続に関わる投資の ROI (Return on Investment: 投資利益率) をリカバリー効率を軸に測る仕組みを試行中である。試行のフェーズ 1 は 2005 年 9 月に終了、2007 年 3 月にはモデルの完成を目指す。

(4) 事例：日系大手証券会社 F 社 NY データセンター

9・11 米国同時多発テロで大変な苦労を強いられた F 社の NY データセンターでは、事業継続の訓練を不定期に実施している。センター長がビジネスの繁閑を見極めながら、日中のあるタイミングで「ディザスター宣言」を行い、直後から職員は事業継続計画に従いバックアップ・サイトやバックアップ設備を利用した業務に切替る。この事例でのポイントは、顧客に気づかれずに通常日に訓練を行っているということで、予め決められたシナリオに沿って、休日や夜間に行うのではないということである。

3.1.2 業界としての取組み (欧米・日本・国際)

金融業界では提供する商品・サービスのネットワーク²²依存性が高いため、個別金融機関の事業継続管理だけではなく、業界レベル、更には監督当局も支援するような体制が組まれることが多くなってきた。ここでは、その具体的な事例を調査結果を元に米国、英国、日本の状況として紹介する。

²² 電子的なネットワークだけではなく、手形・小切手などによる資金決済、商品・サービスの外部調達といった金融サプライ・チェーンや、業務アウトソーシングなどの外部依存も含む。

(1) 事例：米国証券業協会

米国市場に参加する証券会社、取引所、決済機関などが加盟する米国証券業協会（SIA：Security Industry Association）は、2005年の10月に業界挙げての事業継続訓練を実施した。この訓練には監督当局は関与していなかったが、この背景には、以前、当局側が事業継続に関する白書を出す前のパブリック・コメントを求めた段階で、バックアップセンター設備の距離や業務復旧目標に関する数値目標の設定を、設定しないよう業界全体で押し戻した経緯があり、今回は業界が“自主的”に実施したものである。内容的には全ての参加者がバックアップ・サイトやバックアップ・システムから接続して、証券取引のデータのやりとりが実施できるか、といった接続テストが主であったが、設定の違いや段取りの間違えで接続すらできなかった参加会社もあったようである。前出の米国投資銀行A行も、接続テストと割り切っていたが、そこには証券取引はデータ交換などのコミュニケーションラインさえ確保できれば何とか復旧することができる、という割り切りがある。

なお、同様の訓練は2006年も同様に行われる。

(2) 事例：英国FSA

英国の金融サービス機構（FSA：Financial Service Agency）は、英国におけるすべての金融サービス業務を監視・監督する機関だが、2005年には金融機関の事業継続管理体制に関わるベンチマーキング調査が実施された。調査にはベンチマーキング専用のWEBツールが使用され、各金融機関が入力したデータは個別にはFSAしか見ることが出来ず、参加機関や集計をとりまとめた会計事務所は見ることができない仕組みになっている。FSAに自らの事業継続管理体制の状況を不十分な点も含めてさらけ出すインセンティブについていくつかの参加金融機関に確認したところ、そこまでしてでも自分たちの業界内での位置を確認したいこと、また、FSAを検査などで突然びっくりさせたくないこと、などが確認された。この背景には、FSAが日本の金融庁とはその性格が異なり、業界に対する日常的なアドバイザー機能も持ち合わせているということもあるが、12月に公開された報告書では、FSAと参加機関双方にいろいろと学ぶところは大きかったようである。

その報告書では、各組織のオフィスやバックアップサイト全体がロンドン近郊に集中しているリスク、ITCベンダーを中心としたIT、通信や各種アウトソーシング分野で依存している先への考慮不足、業界挙げての訓練・ドリルが更に必要であることなどが示されていると同時に、今後、またフォロー・アップのベン

チマーキング調査が継続されることも表明されている。

(3) 事例：英国決済業協会

英国の決済業務を担う金融機関（英国銀行：Bank of England も含む）の業界団体である英国決済業協会（APACS: Association for Payment and Clearing Services）では、英国の決済システムの信用力、競争力向上のために参加金融機関の決済状況をモニタリングして、月次で集計、決済遅延、送金先の相違・金額相違などのミス・オペレーション、決済モレなどの障害状況で評価している。評価がある基準を下回ると、APACS の上層機関で障害報告と改善案の提示を求められるなど、監督当局からの指示ではなく、業界で自主的に決済システムのレジリエンシー向上を図っている。この背景には、EU 内での決済システム間の競合という経営環境もあるが、ひとつの業界主導の事業継続管理体制のひとつであるとも言える。

(4) 事例：金融情報システムセンター

金融庁検査や日本銀行考査でも正式に参照されている、財団法人 金融情報システムセンター（FISC: Financial Information System Center）の「コンティンジェンシープラン策定の手引書」が金融機関、日本銀行、ICT ベンダーと有識者を加えて改訂が 2006 年 2 月に終了、事業継続の概念を取り入れた形で 2006 年 3 月より全国の金融機関に展開される。その後、金融庁検査や日本銀行考査にも反映されることから、日本のレベルより先行しているとの自負を持つ欧米系投資銀行でも、その改訂内容が現行事業継続計画や事業継続管理体制とどう関連するかに検査・考査対応の観点から極めて高い関心を示している。

(5) 事例：日本銀行

日本銀行は 2006 年に入り、総裁を通じて金融界に対して、①画一的ではない新しい金融サービスの提供、②リスクへの挑戦と説明責任、そして③業務の継続性が重要であると指摘している。特に CSR（企業の社会的責任）の観点からも、決済システムの担い手として、決済システムの業務を遮断させない業務の安全性・継続性を確保するため、必要な経営資源を投入すること、としている²³。

²³ ニッキン、2006 年 1 月 13 日号、「福井 日銀総裁に聞く」より。

(6) 事例：バーゼル委員会

バーゼル委員会を構成する主要国中央銀行、証券監督局、保険監督局が、共同で“Consultation paper on ‘high-level principles for business continuity’”²⁴というジョイント・フォーラムで策定された各国共通の業務継続原則の策定を目指すペーパーを2005年12月に公開。3月までのパブリック・コメント期間を経て制定される。各国の金融機関のみならず、監督当局にも共通する原則で、具体的な目標値を設定することが強く推奨され、その点に関して内外からのモニタリング体制を構築することが主なポイント。事例分析の中には、2004年10月の新潟県中越地震も取り上げられている。

原則1：取締役会および上級管理職の責任

業務継続に共同責任を有する。

原則2：重大な業務中断

監督当局の事業継続体制は、所管領域の重大な業務中断への対応も含む。

原則3：復旧目標

目標は監督当局と協議、または当局によって設定されることもある。

原則4：連絡体制

金融機関と監督当局は組織内や関係外部との連絡体制を構築しておく。

原則5：国際間の連絡

国境を越えて影響が伝播するような業務中断の際の国際連絡体制を準備する。

原則6：訓練

金融機関と監督当局は業務継続計画に基づき訓練を実施、実効性を検証する。

原則7：監督当局による業務継続体制の検証

監督当局は金融機関のモニター内容に業務継続体制の審査も含める。

ケーススタディ

- ① 北米大停電
- ② 香港 SARS
- ③ カナダ SARS (トロント)
- ④ 新潟県中越地震
- ⑤ 英国同時多発テロ (ロンドン)

²⁴ 仮訳は日本銀行 http://www.boj.or.jp/intl/05/bis0602b_f.htm より入手可能。

3.2 製造業

わが国でも、事業継続を実践する際に、多くの企業で取り組まれてきた地震対策などの緊急事態準備(エマージェンシー・プリペアドネス)やクライシス・マネジメントとの関係が議論になる。

ここで取り上げる米国の製造業における事例は、これらの活動を構成要素として位置付ける形で取り組まれている事業継続の形である。この企業では、事業継続を、「緊急事態準備」、「クライシス・マネジメント」、「IT ディザスター・リカバリー」、「事業再開 (ビジネス・リザンプション)」の4つの要素から構成されるものと捉えている (図 9)。

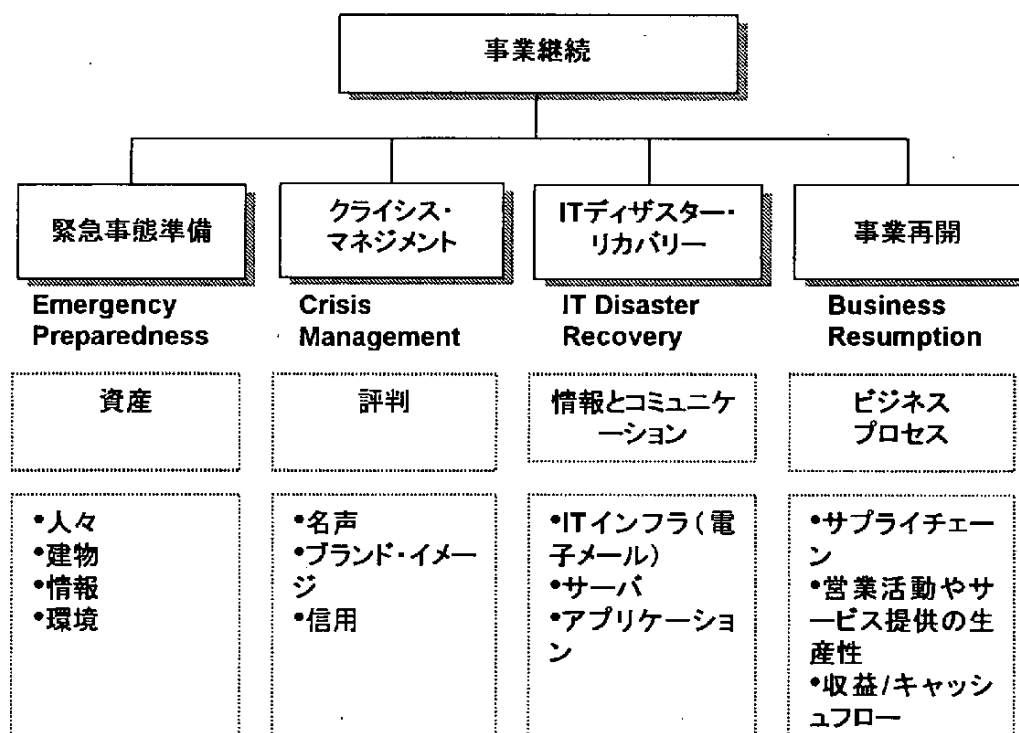


図 9 事業継続の構成要素(事例)

緊急事態準備は、事象発生直後に起動し数時間という短いタイムスパンで行う現場対応のための計画策定などの準備を中心とした活動である。直近では、周辺で有害化学物質に関連する事故が発生した際に、従業員をすみやかに建物内に

収容する「Shelter-in-place」という計画を新たに策定したということであった。

クライシス・マネジメントは、主に経営層がトップレベルの意思決定やマスメディアへの対応を検討し実施するなど、会社としての事業継続に深刻な影響を与える事件や事故が発生した際に必要となる活動である。緊急事態準備が主に現場レベルの対応を所管するのに対して、会社全体に影響を与えるような問題を取り扱う。

IT ディザスター・リカバリーは、事業継続の技術的側面を担当する。重要な事業プロセスが依存する IT アプリケーションやインフラ・サービスに関する計画を策定しテストを行う。

事業再開（ビジネス・リザンプション）は、事業プロセスを分析し、再開に向けて必要な計画を策定するもので、図 10 に示すステップを踏んで行われる。

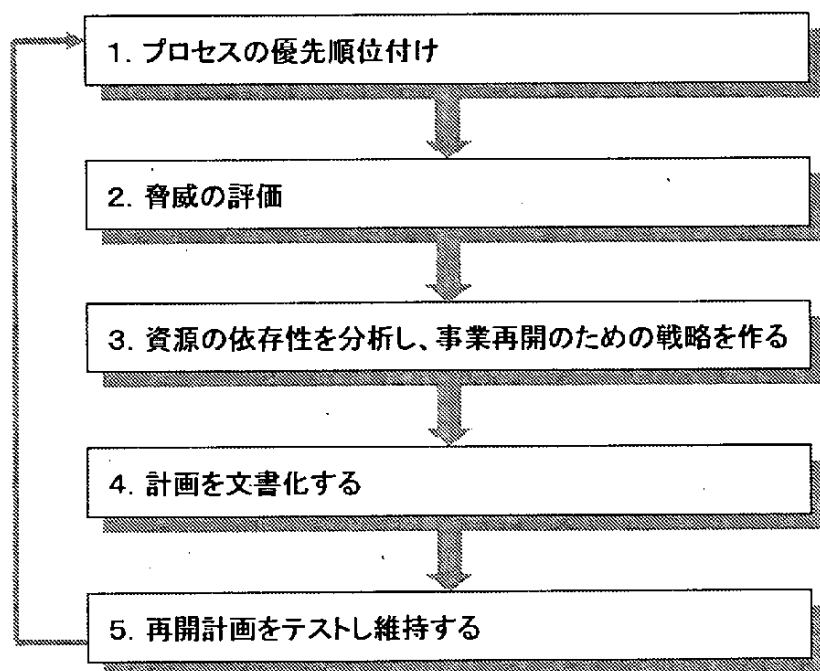


図 10 事業再開（ビジネス・リザンプション）の各ステップ

事業継続の担当者は、平常時、これらの構成要素の相互調整と統制を行っている。統制活動では、トラッキング・システムを導入し、個々の活動が計画通りに実施されているかが把握できるようになっている。

重要な情報資産は、事業再開計画を策定する中で実施されるヒアリングにおいて特定される。事業プロセスの一部としての情報管理を洗い出す過程で使用されている文書などが明らかになる。その分析中に特定される資産の中に重要であればバイタル・レコードとして位置付けられるということであった。

4 事業継続に必要なスキルと人材

4.1 人材・プロフェッショナル育成の重要性

ここでは、事業継続管理体制に必要なプロフェッショナル人材の要件について考えてみたい。まず、現存する事業継続管理関連の資格は主に英国 BCI (Business Continuity Institute²⁵) と米国 DRII (Disaster Recovery Institute International²⁶) のふたつであるが、これらは個人に与えられるプロフェッショナル資格である。一方、事業継続管理関連のガイドラインや ISO などの標準化の動向に目をやると、こちらは企業や自治体などの組織が遵守・導入するものである。また、個人が取得する BCI、DRII の資格は、フレームワーク（枠組み）を理解・習得しているということよりも、手順・手続きに精通していることを求められ、事業継続管理を実践するコア人材として期待される。

事業継続マネジメント体制の構築には、もちろん組織が何らかのフレームワークを導入し、社内の手順や手続きを制定する必要があるが、それを実行するプロフェッショナル人材が不可欠であることは言うまでもない。このような人材は、社内外の過去の事故・障害事例や各部門や業界団体で記録・分析しているインシデント関連統計データなどを積上げた事業継続計画策定のアプローチ（ボトムアップ）と、重要業務の選定、複数箇所における複合事故・障害の同時・連鎖発生を想定したシナリオに基づくアプローチ（トップダウン）を、確かな知識と経験によって調整することも求められている。

4.2 英国 BCI の資格概要

事業継続管理に関する実務経験の専門性と従事期間の長さ、及び後述の 10 のスキル・セット分野の経験範囲により、Fellow・Member・Specialist・Associate・Affiliate・Student・Corporate Partner にランクづけされる。職場での評価や実務経験の査定なども行われ、Fellow については面談も行われる。会員は事業継続管理に関する専門家どうしの情報交換や、研修・トレーニングといった啓発の機会、また会員向けの詳細情報を得る機会を提供される²⁷（図 11）。

²⁵ 1994 年設立の非営利団体。詳しくは <http://www.thebci.org/> 参照。PAS 56 の原案を BSI (British Standard Institute: 英国規格協会) と共同で作成。

²⁶ NFPA 1600 の現行版に関与、また金融関係当局検査のマニュアルである FFIEC も DRII の手順を参照している。DRII の詳細は <http://www.drii.org/> 参照。

²⁷ 詳細は <http://www.thebci.org/membershipcriteria.htm> 参照。BCM 関連人材に特化した求人情報も得ることができる。

Category	Summary	Experience	References	Competence in BCI Standards	Entry Method
ABCP	Associate Business Continuity Professional	2 years of business continuity management experience	BCI Standards, BCI Handbook, BCI Journal, BCI News, BCI Website	BCI Standards, BCI Handbook, BCI Journal, BCI News, BCI Website	Submit an application form
CFCP	Certified Functional Continuity Professional	3 years of business continuity management experience	BCI Standards, BCI Handbook, BCI Journal, BCI News, BCI Website	BCI Standards, BCI Handbook, BCI Journal, BCI News, BCI Website	Submit an application form
CBCP	Certified Business Continuity Professional	5 years of business continuity management experience	BCI Standards, BCI Handbook, BCI Journal, BCI News, BCI Website	BCI Standards, BCI Handbook, BCI Journal, BCI News, BCI Website	Submit an application form
MBCP	Master Business Continuity Professional	7 years of business continuity management experience	BCI Standards, BCI Handbook, BCI Journal, BCI News, BCI Website	BCI Standards, BCI Handbook, BCI Journal, BCI News, BCI Website	Submit an application form
APPLICANT	Applicant	None	None	None	Submit an application form
STUDENT	Student	None	None	None	Submit an application form
COMPANION	Director and senior staff of organizations subscribing to the BCI aims.	Professional interest in BCI	None required	Not relevant	Nomination to membership by existing BCI member
CORPORATE PARTNER	Organizations subscribing to the BCI aims.	Not applicable, but must demonstrate or declare support for BCI aims	None required	Not relevant	Submit an application form

(<http://www.thebci.org> より)

図 11 BCI の会員資格レベル

4.3 米国 DRII の資格概要

BCI の資格と大きく異なるのは、資格試験を課すことである。研修・トレーニングを受講して受験するが、その専門度合いや専門領域によって資格がレベル分けされている。ここでも 10 のスキル・セット分野が基準となるが、これは BCI と共有されているものである (図 12)。

- ① ABCP: Associate Business Continuity Professional
実務経験 2 年以内の初任者。試験のみ。
- ② CFCP: Certified Functional Continuity Professional
3 つ以上の専門分野で 2 年以上の事業継続管理実務経験が必要。試験と評価委員会の審査が必要。
- ③ CBCP: Certified Business Continuity Professional
5 つ以上の専門分野で 2 年以上の事業継続管理実務経験、試験と評価委員会の審査が必要。
- ④ MBCP: Master Business Continuity Professional
7 つ以上の専門分野で 5 年以上の事業継続管理実務経験。試験と評価委員会の審査が必要。

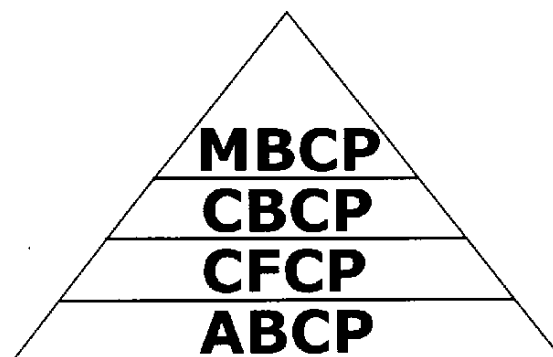


図 12 DRII の資格階層

4.4 事業継続管理に必要なスキル・セット分野

ここでは、英国 BCI と米国 DRII で共有されている、事業継続管理に必要なスキル・セット分野について簡単に解説する。

① **Initiation and Management** (事業継続管理の始動とマネジメント)

事業継続計画の立案に際し、脆弱性の抽出、及び想定事象に関する対応・リカバリー的能力、継続オペレーションに必要な経営資源配賦にかかわる選択肢の提示などを、重要な機能として提供できること。

② **Business Impact Analysis** (ビジネス影響度分析：BIA)

事業継続を脅かす諸要因のビジネス・オペレーション上の影響について定量的・定性的な分析・評価が行えること。またその過程において、強化対策の優先度の高い業務オペレーションの特定、更に RTO (Recovery Time Objective：復旧目標時間) 設定などが実施できること。

③ **Risk Evaluation and Control** (リスク評価とコントロール)

事業継続を脅かす諸要因について分析を行うと同時に、リスク対応策や選択肢に係る経済性分析が遂行できること。

④ **Developing Business Continuity Management Strategies** (事業継続マネジメントに係る戦略立案)

事業継続管理に係る戦略立案において、RTO、RPO (Recovery Point

Objective : 復旧時点目標) を設定、重要オペレーションのレジリエンス確保に貢献すること。

- ⑤ **Emergency Response and Operations** (危機対応と緊急措置の運用)
障害発生時とその後の復旧プロセスにおける段取りを、危機対応センターを中心とした体制で運用できるよう手配できること。
- ⑥ **Developing and Implementing Business Continuity and Crisis Managements Plans** (事業継続と危機管理に関する計画の策定と導入)
事業継続計画及び危機対応計画の立案、導入、定着を支援し、RTOの達成確保を確実にできること。
- ⑦ **Awareness and Training Programmes** (啓発とトレーニングのプログラム)
事業継続管理の社内浸透・定着のための研修や諸プログラムについて支援が行えること。
- ⑧ **Maintaining and Exercising Business Continuity and Crisis Managements Plans** (事業継続と危機管理に関する計画の更新と訓練の実施)
事業継続計画の実効性を確保するための訓練の計画・実施に際し、必要となる機器・ファシリティの手配を行い、訓練後のフィードバックに対して必要な体制・組織の更改や新規導入の手配ができること。
- ⑨ **Crisis Communications** (危機広報)
社内のみならず顧客も含めたステークホルダー(株主、ベンダー、納入業者、地域など)とのコミュニケーションを確実にし、事業継続計画や災害復旧計画(DRP: Disaster Recovery Plan)の発動を確実にすること。
- ⑩ **Co-ordination with External Agencies** (行政機関との調整)
監督当局や地方自治体などの行政とのコミュニケーション確保を通じて、事業継続管理を確実にするための側面支援を得たり、コンプライアンス上の不必要な瑕疵発生を回避することに貢献できること。

以上、いずれの分野も事業継続マネジメント体制の実効性を高めるには必要な専門分野であり、これに沿ってBCI、DRIIはそれぞれのアプローチでプロフェッショナル人材育成を推進している。日本からの資格取得者はまだ少ないよう

だが、外資系金融機関²⁸やコンサルティング会社を中心に増加しつつあるようである。

4.5 事業継続に係る職種

参考までに、事業継続管理関連の求人情報から具体的な職種をピックアップし、下記に例示した。

① Business Continuity Relationship Manager

事業継続に係るポリシーや戦略立案、事業継続技術マネージャ及び、危機対応マネージャの支援、顧客対応を担当。

② Business Continuity Technology Manager

事業継続に必要な情報システムリスクのマネジメント及び、事業継続や危機対応に必要な技術の導入・手配を行う。

③ IT Continuity Analyst

情報システム関連資産の統合分析や事業継続のための脆弱性分析を行い、対応策を発案する。

④ Disaster Recovery Coordinator

業務機能レベルのリスク分析を行い脆弱性を抽出、災害復旧における選択肢の提示やリスクマネジメントの戦略を立案する。現場のラインマネージャに権限を委譲した上で、コーディネーターがその間をコントロールするという場合に設置される。

⑤ BCM Auditor

事業継続管理に係る体制や実務について監査を実施する。

4.6 事業継続に必要なスキルと人材

以上、事業継続管理の体制構築・運用に必要なスキル・セットの議論を展開したが、最後に事業継続マネジメント全体に係る今後の課題における重要性としてとりまとめを行う。

4.6.1 事業継続管理体制構築におけるプロフェッショナル人材育成

事業継続管理の分野で必要なスキル・能力を大きく事業継続計画力と事業継

²⁸ 本国を中心にグローバルでBCM体制を統一しようという意向は、特に9・11（米国同時多発テロ）以降、強まっている。その一環として在日オフィスにも専門人材を配備、もしくは内製化に着手している。

続実行力に大別すると、事業継続計画力のうち基礎的な部分は組織内のそれぞれの持ち場の状況を勘案して計画できる能力に加え、組織全体やサプライ・チェーン、業界、地域といった組織外との調整できる専門資格が要求されるようなレベルが設定できる。一方、事業継続実行力については、訓練・ドリルなどで所謂「身体で覚える」レベルから事業継続が脅かされるような事態を直接経験したり、また間接的にシミュレーションや知識習得により体感することでより高いレベルの実行力を保持することができる。

図 13 ではこのような分類の中で、組織において事業継続管理のプロフェッショナル育成を中心にした事業継続管理体制構築のアプローチを例示した。

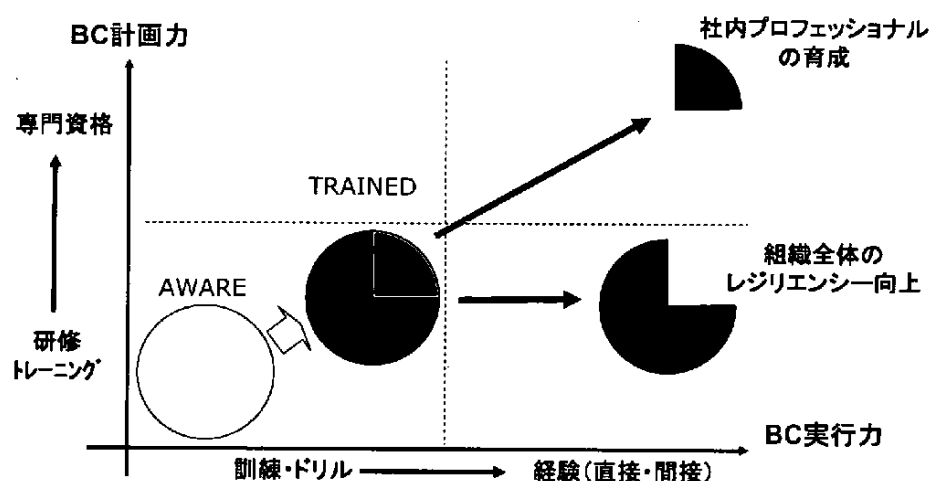


図 13 プロフェッショナル育成を中心としてアプローチの例示

(1) 第1段階

まず組織全体で研修・トレーニングを行うことで、事業継続計画力の基礎を定着させ、事業継続実行力においては訓練・ドリルの実施により、体感させることを開始する。欧米では Awareness Program と称して、とにかく組織内の人間に事業継続管理の重要性や各持ち場での対応について何らかの“気づき”をもたらすことを目的に普及・啓発活動を展開することが多い。この段階で組織全体が“AWAERE（気づいている状態）”になる。この段階では、必要に応じて外部の専門家やコンサルタントの助けを得ることが効果的な場合もある。

(2) 第2段階

“AWARE”の状態から引続き事業継続計画力向上のための研修・トレーニング、事業継続実行力向上のための訓練・ドリルを重ねてゆくと、組織の状態は“TRAINED（訓練された状態）”になる。この段階で、組織内に事業継続管理を率先するに値する資質とセンスを持ち合わせたような人材が浮上してきた場合、その人材を抽出し、人事・評価体系の調整や本人のキャリア・プラン策定も含めて組織内専門家育成の検討をすべきである。その背景には、国内外の多くの先進事例から事業継続管理の推進には属人的な資質・スキル（事業継続管理責任者がどの位リスクマネジメントに対してのセンスがあり、また、実際の災害復旧などの経験を持ち合わせているかなど²⁹⁾）が不可欠であり、通常の企業経営に必要とされるスキルとは異なる、あるいは既存の経営陣がそれを持ち合わせていないことが多いという現実がある。

(3) 第3段階

その後、専門家育成要員として抽出された人材は、前述の専門資格を取得させたり、業界団体などの外部との交流を推奨することでより専門性を高めると同時に、組織内の事業継続管理に関わる戦略立案、研修・トレーニングの計画・実施、訓練・ドリルの計画・実施などを、ひとつのマネジメント・サイクルとして率先して回る中心人物と位置付けられる。一方、組織全体については、引続き研修・トレーニング、訓練・ドリルを続けることで、事業継続実行力をより高いレベルで向上させることができる。その際の重要なポイントは、組織内で発生した事業中断の事例やニアミスの分析に積極的に取り組み、また、他組織で発生したような事例であっても「他山の石」として自らのBIAに反映してみる、といった柔軟な体制が不可欠であるということである。

4.6.2 今後の事業継続の課題における人材育成

ビジネス・コミュニティにおける事業継続管理体制の共有化には、共通の方

²⁹⁾ 欧米でも初期段階ではBCM担当者は軍隊経験者が多いような時期もあったが、最近では企業経営活動の一環として、必ずしもそうではない。要は、いかにリスクに対する感応度が高く、その影響度を幅広く想定でき、また、様々な経験を直接・間接的にすることでノウハウとして心身に持ち合わせているような人材である。

法論導入や標準化が多大な貢献をすることは間違いなく、共通言語として社外とコミュニケーションできるプロフェッショナル人材とその人的ネットワーク³⁰が必要となる。

このような専門家ネットワークが構築された場合、図 14 に見られるような相乗的なメリットも期待できる。

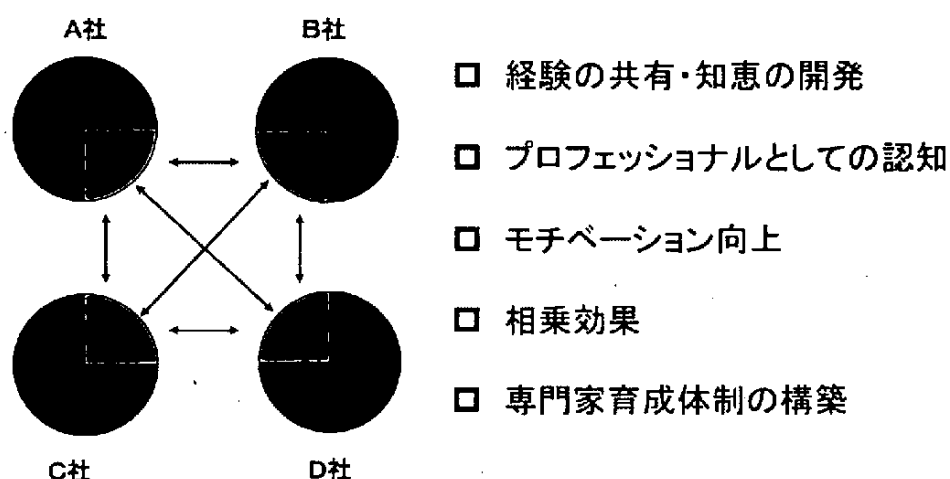


図 14 専門家ネットワークの効用

事業継続管理に係るプロフェッショナル人材育成の重要性を確認したが、実際の育成プロセスは企業単体では限界があり、かつ偏りが生ずる可能性も否めないことから、可搬性（portability）のある客観的な資格³¹として位置付けることを行政や業界団体が早急に検討すべきタイミングにきているといえよう。

³⁰ 弁護士、医師、研究者といったプロフェッショナルは所属する組織（事務所、病院、大学など）を超えた形態のネットワーク（例えば弁護士会、医師会、学会などに加え個人的な繋がり）を持っている。

³¹ 先の弁護士、医師などと同様。

5 重要な情報資産の保護

5.1 バイタル・レコードの概念

ここでは、事業継続と情報資産保護の関連性の視点から、様々な規格やガイドラインで取り上げられているバイタル・レコードを中心にまとめた。

5.1.1 バイタル・レコードの定義

バイタル・レコードは、一般的に「組織の事業を継続するために必要不可欠な記録」のことをいう。各規格やガイドラインにより、定義は少しずつ異なるが、ここでは、ARMA(Association of Information Management Professionals)とANSI(American National Standards Institute)により2003年3月17日に発行された規格「ANSI/ARMA 5-2003; Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records」における定義を参照する(表4)。

表4 ANSI/ARMA 5-2003におけるバイタル・レコードの定義

バイタル・レコード
バイタル・レコードは、組織が機能するために欠かせない基盤である。バイタル・レコードの中には、危機的状況において、もしくは危機発生直後において、組織が業務を継続するか生き残るために重要な情報を含まれている。そのような記録は、異常事態においても遅れることなく業務を継続するために必要なものである。それは、組織の法的および財務の状況を再構築するために必要な情報や、従業員、顧客、投資家、市民を含むステークホルダーの権利と義務を保護するための情報を含む。 ある種のバイタル・レコードは、唯一つしかないものであったり、容易に再生できないものであるかもしれない。また、再生や取替えに、かなりのコストがかかるものであるかも知れない。そういったものは、証拠として要求される事項に合致したり、満足したりするために、オリジナルな形式であることを要求されるかも知れない。記録の中で、重要なビジネスプロセスを支援したり、上記した要求事項を満たしたりする限りにおいてのみ、バイタルと分類されるべきである。また、役割を完了した後は、再分類されるべきである。

(注: 筆者訳)

この定義から、バイタル・レコードとして分類される情報は、次のような要件を満たすものであるといえる。

◆ 内容に関する側面

- 危機的な状況や危機発生直後に必要な情報
- 法的に要求されている情報
- 財務に係る情報
- ステークホルダーの権利と義務を保護するために必要な情報

◆ 代替可能性

- 唯一つしかないもの
- 容易に再生できないもの
- 再生や取替えに、かなりのコストがかかるもの

◆ 形態

- オリジナルな形式、つまり改ざんなどの行為により元の内容から変更されていない正式な文書であること

5.1.2 記録、文書、および情報、データ

ARMA の定義に基づくと、バイタル・レコードには、事業継続において重要視されているのは、改ざんすることができない正式な文書という概念が含まれる。しかしながら、記録（レコード）と文書との違い、さらには情報との関係については、まだ必ずしも議論が集約されているとはいえない。

ここでは、これらの捉え方について言及しているいくつかの規格やガイドラインなどを紹介する。

(1) ISO15489-1:2001(JIS X 0902-1:2005)

記録（レコード）と文書の違いについて、参照すべき国際規格として、ISO15489-1:2001(JIS X 0902-1:2005)「情報及びドキュメンテーション—記録管理—第1部：総説」がある。ISO15489-1:2001では、「記録」、「情報」および「記録管理」について、それぞれ次のように定義している。

文書(document)

一つの単位として取り扱われる記録された情報、又はオブジェクト。

記録(records)

法的な責任の履行、又は業務処理における、証拠及び情報として、組織、又は個人が作成、取得及び維持する情報。

記録管理(records management)

記録の作成、取得、維持、利用、及び処分の効率的で体系的な統制に責任を持つ管理の分野であって、記録の形で業務活動及び処理に関する証拠及び情報を取り込み、維持するためのプロセスを含む。

参考 記録管理(records management)の管理対象は、記録(records)であるが、我が国で一般に使われている文書管理は、記録(records)のほかに文書(documents)をも管理対象としており、その範囲が広い。

ISO15489-1:2001 は、2001 年の制定から約 5 年を経過し、改訂に向けての検討が進められている。

また、記録(records)について ARMA 東京支部では、次のように説明している。

…文書は情報の集合であり、物理的実体として、アナログ(本、羊皮紙、楽譜、マイクロフィルムなど)か、デジタル(ワープロで作成のファイルのような)となり得る。文書と記録の重要な違いは、記録はビジネス取引・活動の証拠となり、法律や規定を満たしていることを説明(アカウンタビリティ)できなければならない…³²。

(2) 記録管理学会

1989 年に設立された記録管理学会の「記録管理と記録管理学会の Q&A」では、「記録管理」および「記録管理と文書管理の関係」について、次のような説明がなされている³³。

³² http://www.arma-tokyo.org/about_arma.htm

³³ <http://www.soc.nii.ac.jp/rmsj/qanda/qanda.html>

Q 1 : 記録管理とはどのようなものですか

A) 企業・行政機関などの組織が活動を行う上で、様々な「記録」(文書など)が作成されます。「記録管理」とはその記録の作成から組織化、活用、保管、最終処置(永久保管・廃棄)までのライフサイクルを対象とした統合的な管理をいいます。

Q 2 : 記録管理と文書管理とは同じものですか

A) 日本では「記録」と「文書」とが厳密に使い分けられていないため、記録管理と文書管理はほぼ同義語として使われています。一方、欧米では「記録」(Records)と「文書」(Document)は厳密に区別されていますので、「記録管理」(Records Management)と「文書管理」(Document Management)とは別のものです。

「文書」と「記録」のもっとも大きな違いは、文書が単なる記録化された情報であるのに対し、記録は法的な義務の履行又は業務処理の証拠として作成保存されるもので、記録は基本的に修正・変更をしてはならないという原則がある点です。「文書」 $\geq$ 「記録」の関係があり、一般的な文書の内、記録管理システム(Recordkeeping System)に組込まれたもののみが記録です。

(3) JIS Z 6016

e-文書法³⁴とも関連する JIS X 6016: 2003「紙文書及びマイクロフィルム文書の電子化プロセス」においては、「文書」及び「電子文書」、「電子化文書」は次のように定義されている。

文書

人の意思を文字その他の記号、画像などの手段で紙、マイクロフィルム、磁気テープ、光ディスク、磁気ディスクなどに記録したもの。
磁気テープ、光ディスク、磁気ディスクなどは、電磁的記録媒体とい

³⁴「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」と「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」の2法を総称して、「e-文書法」と呼ぶ。平成17年4月1日から施行されている。

「e-文書法」は民間事業者等に対して法令で課せられている書面(紙)による保存等に代わり、電磁的記録による保存等を行うことを容認する法律となっている。

(<http://www.kantei.go.jp/jp/singi/it2/others/e-bunsyu.html>)

い、電磁的記録とは、電子的方式、磁気的方式など、人の知覚によっては認識することができない方式で作られる記録をいう。

電子文書

ワードプロセッサ、PC（パーソナルコンピュータ）上のソフトなどで作成されたコードデータで構成されたもの。

電子化文書

紙文書又はマイクロフィルム文書を電子画像（ビットマップ）化した文書。

(4) DIRKS（オーストラリア）

オーストラリア公文書館 NAA（National Archives of Australia）が公開している DIRKS（Designing and Implementing Recordkeeping Systems）は、オーストラリアの公文書記録管理に関する方法論である。この DIRKS には、記録（Records）と情報について、次のような説明がある³⁵。

…記録は、情報の部分集合である。情報は、論文、雑誌、新聞、科学技術文献、および収集データのような発表、および未発表の文書を含む。情報は、組織の知識基盤に貢献し、目標の達成を支援する。そのような情報は、事業活動に関連して収集されるかもしれないし、事業活動を支援するかも知れないが、それ自身は、活動の証拠を提供しない。…

(5) まとめ

これまで紹介してきた定義などをもとに、記録、文書、情報、さらにデータの間関係を整理する。本報告書の冒頭でも述べたように、A.M.マクドノウの定義によると、「情報とは、特定の状況における価値が評価されたデータ」とされている³⁶。企業活動において使われるデータは、その意味において、すべて情報を言うてよいであろう。その中で、記録化された情報が文書といえる。さらに、文書の中で、活動の証拠を提供する情報が記録として位置付けられる。ただし、記録管理学会

³⁵ DIRKS methodology – users guide

(<http://www.naa.gov.au/recordkeeping/dirks/dirksman/part1.html#fn2>)

³⁶ 経営情報システム、島田達巳・高原康彦、日科技連、2003年

の Q&A の Q2 でも説明されていたように、わが国では、記録と文書が欧米のように明確に区別されて使われていないのが実態である。

バイタル・レコードは、「組織の事業を継続するために必要不可欠な記録」として、事業継続の文脈において定義される記録である。「はじめて学ぶ文書管理 レコードマネジメント入門」において、その関係がよく説明されている。なお、バイタル・レコードは、基幹文書と表記している³⁷。

基幹文書は災害を念頭においている。この災害は、米国における基幹文書の保護の実情を見ると主として天災に目を向けている。「天災から保護する文書はそのまま人災から保護する文書ともなる。だがその逆は成り立たない」(Benedon[1988:208])

また、同書でも触れているが、バイタル・レコードは、文書全体の 1~2%とされている。

次項において、個々の規格でバイタル・レコードがどのように定義されているかをさらに詳しく紹介する。

5.2 事業継続関連規格等におけるバイタル・レコード

事業継続に関する国際規格やガイドラインを中心に、バイタル・レコードがどのように取り上げられているかをまとめる。

5.2.1 NFPA1600

米国防火協会 (National Fire Protection Association) が発行した『NFPA1600 Standard on Disaster/Emergency Management and Business Continuity Programs 2004 Edition』では、Chapter5 Program Elements (プログラムの内容) の 5.7.2 Plans (計画) の一項目として、A5.7.2.5 に、「事業継続計画に含めることを検討すべき特定領域」があり、選定すべき項目の一つとしてバイタル・レコードを、含めている。

バイタル・レコードは、次のように説明されている。

³⁷ 「はじめて学ぶ文書管理 レコードマネジメント入門」 門倉百合子 編著 ミネルヴァ書房

「バイタル・レコード: 例えば、財務情報、個人情報、エンジニアリング図面などの実在のバイタル・レコードを保護する媒体に応じた対策を選択する。バイタル・レコードは災害や緊急事態の間は、利用可能である必要がある。そしてその権利と利益を保護しなければならない。」(注: 筆者訳)

5.2.2 PAS56 および BCI ガイドライン

英国規格協会 (BSI: British Standards Institution) による『PAS56 事業継続管理のための指針 (PAS56: Guide to Business Continuity Management)』では、まず「2 用語と定義」において、バイタル・レコードを次のように定義している。

バイタル・レコード (2.44 項で規定)

組織の事業を継続するために必要不可欠な記録 (全ての媒体)

(注: 筆者訳)

さらに、バイタル・レコードは、ビジネスインパクト分析 (BIA) を実施した成果として、特定され、文書化されることが望ましいとしている(6.2.3 項で規定)。

また、PAS56 の元となった「The Business Continuity Institute」作成の『BUSINESS CONTINUITY MANAGEMENT GOOD PRACTICE GUIDELINES (2005)』では、「組織内の各事業機能が活動を継続または再開できるようにする資源要件のひとつ」とし、「バイタル・レコードとデータが最新であること (目標復旧ポイント)」を要求している。

5.2.3 TR19 (シンガポール)

TR19 事業継続管理のためのテクニカル・リファレンス (Technical Reference for Business Continuity Management) は、SARS の発生をきっかけとして、事業継続の重要性を認識し、貿易産業省 (Ministry of Trade and Industry) の傘下にある規格・生産性・革新庁 (SPRING: Standards, Productivity

and Innovation Board) が作成した。

TR19 では、バイタル・レコードを次のように定義している。

バイタル・レコード (2.44 で規定)

組織の事業運営を維持、継続、再構築し、組織や従業員や顧客やステークホルダーの権利を守るために必須である、電子化もしくは紙面上の記録。

さらに「4.3.5 バイタル・レコード」では、「重要なビジネス機能(クリティカル・ビジネス・ファンクション)を支援するために必要なバイタル・レコードを識別、分類し、優先順位を決定するプロセスを確立しなければならない」としている。

バイタル・レコードの識別のために、「説明」や「所有者」など、いくつかの要素を含めなければならないとする。また、バイタル・レコードの分類や優先順位を決定する際に考慮する要素、たとえば、「失われた情報を再構築するために要する時間」などを例として提示している。

「6.3.9 インベントリーリスト」では、「処理を再開するために必要な重要資源およびバイタル・レコードのインベントリーリストを作成し、常に最新の状態に更新し続けなければならない。」としている。

5.2.4 米連邦危機管理庁におけるバイタル・レコード

元来、文書管理や記録管理は、公文書の保管と維持のノウハウとして発展してきた。したがって、政府組織など公共機関におけるバイタル・レコードに関する規程やガイドラインは多い³⁸。近年の危機管理意識の高まりや IT 化による文書や記録の形式変化などもあり、これらも見直しが行われているようである。

ここでは、米国の政府機関である連邦危機管理庁(FEMA: Federal Emergency Management Agency)が 2004 年 6 月に発行した、連邦政府機関が実施する業務継続 (COOP: Continuity of Operation Plans) についてのガイドライン「FPC65 FEDERAL EXECUTIVE BRANCH CONTINUITY OF OPERATIONS³⁹」を紹介する。

³⁸ カナダのアルバータ州が 2005 年 2 月に発行した「Vital Records Resources Guide」には、多くの資料が提示されている。公文書館や博物館、政府機関に関する資料が多いが、企業で実践する際にも参考になる。(http://www.im.gov.ab.ca/publications/pdf/VitalRecordsResGuide.pdf)

³⁹ FPC: Federal Preparedness Circular

FPC65 では、すべての機関の COOP 計画は、バイタル・レコードとデータベースについて、「電子及びハードコピーの文書、リファレンス、記録および情報システムが、特定され、保護され、使えるようになっていることが、実行可能な COOP 計画の重要な要素である」としている。必須の機能を果たすために記録やシステムにアクセスでき使えること、および保護し更新するための手順も必要であるとしている。最低限必要な記録として、「緊急時のオペレーティング・レコード」と「法律及び財務関連のレコード」を提示している。

FPC65 の「付録 G・バイタル・ファイル、レコードおよびデータベース」は、11 項目に渡り、取り組むべきことが詳細に記載されている（表 5）。

表 5 付録 G・バイタル・ファイル、レコードおよびデータベースの 11 項目（要約）

1. 組織内に、バイタル・レコード・プログラムに関する仕組みや責任を確立すること。（目的や適用範囲の特定、役割と責任の割当て、訓練の実施、定期的なレビューとテストなど）
2. バイタル・レコードへアクセスするための適切な媒体の確立。COOP 計画が動き出した 12 時間以内に代替施設で LAN、バイタル・電子・レコード、重要な情報システムとデータ、内部と外部の電子メールとアーカイブ、バイタル・ハード・コピー・データにアクセスできること。
3. 「緊急時のオペレーティング・レコード」と「法律及び財務関連のレコード」において特定された記録の完全な目録を維持管理すること。
4. リスクアセスメントの実施。
5. バイタル・レコードの適切な保護方法の選定。
6. バイタル・レコードを常に最新情報にするための定期的な更新手続き。
7. 記録が損傷した場合に復旧を支援する専門家やベンダーの特定。
8. バイタル・レコード計画の開発と維持。
9. バイタル・レコード・プログラムに参加するすべての人員に対する訓練プログラムの開発。
10. バイタル・レコード・プログラムの定期的なレビュー。
11. 機密および非機密のバイタル・レコードとデータベースを保護し、かつ代替施設からアクセスできる能力を半年ごとにテストしなければならない。

（注：筆者訳）

バイタル・レコードとデータベースには次のような表の活用を例示している（表 6）。

表 6 バイタル・ファイル、レコードおよびデータベース

バイタル・ファイル、レコードまたはデータベース	レコードの形式(ハードコピー、電子)	代替施設に準備済みか	代替施設に持ち込むか	保管場所	メンテナンスの頻度
		☐	☐		
		☐	☐		
		☐	☐		
		☐	☐		

なお、COOP の実施状況について、FEMA は 2004 年に 40 以上の政府機関について、テロ攻撃の際のシミュレーションをベースに、「Forward Challenge 04」というテストと評価を実施している。評価の対象として 5 項目を設定したが、その内のひとつは、「代替施設から、通常のオペレーションを実施するために必要なバイタル・レコードに、アクセスする能力を示すこと」であった。

FEMA はまた、官民連携 (PPP: Public-Private Partnership) として、あらゆる規模の企業向けの緊急事態準備計画、対応及び復旧にむけてのステップ・バイ・ステップのアプローチである「事業と産業のための緊急時マネジメントガイド」を公表している⁴⁰。

同ガイドにおける「記録保護」の項では、次のようなバイタル・レコードが、例示されている。

- 財務および保険情報
- 技術計画及び図面
- 製品リスト及び仕様
- 従業員、顧客および供給者データベース
- 書式及び営業秘密
- 人事ファイル

また、バイタル・レコードは、業務の早期回復に必須であるとし、その分析は、次の事項を含むとしている。

⁴⁰ <http://www.fema.gov/library/biz2.shtm>

- 機能分野により業務を分類する。たとえば、財務、生産、販売、管理業務など。
- 業務の再開と遂行を維持するために必須の機能を定義する。たとえば、財務、生産、販売、など。
- 必須の機能を果たすためにすぐにアクセスできるようにしておかなければならない最小限の情報を特定する。たとえば、顧客からの集金を維持するには、勘定書にアクセスできる必要があるかもしれない。
- 必須の情報を含む記録とそれがどこにあるかを特定する。
- 情報にアクセスし、活用するために必要な機器や材料を特定する

バイタル・レコードを保護しアクセスするための手順を確立する。数多いアプローチの中で次のような事項が例示されている。

- バイタル・レコードをラベリングする。
- コンピュータ・システムをバックアップする。
- 記録のコピーを作る。
- 隔離した容器にテープとディスクを保管する。
- 施設に影響を与える事象により損害を受けないオフサイトにデータを保管する。
- コンピュータ施設のセキュリティを強化する。
- バックアップ施設への記録の避難をアレンジする。
- サービス部が担当するシステムをバックアップする。
- バックアップ電源のアレンジをする。

(注: 筆者訳)

5.2.5 米国土安全保障省の「重要な記録」

また、小規模企業における事業継続計画策定の普及を目的として、米国土安全保障省(DHS: Department of Homeland Security)が提供している「Every Business Should Have A Plan」にも、「重要な記録 (important records)」について、次のような記述がある。

- 防水性があり、防火性のある持ち運び可能な容器に、以下のよう

な、重要な記録の複写を保存しなさい。

- 地図、
- 建築計画、
- 保険証書、
- 雇用契約書、
- 身分証、
- 銀行の口座記録、
- 取引契約リスト、
- コンピュータ・バックアップ、
- 緊急時または法的に要求されている
- 契約関連情報、
- その他の優先度が高い文書、など

- 複写した一連の文書は、離れた場所に保管しなさい

(注: 筆者訳)

5.2.6 経済産業省の事業継続計画策定ガイドライン

わが国でも事業継続関連のガイドラインが公表されており、その中でバイタル・レコードについて言及している。

経済産業省が、2005年3月に公表した「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;事業継続計画策定ガイドライン」では、「3.4. 業務再開フェーズにおける対応のポイント(3) 物的資源の確保」に次のような記述がある。

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。

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。

5.2.7 内閣府の事業継続ガイドライン

内閣府が 2005 年 8 月に公表した「事業継続ガイドライン 第一版— わが国企業の減災と災害対応の向上のために」では、「2.2.4 重要な要素の抽出」などに、次のような記述がある。

重要業務が受ける被害の想定に基づき、そこが復旧しない限り生産の再開や業務復旧ができない主要な生産設備や情報などの資源を、重要な要素（復旧時間が一番長いクリティカルパス、あるいは生産量を限定させてしまうボトルネックなど）として把握する。

対応策の基本的事項を例示すると以下のとおり。

□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）のバックアップを行う。

※バイタル・レコードには、設計図、見取図、品質管理資料等、災害時に直接的に必要な文書やコーポレートガバナンス・内部統制維持、法令遵守、説明責任確保のための文書、権利義務確定、債権債務確保のための文書等、間接的に必要な文書がある。

5.3 ARMA のバイタル・レコード・マネジメント

ARMA は、記録・情報管理に関わる専門家が、情報交換や研究を行う場として、1955 年に設立された非営利団体である。全世界 30 カ国、1 万人以上の会員が所属している。

ARMA のバイタル・レコードに関する定義は、本報告書の「5.1 バイタル・レコードの概念」でご紹介したとおりである。

5.3.1 ANSI/ARMA 5-2003 の全体構成

ANSI/ARMA 5-2003 は、企業などの組織によるバイタル・レコードの特定から管理について規定した規格である。全体は、表 7 に示す項目から構成されている。

表 7 ANSI/ARMA 5-2003 の全体構成

- 1 序論
- 2 引用規格
- 3 定義
- 4 バイタル・レコード・プログラム
- 5 バイタル・レコード・プログラムの責任
- 6 リスク・マネジメントプロセス
- 7 バイタル・レコードの特定
- 8 保護の手段
- 9 バイタル・レコード一覧表
- 10 バイタル・レコードマニュアル

Appendix A 記録分類例

Appendix B バイタル・レコード保護例・クラス 1

Appendix C リスクアセスメントデータ例

Appendix D 保管場所調査例

Appendix E バイタル・レコード・スケジュール例

Appendix F 水害により損傷した記録の復元

Appendix G 水害により損傷した本や記録のための乾燥技術

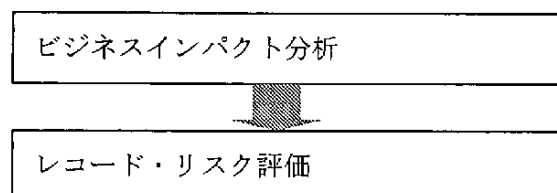
出典:『 ANSI/ARMA 5-2003 Vital Records Programs 』

※上記の引用は仮訳であり一部抜粋をしています。実際にプログラムを導入検討される際には英文の原本を参照下さい。

5.3.2 リスクアセスメント

保護すべきバイタル・レコードを特定する事前プロセスとしてリスクマネジメントを実施することとしている。

リスクマネジメント・プロセスは、次の項目から構成される (図 15)。



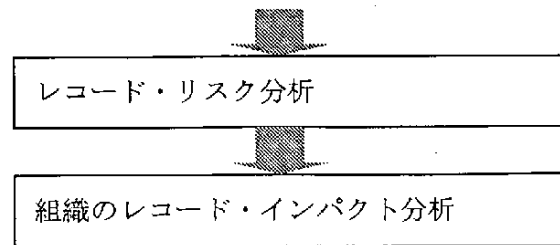


図 15 バイタル・レコードのリスクマネジメント

ビジネスインパクト分析は、バイタル・レコードプログラムの責任者や事業継続計画担当者、リスク・マネージャーなどにより実施される。個々のプロセスについて最低限の復旧時間、たとえば、復旧に関する契約や機器の購入に要する時間などに基づいて決める。

レコード・リスク評価は、火災や電子データの喪失といったリスク、台風や洪水などの脅威、機器による安全プログラムの欠如といった脆弱性などから、記録（レコード）や情報に関するリスクを評価する。

レコード・リスク分析は、記録（レコード）や情報の損壊によるリスクの大きさを起こりやすさと影響の大きさに基づき分析するもので、マトリクス形式の表が提示されている。

組織のレコード・インパクト分析は、負の影響が事業にあまりに大きくなりすぎない程度に抑えるように、ビジネスインパクト分析で特定した重要なビジネス機能の分析を行い、記録や情報の最大受容可能な損失の定義をするものである。

5.3.3 バイタル・レコードの特定と優先順位付け

特定され評価されたバイタル・レコードや情報に対して、必要な復旧時間などから優先順位を決め、適切な施策を講じる。それは、バイタル・レコード一覧表としてまとめられる。

記録は、「クラス1 バイタル・レコード」、「クラス2 重要なレコード」、「クラス3 有用なレコード」に分類される。

個々の分類の定義、該当する記録（レコード）、保護方法は、表 8 のように例示される。

表 8 記録(レコード)の各分類、該当する記録、保護方法の例

分類	定義	例	保護方法の例
クラス1: バイタル	これらの記録は危機に直面している時やその直後の組織の継続や存続に必須の情報を含む。それらは異常な状況のもとで猶予なしにオペレーションを継続するために必要である。それらは組織の法的そして財務的な状態を復元するために必要な情報を含む。そして従業員・顧客・投資家・市民を含むステークホルダーの権利と義務を保護するために必要な情報を含む (以下、省略)	請求書(債権・債務)	オフサイトのバックアップテープに保存
		顧客または得意客のファイル	バックアップテープとオフサイトのマイクロフィルムに保存
		調査資料	イメージングサーバーから遠隔地のデータベースへモデム経由で送信したバックアップファイル
		契約書や協定書	普及型の記録保管庫に格納された台帳と取引記録
クラス2: 重要	これらの記録はビジネスを継続するために必須のものである。これらは代替したり再生することができるが、多大な時間とコストを必要とする	未監査の財務記録	記録のオリジナルをオフサイトの保護された保管庫に転送し参照のためのコピーを持つ
		土地、建物、設備そして車の権利証	オフサイトに保管されたイメージメディアのバックアップ、定期的な分散保管
クラス3: 有用	これらの記録はビジネスの継続に役立つものである。それらは代替できるが、損失した場合一時的な不便をもたらす。	納税記録	定期的・計画的な分散保管
		銀行取引明細書	定期的な分散保管
		書簡	定期的な分散保管

出典『ANSI/ARMA 5-2003 Vital Records Programs』

※上記の引用は仮訳であり一部抜粋をしています。実際にプログラムを導入検討される際には英文の原本を参照下さい。

6 事業継続を支援する技術

本項では、情報資産保護の視点から、事業継続を支援する情報通信システム技術における最新の動向をまとめた。

事業を支える情報通信システムの中でも、基幹システムは、ホストコンピュータの時代から歴史的に災害対策が比較的進んでいる領域といえる。通常、データベースはデータセンターなどに集中しているので管理も行いやすい。後述するデータベースのバックアップサイトへのリモートコピーの仕組みなど復旧時点目標 (RPO) や復旧目標時間 (RTO) を短縮する仕組みが考案され、実際に大手企業などを始めとして導入が進んでいる。

しかし、基幹システム以外の情報資産についての災害対策は不十分なことが多い⁴¹。全社の重要な情報資産を特定し、最適化した情報資産保護の仕組みが存在する企業はまだ少ない。

したがって、多岐に渡る最新の関連技術動向の中から、ここでは、特に次の事項に焦点を絞ってまとめた。

- ストレージ・セントリック

企業内に点在するハードディスクなどの記憶媒体を集約し、情報資産を集中管理することを狙いとしたストレージ・セントリックという手法について記載する。

- 事業継続に関連するネットワークの動向

事業継続を考慮したシステム構成では、ストレージとネットワークは不可分の関係になりつつある。ここでは、次に記載するバックアップとリストアに関連するネットワークの動向について記載する。

- 事業継続のためのバックアップとリストア

上記2点を踏まえて、事業継続のための情報資産のバックアップとリストアの技術動向について記載する。

- 情報ライフサイクル管理

バックアップ運用を設計する際に、その情報の資産価値に応じた取得方法や媒体

⁴¹ 2001年9月11日の米国同時多発テロの事例では、「ほとんどの金融関連と大企業は、基幹システムリカバリープランに沿って、バックアップサイト又は、被害を受けた場所で修理、テストするなどして迅速に復帰させたようだ」が、「基幹システム以外の各部門のサーバーを再構築するには時間がかかったようだ」。 出典:『テロ事件とITシステム』 SRA America Newsletter

の選択が必要である。ここでは、その選択の際に参照すべき考え方として、TCO⁴²の削減と情報資産価値の最大化を目指した情報ライフサイクル管理（ILM:Information Lifecycle Management）というコンセプトについて記載する。

6.1 ストレージ・セントリック

今や情報資産の管理は経営課題となった⁴³。特に、情報資産の主要な媒体である紙と電子の両方について、適切かつ十分な管理を行うことが重要である。電子情報は複製が容易なため、個人のデスクトップ、部門サーバー、全社サーバーに無秩序に点在していることが多い。しかしながら、全社レベルで情報資産の所在を把握している企業は少ない。

1980年代後半から、オープンな技術を利用したクライアント・サーバーシステムが導入されはじめた。1990年代に入るとクライアント・サーバーシステムを利用したエンドユーザーコンピューティング（EUC）の全盛期となった。その当時は LAN の回線も細く、ましてや WAN となると最速でも数 MB 程度の帯域以下の利用が限界であった。部門内のシステム構築は EUC の流行と共に、物理的にエンドユーザーの近くにサーバーを配置してその数を増やした。

その結果、現在サーバーは点在し、運用・管理コストが増大している。例えば、製造業では生産管理や技術情報、人事や経理といったシステム単位にサーバーが存在し、それに伴いデータが点在していることが多い。

現状を概観すると、集中管理が比較的容易な「定型情報」⁴⁴に比べて、「非定型情報」は、圧倒的に量が多い。しかしながら、この「非定型情報」について、全社的な統制が取れていない状況にあるといえる。前述のとおり、情報は増加する一方であり、問題は深刻になりつつある。

2004年10月に起きた新潟県中越地震の際には、データ・センターで管理しているサーバーは比較的問題が少なかったが、拠点に分散していたサーバーは大きな損害を受けたといわれている。耐震ラックなどにサーバーを格納していたとしても、火災・水害等の二次災害や、被災直後にオフィスが所在している地区全

⁴² TCO:Total Cost of Ownership コンピュータシステムの導入、運用・管理などの費用の総額のこと。

⁴³ 「セキュアな情報資産の管理とガバナンスは、まさに経営、国家、社会の課題である」 出典:『情報化白書 2005 の概要』 2005 年 10 月 財団法人日本情報処理開発協会

⁴⁴ 一般的に、情報は「構造化（定型）情報」と「非構造化（非定型）情報」に大別される。「定型情報」は、基幹システムなどに整然と格納されており、その割合は情報全体の 20～30%が該当するといわれている。「非定型情報」は一般文書、電子メール、画像、音声、動画などであり 70～80%が該当する。

体への立入り禁止、ビルの使用不能などを考慮すると、通常のオフィスでのサーバー運用は危険である。被災状況にもよるが、少なくともデータセンターで管理されているサーバーに比べて復旧の時間が長くなることは言うまでもない。

そうした事実から、運用・管理コストの低減や事業継続、情報セキュリティ対策などを目的に、サーバーをデータセンターに集めて全拠点からアクセスする形態で運用を行っている企業が増えている。

ストレージ・セントリックは、サーバーのデータ・センターへの配置とともに行われている情報資産の集約化の手法である。重要な情報資産を一極集中し、それを遠隔地に複製する運用などは、事業継続の観点からも有効と考える。

6.1.1 ストレージ・セントリックとは

ストレージ・セントリックとは、全社に点在するストレージをセンターに集約管理する手法である⁴⁵。サーバーに別個に存在するストレージ機能を抽出してその集約を目指したものである。具体的には、ストレージ専用のネットワークを構築し、サーバーに直結していたストレージをネットワーク経由で接続する形態を採る。場合によっては、ストレージ・セントリック・ネットワークと呼ばれることもある。このストレージ・セントリックの導入により、サーバー直結よりも大容量のストレージを複数のサーバーで効率よく共有することが可能となる。

ストレージ・セントリック技術の代表的なものとして SAN と NAS がある。ここでは、それぞれの技術の概要を記載し、その違いを記載する。

6.1.2 SAN

SAN は Storage Area Network の略称でストレージ装置専用のネットワークのことである。複数のサーバーと複数のストレージをネットワークで結び、異種 OS 環境の中で利用することができる。

(1) SAN 誕生の背景

1990 年代前半のストレージは内蔵もしくは外付けのサーバーに直結された機器が中心であり、DAS(Direct Attached Storage)と呼ばれている。物理的には SCSI⁴⁶という規格のパラレルケーブルでサーバーとハードディスク装置やテー

⁴⁵ ストレージ・セントリックという用語は 2003 年 11 月に NTT 持ち株会社と日立製作所が発表した。

⁴⁶ SCSI: Small Computer System Interface の略称。アメリカ規格協会 (ANSI) により標準化されたインタフェース規格のこと。複数の機器を繋いで接続する方式 (デジチェーン接続) を採用している。初期の「SCSI-1」のデータ転送速度は 5MB/s であったが、現在リリースされている「Ultra2

プ装置などを直結して利用する形態が主流である（図 16）。

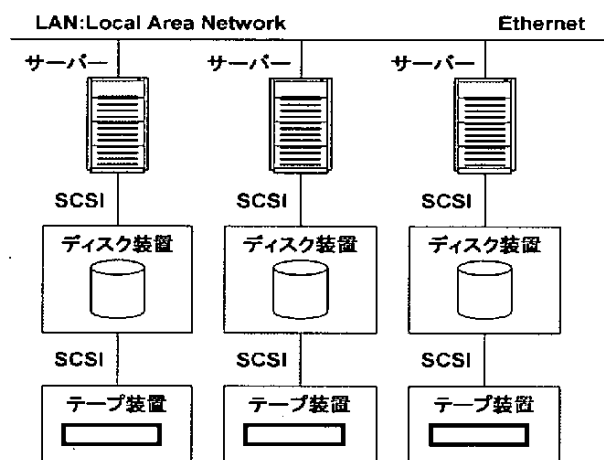


図 16 DAS のイメージ

DAS の構成では、サーバーが増加するに連れて運用負荷が増大する。また、ディスク等の資源利用率のばらつき、保守コストの増大などの問題が発生する。

SCSI 特有の障害の特徴は、1 台の装置の故障が全体に影響することである。例えば外付けディスク装置が故障するとテープ装置が利用出来ないなど、サーバーの可用性を阻害する場合がある。

(2) SAN の特徴

SAN はネットワークの媒体としてホストコンピュータなどで実装されているチャンネルインタフェースと同様な機能を持つファイバー・チャンネル（以下、FC とする。また、FC を利用した SAN を FC-SAN と表記する）を用いることが多い。具体的には「ファイバー・チャンネル・スイッチ (FC-SW)」と呼ばれる Ethernet で利用されるスイッチやルーターに該当するものが各ストレージの中継装置として配置され、サーバーとストレージ装置を接続しデータにアクセスできる環境を提供する（図 17）。

SAN のストレージには選択肢が用意されている。例えば、高速ディスク装置としては RAID⁴⁷装置、中速ディスク装置として S-ATA⁴⁸装置、またバックアップ

Wide SCSI」のデータ転送速度は 80MB/s と大幅なスピードの向上を実現している。尚、「Ultra2 Wide SCSI」の最大接続台数は 16 台で最大ケーブル長は 12m である。

⁴⁷ RAID: Redundant Array of Independent Disks の略称。複数の HDD にデータを分散して保存する装置のこと。

⁴⁸ S-ATA: Serial-Advanced Technology Attachment の略称。ハードディスクの転送方式のこと。転

装置としてはテープライブラリ⁴⁹を利用することが多い。

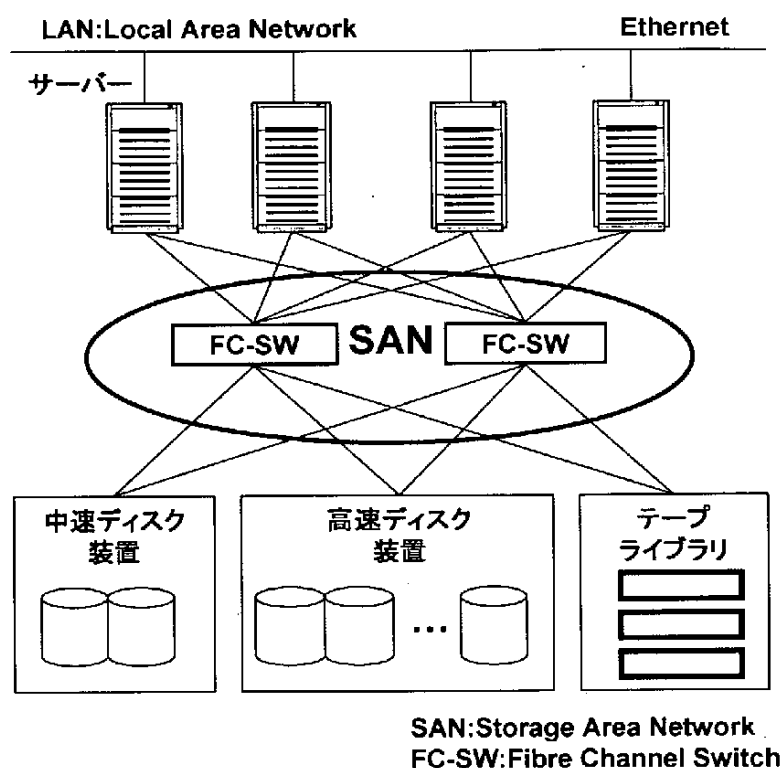


図 17 SAN のイメージ

SAN の特徴を以下に記載する。

- ストレージの一元管理
ストレージをサーバーから独立させて、一元管理を可能にする。
- 高信頼性
サーバーやストレージを柔軟に組み合わせることにより、システムの高信頼性を実現する。
- FC 技術の採用
FC 技術によりネットワークの高信頼性と高速性を実現する。高速なものとして 2Gbps の通信速度に対応するスイッチがリリースされている。但し、導入・運用のためには、FC を理解した技術者が必要である。
- バックアップ時間の短縮化、効率化

送速度 300MB/秒を実装している製品がリリースされている。

⁴⁹ 複数のテープを利用できる装置。ストッカーにテープを保管し、テープ交換は自動で行う。

SAN ネットワークでの「バックアップ統合⁵⁰」により、サーバーや LAN に負荷をかけないバックアップを実現する（サーバーフリー、LAN フリーバックアップと呼ばれる）。サーバーごとにバックアップを取得する必要がなくなる。その結果バックアップ作業の負荷軽減とバックアップ時間を大幅に短縮する。

- バックアップサイトなど遠隔地とのミラーリング（サイト間ミラーリング）
WAN 技術との組み合わせにより、被災時の復旧をより早くする（後述する）

一般に SAN ではストレージを仮想化する。これは、複数のストレージをまとめて全体を一つのストレージプールとして仮想化し、アプリケーションなどに配分する仕組みである。これによりストレージの有効利用や運用管理の容易性などを実現する。記憶容量としては、全体で数 10T バイトから 100T バイトを超える構成も具現化されている（図 18）。

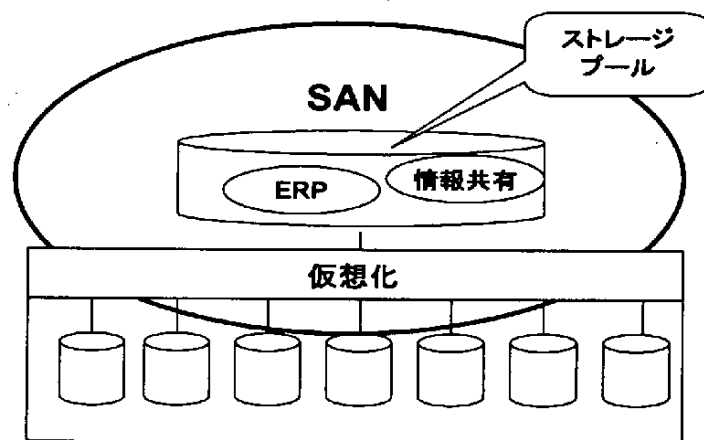


図 18 ストレージ仮想化のイメージ

⁵⁰ バックアップ統合:テープ装置やテープライブラリなどのバックアップデバイスを共有すること。

(3) SAN の適用システム (例)

一般的に SAN を適用しているシステム例として、「データベースシステム」がある。「データベースシステム」は、ランダムアクセスが前提のオンラインシステムなどで、大量のデータを高速にアクセスする必要があるシステムである。高い性能と 24 時間 365 日稼動という可用性、高信頼性が要求されることが多い。

FC-SAN のメリットを享受するために障害となる一つの要因はそのコストにある。FC-SW など FC-SAN を構成する要素は、Ethernet のスイッチやルーターに比べて高価である。コストをはじめ導入のしやすさなどにより、IP プロトコルと Ethernet を利用した SAN(IP-SAN)が普及してきた。次にその IP-SAN について記載する。

(4) IP-SAN

IP-SAN とはプロトコルに IP⁵¹および iSCSI⁵²を採用した SAN である。IP および iSCSI プロトコルの採用により、通常の LAN で利用されている Ethernet を利用できる。その結果、FC-SAN と比較して低コストで SAN を構築することが可能となった。また、IP や Ethernet に関しては技術者が多く、新たな専門知識を習得する技術者をアサインする必要がない。従って FC-SAN と比べて導入しやすい、といえる。

IP ネットワークを使うことで従来の FC-SAN の接続距離の制限(FC は最大 10km⁵³)がなくなり、遠隔地からのストレージアクセスや、後述するサイト間のミラーリング (同期・非同期)、リモート・バックアップ等がきわめて容易に実施できる。

IP-SAN では、従来の SCSI プロトコルを利用してブロック I/O (HDD デバイスのアドレス、データサイズを指定し読み書きを行うこと)を行うため、どのようなアプリケーションでも利用することができる。

但し、調査した中では、FC と iSCSI を併用している事例が多く見受けられる。データセンター内ではより信頼性の高い FC⁵⁴を利用して、遠隔地のストレ

⁵¹ IP:Internet Protocol の略称。インターネットで利用されているプロトコル (通信手順)。

⁵² iSCSI は、IP-SAN を実現する手法の一つ。Ethernet 上で SCSI コマンドセットを直接ストレージに転送するために IP パケットにカプセル化して転送するプロトコルの規格である。

⁵³ FC でもプロトコル変換装置と光回線 (SDH/SONET など) を利用することで数 1,000km まで延長することが可能である。

⁵⁴ 信頼性の高い FC:一般的に FC では TCP/IP や Ethernet と比較して、パケット損失やパケット

ジにスナップショット（後述する）を iSCSI を利用して伝送する、などの実例が存在した。

尚、IP ストレージの主なプロトコルは iSCSI だけではなく、iFCP(internet Fiber Channel Protocol)、FCIP(Fiber Channel Over TCP/IP)などが存在する。これらはインターネット技術の標準化推進団体である IETF(Internet Engineering Task Force)の IP ストレージワーキンググループで標準化したものである。

iSCSI は FC を IP ネットワークで代替する目的で使われることが多く、iFCP と FCIP はすでにある FC を延長する、または遠隔地の FC 同士を接続するために利用されることが多い。

6.1.3 NAS

ストレージ・セントリックの具現化に関して、SAN とともに普及している NAS(Network Attached Storage)について記載する。NAS を簡単に表現すると「専用ファイル・サーバー」である。

NAS 自身が専用 OS の上で NFS(Network File System:UNIX のファイル共有システム)や CIFS(Common Internet File System:Windows のファイル共有プロトコル)を実装している。従って UNIX や Windows の共有ファイル・サーバーとして利用することができる（図 19）。

また、NAS をバックアップ先デバイスとして利用する例も存在する。NAS は短時間のバックアップおよびリストアを目的としたものやクライアント PC のバックアップ先としても利用されている。

NAS のストレージは SAN 同様に選択肢が用意されている。ハイエンドクラスでは RAID 装置を利用することが多い。ローエンドクラスでは S-ATA や IDE⁵⁵(ATA)ディスク、SCSI ディスクなどを利用することが多い。

の送信順の誤りなどが発生する可能性が低い、といわれている。

⁵⁵ IDE: Integrated Drive Electronics の略称。コンピュータとハードディスクを接続する規格のひとつである。

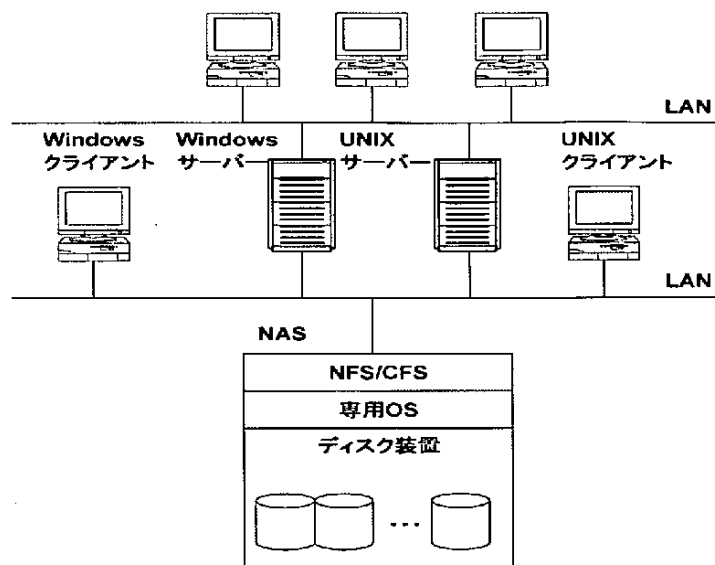


図 19 NAS の例

尚、SAN 同様に NAS にも仮想化機能が実装されている。複数台の NAS を仮想化することにより、ユーザーからは 1 台の NAS のように見える。システム管理者が NAS の増設を行っても、ユーザーは設定変更などの作業を行う必要はない。

(1) NAS の特徴

- クライアントの増加に際してもパフォーマンスを維持
汎用サーバーと違いクライアント数が大幅に増加した場合でも、チューニングなどによりパフォーマンスの低下を回避しやすい。
- ネットワークに IP を利用
前述の FC-SAN と違い専用のネットワークを利用しない。通常の LAN で利用されている IP を利用する。そのため導入や運用が比較的容易である。
- 複数のファイル共有システムの採用
NFS や CIFS を採用している。
- ファイル単位のデータアクセス
サーバーとファイル単位でデータのやりとりを行う。一般的に SAN と比べてパフォーマンスが低速になる可能性がある。
- ジャーナルファイルシステム
異常停止時にデータ消失を回避するための機能である。データの保全性を確保す

るための構成情報（メタデータ）やユーザーデータなどを保存する。性能向上のために書込み用キャッシュとして NVRAM（不揮発メモリ）を実装する装置が多い。

- スナップショット
ある時点でのファイルシステムのイメージを取得する（後述する）。
- ディスクのホットスワップ対応
故障などでディスクを交換する必要があった際にシステムを止めずに交換できる。また、容量の拡張も無停止で可能である。
- 管理ツールの充実
システム管理者がファイルの使用状況やアクセス状況を把握出来るような機能を有している。

(2) NAS の適用システム（例）

- ファイル共有システム
汎用のサーバーと比べて多くのクライアントに対して、高速にファイルを共有できる。例えば三次元 CAD ファイルなど大容量のファイル共有に威力を発揮する。
- ストリーミングシステム
ファイルサイズの大きな動画ファイルなどを多数のクライアントへ同時に配信するシステムなどに有効である。

あるデータベースソフトウェアメーカーは NAS ベンダーと業務提携を行っている⁵⁶。その中で NAS のスナップショット機能を利用したバックアップソリューションなどを提供している。一概にデータベースには SAN が適切であり、NAS には不適であるとはいえない。

6.1.4 NAS と SAN の相違点

NAS と SAN との大きな違いは、NAS がファイルシステムを保持していることにある。SAN に接続されるストレージは、ファイルシステムを持っておらず、サーバーからは単なるブロックデバイスとして見える。

前述のとおり、SAN のネットワークはストレージ専用のネットワークであり、上位プロトコルとしては SCSI を利用するのが一般的である。NAS というネットワークは、通常 Ethernet を利用した IP ネットワークであり、TCP/IP 上のファ

⁵⁶ NAS が提供する NFS や CIFS 上にデータベース関連ファイルを配置する（マウントやシェアを利用）。

イル共有プロトコルが利用されている。

NAS は既存の LAN 上に設置することができるので、よりオープンなシステムに対して利用可能であり、そのことが利点の一つになっている。

また、NAS を大容量ファイルサーバーの位置づけで、SAN のネットワークデバイスのひとつとして組み込むことも可能である。

上記のように、SAN と NAS を融合させたストレージ・セントリックも実装可能となっている。それぞれの特徴を活かしたストレージ・セントリックが実現している。

6.2 事業継続に関連するネットワークの動向

前述のとおりストレージとネットワークは不可分の関係になりつつある。「ストレージ・セントリック・ネットワーク」という用語に代表されるように、これまで別々に考えられてきたストレージとネットワークはひとつのインフラとして扱うべき対象になっている。

特に事業継続という観点からは、プライマリーサイトとバックアップサイトでシステムを継続するためのバックアップデータの転送や被災時のサイト切り替えなど、ネットワークは極めて重要な要素である。

ここでは、事業継続に利用することが可能な通信事業者が提供する広域ネットワークサービスの動向をまとめる。

6.2.1 広域イーサネット

広域イーサネットとは、LAN で利用するイーサネット・フレームをそのまま中継できる WAN サービスのことである。遠隔地のネットワーク同士をあたかも LAN で接続しているかのように利用できる。

また、広域イーサネットはネットワーク構成の自由度が高く拠点の追加などが行いやすい。通信するプロトコルに制約が無いこと（ホストコンピュータで利用される SNA などでも利用可能である）も特徴的である。

提供速度については 128kbps⁵⁷～1Gbps までなど様々なメニューが用意されている。帯域保証や保守などの付加サービスにより料金は異なる。

イーサネットは、データの衝突を防ぐためにネットワークの状態を定期的に

⁵⁷ bps:bits per second の略称である。bps はデータ転送速度の単位である。1bps は 1 秒間に 1bit 転送できることを表す。

監視し、ネットワークが利用されていないタイミングにデータ送信を行う方式を採用しており（CSMA/CD⁵⁸方式）、また一つの回線を共有して送信・受信を交互に行う半二重通信が基本であった。

この方式では衝突検出を行うために通信距離が制限される。現在は回線を 2 つ利用する全二重通信が主流となっている。その結果、衝突検出の必要がなくなり、距離の制約が解消された。

広域イーサネットは、次に説明する IP-VPN と並び WAN サービスの中核に位置づけられる。

6.2.2 IP-VPN

IP-VPN は通信事業者の保有する広域 IP 通信網を経由して構築される仮想私設通信網(VPN⁵⁹)のことである。利用可能なプロトコルは IP に限定されている。広域イーサネット同様、WAN を意識しないで利用できる。通信速度は 10Mbps ～1Gbps が中心で、付加サービスの選択により料金が相違する。

IP-VPN サービスとしては、IP 網上にネットワーク同士を直結する仮想専用線を構築するものと、仮想ルータを提供してルーティングまでを通信事業者が提供するものがあり、後者が特に注目されている。ルーティングサービスを提供する IP-VPN サービスでは、プライベート IP 網内の通信経路探索に MPLS⁶⁰を採用しており、どの VPN の通信であるかを確実に判別することができる。そのため VPN 同士でのアドレスの衝突や、他 VPN への誤送信などが発生しないように設計されている。

尚、インターネット上で実現される VPN はインターネット VPN と呼ばれて IP-VPN とは区別される。

IP-VPN では、インターネットを利用しないことなどによりセキュリティや通信品質を向上させている。

⁵⁸ CSMA/CD: Carrier Sense Multiple Access with Collision Detection の略称。Ethernet が採用している技術である。

⁵⁹ VPN は Virtual Private Network の略称である。

⁶⁰ Multi Protocol Label Switching IP パケットにラベルを付与して、ユーザーを識別する技術のこと。

6.2.3 専用線

専用線は、従来から利用されている完全帯域保証で QoS⁶¹が担保されている回線である。物理的にインターネットなどの公衆網と完全に分離したプライベートなネットワークである。政府や金融機関などの重要拠点間の接続は信頼性を重視して専用線を利用する場合が多い。

一般的に専用線は信頼性は高いが高コストとの印象が強い。しかし、1990年と比べて 6Mbps から 100Mbps にスピードを向上させて、且つ 1Mbps あたりの単価を 1/67 に低下したサービスを提供しているベンダーが存在する⁶²。以前に比べてコストを大幅に低減することが可能である。

現在、企業の広域ネットワークの中心となっているのは、広域イーサネットであり、IP-VPN である。高速・安価で容易に使えることで利用度が高まっている。後述する「事業継続のためのバックアップとリストア」の回線として利用されている事例も多い。また、専用線も信頼性の面から業種や業務によっては利用が継続している。

尚、インターネット VPN や ADSL、ISDN などもバックアップ回線として採用されている場合が散見される。中でもインターネット VPN は設定の容易性や通信品質の向上など提供サービスの向上が著しい。コストやサービスレベルなどを検討して適材適所の観点から回線を選択することが重要である。

6.3 事業継続のためのバックアップとリストア

2000 年頃までのオープンシステムのバックアップは、深夜や休日などシステムの運用が停止している時間帯に取得することが多かった。その際、バックアップ取得時点の整合性を維持するために、データベースなどシステムを停止することが常であった。また、記憶媒体としては磁気テープを利用することが一般的であった。

リストアについてもミラーリングや RAID5 などのディスク装置自体の自動リカバリは利用されていたものの、RAID コントローラやサーバー内蔵のディスク装置の故障時などには、磁気テープからリストアを行っていた。

ホストコンピュータがメインの時代には、オープンシステムでは、フォール

⁶¹ QoS: Quality Of Service の略称。通信回線品質のこと。

⁶² 東京と大阪間の接続事例である。

ト・トレラント⁶³を考慮したシステムの構築例は少なかった。しかし、現在は ERP など基幹システムのメイン・プラットフォームはオープンシステムに移行している。

オープンシステムが事業継続に不可欠なシステムとして成長するにつれて、その RTO や RPO の短縮要求がますます強くなってきている。どのような災害が起ころうとも事業を行う上で必要なシステムについては、最長でも数秒のオーダーでデータの損失が全くなく、システムが自動的に待機系システムに切り替わるのが理想である。それを実現するためのサービスやシステムのリリースがここ数年で非常に多くなっている。

但し、RTO や RPO を短縮するための対策を講じるためには、そのためのコストが必要であり、全てのシステムについて同じレベルで対策を講ずることは、現実的ではない。

確かにハードウェアやネットワークなどの設備に関するコストは大きく低下し続けている。前述の広域イーサネットや IP-VPN などを経由してバックアップサイトへ常時データ転送することがパフォーマンスやコスト的にも実用レベルに到達しており、実際に運用が始まっている。

いかに取り返しがつかないデータの消失からデータを保護するか。ビジネスインパクト分析などにより、復旧優先度とその情報価値評価などから RPO・RTO を定めた上でシステムの実装を行うことが重要である。特に様々な選択肢がある。現在は、自社の要求仕様やコストなどについて十分な検討が必要である。

次に、最近の動向としてサービス提供が増えている「バックアップサイト」と前述の SAN や NAS、ネットワークサービスを利用した「バックアップ技術動向」について記載する。

6.3.1 バックアップサイト

今回の調査で、バックアップサイトの有無とそのレベルが大きく RTO を左右することが判った。災害復旧で最も重要となる事項のひとつが復旧作業を行うための場所の確保である。この場所のことを一般的にはバックアップサイトと呼ぶ。災害発生により、プライマリーサイトが利用できなくなった場合は、バックアップサイトにデータセンターを再構築し、プライマリーサイトが復旧するまでシステムの稼動を行う体制を保有していることが、事業継続上重要と考える。

⁶³ システムの一部が故障しても全体の運転には影響を与えないようにするフェイルセーフなど、故障の影響を最小限に押さえて、信頼性を向上する機能のこと。

そのバックアップサイトには次の3種類が存在する⁶⁴。

- 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）

言うまでもなく、RTO を最も短縮出来る反面コストが最もかかるのがホットサイトである。逆に最も RTO が長くなる反面コストが低いのがコールドサイトであり、その中間がウォームサイトである。

これらのサイトは、自社で個別に構築する場合とベンダーが提供するサービスを利用する場合がある。提供サービスは、免震・耐震構造を持ったデータ・センターの利用を前提とし、ユーザーの要望に応じて柔軟に対応するサービス体系を用意しているベンダーが多い。

ここでは、ホットサイト、ウォームサイト、コールドサイトのバックアップとリストアの例を記載する。前提としてプライマリーサイトが被災し、全く運用ができない場合を想定して記載する⁶⁵。

⁶⁴ バックアップサイトにはサービス提供者などにより提供形態が相違する。ここでは、以下の記述を参照した。『事業継続計画（BCP）策定ガイドライン』 経済産業省商務情報政策局情報セキュリティ政策室編 <情報システム・データの維持・復旧のための方法>

⁶⁵ 以下の事例を参照して想定の設定を行った。「2001年9月11の同時多発テロの際に、世界貿易センタービルに本社のあった金融機関の殆どが基幹データを離れた場所に保存していたので、2日間程度で顧客向けサービスを完全復旧している」 出典：『地域情報基盤としての地域情報ネットワーク有効活用に関する調査研究 報告書』 2003年3月 財団法人マルチメディア振興センタ

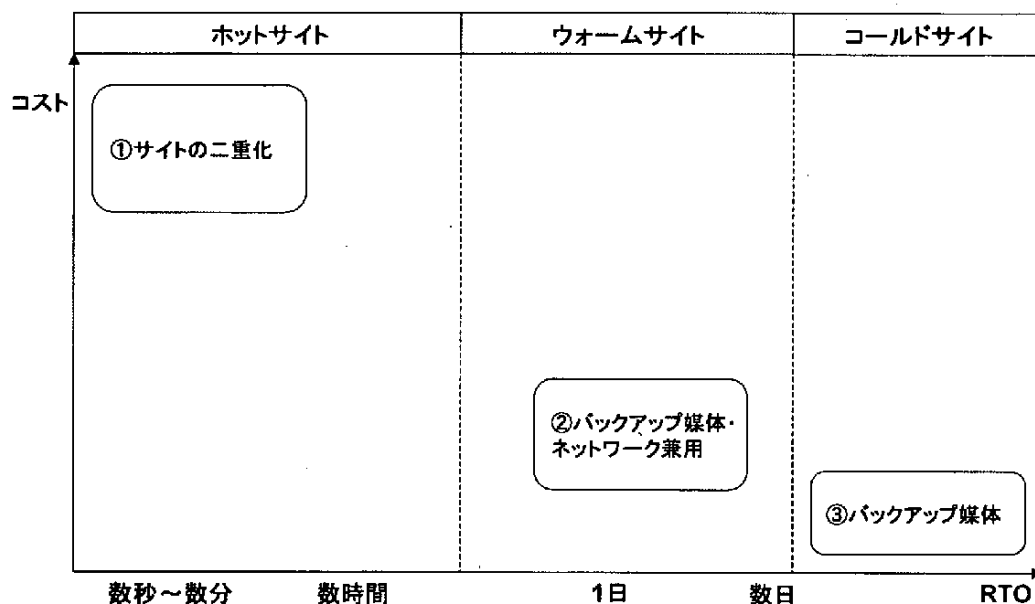


図 20 バックアップサイトとリストア方法の例

(1) ホットサイトのバックアップとリストア例

① サイトの二重化

同時に被災した場合のリスクを回避するために、プライマリーサイトとの距離を十分に取った遠隔地のホットサイトの利用を前提に対策を講じている例がある。

最も RTO が短い方法（数秒から長くて数分）としてサイト間のミラーリングにより自動復旧する手法が存在する（図 20①「サイトの二重化」）。この場合、ネットワークの切り替えだけで、そのままシステムの稼動を継続できる。ストレージについては、前述の SAN や NAS を利用するケースが多い（後述する）。

図 21 では、東京にプライマリーサイト、大阪にホットサイトを開設した例を記載している。この場合、両方のサイトが全く同じシステム構成である必要がある。

図 21 にも例示しているが、サイト間でミラーリングを行う方法には同期式リモートコピー（図 21①:図では実線表示）・非同期式リモートコピー（図 21②:図では点線表示）が存在する。

以下に、同期式・非同期式リモートコピーそれぞれについて記載する。

② 同期式リモートコピー

同期式リモートコピーは常にサイト間で同期をとっているため、データの損失はほとんどない。但し、バックアップサイトの処理完了を待つのでアプリケーションのパフォーマンスが悪化する場合がある。

③ 非同期式リモートコピー

非同期式リモートコピーはバックアップサイトへの処理完了を待たないので、アプリケーションのパフォーマンスは悪化しない。但しプライマリーサイトで発生した更新をバックアップサイトへ反映する前にプライマリーサイトが被災すると、データ損失が発生する可能性がある。

◆プライマリーサイト(例:東京)

◇ホットサイト(例:大阪)

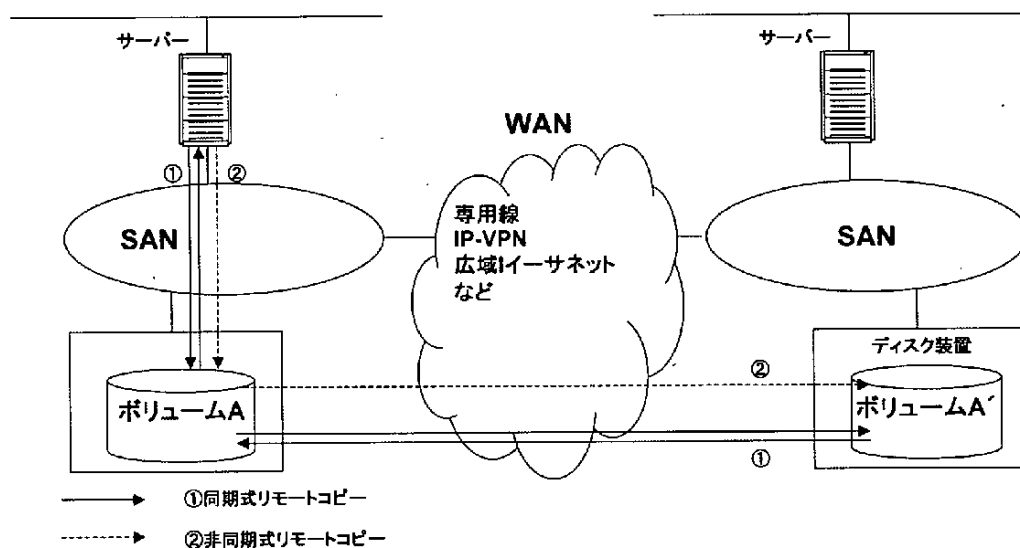


図 21 サイト間ミラーリングの例

尚、バックアップソフトウェアの中には、同期式を基本とするが、しきい値を予め設定しそれを超えてもホットサイトから処理完了通知が来なかった場合に、自動的に同期式から非同期式に変更する機能を実装するものがある。

(2) ウォームサイトのバックアップとリストア例

ウォームサイトは、共同利用を前提にしたコンピュータをサイトに確保し、アプリケーションソフトの保管や定期的にバックアップデータを送付しておく形

態が一般的である。被災時にアプリケーションやデータのインストールを行うなど、ホットサイトに比べてシステム立上げまでに時間がかかる。また、バックアップデータの取得時点までの復旧が限界であり、データの損失が発生するケースが多い。但し、コストについては大幅に低減できる。

ウォームサイトではネットワークが利用できるため、プライマリーサイトとは別の場所に保管しておいたバックアップデータが存在すれば、その転送によりサービスの開始を早めることができる。但しこの場合利用できる回線の帯域は細いのでリストアまでに時間がかかる（図 20②「バックアップ媒体・ネットワーク兼用」）。

(3) コールドサイトのバックアップとリストア例

コールドサイトの場合は、サーバー等の機器調達を行い、プライマリーサイトで作成したバックアップ媒体を配送し、サイトに保管しておく。リストア時にはその保管媒体を利用する。ネットワークについても別途機器を調達し、環境設定を行いサイトを立ち上げる（図 20③「バックアップ媒体」）。

この場合も、ウォームサイト同様データの損失が発生する。また、リストアまでに場合によっては数日の期間を費やす可能性がある。当然であるが、コストは最も安価である。

ここまでは、バックアップサイトについて解説した。次にバックアップの技術動向について記載する。

6.4.2 バックアップ技術動向

現在も磁気テープ装置はバックアップの重要な位置を占めている。但し、バックアップ技術には、ストレージやネットワークの進化に合わせて下記のような様々なバリエーションが出現している。

- ディスク経由のバックアップ
- LAN（ネットワーク）経由のバックアップ
- SAN のバックアップ
- NAS のバックアップ
- スナップショット

以下、それぞれについて記載する。

(1) ディスク経由のバックアップ

前述のデータ量の増加と相反する要件であるバックアップ取得時間の短縮を実現するために行われている基本的な方法は、ディスク経由のバックアップである。

これは、バックアップ対象データを一旦ディスクに蓄え、そのディスクからテープにバックアップを取得する方法である。この方法を「DtoDtoT(Disk to Disk to Tape)」と呼ぶ場合がある(図 22)。尚、リストアもディスクから行うことが可能な場合が多く、その際には大幅にリストア時間を短縮できる。

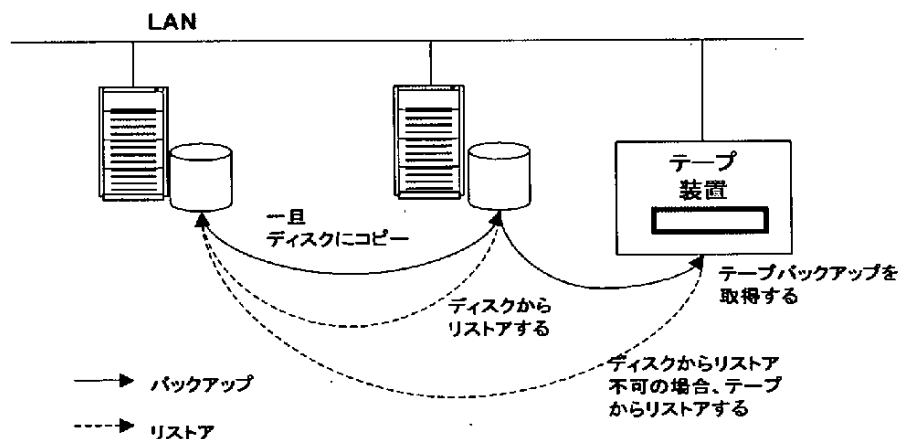


図 22 ディスク経由のバックアップとリストアの例

(2) LAN 経由のバックアップ

テープライブラリなどのバックアップ装置を接続したバックアップ専用サーバーにネットワーク経由で各サーバーのバックアップを集中して取得する方式である。

前述のとおり、以前は個別にサーバーごとに SCSI 接続されたテープ装置などで、バックアップを取得していた。

専用サーバーにはバックアップ管理ソフトウェアを実装し、対象となるサーバーには通常バックアップ管理ソフトのエージェント・モジュールをインストールし、バックアップ取得を自動化する(図 23)。

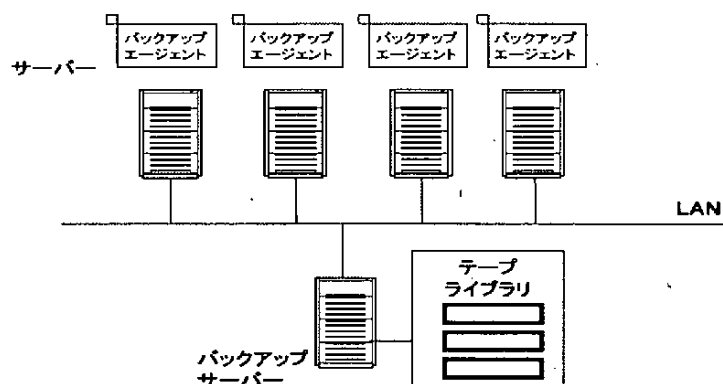


図 23 LAN 経由のバックアップ例

(3) SAN のバックアップ

LAN 経由のバックアップ取得でバックアップ作業の効率化は実現できた。しかし、バックアップ取得時に LAN 上に大量のトラフィックが流れネットワークに負荷がかかる。バックアップ取得時間帯などにも依存するが、業務運営に影響を及ぼす可能性がある。

SAN のバックアップ方式では、前述のとおり LAN とは別のストレージ専用ネットワークを利用して、SAN に接続されたディスクからテープにデータが転送される。このデータ転送には、SCSI の拡張コピープロトコルを利用する。この機能は前述の SNIA⁶⁶が開発した技術標準に基づき実装されている。

(4) NAS のバックアップ

NAS のバックアップは、ネットワーク接続されているサーバー経由で行うことが最も簡単な方法である。しかし、この方法を利用するとバックアップデータが LAN に流れてしまいネットワーク負荷などの問題が発生する。

NAS は専用 OS 上で稼動するので、テープ装置などの外部記憶装置を直接接続することは難しい。NAS にテープ装置などを接続し制御するための技術として NDMP(Network Data Management Protocol)が存在する。この NDMP プロトコルにより NAS サーバーからテープ装置などにダイレクトにバックアップが取得

⁶⁶ SNIA (Storage Networking Industry Association) は、後述の SNA(Storage Area Network) や NAS(Network Attached Storage)などのストレージネットワーク技術に関する標準化や啓発などを推進している世界最大の業界団体である。2001 年 8 月に SNIA 日本支部が設立されている。

できる。

また、NAS にはファイルの追加時などに遠隔地の NAS にデータを自動的に送り複製するレプリケーション機能と呼ばれるものがある。この機能を利用すると、同時に複数の NAS への複製が可能になる。東京の NAS をマスタとして大阪、九州に複製の NAS を設置しているシステム構成を想定してみる。

この場合、マスタである東京の NAS だけにファイルを追加すれば、各地の NAS にも同時にファイルが追加される。

尚、遠隔地に NAS サーバーを配置する場合、100M ビット/秒や 1G ビット/秒という高速回線を使用しても実効速度の遅さを体感する場合がある。その実効速度のパフォーマンス向上のために WAN 高速化装置を採用するという選択肢がある。本格的な国内リリースが 2005 年中ごろから始まった。

Windows のファイル共有プロトコルの CIFS を利用する場合、ファイルをクライアントにダウンロードする際にクライアントとサーバー間で数多くの制御情報の交換が必要になる。この場合、回線を高速化しても解決には至らない場合が多い。WAN 高速化装置は代理応答やキャッシュ機能などを実装しているので、パフォーマンス向上が図れる。

但し、まだまだ成長過程の市場であり、10 社近いメーカーが複数のモデルをリリースしている。また、その機能はばらついているので、導入に当たっては、対象データの特性を明確にし、それに適合した機能を保持する製品を選択する必要がある。

(5) スナップショット

スナップショットは、上記 SAN や NAS で利用されるファイルシステムのイメージをバックアップする技術である。スナップショットはある任意の時点のコピーであり、ファイル管理情報（ポインタ）のみをバックアップデータとして取得するため、短時間で取得できる。

スナップショット取得の例を記載する。例えば、データベースのスナップショットを取得する場合、整合性がとれた状態をディスク上に確保するためメモリー上のデータをディスクに書き込みデータベースを一旦停止する。その後スナップショット取得を指示する。この指示をストレージ装置が受け付けた時点で、停止状態を解除しデータベースを起動することができる。この場合のデータベースの停止時間は一般的に数秒から 10 数秒程度である。実際のバックアップファイルは、この後でスナップショットからファイルを取得して作成される（図 24）。

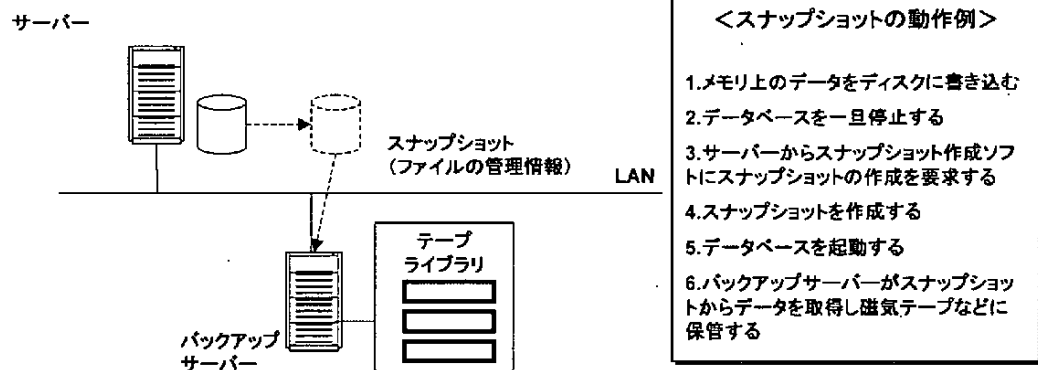


図 24 スナップショットのイメージ

尚、スナップショットにはボリューム単位などディスクイメージをまるごと取得する製品も存在する。この場合には、データだけではなく OS やアプリケーションも対象になる。

6.4.3 バックアップ関連の特記事項

最近のバックアップに関連するストレージ技術やサービスについて記載する。

- RAID6
- WORM 装置
- ストレージ・サービス・プロバイダー

(1) RAID6

RAID は「望ましいコスト、データの可用性および性能特性をホスト環境に提供するために性能特性をホスト環境に提供するために複数ディスクを管理する技術群⁶⁷⁾と定義されている。これまでの RAID 装置では、ハードディスク 1 台の故障時に継続して運用可能な構成が最高の自動復旧レベルであった。RAID6 では、RAID5 にパリティ⁶⁸⁾をさらに追加したことで、ハードディスク 2 台の故障時にも継続運用が可能となった (図 25)。

⁶⁷⁾ 出典:『ストレージネットワークング技術』喜連川 優編著 オーム社

⁶⁸⁾ データエラーを検出する方法の一つである。

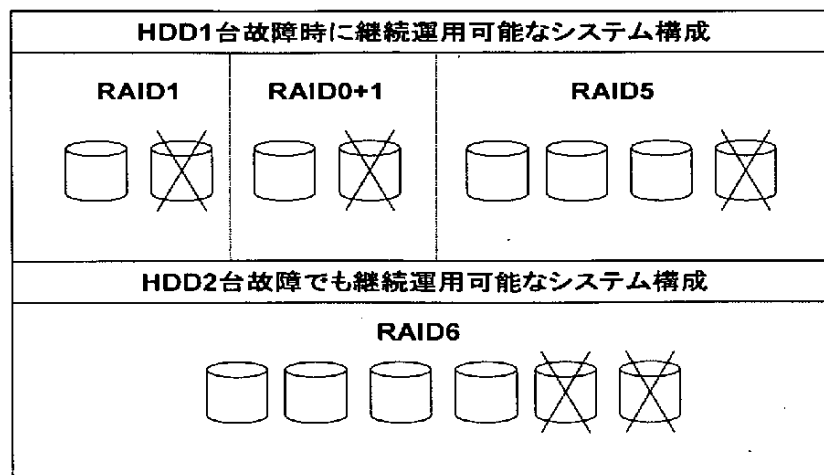


図 25 RAID のイメージ

(2) WORM 装置

WORM (Write Once Read Many) 装置とは、文字通り一度だけ書込みが可能であり、一度書き込んだデータは、変更や消去ができないストレージのことをいう。これまで、CD-R や DVD-R などの追記型の光ディスクを使用したストレージ製品が WORM 装置の代表的なものであった。現在、最大の記憶容量を実現している光ディスクの一つであるブルーレイディスクでは、記憶容量が 25GB(1 層)あるいは 50GB(2 層)、データ転送速度が 36Mbps という仕様で実装されている。

米国の SOX 法では、財務データなどを長期間にわたって保管するとともに、そのデータが改ざんされていないことを保証することが求められる。データの更新ができない WORM を採用したストレージ製品は、これを物理的に保証する手段として利用され始めている。メールサーバーのデータなどについてもアーカイブして WORM 装置に保存するなど実例が出ている。

磁気ディスクでもソフトウェアの制御により、一度書き込んだデータを変更できないストレージ装置を仮想的に作り出すという製品も現れた(WORM ディスク)。同様に WORM テープのリリースも既に行われている。

(3) ストレージサービスプロバイダー (Storage Service Provider:SSP)

企業などに向けて、ネットワークを通じて大規模なストレージを提供するサービスを提供するプロバイダーが現れている。

耐震・免震性や自家発電設備、高速な回線などのインフラを備えた専用の施設(データセンター)に、ネットワークに接続して外部から利用する大容量のストレージを設置し、企業に貸し出すサービスを提供する。ストレージは多重化やバックアップで耐障害性・可用性を高めており、24 時間 365 日の監視や障害時の緊急対応などを提供するプロバイダーも存在する。プライマリーサイトとして利用することが可能である。

大容量のデータを扱う企業にとっては自社でストレージシステムを構築・保有するよりも低コストで、高品質なストレージを必要なときに必要なだけ利用することができる。

尚、プライマリーサイトは自社に配置し、ホットサイト、ウォームサイトなどバックアップサイトについては SSP を利用する、という運用についても実際に導入されている。

6.4 情報ライフサイクル管理 (ILM)

6.4.1 ILM 誕生の背景

前述のとおり、記憶媒体には RAID、ハードディスク、DVD、磁気テープなど、様々な種類が存在し、記憶容量や入出力性能、信頼性など実装レベルやコストが相違した製品が多数リリースされている。

作成から廃棄に至る情報資産のライフサイクルの中で、どの工程でどの記憶媒体を利用すれば最適な運用ができるか、コスト面を含めて検討する必要性が生じている。

事業継続の面からも、情報のライフサイクルに応じて最優先にリストアすべき情報資産を選定して、バックアップ運用設計を行う必要がある。

6.4.2 ILM とは

ILM は 2002 年頃からアメリカの大手ストレージメーカーが自社の戦略として提唱しはじめ、現在注目を集めているコンセプトである。ネットワーク・ストレージ業界団体の SNIA は ILM を下記のように定義している。

「情報が生成されてから最終的に破棄されるまでの間、情報のビジネス価値

を、最適でコスト効率の高い IT インフラストラクチャに連携させるためのポリシー、プロセス、手法、サービスおよびツール」

上記をより具体的に解釈すると、次のように表現できる。「情報のライフサイクルに応じて情報資産価値を評価し、それに見合う記憶媒体の仕様やコストなどを検討する。そして、工程ごとに適切な記憶媒体を選定して利用する。工程の遷移に伴う記憶媒体の移行（例、ハードディスクから磁気テープ）については、自動化ツールの利用なども検討する。」

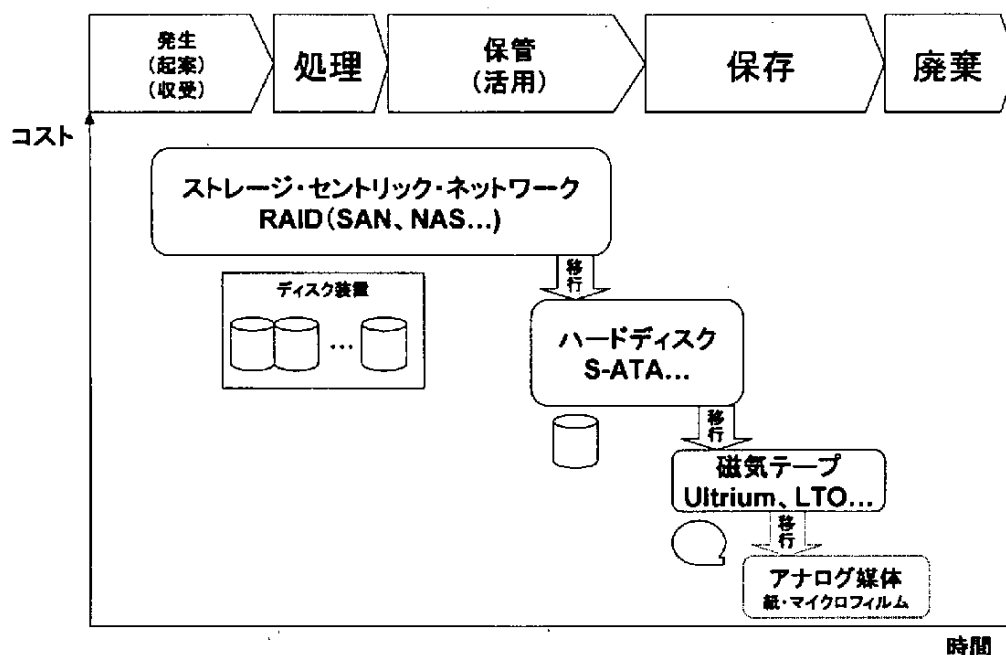


図 26 ILM の例

図 26 にあるように、作成工程から保管工程まで比較的参照頻度が高い時期については、高速で信頼性が高いストレージ・セントリック・ネットワークを構成する RAID 装置に格納する。

情報鮮度が悪くなり、参照頻度が少なくなっているが、参照する可能性が残っている情報に関してはコストパフォーマンスの高いディスク装置に移動する。大容量でシーケンシャルな読み出し性能が高い S-ATA ドライブなどの利用が有効である。

さらに時間の経過により、参照する可能性がほとんど考えられなくなったが、法的要件などで廃棄できないもののみを、磁気テープなど外部記憶媒体に移動す

る。Ultrium⁶⁹、AIT⁷⁰などの他、それらの自動交換機能などを実装した大容量のテープライブラリ装置などが利用されている。

その際、保存する必要のない情報は破棄する。参照頻度とは関連性が薄く、永年保存に近いものに関しては、OS やアプリケーション、装置などに依存しないマイクロフィルムや紙などのアナログ媒体に保存することも考えられる。

尚、長期安全保存を目的として、ハードウェアやソフトウェアに依存しない形式でストレージの外部にデータを取り出すことをアーカイブと呼ぶ。磁気テープやアナログ媒体などがこのアーカイブの媒体となる。

前述のとおり、ILM は時間とともに変化する情報の価値に応じて最適なストレージを利用するという考え方である。この ILM の実践により情報資産の管理について、活用とコストの最適化を図ることが可能になる。

媒体の移行については、既に各種のソリューションが提供されている。例えば、データのアクセス頻度を評価して高価な RAID 装置から安価なディスク装置に自動的に移行を行う機能を持つものがある。この場合、ユーザーはデータの移行を意識しない。

特に、どの段階で保管（活用）フェーズから保存フェーズに移すか、という設計をその時間軸に沿って行っておく必要がある。

ILM はあくまでも手段であり、目的ではない。全社レベルで企業の情報資産を有効活用し、且つ保護することを目的に、情報資産価値に応じた適正なコストで効率的に管理する概念である。その点を改めて認識しておきたい。

事業継続の視点からも、前述したバックアップとリストアの構成を検討する上で、資産に対して工程ごとに記憶媒体を選定するなど、ILM の考え方を反映することは有効である。

⁶⁹ Ultrium: 転送速度 40MB/s～80MB/s、記憶容量 400GB(データ圧縮時)を実現する。

⁷⁰ AIT:Advanced Intelligent Tape 転送速度 12MB/s 非圧縮時 100GB を実現する (AIT-3)。

7 まとめ

7.1 事業継続に関する全体動向

本報告書の第2章の冒頭で触れているように、事業継続に関する概念は、現時点で、充分整理されているとはいいがたい。しかしながら、同時多発テロ、SARS、水害や地震といった自然災害など、動機は異なるが、各国で官民を挙げた取組みが急加速しているのも事実である。もはや、対応の遅れや不手際について、予測できなかったという単純な言い訳が許される時代は過ぎつつある。

平時から、事業継続計画を構築し準備しておくことは、企業等の組織における経営責任である。それぞれの組織は、社会情勢など、自分の組織を取り巻く環境変化、業種特性、事業形態、業務フロー、投入可能な要員など、あらゆる要素を勘案して、主体的に事業継続計画の策定と実装、および運用を行わなければならない。国内外で作成されている規格やガイドラインは、その取組みを支援するものとして活用できる。

7.1.1 事業継続の規格やガイドラインについて

規格やガイドラインは、総じてどのようなステップを踏んで計画を策定すればよいかというフレームワークだけを示すに止まっている。その背景には、組織の形態や業態により、自己判断の部分を多くし、柔軟性を持たせる意図がある。

フレームワークのポイントは、次のようにまとめられる。

- 事業継続計画策定と維持継続のための組織体制を構築すること。
- 事業継続計画を策定し、更新すること。
- リスクアセスメントやインパクト分析などを行い、考慮すべき脅威や保護すべきビジネスプロセスなどについて、優先順位付けをし、戦略的な計画策定や取組みを可能にすること。
- 啓発や訓練などを通して、文化や意識の構築と定着を図ること。
- 監査などを実施し、継続すること。

事業継続計画に取り組む組織は、実装や運用について、専門家の助言を仰いだし、組織内で専門知識を有する人員を育成したり、試行錯誤を重ねたりなどして、進めていかなければならない。

しかしながら、個々の組織で考えながら取り組むのは負担が大きく効率も悪

い。事業継続関連の取組みを支援するために、地域特性や業界特性を反映したガイドラインなどが、さらに充実することが望まれる。また、いずれにしても最終的に、各組織の意思決定に依存する部分が多く残されるのであるから、組織長や最高意思決定機関の関与もまた、事業継続のためには欠かせない要件という認識が広まることが重要である。

7.1.2 欧米における取組みの現状から

事業継続の中でも、情報通信関連の対策が重要であるとの意識が高い金融機関では、その取組みが製造業より進んでいる。今回の欧米における調査も、自ずと金融機関における現状調査が有益な情報を提供した。その特徴を次にまとめる。

- できるだけシンプルに準備・導入ができるようにしている。
- 訓練や啓発を重視している。
- 拠点ごとの違いや、法制度の変化などの環境変化に柔軟に対応できるマネジメントを実施している。

製造業における取組みにおいても、従来からの緊急事態準備やクライシス・マネジメント、IT ディザスター・リカバリー、事業再開など、重なり合う領域を対象とするマネジメントシステムとの共生が図られている。いずれのケースでも、できるところから実装していこうというアプローチが取られており、無理な計画を立てていない点が特筆される。

また、専門のサービス提供会社の活用も参考になる。バックアップのためのデータ・センターはわが国でも一般的であるが、従業員用ワーク・スペースや移動式データ・リカバリーセンターなどが上手に使われている。

わが国でも、このようなサービスが提供され、ユーザー側も活用できるようになれば良いと考える。ただし、専門家の利活用が可能な欧米で使われているサービスや支援をそのままわが国に持ち込むと、使いこなせないなどの不具合も生じるであろう。わが国の現状に則したサービスの開発と提供が望ましい。

欧米では一般的であるが、わが国ではあまり活用されていないソフトウェア・ツールとして、マネジメントを支援するツールがある。まず、リスクアセスメントやインパクト分析など、‘分析’と意思決定を支援するツールが活用されている。ワンタイムで、多くの従業員を動員したり、コンサルタントを雇用して詳細なリ

スク分析しても、メンテナンスしなければ、一年も経つと組織や業務は変化し、分析結果は現状を反映しない。事業継続計画は、常に更新し、その際には保護すべき情報資産の優先順位などを見直す必要がある。

また、事故対応が発動した際に使われる情報も、更新しておかなければならない。たとえば、緊急時の連絡相手が、少し前の人事異動で他部門へ移っていたが、緊急連絡先リストは古いままだったというのでは、リストの存在意味がない。適時更新が、事業継続には最重要事項であることが、欧米では当たり前のこととして実践されている。これを支援するソフトウェア・ツールの活用もわが国企業にとっては課題のひとつといえるのではないだろうか。ただし、ツールについても、サービスと同様に、わが国の実状に合ったものでなければならない。

7.1.3 事業継続の専門家について

本報告書の「2.1 米国の現況」でも指摘したが、事業継続計画の策定・運用支援ツールは、カスタマイズして使用するものが少なくない。組織の状況に合わせるためには、仕方の無いことではある。しかし、これはツールを使いこなす能力が要求されるということを示している。本報告書の第4章で述べているように、事業継続の専門家として必要な能力は、多岐に渡る。欧米の組織では、資格を有する事業継続の専門家が、計画の立案から定着まで、重要な役割を果たしている。

社会的レベルでは、大学などの教育機関で、今後いかにして必要な人材を育成するかを検討するべきである。また、企業等の組織レベルでも、内部で人材を育成するか否かといった判断が必要となる。欧米のように、専門家が転職してロールアップする人事ローテーションが、社会的に機能していればよいが、わが国はそのような状況にはない。事業継続が、重要な経営課題であると考えた場合には、上級管理者が経験すべきポジションとして設定するなどの案もあるが、いずれにしても、実現可能なアプローチを見出す必要があろう。今後、わが国に事業継続を定着させるためには、教育機関と産業界の連携が不可欠である。

7.2 事業継続と情報資産保護

本調査研究では、事業継続に係る最近の動向に加え、事業継続と情報資産保護の関連性について、焦点を絞り実施してきた。その過程において、様々な規格やガイドラインを調査した結果、共通して触れられているバイタル・レコードに

関する記述を中心にまとめた。

7.2.1 情報管理の変化と事業継続

バイタル・レコードに係るガイドラインなどの記述には、従来、重要書類など、いわゆる文書を対象として管理してきた‘組織の情報’を、事業継続の視点から、改めて見直す際のポイントが指摘されている。その特徴は次のようにまとめられる。

- バイタル・レコードは、ビジネスインパクト分析のプロセスの中で、特定される。
- ‘情報’の態様には、紙と電子の両方があることを考慮しなければならない。
- 記録（レコード）と文書の関係は、まだ明確に定義されていないが、記録は、証拠性を持つなど、いわゆる‘基幹文書’や‘重要書類’などに近いものとして捉えられている。

さまざまな記述を見ると、従来、紙の文書を管理してきた業務プロセスの中に、情報通信技術が導入されてきたことが、管理のための仕組みづくりや実装を難しくしている様子が伺える。以前は、情報管理を実施するに当たり、たとえば重要な文書は、耐火性の金庫や特別なキャビネットに保管するなどしていた。これは、今でも元本性が要求される文書などについては継続している。しかしながら、紙を対象とした管理手法のなかに、新たな態様である電子の文書を対象として含まざるを得なくなったという課題に対して、ガイドラインにおいては、電子の文書も紙の文書と同様であるとの定義はあるものの、具体的な管理手法については、未発達な部分も多く残されている。

7.2.2 コンティンジェンシープランとの関係

電子化された情報という点では、情報通信システムがいかに事故に備えるかという視点で取り組まれてきたコンティンジェンシープランの普及などがある。本報告書では、この分野においては、他に参考になる文献なども多い⁷¹ため、特に調査対象として取り上げなかった。しかし、事業継続と情報資産保護との関連

⁷¹米国における「NIST SP800-34 Contingency Planning Guide for Information Technology Systems(January 2004)」、わが国では、財団法人 金融情報システムセンター（FISC）が作成した「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(1994年1月)」などがある。それぞれ対象が行政機関や金融機関と限られているものの、参考になる資料である。

を議論するにあたって、重要なポイントであることには変わらない。

電子化された情報の保管に関する対応において、情報通信技術が業務に利用され始めた頃は、バックアップにも時間やコストがかかるため、どの情報のバックアップを取るかについては自ずと取捨選択が行われていたようである。しかし、技術の急速な進歩により、取捨選択の手間をかけるよりも、全てのデータをバックアップしておく方が、時間もコストも削減できるようになった。その流れの中で発展を続けているのが、バックアップやストレージ・セントリックの技術である。さらに時間が経過し、情報通信技術の便利さにより情報量が膨大になってしまった現在、「とても全てのデータのバックアップは取れない」という状況にある。

コンティンジェンシープランについて、たとえば、すでに公表されている NIST SP800-34 は、IT システムに関するコンティンジェンシー・プランニング・ガイドと、対象を IT システムに限定しているが、FISC の手引書は、代替オフィスや安否確認についても言及しており、情報システム関連を中心にすえているものの、その対象範囲は拡大されている。

このように、定義が流動的な状況ではあるが、バイタル・レコード・マネジメントとコンティンジェンシープランの関係を考える際に、ひとつの解釈として、事業継続の視点から対策の対象とすべき情報資産を特定し、保護すべきレベルを決めるまでのプロセスは、バイタル・レコード・マネジメントのノウハウが主として活用でき、保護すべきレベルを決める際に、システム上の要件からの判断を行い、さらに具体的な対策のための技術選択の段階までを主としてカバーするのが、コンティンジェンシープランという捉え方も可能であろう。

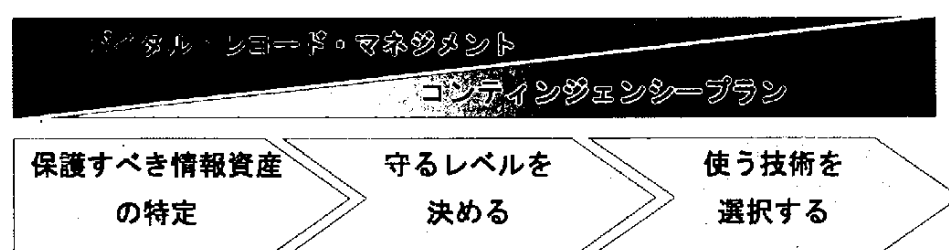


図 27 バイタル・レコード・マネジメントとコンティンジェンシープラン

FISC のように、コンティンジェンシープランを緊急事態準備計画と同等と

位置づける場合、バイタル・レコードに係る施策もその一部として、プロセスの中で特定し管理のための仕組みや対策を考えるという相互関係もあり得る。この点については、用語の定義や解釈が統一されていない現状では、個々の組織において、実装段階で整理することによる対応が適当であろう。

いずれにしても、今必要なのは、情報管理、もしくは文書管理の分野で培ってきたノウハウを、いかにして、電子化された情報の管理に展開するかを考えることである。実際、すでに、それを志向した支援技術である ILM も開発されており、今後更なる発展が望まれる。

7.2.3 事業継続におけるバイタル・レコード

欧米におけるバイタル・レコードの概念は、わが国でも活用できるのかについて考察したい。

まず、情報の分類や活用・保管形態について、法的に要求されている事項と個々の組織で意思決定をしなければならないことを理解し、適切な判断を下さなければならないという点は、自明である。

法的に要求されている事項の例として、わが国では、表 9 に示すように、経営上の重大な意思決定に関する記録や財務関連文書などの保存年限がある。

表 9 文書の法定保存年限（例）

文書例	保存年限例	法令
株主総会議事録	10 年	商法
取締役会議事録	10 年	商法
固定資産台帳	10 年	商法
伝票類	7 年	法人税法
有価証券報告書	7 年	法人税法
会計士監査報告書	5 年	商法
代金支払に関する書類	7 年	法人税法
売買基本契約書	5 年	商法
個別契約書（注文書・請書）	5 年	商法
業務委託に関する契約書	5 年	商法
図面に関する書類（図面・設計変更通知書等）	10 年	製造物責任法
特許出願に関する書類（出願明細書・経過書類）	20 年	特許法

このように保存年限や元本性などの法的要求事項が明確な場合、該当する文書や記録は、バイタル・レコードとして分類可能である。しかしながら、法的要求事項に不明瞭な点が残っている場合は、対応する側は、難しい決断を迫られる。e-文書法などに関連して議論されているが、日常的な業務の中で、文書を最初から電子的に作成するケースが増えた現在、電子的な文書がどのような技術要件を満たせば、これまで紙の文書において認められてきた証拠性などの要件と同等とみなされるかについて、さらに活発な議論が必要である。あいまいさが残った場合、マネジメント上は、どうしても安全サイドに振り、“紙の文書も保管しておこう”という判断を下すことになる。これは、効率化やコスト削減の観点からは決してよいことではない。特に、今後、法制度において、文書形態や保存年限、元本性や真正性の保証に係る規定がなされる場合は、参照されるガイドラインなどにおいてもまた、法と同等の厳格さが必要であろう。

法制度上の要求事項がない情報については、その保管方法や期間などは、個々の組織の判断に委ねられる。バイタル・レコードの特定方法も、各組織で開発することになるが、その際のポイントは、事故などが発生した後、喪失したり損傷したりすることによって、業務遂行上、大きな影響を与える情報は何かという点である。この範疇に入る情報の中でも、まず考えられるのが、組織全体で、真正性の確保や長期保管が必要と判断した“情報”であり、企業であれば全社的な共通ルールで規定する類の文書や記録である。それ以外の情報については、個々の業務プロセス分析の過程で、重要であると認定することになる。どちらの分類においても、バイタル・レコードとして特定されるものが含まれる。

規格やガイドラインによると、こういった一連のバイタル・レコード特定作業は、ビジネスインパクト分析プロセスの一部として組み込まれている。

組織の規模にもよるが、業務プロセス分析、もしくはビジネスインパクト分析は、経験やヒアリングのための時間がかかる。したがって、法的な要求事項の対象となる情報に加え、規格やガイドラインを参照し、分析せずとも明らかにバイタル・レコードとして分類可能な情報については、各部門での分析プロセスと同時進行で対策を考えていく方が、現実的であろう。事故や事件は、いつおこるかわからない。必ずしも全ての分析結果を受けて対策を考えるのではなく、できるところから対策を打つといった柔軟な考え方もまた必要である。

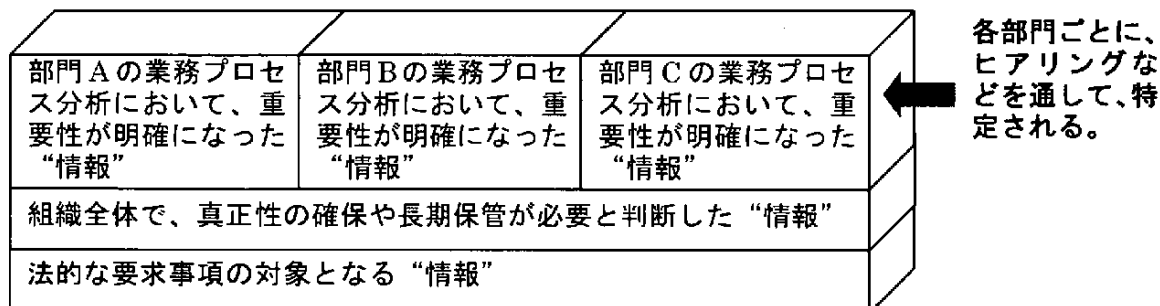


図 28 情報の重要度特定プロセス

一連の分析プロセスの結果として落とし込む情報の分類例としては、「クラス 1：バイタル」、「クラス 2：重要」、「クラス 3：有用」の 3 段階に分けている「ANSI/ARMA 5-2003 Vital Records Programs」などが参考になる。今後は、このような情報の分類についても、わが国の現状、業種ごとの違い、業務内容ごとの違いなどを考慮したガイドラインや参考資料が充実していくとよいであろう。また、これらは、前述の専門家の育成とも連携しながら進めることが望ましい。

7.2.4 支援技術との関連

分類された情報、なかでもバイタル・レコードとして特定した情報を、どう管理するかという課題に取り組むには、現状において、組織の情報、特に電子化された情報がどのように管理されているかを基盤にしなければならない。

情報管理に係る技術の変遷を概観すると、1980 年代から 90 年代に渡って、導入が進んだエンドユーザーコンピューティング (EUC) により、サーバーが様々な拠点に分散し、管理が困難になっているという現状が指摘できる。わが国の多くの企業などでは、情報資産が物理的に点在し、且つ会社として完全には把握できていないのではないだろうか。そのような状態では、重要な情報資産の在り処や、冗長性を持たせるべきシステムについて、誰も判断できない。

現在、事業継続は注目されており、「事業継続」と銘打った様々なソリューションやサービス、ハードウェアやソフトウェアがリリースされている。その技術の基本的な事項を理解し、何がどの程度できるのか、実運用に耐えるレベルにあるかなどを検証することが重要である。たとえば、第 5 章で取り上げた、バックアップ技術については、すでに多くのサービスが提供されており、利用している組織も少なくない。技術的にも、業務の復旧が数秒～数分の間にできるように、

完全に二重化を行うホットサイトと呼ばれるバックアップサイトなどの導入も進んでいる。また、ストレージ・セントリックは、サーバーを統合して管理しようという考え方で、すでに SAN や NAS と呼ばれる技術が普及しつつある。

しかしながら、これらの技術上の議論は、“どの情報を対象とするか”という点には言及していない。極端に言えば、“とにかく全て取っておこう”という考え方である。金融機関や行政機関など、コストをかけてでも、二重化をしておく価値がある業務であれば可能であるが、その他の業種や業務プロセスにおいては、膨大な情報を取り扱うようになった現在、やはり情報の分類や使われている状況によって、利用する技術も変えるという発想が必要であろう。

どの技術を採用するにしても、まず行うべきは情報資産の整備である。そのためには、情報資産の洗出しを行いサーバーの統廃合やストレージ・セントリックを含めた情報資産の再配置を検討する必要がある。

情報資産の整備を行い、まず最優先に復旧させる必要のある情報資産を特定し、その運用やバックアップ・リストア体制の評価を早急に行う必要がある。その中で脅威が想定される場合には、技術動向を考慮した上で新たな対策を講じることが重要である。

そのような考え方に基づいた技術も最近登場している。第 6 章の最後に紹介している『Information Lifecycle Management (ILM)』と呼ばれるもので、情報の「発生」⇒「処理」⇒「保管」⇒「保存」⇒「破棄」という一連のライフサイクルの中で、各段階でどのような技術を活用していけばよいかを考えたものである。技術の選択が変化する段階で、たとえば、本当に保管する必要がある情報なのか、といったかたちで情報の取捨選択が行われる。

ILM は、まさに、これまでの紙の文書を対象とした文書管理のノウハウと情報通信システム上のデータの処理方法とが融合したコンセプトといえよう。このような考え方が、今後さらに発展することにより、コストを抑えながらも重要な情報資産が保護され、必要なときに使えるようになり、目指す事業継続が実現するものと思われる。

7.3 社会的課題

事業継続に係る課題について、直面している社会的な課題や、さらに発展させる必要があると思われる点について、これまで触れなかった内容を中心に、ここで、まとめる。

7.3.1 事業中断リスクの計量化（含む再構築コスト）

実際の事業継続マネジメント体制の構築に、どれほどの経営資源を投入すべきか、といった経営判断は極めて難しいとされるが、その経営判断をできるだけ客観的にできるよう支援する事業中断リスクを科学的に分析・計量化がシミュレーションできるような方法論やツールの開発もスキル開発と併せて必要である。

7.3.2 インシデント及びニアミスのデータ収集と分析

事業中断リスクの計量化の精度向上やトップダウン・アプローチにおけるシナリオの現実性向上のためにも、実際に発生した事故や発生に至らなかったニアミス事例の収集と分析を行えるような仕組みの導入とスキル開発が望まれる。

7.3.3 業界内の知識・ノウハウ共有

マーケットでは競合するものの、同業がゆえに共通する業務プロセスや発生可能性の高い障害や事故パターンについては、原因分析や対応策に関する知識・経験の共有をプロフェッショナル人材を通じて積極的に行うことで、業界全体のレジリエンシーを向上させる、というスタンスを特に日本の主要業界は持つべきである。

7.3.4 経営判断プロセスへの反映

プロフェッショナル人材のみならず、経営者自らも業務継続マネジメントの方法論や手順を理解し先導することで、実際の経営判断に活かすことが可能となる。事業継続マネジメントと経営判断プロセスの間に乖離がある場合は、大きな戦略的欠落となり、「想定外」⁷²の要因で事業中断を回避できなくなる可能性も高くなる。

7.3.5 レジリエンシー文化の定着

事業継続マネジメント体制の実効性は、末端の一従業員のマインド・セットにまで浸透していなければ全社的なプログラムとしてのレジリエンシーは保証されない。これはごく少数の従業員による不祥事や誤判断が全社に影響を及ぼし、マスコミ経由の社会的な制裁のみならず、経済的なダメージを受けることで中には事業を諦めざるを得なくなった事例がこのところ散見されることから、企業文化としてしっかりと定着させることがいかに重要かがわかる。

⁷² 戦略的に事業継続マネジメント体制を構築・運用していれば想定されていた。

7.4 まとめ

本報告書では、事業継続に係る最新動向や情報資産保護について、国内外の調査をもとにまとめてきた。全体を概観すると、事業継続が古くて新しいテーマであるという姿が見えてくる。わが国では、地震防災として蓄積され開発されてきた多くの知識や技術がある。しかし一方で、事業継続については基本となる言葉の使い方が統一されていない、プロフェッショナル人材が不足している、実践上の方法論も未発達であるなど、多くの課題を抱えている。もともと、これはわが国だけの問題ではない。9・11同時多発テロ以降活発化してきた米国での取組みやシンガポールにおける政府主導の普及活動、そして国際標準化の動きなど、グローバルなレベルでも事業継続の浸透はこれからという感がある。

では、企業等の組織は、どうすべきか。先進的に取り組んでいるさまざまな組織での調査結果が物語るのは、状況に合わせた柔軟なアプローチである。事業継続の基本方針をできるだけ簡略化し、グローバル展開を容易にしたり、コミュニケーションラインさえ確保できれば何とか復旧できるとして、接続テストに絞った検査を行うなどの割り切りがある。情報資産保護についても、法的要求事項に該当する記録を中心としたバイタル・レコードをまず特定して保護するという考え方も同様である。

事業継続に関して、実は我々は過去に良い経験をしている。Y2K問題である。当時、多くの組織は、シナリオシミュレーションを行い、対応計画を策定した。残念なのは、その際の経験が、今に生かされていないことである。いつ、どのような形で起こるかわからない事故や事件に対して、危機感を持ち続けるのは容易ではない。しかしながら、計画を更新し、必要な資産を保護し、復旧への訓練を繰り返して備えることが、事業継続の本質である。各々の組織は、まず、このような継続的な取組みを支える体制を構築することが重要である。また一方で、社会的取組みとして、ガイドラインなどのさらなる整備やプロフェッショナル人材の育成などの支援策も、産官学が一体となって推進する必要がある。

— 禁 無 断 転 載 —

平成 18 年 3 月発行

編集：富士ゼロックス 株式会社

〒107-0052 東京都港区赤坂二丁目 17 番 22 号 赤坂ツインタワー東館

TEL:03-3585-3211 (代表)

発行者：財団法人 日本情報処理開発協会

〒105-0011 東京都港区芝公園 3-5-8 機械振興会館内

TEL:03-3432-9386

E-mail:info@isms.jipdec.jp

印刷所：山 陽 株 式 会 社

東京都千代田区神田神保町 1-18

TEL:03-3293-5411

