TTC技術レポート
Technical Report

TR-1047

クラウドセントリック ディザスタリカバリ計画 ガイドライン

Guideline of cloud centric disaster recovery planning

第 1 版

2013 年 11 月 28 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

目　次

＜参考＞

１．　国際勧告等との関連

本技術レポートに関する国際勧告はない。

２．改版の履歴

版数	制定日	改版内容
第1.0版	2013年11月28日	制定

３．参照文章

主に、本文内に記載されたドキュメントを参照した。

４．技術レポート作成部門

第１．０ 版　：　セキュリティ専門委員会

５．本技術レポートの作成について

本技術レポートは、総務省が委託により実施した研究開発プロジェクト「災害に備えたクラウド移行促進セキュリティ技術の研究開発」の成果の一部としてまとめられた文書を、TTCセキュリティ専門委員会の審議を経てTTC技術レポートとして公開するものである。

1. 目的と適用範囲

1.1 目的

クラウド環境を利活用した ICT(Information and Communication Technology)サービスの提供が進展し、国民生活や社会経済活動を支える基盤となりつつある。一方、利用・共有型となるクラウド環境を利活用し、大規模災害等が発生しても機能不全や情報損失が起こらぬよう、利用者にとって安心・安全な ICT 利活用環境を実現することが必要である。

本ガイドラインは、その中で、2011 年 3 月 11 日の東日本大震災や昨今のクラウドサービスにおけるデータ損失事故などから情報システムにおけるデータ・システムのバックアップが重要視されてきていること、従来の所持・占有型のシステムに比べコスト対効果が高い利用・共有型のクラウドサービスが普及してきていることから、大規模災害等を踏まえてクラウドの利用も視野に入れたディザスタリカバリ計画(DRP)を策定することを支援するものである。

特に、現状ディザスタリカバリ(DR)向けのバックアップに関する広く知られた標準的な手法やガイドラインなどが無いことにより、効果的なバックアップを行えていない、間違ったバックアップを行っている等の問題があり、クラウドの利用を踏まえたディザスタリカバリ向けのバックアップシステムの要件定義を支援することを目的としている。

1.2 適用範囲

本ガイドラインでは図 1-1 に示すように、組織(業務・サービス含む)の事業継続管理/計画(BCM/BCP)のうち、IT システムに関する部分の機能継続管理/計画は IT-BCM/BCP と定義し、そのうち、データセンタ機能を喪失するような大規模災害への対策やその計画を DR/DRP として定義している。また、IT システム全体の機能継続性を確保する目標を達成するための手段となる高信頼化技術の中で、事後回復のための高信頼化技術として、障害復旧のために適用されるバックアップ技術の一つとして位置づけられるものが、DR 向けバックアップ技術である。

本ガイドラインはこのような位置付けの DR 対策やその計画(DRP)を策定する際に適用されるもので、その実現手段となる DR 向けバックアップシステムをコスト対効果の良いクラウドの利用も視野に入れ、実現する場合に利用する。

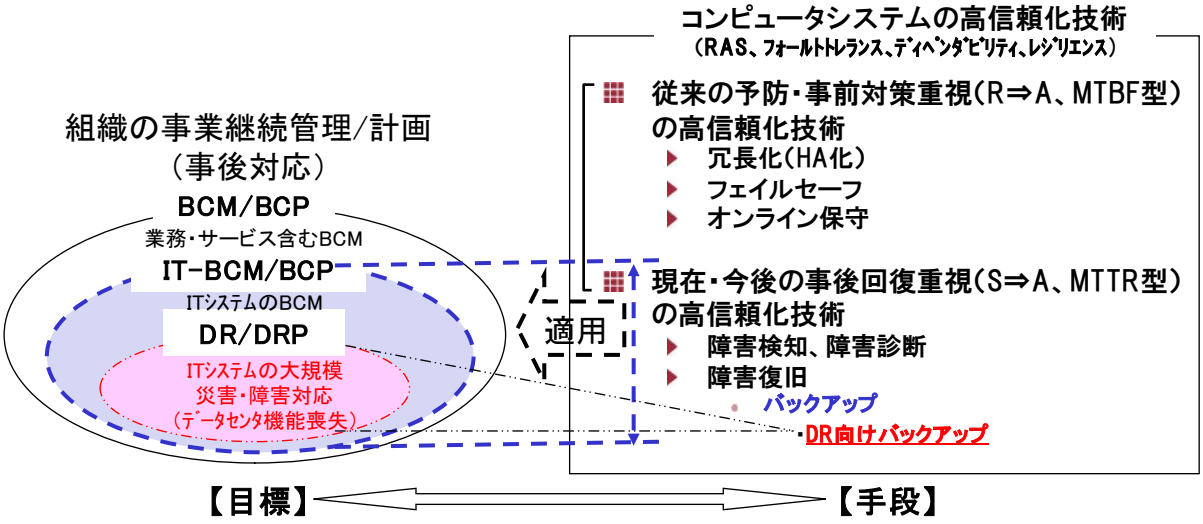

図 1-1　本ガイドラインの位置づけ

本ガイドラインの範囲は、バックアップシステムを実現するプロセス(計画、構築、監視・監査)においては計画フェーズで利用するもので、そのアウトプットは DR 向けバックアップシステムの要件仕様(計画書やスケジュール作成は含まない)である。そのため、本ガイドラインは構築フェーズの基本設計に反映されるものとなり、実装上の方式などは構築フェーズの詳細設計で実施することを想定している。
またバックアップシステムの構築にあたっては、新規開発する場合と既設のバックアップシステムを持つ場合があり、既設のバックアップシステムを持つ場合は、本ガイドラインを用いて最適なバックアップシステムを決定した後、既設のバックアップシステムとのギャップ評価を行い、移行性を考慮してバックアップシステムを決定、移行計画の策定などを実施することを想定している。

1.3 ガイドラインの見方

本ガイドラインの利用者は、DR システムの構築(新規・移行)を検討している組織の情報システム部門の技術者(企画・構築担当)を基本的に対象にしている。また、本ガイドラインでは、バックアップシステムとしてクラウドを利用する場合の“クラウド”とは、クラウド事業者によって提供されるパブリッククラウドのことを指している。

1.4 用語定義

本ガイドラインで利用する用語の定義を表 1-1 に示す。

表 1-1　用語の定義

用語及び略語	定義
BCM(Business Continuity Management) 事業継続管理	事業継続計画の策定から、その導入・運用・見直しという継続的改善を含む、包括的・統合的な事業継続のための管理プロセス。
BCP(Business Continuity Plan) 事業継続計画	通常業務の遂行が困難になる事態が発生した際に、事業の継続や復旧を速やかに遂行するために策定される計画。
CDP(Continuous Data Protection)	書き込まれるデータの更新内容を常に監視し、変更箇所を継続的にコピーすることで、更新データをよりリアルタイムにバックアップデータに反映する技術。
DR(Disaster Recovery) 災害対策	大規模(広域)災害・障害などによりコンピュータシステムが大規模レベル(例：データセンタ機能喪失)でダウンしても、あらかじめ想定した時間内に復旧するために実施する手段のこと。
DRP(Disaster Recovery Plan) 災害復旧計画	大規模(広域)災害・障害などによりコンピュータシステムが大規模レベル(例：データセンタ機能喪失)でダウンしても、あらかじめ想定した時間内に復旧するための計画。
HA(High Availability) 高可用性	コンピュータシステムの可用性が高い状態のこと。
IT-BCM(IT Business Continuity Management)	BCM のうち、IT に関わる部分。 業務としての継続性を確保するために、コンピュータシステムがダウンしても、あらかじめ想定した時間内に復旧できるよう管理すること。
IT-BCP(IT Business Continuity Plan)	BCP のうち、IT に関わる部分。 業務としての継続性を確保するために、コンピュータシステムがダウンしても、あらかじめ想定した時間内に復旧するための計画。
LAN フリーバックアップ	バックアップを行うときのデータ転送に LAN などのネットワークを使用しないでデータストレージ専用の高速ネットワーク環境を使用すること。
MTBF(Mean Time Between Failure(s)) 平均故障間隔	コンピュータシステムが、使用を開始してから故障するまでの時間の平均値。
MTTR(Mean Time To Recovery) 平均復旧時間	故障したコンピュータシステムの復旧にかかる時間の平均値。
RAS(Reliability, Availability, Serviceability)	コンピュータシステムが期待された機能・性能を安定して発揮できるか否かを検証するための評価軸で、信頼性(Reliability)、可用性(Availability)、実用性(Serviceability)の頭文字をとったもの。
RPO(Recovery Point Objective)	システム障害などでデータが損壊した際に、データのリストアによってリカバリ可能な過去のある時点の目標。

用語及び略語	定義
目標復旧時点	
RTO(Recovery Time Objective) 目標復旧時間	コンピュータシステムが障害などで停止した際に、復旧するまでの目標時間。
SLA(Service Level Agreement) サービス品質保証契約	あるサービスについて、事業者が提供するサービスの品質を定量的な指標によってあらかじめ明示する品質保証契約。
オフラインバックアップ	サーバを停止している状態でバックアップをとること(反対語は、オンラインバックアップ)。
オンラインバックアップ	サーバが起動している状態のままバックアップをとること(反対語は、オフラインバックアップ)。
仮想データセンタ	複数のデータセンタの IT リソースを統合し、アプリケーションの要求に合わせて、IT リソースを割り当てる技術。
機密分散データ保管	暗号化した情報を分散化して管理し、その一部が流出・漏えいしても元の情報を推測できないようにするセキュリティ技術。
クラウド	従来は手元のコンピュータで管理・利用していたようなソフトウェアやデータなどのコンピューティング資源を、インターネットなどのネットワークを通じてサービスの形で必要に応じて利用する方式。 クラウドの実装方式としては、一般に公開利用されるパブリッククラウドや特定の企業等で利用されるプライベートクラウドがあるが、本ガイドラインでは、パブリッククラウドの意味で利用する。
サイト間フェイルオーバ	コンピュータシステムに障害が発生した際、別サイトのシステムに自動的に処理を切替え、そのまま処理を続行すること
差分バックアップ	前回のフルバクアップ時からの変更／追加されたデータのみを複製するバックアップ方式。
センタバックアップ	異なるセンタの IT システム間で、空きリソースを利用して相互にバックアップを行う手段。双方が本番仮想するシステムである Active-Active 型や本番環境と開発環境でバックアップを行うタイプなどがある。
増分バックアップ	前回のフルバックアップ時からの変更／追加されたデータのみを複製するが、次回増分バックアップを行う際は直前の増分バックアップの変更／追加分だけが複製されるバックアップ方式。
重複除外技術	バックアップ先のデータと重複しないデータをデータブロックレベルで増分バックアップすることで、バックアップデータの転送容量を削減する技術。

用語及び略語	定義
ディペンダビリティ	信頼性（Reliability）、保全性（Maintainability）、可用性（Availability）などを総合した広義の信頼性のこと。確率的な意味を持つ「Reliability」にとどまらず、人間の操作ミス、悪意のあるデータ改変といったエラーがあっても動作するなど、システムがどの程度頼りになるかの概念。
テープ/ディスクベースバックアップ	バックアップデータをテープ/ディスクに取得し、障害時にそのデータをリストアする技術。
バックアップ	バックアップとは、支援や予備のことであり、データやシステムのバックアップとは、複製(コピー)をあらかじめ作成し、たとえ問題が起きてもデータを復旧できるように備えておくこと。
バックアップシステムオプション	バックアップシステムの候補。
バックアップシステムの信頼性	バックアップシステムに対する利用者の安心感の度合い。評価要素としては、バックアップシステムが自前(オンプレミス)かあるいは借用(クラウド利用)か、クラウドであれば、サービス品質の保証、セキュリティ対策の可視化、コンプライアンスやフォレンジックへの対応の充実度などが挙げられ、これら要素を考慮して定性的に評価。
フェイルオーバ	コンピュータシステムに障害が発生した際、予備のシステムに自動的に処理を切替え、そのまま処理を続行すること。
フェイルセーフ	コンピュータシステムにおいて、誤操作・誤動作による障害が発生した際、常に安全側に制御すること。
フォールトトレランス	コンピュータシステムに障害が発生した際、正常な動作を保ち続けること。
フルバックアップ	必要なデータ全てを一度にまとめて一括に複製するバックアップ方式。
ミラーリング	ハードディスクに記録する際に 2 台以上のディスクを用意し、全部のディスクに同じデータを書き込むことで信頼性を上げること。
リストア	データが損壊した際に、バックアップされたデータを用いて、データを復元すること。
レジリエンシス	大規模(広域)災害・障害などによりコンピュータシステムが大規模レベル(例：データセンタ機能喪失)でダウンしても、影響範囲を最小限に抑え、サービスを復旧させる回復力。
レプリケーション	あるデータベースと同じ内容の複製(レプリカ)を別のコンピュータ上に作成し、内容を同期させること。

2. 最近の震災・事件から再確認されたバックアップの重要性

2011 年 3 月 11 日に発生した東日本大震災以降、企業では事業継続計画(BCP)への取り組みの強化に対する意識が高まっており、特にディザスタリカバリ(DR)に対する取り組みが重要視されてきている。ディザスタリカバリの有効な手段にバックアップがあり、情報システム部門に対して行った BCP の強化に伴って利用が進みそ

うな ICT 分野についてアンケートを実施した結果(出典；日経 BP ムック「IT で実現する 震災・省電力 BCP 完全ガイド」(2011.6.16)[1])では、最も回答が多かったのは「サーバ等の分散化、別拠点バックアップ」となっており、バックアップの利用が増加する傾向にあるといえる。また、「クラウドコンピューティング関連」についても特に流通業において「サーバ等の分散化、別拠点バックアップ」に次ぐ関心を得ており、BCP の強化にクラウド利用への関心が高いことがわかる。その他の調査結果(出典；JUAS (一般社団法人 日本情報システム・ユーザー協会)「企業 IT 動向調査 2012」(2012.5.28)[2])からも、BCP の対策状況として検討中の対策で最も多かった回答が「クラウド・コンピューティングへの転換」(検討中：38.0%)となっており、今後クラウドの利用を重要視していることかがわかる。

以上からも、今後、BCP やディザスタリカバリの対策として、バックアップとクラウドの利用が増加する傾向にあることがうかがえる。また、従来の独自構築型バックアップシステムによるディザスタリカバリ対策では、本番サイト以外の遠隔バックアップサイトを設けるため二重投資を必要とするものであり、これまで中小企業などでは、コスト面で対応困難なものであった。しかし、従来の数十%のコストで実現可能な手段になってきているクラウド利用によるバックアップシステムの構築は、特にこのような中小企業などにとって、今後は有望になるものと考える。

ただし、今後クラウド利用が加速していくには、一般的にクラウド利用に期待されるコスト削減や効率良く情報システムを立ち上げられるという経済性や移行性だけでなく、クラウド環境の信頼性・安全性を一層強化させることが必要である。これは、2012 年 6 月 20 日に発生したあるクラウド事業者提供のクラウドサービスで大量データが消失する事故からも伺える([3])。この事故により約 5,700 件の利用サービスのデータが消失し、本番データと同じサーバ環境下に置いていたバックアップデータも消失したことにより、多くの顧客データが復旧できない事態に陥っている。このようにマルチテナント環境で構築されるクラウドでは、一旦データ消失などの事故が発生すると多数の利用顧客に多大な影響を及ぼす可能性があり、そのようなことがないようクラウド環境の信頼性・安全性を確保し、利用者に安心感を提供してクラウド利用を促進するために、データ・システムのバックアップ技術は、核になる技術として重要となる。

3. DR 向けクラウドバックアップの計画プロセス概要

DR 向けクラウドバックアップの計画プロセスは、図 3-1 に示すように利用者組織にて策定された IT-BCP を受けて、対象となる業務・IT システム毎に、DR アセスメント、DR 要件定義、DR 対策策定の順で実施し、各業務・IT システムに適したバックアップシステムを特定する。特定したバックアップシステムが実際の実装機能の状況や制約等、実現・実装制約上可能かを確認し、可能であれば特定したバックアップシステムを最適なバックアップシステムとして決定する。また、不可能な場合には、まずは DR 対策策定時の代替のシステム候補(オプション)で対応可能かを確認し、それでも対応不可能な場合は、DR 要件定義に戻り、特定バックアップシステムを基に、実現・実装制約を満足するようにバックアップ技術を組み合わせたカスタムシステムオプションを作成し、実現・実装制約を満たすバックアップシステムを決定する。通常、IT システムの要件定義段階では、実装を意識しないものであるが、要件の実現可能手段がないものでないかどうか(特にクラウド利用の場合)を事前に確認する目的で、このような確認・フィードバック処理も設けている。

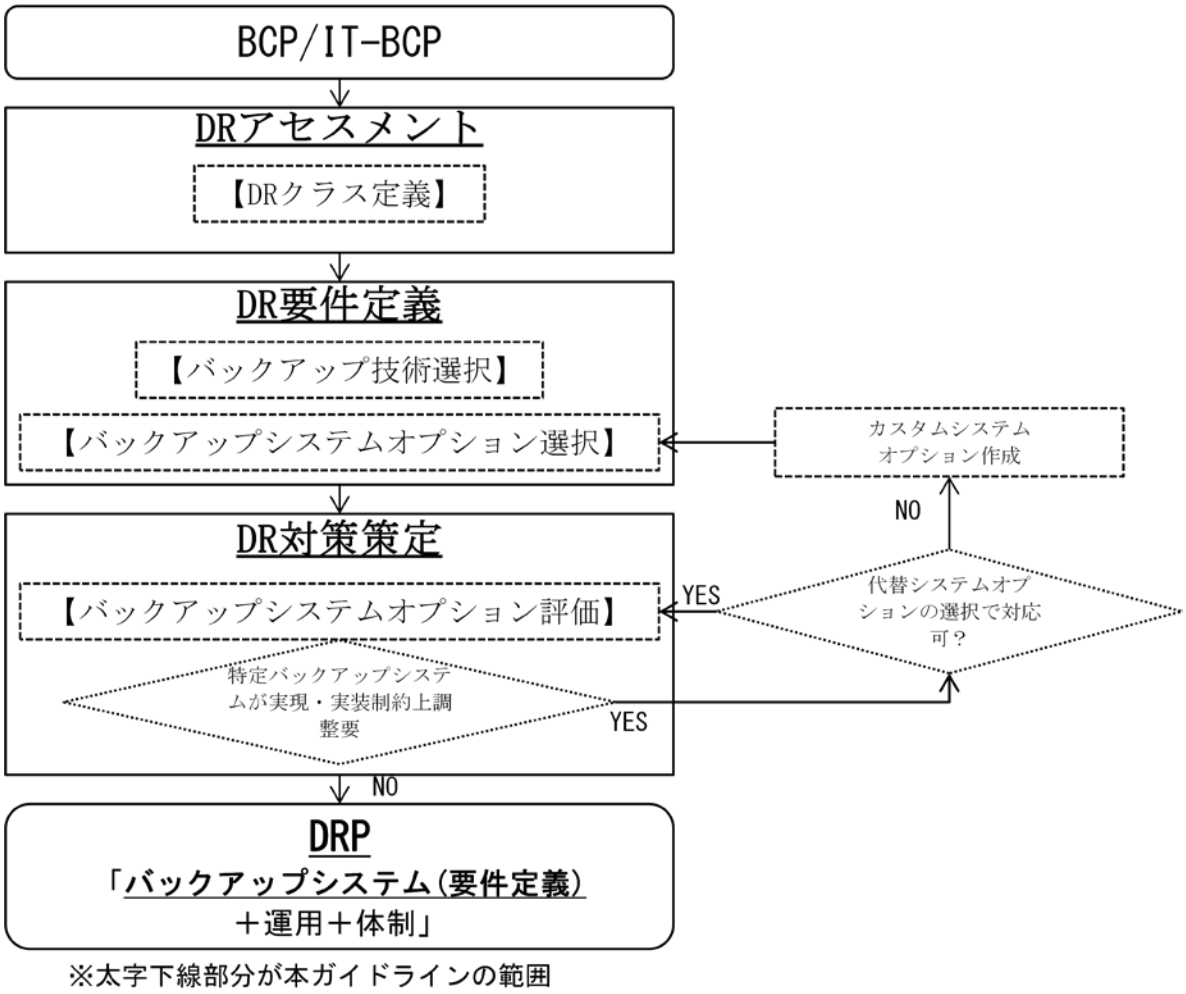

図 3-1　DR 計画プロセス

以下に、本ガイドラインで定義する計画プロセスの入力と出力を示す。

【本ガイドライン計画プロセスの入力】

利用者組織にて IT-BCP が策定されていることを前提に、以下の策定結果を入力とする。

＜IT-BCP からの入力＞

・ 業務・IT システムの一覧
・ 業務・IT システムの影響分析結果
・ 許容総コスト
・ 業務別想定リスク一覧

＜IT-BCP 外からの入力＞

・ 対象 IT システムの仕様(データ量、既存バックアップ資産など)

【本ガイドライン計画プロセスの出力】

出力される DRP については、バックアップシステムの要件仕様(要件定義)までを範囲とし、運用、体制にかかわる計画書や実行スケジュールは、バックアップシステムの要件仕様をもとに各利用者が個別に検討・作成す

る。

図 3-1 のプロセスによりバックアップシステムを検討するための方式概要を図 3-2 に示す。

本方式は IT-BCP 及び IT-BCP 外からの入力情報をもとに、「DR クラス定義表」、「バックアップ技術選択表」、「バックアップシステムオプション選択表」、「バックアップシステムオプション評価表」を参照ツールとして用いた誘導型で容易にバックアップシステムを決定する方式としている。

まず、「DR アセスメント」プロセスにおいて、対象 IT システムのバックアップの対策優先順位を反映した DR クラスを選定する。次に、「DR 要件定義」プロセスにおいて、選定した DR クラスに該当するバックアップ技術やその組合せで構成されるバックアップシステムオプション(バックアップシステム候補群)を、バックアップ技術選択表とバックアップシステムオプション選択表より選択する [1]。最後に、「DR 対策策定」プロセスにおいて、選定した複数のバックアップシステムオプションを、バックアップシステムオプション評価表により評価し、オプションの中から最適なバックアップシステムを決定する。

なお、「DR アセスメント」プロセスにおいて、バックアップ対象 IT システムの対策優先順位を示す DR クラスに適当なクラスがない場合には、カスタム DR クラスとして、最も近い DR クラスを参照して、独自に、バックアップ技術を選択し、選択したバックアップ技術を組み合わせたカスタムシステムオプションを生成・評価して、バックアップシステムを決定することもできる。

[1] バックアップ技術選択表とバックアップシステムオプション選択表は、バックアップの最新技術動向を踏まえて、定期的に改訂することが望ましい。

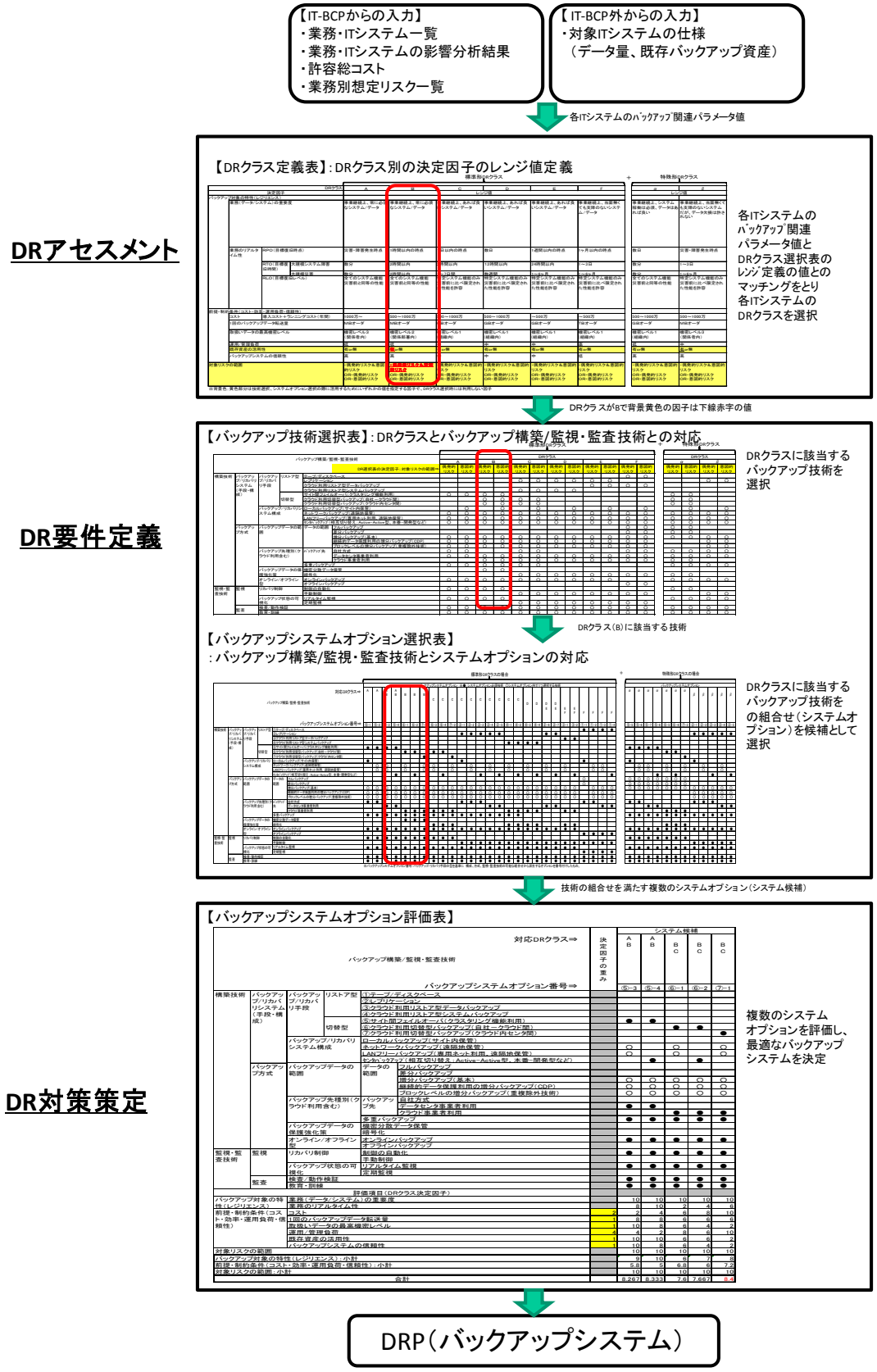

図 3-2　バックアップシステム検討方式概要

4. DR 向けクラウドバックアップの計画プロセス詳細

4.1 DR アセスメント

IT-BCP の策定の結果(業務・システムの影響分析結果)として、DR 対策の対象とした各 IT システムのバックアップ関連パラメータ値を明確にし、それをもとに DR クラス(DR 対策の優先順位クラス)を選択する。

図 4-1 に DR アセスメントの詳細プロセスを示す。

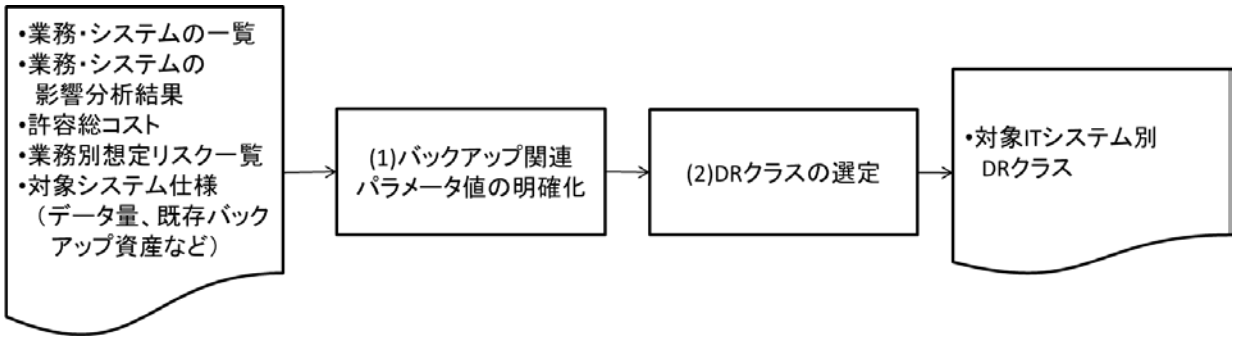

図 4-1　DR アセスメント詳細プロセス

4.1.1 IT システムのバックアップ関連パラメータ値の明確化

以下の関連パラメータ値を明確化する。その際、値の定性値や定量値の取り方は「DR クラス定義表」(図 4-2)を参考に設定する。

(1) バックアップ対象の特性(レジリエンス)に関するパラメータ

- 業務(データ／システム)の重要度
- 業務のリアルタイム性；RPO(目標復旧時点)
- 業務のリアルタイム性；RTO(目標復旧時間)
- 業務のリアルタイム性；RLO(目標復旧レベル)

(2) 前提・制約条件(コスト・効率・運用負荷・信頼性)に関するパラメータ

- 許容対策コスト；(導入コスト＋ランニングコスト(年間))
- １回のバックアップデータ転送量(※データの保管期間が定められている法/制度により、データ量が異なることに留意)
- 取扱いデータの最高機密レベル
- 運用/管理負荷
- 既存資産の活用性
- バックアップシステムの信頼性(※個人情報を取り扱うシステムのバックアップについては信頼性の高いデータの保管場所にすることに留意)

4.1.2 DR クラスの選定(対象を DR クラス分け)

各 IT システムのバックアップ関連パラメータ値と、DR クラスの各決定因子のレンジを定義した「DR クラス定義表」(図 4-2)のレンジ定義の値とのマッチングをとり、各 IT システムの DR クラス(DR 対策の優先順位クラス)を選択する。 なお、「既存資産の活用性」と「対象リスクの範囲」の決定因子(背景色；黄色部分)は技術選択、システムオプション選択の際に活用するためにいずれかの値を指定する因子で、DR クラス選択時には利用しない因子となる。

ここで、DR クラスは、標準形クラス 6 つと特殊形クラス 2 つを定義している。これらは、従来事例(バックアップシステムの計画指針の事例)を調査・整理した結果、代表的・基本的に識別することが効果的な特徴を持つ主なタイプを分類・定義したものである。標準形 DR クラスとは、業務バックアップ対象の業務(データ)の重要度が高く、よりリアルタイム性が求められる標準的なケースについて、A～F の順に 6 段階で 6 つのクラスを定義しているものである。

また、特殊形 DR クラスとは、RPO・RTO のいずれか一方が極端に重視される特殊なケースについて、2 つのクラス(α、β)を定義しているものである。それぞれの特殊ケースについては以下のような利用例となる。

・ 特殊ケース１：リアルタイムなデータ復旧は不要だが、システム復旧は即時要

例えばエレベータを稼動・管理するエレベータシステムなど、閉じ込めなどによる事故を防止するため、災害発生時にエレベータを稼動させる機能などを優先復旧させるが、システム稼動に必要ないデータの復旧についてはある程度の余裕がある場合などが特殊形 DR クラス α に該当する。

・ 特殊ケース２：リアルタイムなシステム機能復旧は不要だが、データ欠損は許されない

例えば、銀行 ATM の電子ジャーナルシステムなど、取引データなど欠損が許されないが、システム機能の復旧自体は優先されないシステムの場合、特殊形 DR クラス β に該当する。

			標準形DRクラス						特殊形DRクラス	
DRクラス			A	B	C	D	E	F	α	β
決定因子			レンジ値						レンジ値	
バックアップ対象の特性(レジリエンス)										
	業務(データ/システム)の重要度		事業継続上、常に必須なシステム/データ	事業継続上、常に必須なシステム/データ	事業継続上、あれば良いシステム/データ	事業継続上、あれば良いシステム/データ	事業継続上、あれば良いシステム/データ	事業継続上、当面無くても支障のないシステム/データ	事業継続上、システム稼働は必須、データはあれば良い	事業継続上、当面無くても支障のないシステムだが、データ欠損は許されない
	業務のリアルタイム性	RPO(目標復旧時点)	災害・障害発生時点	1時間以内の時点	1日以内の時点	数日	1週間以内の時点	1ヶ月以内の時点	数日	災害・障害発生時点
		RTO(目標復旧時間) 大規模システム障害	数分	2時間以内	2時間以内	12時間以内	24時間以内	1～3日	数分	1～3日
		RTO(目標復旧時間) 大規模災害	数分	2時間以内	1～7日間	数週間	1～6ヶ月	1～6ヶ月	数分	1～6ヶ月
		RLO(目標復旧レベル)	全てのシステム機能 災害前と同等の性能	全てのシステム機能 災害前と同等の性能	特定システム機能のみ 災害前に比べ限定された性能を許容	特定システム機能のみ 災害前に比べ限定された性能を許容	特定システム機能のみ 災害前に比べ限定された性能を許容	特定システム機能のみ 災害前に比べ限定された性能を許容	全てのシステム機能 災害前と同等の性能	特定システム機能のみ 災害前に比べ限定された性能を許容
前提・制約条件(コスト・効率・運用負荷・信頼性)										
	コスト	導入コスト+ランニングコスト(年間)	1000万～	500～1000万	500～1000万	500～1000万	～500万	～500万	500～1000万	500～1000万
	1回のバックアップデータ転送量		MBオーダ	MBオーダ	GBオーダ	GBオーダ	GBオーダ	TBオーダ	GBオーダ	MBオーダ
	取扱いデータの最高機密レベル		機密レベル3 (関係者内)	機密レベル2 (関係部署内)	機密レベル1 (組織内)	機密レベル1 (組織内)	機密レベル1 (組織内)	機密レベル1 (組織内)	機密レベル1 (組織内)	機密レベル3 (関係者内)
	運用/管理負荷		低	低	中	中	中	高	低	中
	既存資産の活用性		有or無	有or無	有or無	有or無	有or無	有or無	有or無	有or無
	バックアップシステムの信頼性		高	高	中	中	中	低	高	高
対象リスクの範囲			・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク	・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク	・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク	・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク	・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク	・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク	・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク	・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク

※背景色:黄色部分は技術選択、システムオプション選択の際に活用するためにいずれかの値を指定する因子で、DRクラス選択時には利用しない因子

図 4-2　DR クラス定義表

なお、図 4-2 の決定因子は、標準的なバックアップ計画技術(指針)が現状見当たらないことから、従来の個別バックアップ計画指針事例での決定因子をマージし、バックアップ対象の特性(レジリエンス)、前提・制約条件、リスクの範囲の分類構成で体系的にまとめたものである。各 DR クラスの決定因子のレンジ値を定義した考え方を表 4-1 に示す。

表 4-1　DR クラス別レンジ値定義の考え方

DR クラス	レンジ値定義根拠
DR クラス A	DR クラス A は、事業継続上、常に必須なシステム/データで、システム停止やデータの欠損が許されない最もリアルタイムな復旧が求められる IT システムをバックアップ対象としたものである。 したがって、復旧目標としては「RPO」は災害発生時点、「RTO」は大規模なシステム障害、災害に関わらずに数分、「RLO」は全てのシステム機能について災害前と同等の性能での復旧を求められるものである。 また、この目標を実現するための前提・制約条件としては、リアルタイムな復旧が求められることから実現するための「コスト」が最も高く(導入＋ランニングコスト；1000 万～/システム)、リアルタイムなバックアップデータの同期が必要なため「1 回あたりのバックアップデータ転送量」を最小；MB オーダ(～999MB)とし、バックアップシステムの方式・手段も複雑になることから自動化などによる運用/管理負荷の軽減(「運用/管理負荷；低」)が必要となるものである。加えて、事業継続上常に必須なデータで欠損が許されないデータであることから、想定される「取扱データの最高機密レベル」が最も高く(機密レベル３(関係者内))、バックアップシステムへ高い信頼性(「バックアップシステムの信頼性」；高)が求められるものである。
DR クラス B	DR クラス B は、事業継続上、常に必須なシステム/データで、DR クラス A ほどのリアルタイム性が求められない数時間以内のシステムとデータの復旧が求められる IT システムをバックアップ対象としたものである。 したがって、復旧目標としては「RPO」は 1 時間以内の時点、「RTO」は大規模なシステム障害時、災害に関わらずに 2 時間以内、「RLO」は全てのシステム機能について災害前と同等の性能での復旧を求められるものである。 また、この目標を実現するための前提・制約条件としては、DR クラス A に比べ平均的なコスト(500 万～1000 万)で実現することが求められるが、DR クラス A 程ではないが「RPO」を 1 時間以内の時点とするようなリアルタイムなバックアップデータの同期が必要なため「1 回あたりのバックアップデータ転送量」を DR クラス A 同様の最小；MB オーダ(～999MB)とし、バックアップシステムの方式・手段も複雑になることから自動化などによる運用/管理負荷(「運用/管理負荷；低」)の軽減が必要となるものである。加えて、事業継続上常に必須なシステム/データであるため、DR クラス A 同様、バックアップシステムへ高い信頼性(「バックアップシステムの信頼性」；高)が求められるが、1 時間以内のデータ欠損ならば許されるデータであることから、データ欠損の許されない DR クラス A までの取扱データの機密レベルは必要ないと想定し、「取扱データの最高機密レベル」については機密レベル２(関係部署内)となるものである。

DR クラス	レンジ値定義根拠
DR クラス C	DR クラス C は、事業継続上、あれば良いシステム/データで、データについては 1 日以内の時点、システムについては最短で 2 時間以内の重要なシステム機能の復旧が求められる IT システムをバックアップ対象としたものである。 したがって、復旧目標としては「RPO」は 1 日以内の時点、「RTO」は大規模なシステム障害時には DR クラス B 同様 2 時間以内、大規模な災害時には 1 ～7 日間以内、「RLO」は特定システム機能のみ災害前に比べ限定された性能を許容されたレベルでの復旧を求められるものである。 また、この目標を実現するための前提・制約条件としては、DR クラス B 同様、平均的なコスト(500 万～1000 万)で実現することが求められるが、DR クラス B ほどの「RPO」を実現する必要がなく、日次でのバックアップも許容されることから「1 回あたりのバックアップデータ転送量」が中程度(GB オーダ(1GB～999GB))となり、DR クラス B に求められるようなリアルタイムなバックアップデータの転送やバックアップシステムへの復旧が必要とならないことから部分的には手動での運用とすることが可能(「運用/管理負荷；中」)とされるものである。加えて、事業継続上、あれば良いデータ/システムであるため、想定される「取扱データの最高機密レベル」を機密レベル 1 (組織内)とし、「バックアップシステムの信頼性」も中程度となるものである。
DR クラス D	DR クラス D では、DR クラス C と同様、事業継続上、あれば良いシステム/データだが、DR クラス C ほどのリアルタイム性は求められず、データについては数日の時点、システムについては最短で 12 時間以内の重要なシステム機能の復旧が求められる IT システムをバックアップ対象としたものである。 したがって、復旧目標としては「RPO」は数日の時点、「RTO」は大規模なシステム障害時には 12 時間以内、大規模な災害時には数週間、「RLO」は特定システム機能のみ災害前に比べ限定された性能を許容されたレベルでの復旧を求められるものである。 ただし、この目標を実現するための前提・制約条件としては DR クラス C と同レベルのものが求められ、「コスト」は平均的な(500 万～1000 万)、「1 回あたりのバックアップデータ転送量」が中程度(GB オーダ(1GB～999GB))、部分的には手動での運用とすることが可能(「運用/管理負荷；中」)、「取扱データの最高機密レベル」を機密レベル 1 (組織内)、「バックアップシステムの信頼性」も中程度となるものである。

DR クラス	レンジ値定義根拠
DR クラス E	DR クラス E については、DR クラス C、D と同様、事業継続上、あれば良いシステム/データだが、DR クラス D ほどのリアルタイム性は求められず、データについては 1 週間以内の時点、システムについては最短で 24 時間以内の重要なシステム機能の復旧が求められる IT システムをバックアップ対象としたものである。 したがって、復旧目標としては「RPO」は 1 週間以内の時点、「RTO」は大規模なシステム障害時には 24 時間以内、大規模な災害時には 1 ～6 ヶ月、「RLO」は特定システム機能のみ災害前に比べ限定された性能を許容されたレベルでの復旧を求められるものである。 また、この目標を実現するための前提・制約条件としては、DR クラス D ほどのリアルタイム性が求められないことから「コスト」を最小(～500 万)とすることが必要となるが、それ以外は DR クラス C と同じ事業継続上、あれば良いシステム/データとなることから同レベルのものが求められ、「1 回あたりのバックアップデータ転送量」が中程度(GB オーダ(1GB～999GB))、部分的には手動での運用とすることが可能(「運用/管理負荷；中」)、「取扱データの最高機密レベル」を機密レベル 1 (組織内)、「バックアップシステムの信頼性」も中程度となるものである。
DR クラス F	DR クラス F については、事業継続上、当面無くても支障のないシステム/データで、データについては 1 ヶ月以内の時点、システムについては最短で 1～3 日以内の重要なシステム機能の復旧が求められる IT システムをバックアップ対象としたものである。 したがって、復旧目標としては「RPO」は 1 ヶ月以内の時点、「RTO」は大規模なシステム障害時には 1～3 日以内、大規模な災害時には 1 ～6 ヶ月、「RLO」も最低限、特定システム機能のみ災害前に比べ限定された性能を許容されたレベルでの復旧でも許されるものである。 また、この目標を実現するための前提・制約条件としては、DR クラス E 同様、「コスト」を最小(～500 万)とすることが必要となるが、DR クラス E ほどの「RPO」を実現する必要がなく、月次でのバックアップも許容されることから「1 回あたりのバックアップデータ転送量」が大(TB オーダ(1TB～))となり、バックアップデータの転送やバックアップシステムへの復旧に余裕があることから全体的に手動での運用とすることが可能(「運用/管理負荷；高」)とされるものである。加えて、事業継続上、当面無くても支障のないデータ/システムであるが、ある程度の機密性のあるデータも含まれることが想定されることから、想定される「取扱データの最高機密レベル」は DR クラス E 同様の機密レベル 1 (組織内)とし、「バックアップシステムの信頼性」については DR クラス E に比べ低となるものである。

DR クラス	レンジ値定義根拠
DR クラス α	DR クラス α は、事業継続上、システムの稼動は必須となるが、データはあれば良いもので、DR クラス A 同様システム停止は許されないが、データは DR クラス D 同様数日前の時点に復旧できればよい IT システムをバックアップ対象としたものである。 したがって、復旧目標として、「RPO」は DR クラス D と同じ数日、「RTO」/「RLO」は DR クラス A と同じレベル(「RTO」; 大規模なシステム障害、災害に関わらずに数分、「RLO」; 全てのシステム機能について災害前と同等の性能)での復旧を求められるものである。 また、この目標を実現するための前提・制約条件としては、データについては DR クラス A ほどのリアルタイム性が求められないことから平均的なコスト(500 万～1000 万)で実現することが求められ、DR クラス D と同レベルの「1 回あたりのバックアップデータ転送量」; 中程度(GB オーダ(1GB～999GB)となるが、システムについては DR クラス A と同様、リアルタイムな監視と障害発生時の待機系システムへの即時切換えといった複雑なシステムとなることから自動化などによる運用/管理負荷の軽減(「運用/管理負荷 ; 低」)が必要となるものである。加えて、データについてはあればよいレベルのため、DR クラス D と同様で「取扱データの最高機密レベル」を機密レベル 1 (組織内))とするが、システム停止は許されないことから「バックアップシステムの信頼性」は高となるものである。
DR クラス β	DR クラス β は、事業継続上、当面無くても支障のないシステムだが、データ欠損は許されないもので、システムについては DR クラス F 同様、最短で 1～3 日以内の重要なシステム機能の復旧が求められるが、データについては DR クラス A と同じ災害復旧時点に復旧する必要がある IT システムをバックアップ対象としたものである。 したがって、復旧目標として、「RPO」は DR クラス A と同じ災害・障害発生時点、「RTO」/「RLO」は DR クラス F と同じレベル(「RTO」; 大規模なシステム障害時は 1～3 日、大規模災害時は 1～6 ヶ月)での復旧を求められるものである。 また、この目標を実現するための前提・制約条件としては、システムについては DR クラス A ほどのリアルタイム性が求められないことから平均的なコスト(500 万～1000 万)で実現することが求められるが、リアルタイムなバックアップデータの同期が必要なため「1 回あたりのバックアップデータ転送量」を最小 ; MB オーダ(～999MB)となり、データの同期については自動化など必要だが、リアルタイムな監視と障害発生時の待機系システムへの即時切換えなどは必要でないことから、部分的には手動での運用とすることが可能(「運用/管理負荷 ; 中」)とされるものである。加えて、データについては DR クラス A 同様事業継続上常に必須なデータで欠損が許されないデータであることから、想定される「取扱データの最高機密レベル」が最も高く(機密レベル 3 (関係者内))、そのようなデータを保管する必要があるため「バックアップシステムの信頼性」も高となるものである。

4.2 DR 要件定義

各 IT システムの DR クラス選択結果をもとに、DR クラスのバックアップ関連パラメータ値を満たすバックアップ技術を選択し、そのバックアップ技術から候補となるバックアップシステムオプションを選択する。

図 4-3 に DR 要件定義の詳細プロセスを示す。

図 4-3　DR 要件定義詳細プロセス

4.2.1 DR クラス別バックアップシステムオプションの洗い出し

前プロセスで選定した DR クラスと、DR クラスとバックアップ技術の対応を定義した「バックアップ技術選択表」(図 4-4)の DR クラスとマッチングをとり、該当するバックアップ技術を選択する。

このとき、DR クラス別に対象リスクの範囲(偶発的リスク、意図的リスク)によって選択するバックアップ技術が異なるため、該当するリスク範囲のパラメータ値に従ってのバックアップ技術を選択する。対象リスクの範囲のパラメータ値が偶発的リスクと意図的リスクの双方となる場合は、それぞれの該当技術の組合せが選択バックアップ技術となる。

						標準形DRクラス												+	特殊形DRクラス			
バックアップ構築/監視・監査技術						DRクラス													DRクラス			
						A		B		C		D		E		F			α		β	
					DR選択表の決定因子：対象リスクの範囲⇒	偶発的リスク	意図的リスク	偶発的リスク	意図的リスク	偶発的リスク	意図的リスク	偶発的リスク	意図的リスク	偶発的リスク	意図的リスク	偶発的リスク	意図的リスク		偶発的リスク	意図的リスク	偶発的リスク	意図的リスク
構築技術	バックアップ/リカバリシステム（手段・構成）	バックアップ/リカバリ手段	リストア型	テープ/ディスクベース												○	○					
				レプリケーション						○	○	○	○	○	○						○	○
				クラウド利用リストア型データバックアップ										○	○	○	○					
				クラウド利用リストア型システムバックアップ						○	○	○	○									
			切替型	サイト間フェイルオーバ（クラスタリング機能利用）	○	○	○	○										○	○			
				クラウド利用切替型バックアップ（自社ークラウド間）			○	○	○	○								○	○			
				クラウド利用切替型バックアップ（クラウド内センタ間）			○	○	○	○								○	○			
		バックアップ/リカバリシステム構成		ローカルバックアップ（サイト内保管）		○		○		○		○		○		○			○		○
				ネットワークバックアップ（遠隔地保管）	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○
				LANフリーバックアップ（専用ネット利用、遠隔地保管）	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ（相互切り替え：Active-Active型、本番-開発型など）	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ												○	○		○	○		
				差分バックアップ												○	○		○	○		
				増分バックアップ（基本）	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○
				継続的データ保護利用の増分バックアップ（CDP）	○	○	○	○	○	○	○	○	○	○	○	○				○	○
				ブロックレベルの増分バックアップ（重複除外技術）	○	○	○	○	○	○	○	○	○	○	○	○				○	○
		バックアップ先種別（クラウド利用含む）	ﾊﾞｯｸｱｯﾌﾟ先	自社方式	○	○			○	○					○	○		○	○	○	○
				データセンタ事業者利用	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○
				クラウド事業者利用			○	○	○	○	○	○	○	○	○	○		○	○		
			多重バックアップ		○	○	○	○	○	○								○	○	○	○
		バックアップデータの保護強化策	機密分散データ保管				○	○														
			暗号化						○	○	○	○	○	○	○	○		○	○			
		オンライン/オフライン型	オンラインバックアップ		○	○	○	○	○	○	○	○	○	○				○	○	○	○
			オフラインバックアップ												○	○						
監視・監査技術	監視	リカバリ制御	制御の自動化		○	○	○	○										○	○			
			手動制御						○	○	○	○	○	○	○	○				○	○
		バックアップ状態の可視化	リアルタイム監視		○	○	○	○										○	○	○	○
			定期監視						○	○	○	○	○	○	○	○						
	監査	検査/動作検証			○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○
		教育・訓練			○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○

図 4-4　バックアップ技術選択表

なお、表 4-2 のバックアップ構築/監視・監査技術は、標準的なバックアップ技術の体系が現状見当たらないことから、現状のバックアップ技術を調査し、構築/監視・監査技術の分類構成で整理・体系化したものである。各 DR クラスに該当するバックアップ構築/監視・監査技術を選択した際の考え方を表 4-2 に示す。

表 4-2　DR クラス別バックアップ構築/監視・監査技術選択の考え方

DR クラス	バックアップ構築/監視・監査技術選択根拠
DR クラス A	＜構築技術＞ DR クラス A のバックアップシステムは、「RPO」は災害発生時点、「RTO」は大規模なシステム障害、災害に関わらずに数分、「RLO」は全てのシステム機能について災害前と同等の性能といった最もリアルタイムな復旧を目標とし、加えて、「取扱データの最高機密レベル」が最も高く(機密レベル３(関係者内))、バックアップシステムへ高い信頼性(「バックアップシステムの信頼性」；高)が前提・制約条件となるものである。 したがって、その手段としては、リアルタイムなデータ復旧が可能な切替型で、現状セキュリティ面で不安のあるクラウドを利用せず、サイト間ファイルオーバ(クラスタリング機能を利用)の手段を選択する。その構成は、ネットワークバックアップ、LAN フリーバックアップ、センタバックアップに加え、意図的リスクのみが対象リスクとなる場合はローカルバックアップで実現することも可能である。 また、バックアップ方式は上記のようなリアルタイムなバックアップデータ転送が必要な手段となるため、増分バックアップによるオンラインバックアップ方式となり、バックアップデータ量やネットワークの転送容量によっては CDP や重複排除技術といったよりデータ転送量を削減可能な技術を選択する。加えて、高い信頼性が求められることから多重バックアップの実装や、データ機密レベルが機密レベル３(関係者内)となることからクラウド利用による保管は行わず、自社方式・データセンタ事業者を利用した現状のセキュリティ保護策で対策するものである。 ＜監視・監査技術＞ DR クラス A のバックアップシステムを運用するために、リアルタイムな監視、即時の待機系システムの切替えが必要となることから、リカバリ制御の自動化やバックアップ状態のリアルタイム監視の実現が必要なものである。 また、監査については、一般的な情報システム同様、バックアップシステムの検査/動作検証を実施するとともに、管理者に対する教育・訓練を実施する必要があるものである。

DR クラス	バックアップ構築/監視・監査技術選択根拠
DR クラス B	＜構築技術＞ DR クラス B のバックアップシステムは､DR クラス A の次にリアルタイム性が求められ、「RPO」は 1 時間以内の時点、「RTO」は大規模なシステム障害時、災害に関わらずに 2 時間以内、「RLO」は全てのシステム機能について災害前と同等の性能での復旧を目標とするが、DR クラス A に比べて、平均的なコスト(500 万～1000 万)での実現や「取扱データの最高機密レベル」; 機密レベル２(関係部署内)を前提・制約条件とするものである。 したがって､DR クラス A のサイト間フェイルオーバ(クラスタリング機能を利用)に加え、クラウドを利用したコスト対効果の高い切替型の手段も選択肢となる。その構成は、ネットワークバックアップ、LAN フリーバックアップ、センタバックアップに加え、意図的リスクのみが対象リスクとなる場合はローカルバックアップで実現することも可能である。 また、バックアップ方式は上記のようなリアルタイムなバックアップデータ転送が必要な手段となるため、増分バックアップによるオンラインバックアップ方式となり、バックアップデータ量やネットワークの転送容量によっては CDP(Continuous Data Protection)技術や重複排除技術といったよりデータ転送量を削減可能な技術を選択する。加えて、高い信頼性が求められることから多重バックアップの実装が必要となるが、データ機密レベルが機密レベル２(関係部署内)となることから、機密分散データ保管といった高セキュリティな追加セキュリティ保護策を講ずればクラウドを利用可能とするものである。 ＜監視・監査技術＞ DR クラス B のバックアップシステムを運用するために、DR クラス A 同様リアルタイムな監視、即時の待機系システムの切替えが必要となることから、リカバリ制御の自動化やバックアップ状態のリアルタイム監視の実現が必要なものである。 また、監査については、一般的な情報システム同様、バックアップシステムの検査/動作検証を実施するとともに、管理者に対する教育・訓練を実施する必要があるものである。

DR クラス	バックアップ構築/監視・監査技術選択根拠
DR クラス C	＜構築技術＞ DR クラス C のバックアップシステムは、事業継続上、あれば良いシステム/データとなることから、DR クラス B ほどのリアルタイムな復旧を目標とせず（「RPO」は 1 日以内の時点、「RTO」は大規模なシステム障害時には DR クラス B 同様 2 時間以内、大規模な災害時には 1 ～7 日間以内、「RLO」は特定システム機能のみ災害前に比べ限定された性能を許容されたレベルでの復旧を目標）、前提・制約条件も DR クラス B ほど厳しくない。(「1 回あたりのバックアップデータ転送量」が中程度(GB オーダ(1GB～999GB))、部分的には手動での運用とすることが可能な「運用/管理負荷；中」、「取扱データの最高機密レベル」を機密レベル 1 (組織内))、「バックアップシステムの信頼性」を中程度)。 したがって、リアルタイムな復旧が可能な切替型の場合はクラウドを利用してコスト対効果の高い手段を、リストア型の場合はある程度のリアルタイム性を確保できる、クラウド利用リストア型システムバックアップやレプリケーションといった手段を利用する。その構成は、ネットワークバックアップ、LAN フリーバックアップ、センタバックアップに加え、意図的リスクのみが対象リスクとなる場合はローカルバックアップで実現することも可能である。 また、バックアップ方式は上記のようなリアルタイムなバックアップデータ転送が必要な手段となるため、増分バックアップによるオンラインバックアップ方式となり、バックアップデータ量やネットワークの転送容量によっては CDP 技術や重複排除技術といったよりデータ転送量を削減可能な技術を選択する。加えて、DR クラス B に比べ「バックアップシステムの信頼性」は中程度となるが、事業継続上、あれば良いシステム/データの中では最も重要度の高いクラスと位置づけられることから、多重バックアップを実装し、DR クラス B に比べデータ機密レベルが機密レベル 1 (組織内)となることから、暗号化レベルの追加セキュリティ保護策を講ずればクラウドを利用可能とするものである。 ＜監視・監査技術＞ DR クラス C のバックアップシステムを運用するために、DR クラス B に求められるようなリアルタイムなバックアップシステムへの復旧が必要ないことから、リカバリの手動制御や定期監視によって実現されるものである。 また、監査については、一般的な情報システム同様、バックアップシステムの検査/動作検証を実施するとともに、管理者に対する教育・訓練を実施する必要があるものである。

DR クラス	バックアップ構築/監視・監査技術選択根拠
DR クラス D	＜構築技術＞ DR クラス D のバックアップシステムは、DR クラス C ほどのリアルタイムな復旧を目標とせず(「RPO」は数日の時点、「RTO」は大規模なシステム障害時には 12 時間以内、大規模な災害時には数週間、「RLO」は特定システム機能のみ災害前に比べ限定された性能を許容されたレベルでの復旧を目標)、前提・制約条件としては DR クラス C と同レベルのもの(「1 回あたりのバックアップデータ転送量」が中程度(GB オーダ(1GB～999GB))、部分的には手動での運用とすることが可能な「運用/管理負荷；中」、「取扱データの最高機密レベル」を機密レベル 1 (組織内)、「バックアップシステムの信頼性」を中程度)となる。 したがって、切替型を利用する必要はなく、ある程度のリアルタイム性を確保できる、クラウド利用リストア型システムバックアップやレプリケーションといったリストア型の手段を利用する。その構成は、ネットワークバックアップ、LAN フリーバックアップ、センタバックアップに加え、意図的リスクのみが対象リスクとなる場合はローカルバックアップで実現することも可能である。 また、バックアップ方式は、上記のようなリアルタイムなバックアップデータ転送が必要な手段となるため、増分バックアップによるオンラインバックアップ方式となり、バックアップデータ量やネットワークの転送容量によっては CDP 技術や重複排除技術といったよりデータ転送量を削減可能な技術を選択する。加えて、DR クラス C と同様「バックアップシステムの信頼性」は中程度となるが、事業継続上、あれば良いシステム/データの中では重要度が中程度のクラスと位置づけられることから、多重バックアップまでを実装する必要は無いが、DR クラス C と同様でデータ機密レベルが機密レベル 1 (組織内)となることから、暗号化レベルの追加セキュリティ保護策を講ずればクラウドを利用可能とするものである。 ＜監視・監査技術＞ DR クラス D のバックアップシステムを運用するために、DR クラス C 同様なリアルタイムなバックアップシステムへの復旧が必要ないことから、リカバリの手動制御や定期監視によって実現されるものである。 また、監査については、一般的な情報システム同様、バックアップシステムの検査/動作検証を実施するとともに、管理者に対する教育・訓練を実施する必要があるものである。

DR クラス	バックアップ構築/監視・監査技術選択根拠
DR クラス E	＜構築技術＞ DR クラス E のバックアップシステムは、DR クラス D ほどのリアルタイムな復旧を目標とせず(「RPO」は 1 週間以内の時点、「RTO」は大規模なシステム障害時には 24 時間以内、大規模な災害時には 1 ～6 ヶ月、「RLO」は特定システム機能のみ災害前に比べ限定された性能を許容されたレベルでの復旧を目標)、前提・制約条件としては DR クラス D より低コスト(～500 万)での実現が必要だが、それ以外は DR クラス D と同じレベル(「1 回あたりのバックアップデータ転送量」が中程度(GB オーダ(1GB～999GB))、「運用/管理負荷；中」、「取扱データの最高機密レベル」；機密レベル 1 (組織内)、「バックアップシステムの信頼性」；中程度)となるものである。 したがって、切替型ではなくリストア型での実現となり、また DR クラス D ほどのリアルタイム性が必要とならないため、クラウド利用リストア型データバックアップやレプリケーションといった手段を利用する。その構成は、ネットワークバックアップ、LAN フリーバックアップ、センタバックアップに加え、意図的リスクのみが対象リスクとなる場合はローカルバックアップで実現することも可能である。 また、バックアップ方式は、上記のようなリアルタイムなバックアップデータ転送が必要な手段となるため、増分バックアップによるオンラインバックアップ方式となり、バックアップデータ量やネットワークの転送容量によっては CDP 技術や重複排除技術といったよりデータ転送量を削減可能な技術を選択する。加えて、DR クラス D と同様、多重バックアップまでを実装する必要は無く、また暗号化レベルの追加セキュリティ保護策を講ずればクラウドを利用可能とするものである。 ＜監視・監査技術＞ DR クラス E のバックアップシステムを運用するために、DR クラス D 同様なリアルタイムなバックアップシステムへの復旧が必要ないことから、リカバリの手動制御や定期監視によって実現されるものである。 また、監査については、一般的な情報システム同様、バックアップシステムの検査/動作検証を実施するとともに、管理者に対する教育・訓練を実施する必要があるものである。

DR クラス	バックアップ構築/監視・監査技術選択根拠
DR クラス F	＜構築技術＞ DR クラス F のバックアップシステムは、事業継続上、当面無くても支障のないシステム/データで、最もリアルタイム性が求められない復旧を目標とし(「RPO」は 1 ヶ月以内の時点、「RTO」は大規模なシステム障害時には 1～3 日以内、大規模な災害時には 1 ～6 ヶ月、「RLO」も最低限、特定システム機能のみ災害前に比べ限定された性能を許容されたレベルでの復旧を目標)、前提・制約条件としては DR クラス E 同様低コスト(～500 万)での実現が必要で、DR クラス E に比べ、「1 回あたりのバックアップデータ転送量」が大(TB オーダ(1TB～))、「運用/管理負荷」; 高、「バックアップシステムの信頼性」; 低と最低限の条件となるものである。 したがって、DR クラス E ほどのリアルタイム性が必要とならないため、クラウド利用リストア型データバックアップやテープ/ディスクベースといった手段を利用する。その構成は、ネットワークバックアップ、LAN フリーバックアップ、センタバックアップに加え、意図的リスクのみが対象リスクとなる場合はローカルバックアップで実現することも可能である。 また、バックアップ方式は、上記のようなリアルタイム性の低いバックアップデータ転送手段となるため、フルバックアップ、差分バックアップ、増分バックアップによるオフラインバックアップ方式となる。(バックアップデータ量やネットワークの転送容量によっては CDP 技術や重複排除技術といったよりデータ転送量を削減可能な技術を選択することもある。)加えて、DR クラス E と同様、多重バックアップまでを実装する必要は無く、また暗号化レベルの追加セキュリティ保護策を講ずればクラウドを利用可能とするものである。 ＜監視・監査技術＞ DR クラス F のバックアップシステムを運用するために、DR クラス E 同様なリアルタイムなバックアップシステムへの復旧が必要ないことから、リカバリの手動制御や定期監視によって実現されるものである。 また、監査については、一般的な情報システム同様、バックアップシステムの検査/動作検証を実施するとともに、管理者に対する教育・訓練を実施する必要があるものである。

DR クラス	バックアップ構築/監視・監査技術選択根拠
DR クラス α	＜構築技術＞ DR クラス α のバックアップシステムは、事業継続上、システムの稼動は必須となるが、データはあれば良いもので、DR クラス A 同様システム停止は許されないが、データは DR クラス D と同じレベルの復旧を目標(「RPO」は DR クラス D と同じ数日、「RTO」/「RLO」は DR クラス A と同じレベル(「RTO」; 大規模なシステム障害、災害に関わらずに数分、「RLO」; 全てのシステム機能について災害前と同等の性能での復旧を目標)とし、前提・制約条件としては、システムについては DR クラス A、データについては DR クラス D 程度の条件(「コスト」; 500 万～1000 万、「1 回あたりのバックアップデータ転送量」; 中程度(GB オーダ(1GB～999GB)、「運用/管理負荷 ; 低」、「取扱データの最高機密レベル」; 機密レベル 1 (組織内)、「バックアップシステムの信頼性」; 高)が求められるものである。 したがって、リアルタイムな復旧が可能で、データについては厳密な取扱が不要なことから、DR クラス A のサイト間フェイルオーバ(クラスタリング機能利用)に加え、クラウドを利用したコスト対効果の高い切替型の手段も選択肢となる。その構成は、ネットワークバックアップ、LAN フリーバックアップ、センタバックアップに加え、意図的リスクのみが対象リスクとなる場合はローカルバックアップで実現することも可能である。 また、バックアップ方式は、データ復旧についてのリアルタイム性は求められないが、可用性が求められるので、フルバックアップ、差分バックアップ、増分バックアップによるオンラインバックアップ方式となる。加えて、システムについては高い信頼性が求められることから多重バックアップの実装が必要となるが、データの保護強化策はクラス D 同様暗号化レベルの追加セキュリティ保護策を講ずればクラウドを利用可能とするものである。 ＜監視・監査技術＞ DR クラス α のバックアップシステムを運用するために、DR クラス A 同様、リアルタイムな監視、即時の待機系システムの切替えが必要となることから、リカバリ制御の自動化やバックアップ状態のリアルタイム監視の実現が必要なものである。 また、監査については、一般的な情報システム同様、バックアップシステムの検査/動作検証を実施するとともに、管理者に対する教育・訓練を実施する必要があるものである。

DR クラス	バックアップ構築/監視・監査技術選択根拠
DR クラスβ	＜構築技術＞ DR クラスβのバックアップシステムは、事業継続上、当面無くても支障のないシステムだが、データ欠損は許されないもので、システムについては DR クラス F、データに DR クラス A と同じレベルの復旧目標(「RPO」は DR クラス A と同じ災害・障害発生時点、「RTO」/「RLO」は DR クラス F と同じ「RTO」; 大規模なシステム障害時は 1～3 日、大規模災害時は 1～6ヶ月)とし、前提・制約条件としては、システムについては DR クラス F、データについては DR クラス A 程度の条件(「コスト」; 500 万～1000 万、「1 回あたりのバックアップデータ転送量」; MB オーダ(～999MB)、「運用/管理負荷；中」「取扱データの最高機密レベル」; 機密レベル３(関係者内)、「バックアップシステムの信頼性」; 高)が求められるものである。 したがって、リアルタイムなシステム復旧は必要ないがデータ転送が必要となり、「取扱データの最高機密レベル」がクラス A と同じく最も高いことから、現状セキュリティ上の不安があるクラウドを利用しないリアルタイムなデータ転送が可能なレプリケーションの手段を利用する。その構成は、ネットワークバックアップ、LAN フリーバックアップ、センタバックアップに加え、意図的リスクのみが対象リスクとなる場合はローカルバックアップで実現することも可能である。 また、バックアップ方式は上記のようなリアルタイムなバックアップデータ転送が必要な手段となるため、増分バックアップによるオンラインバックアップ方式となり、バックアップデータ量やネットワークの転送容量によっては CDP 技術や重複排除技術といったよりデータ転送量を削減可能な技術を選択する。加えて、高い信頼性が求められることから多重バックアップの実装や、データ機密レベルが機密レベル３(関係者内)となることからクラウド利用による保管は行わず、自社方式・データセンタ事業者を利用した現状のセキュリティ保護策で対策するものである。 ＜監視・監査技術＞ DR クラスβのバックアップシステムを運用するために、DR クラス F 同様リアルタイムなバックアップシステムへの復旧が必要ないためリカバリを手動制御で実現、データはバックアップサイトへ同期転送されていることを確認するためにリアルタイム監視が必要なものである。 また、監査については、一般的な情報システム同様、バックアップシステムの検査/動作検証を実施するとともに、管理者に対する教育・訓練を実施する必要があるものである。

また、各 DR クラスで選択されるバックアップ技術の組合せパターンとなるバックアップシステムオプションを定義したバックアップシステムオプション選択表(図 4-5)から、該当クラスのバックアップシステムオプションをシステム候補として選択する。このときシステム候補として複数のバックアップシステムオプションが選択される。図 4-5 の“●”は必須技術、“○”は選択技術を示しており、選択技術とは同じ技術カテゴリで“○”のついているものの中からいずれかを選ぶものである。なお、偶発的リスクあるいは意図的リスクのどちらか一方を範囲とするバックアップシステムを計画したい場合は、選択された各バックアップシステムオプション群は両者のリスクに対応するものとなっているため、バックアップ技術選択表(図 4-4)を参照して、範

囲としないリスク特有に必要な技術を削除する。

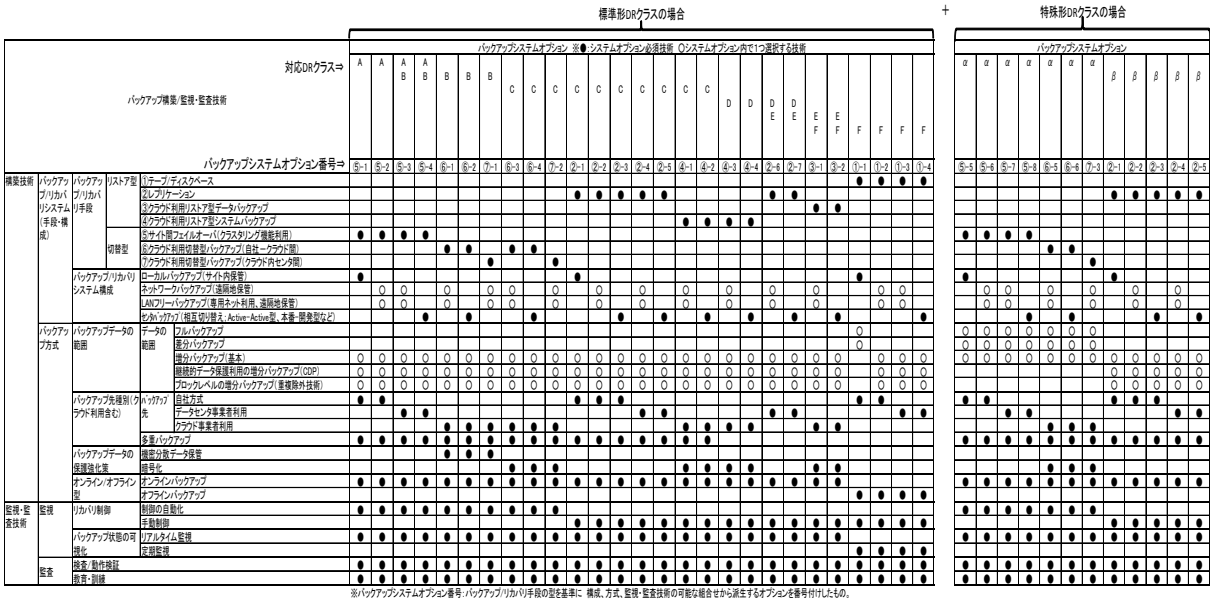

図 4-5　バックアップシステムオプション選択表

4.3 DR 対策策定

各 IT システムのバックアップシステム候補となるバックアップシステムオプションから各 IT システムに最も適合する最適なシステムオプションをバックアップシステムとして決定する。

図 4-6 に DR 対策策定の詳細プロセスを示す。

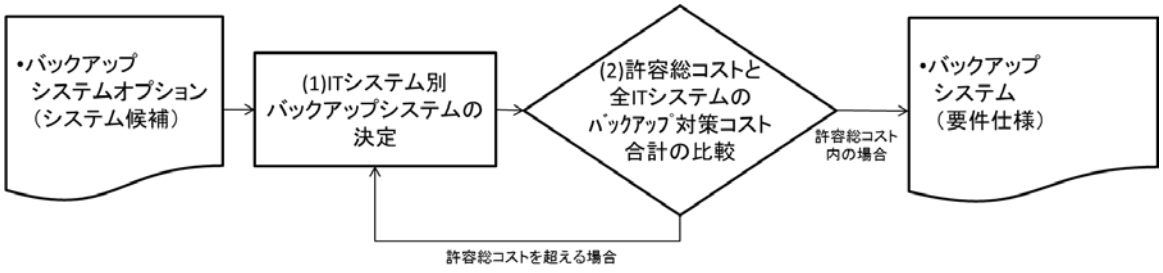

図 4-6　DR 対策策定詳細プロセス

4.3.1 IT システム別バックアップシステムの決定

各 IT システムの該当 DR クラスのバックアップシステム候補であるバックアップシステムオプションごとにランク値(点数付け)による評価を行い、各 IT システムに最も適合する最適なバックアップシステムを決定する。

図 4-7 に、その評価に用いる「バックアップシステムオプション評価表」を示す。

バックアップ構築/監視・監査技術					決定因子の重み	システム候補				
対応DRクラス⇒						A B	A B	B C	B C	B C
バックアップシステムオプション番号⇒						⑤-3	⑤-4	⑥-1	⑥-2	⑦-1
構築技術	バックアップ/リカバリシステム（手段・構成）	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース						
				②レプリケーション						
				③クラウド利用リストア型データバックアップ						
				④クラウド利用リストア型システムバックアップ						
			切替型	⑤サイト間フェイルオーバ（クラスタリング機能利用）		●	●			
				⑥クラウド利用切替型バックアップ（自社ークラウド間）				●	●	
				⑦クラウド利用切替型バックアップ（クラウド内センタ間）						●
		バックアップ/リカバリシステム構成		ローカルバックアップ（サイト内保管）						
				ネットワークバックアップ（遠隔地保管）		○		○		○
				LANフリーバックアップ（専用ネット利用、遠隔地保管）		○		○		○
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ（相互切り替え；Active-Active型、本番-開発型など）			●		●	
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ						
				差分バックアップ						
				増分バックアップ（基本）		○	○	○	○	○
				継続的データ保護利用の増分バックアップ（CDP）		○	○	○	○	○
				ブロックレベルの増分バックアップ（重複除外技術）		○	○	○	○	○
		バックアップ先種別（クラウド利用含む）	バックアップ先	自社方式						
				データセンタ事業者利用		●	●			
				クラウド事業者利用				●	●	●
				多重バックアップ		●	●	●	●	●
		バックアップデータの保護強化策		機密分散データ保管						
				暗号化						
		オンライン/オフライン型		オンラインバックアップ		●	●	●	●	●
				オフラインバックアップ						
監視・監査技術	監視	リカバリ制御		制御の自動化		●	●	●	●	●
				手動制御						
		バックアップ状態の可視化		リアルタイム監視		●	●	●	●	●
				定期監視						
	監査	検査/動作検証				●	●	●	●	●
		教育・訓練				●	●	●	●	●
評価項目（DRクラス決定因子）										
バックアップ対象の特性（レジリエンス）		業務（データ/システム）の重要度				10	10	10	10	10
		業務のリアルタイム性				8	10	2	4	6
前提・制約条件（コスト・効率・運用負荷・信頼性）		コスト			2	2	4	6	8	10
		1回のバックアップデータ転送量			1	8	8	6	6	6
		取扱いデータの最高機密レベル			1	10	8	6	4	2
		運用/管理負荷			4	4	2	8	6	10
		既存資産の活用性			1	10	10	6	6	2
		バックアップシステムの信頼性			1	10	8	6	4	2
対象リスクの範囲						10	10	10	10	10
バックアップ対象の特性（レジリエンス）：小計						9	10	6	7	8
前提・制約条件（コスト・効率・運用負荷・信頼性）：小計						5.8	5	6.8	6	7.2
対象リスクの範囲：小計						10	10	10	10	10
合計						8.267	8.333	7.6	7.667	8.4

図 4-7　バックアップシステムオプション評価表

図 4-7 は、上部が DR クラス対応のバックアップシステムオプションで、下部が各バックアップシステムオプションを評価する評価項目、評価の小計や合計の構成になっている。

以下に下部の各項目(評価項目、小計、合計)について、説明する。

1)　DR クラスの決定因子を評価指標とした評価項目ごとの点数付け

各システムオプションを評価項目ごとに相対比較して点数付け(0～10 点)て記載する。

各評価項目の達成効果(容易性)が高くなる順に 0 から 10 の 11 段階で点数付けすることで評価する。

2)　評価項目の大分類の評価点の小計

各評価項目の点数を評価項目の大分類ごとに平均し小計を求める。

※前提・制約条件の場合は、重み付け値の小計で正規化。

例えば、図 4-7 のバックアップシステムオプション⑤-3 の場合、以下の小計となる。

$$\frac{\sum\ (\text{重み}\times\text{評価項目})}{\sum\ \text{重み}} = \frac{2\times2+1\times8+1\times10+4\times4+1\times10+1\times10}{2+1+1+4+1+1} = 5.8$$

3)　システムオプションの評価点を示す合計

評価項目の大分類の小計点の平均をとったシステムオプションの評価点を示す。

ガイドラインの利用者は、利用者組織固有の要望・嗜好を、前提・制約条件の決定因子に対して重み付けを入力することで評価に反映する。重み付けは次の 1～4 段階で設定する。

1：標準的な重みの項目

2：対象利用者組織でやや重要視される項目

3：対象利用者組織で重要視される項目

4：対象利用者組織で経営者からの支持があるなど最重要視される項目

そして、上記 2）3）の計算により、各システム候補の合計点が計算され、合計点の最も高いシステム候補を最適なバックアップシステムとして決定する。その際、表中の“○”となっている選択技術について、いずれにするかも決定する。

なお、既存のバックアップシステムがある場合は、決定したバックアップシステムと既存とのギャップ評価を行い、評価結果の差分要件に関して移行性を考慮した新システムへの移行計画を検討することとなる。

4.3.2 許容総コストと全 IT システムのバックアップ対策コスト合計の比較

IT システムごとに決定したバックアップシステムの対策コストを見積り、その合計と、IT-BCP からの入力情報である許容総コストを比較し、合計が許容総コスト内であれば、決定したバックアップシステムで確定し、許容総コストを超える場合は、1)に戻り、別のバックアップシステムオプションを選択して、許容総コスト内に収まるバックアップシステムの組合せを特定、確定させる等の調整を図る。

また、以上の結果として、IT システムごとに、決定した最適バックアップシステムにつき、該当 DR クラス、バックアップ関連パラメータ値、選択技術の情報に基づいてバックアップシステムの要件定義としてまとめる。

5. DR 向けクラウドバックアップの計画パターン事例

本ガイドラインを利用した DR 向けバックアップ計画パターン事例として、以下の３つのモデルケースをもとにその計画策定結果を示す。なお、本計画策定事例ではモデルケースの対象 IT システムの１つを事例として示しているため、IT システムごとの見積り、許容総コストをもとに比較・調整などは割愛する。

表 5-1　計画モデルパターン策定モデルケース

	モデルケースⅠ	モデルケースⅡ	モデルケースⅢ
業種	サービス業	サービス業	製造業
業務内容	工業製品の品質、安全性検査や認証等	受託業務を中心としたサービス業の持株会社	機械製造業
従業員数	約 300 名	約 2000 名(グループ連結) 約 50 拠点(グループ連結/国内・海外拠点含む)	約 300 名
対象となる業務(システム)	検査や認証等の管理業務	・ERP システム等で扱う基幹業務 ・メール/グループウェアなどのコミュニケーション業務	生産管理業務

5.1 モデルケースⅠによる計画策定事例

以下にモデルケースⅠの DR アセスメント、DR 要件定義、DR 対策策定の各プロセスの検討結果と決定したバックアップシステムを説明する。

5.1.1 DR アセスメントの検討結果

以下にモデルケースⅠにおける各決定因子の対象 IT システムのバックアップ関連パラメータ値とマッチングする DR クラス表のレンジ値を示す。

表 5-2　モデルケースⅠのバックアップ関連パラメータ値と該当 DR クラスレンジ値

モデルケースⅠ		
業種・組織概要		
業種	サービス業	
業務内容	工業製品の品質、安全性検査や認証等	
従業員数	約 300 名	
対象となる業務(システム)	検査や認証等の管理業務	
決定因子	対象システムのバックアップ関連パラメータ値	該当する DR クラスレンジ値
バックアップ対象の特性(レジリエンス)	-	-
業務(データ/システム)の重要度	最も重要な業務は、顧客への製品の認証に関する情報提供(オンラインのデータベースサービス)で、この情報が無いと顧客は製品の生産や販売ができなくなる(顧客と SLA を設定：最高水準で RTO を 5 分と設定)	顧客向けサービスとして SLA の遵守は必須であることからレンジ値は「業務継続上、常に必須なシステム/データ」(DR クラス A、B)が該当

	業務のリアルタイム性	ＲＰＯ(目標復旧時点)		5 分以内	「1 時間以内の時点」(DR クラス A、B)が該当
		ＲＴＯ(目標復旧時間)	大規模システム障害	5 分以内	「数分」(DR クラス A)または「2 時間以内」(DR クラス B)が該当
			大規模災害	1 日以内	「2 時間以内」(DR クラス B)が該当
		ＲＬＯ(目標復旧レベル)		継続して顧客にサービス提供するため全システム機能を災害前と同レベルのシステム性能で回復	「全てのシステム機能、災害前と同等の性能」(DR クラス A、B)が該当
前提・制約条件(コスト・効率・運用負荷・信頼性)				-	
	コスト	導入コスト＋ランニングコスト(年間)		IT 部門の予算の範囲内で対応(社長への直接判断などは実施しない)	経営者への判断を仰がず IT 部門内判断するためレンジ値は中程度の「500 万から 1,000 万」(DR クラス B)相当
	1 回のバックアップデータ転送量			現状データ転送量は最大約 300MB	「MB オーダ」(DR クラス A、B)が該当
	取扱いデータの最高機密レベル			マーケティング部門で作成する顧客提供情報を含む	関係部署内で作成する情報ため「機密レベル 2 (関係部署内)」(DR クラス B)が該当
	運用/管理負荷			運用要員はメインサイト；1 名、バックアップサイト；1 名の 2 名。短時間の RTO を実現するためリカバリ制御の自動化やリアルタイム監視が必要。	リアルタイムな復旧が必要なため「低」(DR クラス A、B)が該当
	既存資産の活用性			自社内でシステムを二重化し、同構成を遠隔地での自社バックアップサイトにも持つ、切替型のバックアップシステム。専用線 100Mb/s で接続し 5 分間隔でデータ同期。	有
	バックアップシステムの信頼性			バックアップシステムに切り替え後継続して顧客への情報提供が必要なため高い信頼性が必要	切り替え後顧客向けの Web システムとなるためレンジ値は「高」(DR クラス A、B)が該当
対象リスクの範囲				Web 経由での悪意のある攻撃者による攻撃。 大規模災害対応。	偶発的リスク or 意図的リスク

以上から全ての決定因子において DR クラス B のレンジ値が該当することから、モデルケース I では DR クラス B を選択する。

5.1.2 DR 要件定義の検討結果

上記の選択結果、DR クラス B をもとに、バックアップ技術を選択し、そのバックアップ技術から候補となるバックアップシステムオプションを選択する。

図 5-1 に「バックアップ技術選択表」(図 4-4)からモデルケース I が該当する DR クラス B で対象リスク範囲が「偶発的リスク or 意図的リスク」となるバックアップ技術を選択した結果を示す。

バックアップ構築/監視・監査技術						B
				DR選択表の決定因子;対象リスクの範囲⇒		偶発的リスク or 意図的リスク
構築技術	バックアップ/リカバリシステム（手段・構成）	バックアップ/リカバリ手段	リストア型	テープ/ディスクベース		
				レプリケーション		
				クラウド利用リストア型データバックアップ		
				クラウド利用リストア型システムバックアップ		
			切替型	サイト間フェイルオーバ（クラスタリング機能利用）		○
				クラウド利用切替型バックアップ（自社－クラウド間）		○
				クラウド利用切替型バックアップ（クラウド内センタ間）		○
		バックアップ/リカバリシステム構成		ローカルバックアップ（サイト内保管）		○
				ネットワークバックアップ（遠隔地保管）		○
				LANフリーバックアップ（専用ネット利用、遠隔地保管）		○
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ（相互切り替え；Active-Active型、本番-開発型など）		○
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ		
				差分バックアップ		
				増分バックアップ（基本）		○
				継続的データ保護利用の増分バックアップ（CDP）		○
				ブロックレベルの増分バックアップ（重複除外技術）		○
		バックアップ先種別（クラウド利用含む）	ﾊﾞｯｸｱｯﾌﾟ先	自社方式		
				データセンタ事業者利用		○
				クラウド事業者利用		○
			多重バックアップ			○
		バックアップデータの保護強化策	機密分散データ保管			○
			暗号化			
		オンライン/オフライン型	オンラインバックアップ			○
			オフラインバックアップ			
監視・監査技術	監視	リカバリ制御	制御の自動化			○
			手動制御			
		バックアップ状態の可視化	リアルタイム監視			○
			定期監視			
	監査	検査/動作検証				○
		教育・訓練				○

図 5-1　モデルケース I の該当するバックアップ技術

次に、バックアップシステムオプション選択表(図 4-5)から、モデルケース I が該当する DR クラス B のバックアップシステムオプションをシステム候補として選択した結果を図 5-2 に示す。

バックアップ構築/監視・監査技術						バックアップシステムオプション ※●：システムオプション必須技術 ○システムオプション内で1つ選択する技術				
					対応DRクラス⇒	A B	A B	B C	B C	B C
					バックアップシステムオプション番号⇒	⑤-3	⑤-4	⑥-1	⑥-2	⑦-1
構築技術	バックアップ/リカバリシステム（手段・構成）	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース						
				②レプリケーション						
				③クラウド利用リストア型データバックアップ						
				④クラウド利用リストア型システムバックアップ						
			切替型	⑤サイト間フェイルオーバ（クラスタリング機能利用）		●	●			
				⑥クラウド利用切替型バックアップ（自社－クラウド間）				●	●	
				⑦クラウド利用切替型バックアップ（クラウド内センタ間）						●
		バックアップ/リカバリシステム構成		ローカルバックアップ（サイト内保管）						
				ネットワークバックアップ（遠隔地保管）		○		○		○
				LANフリーバックアップ（専用ネット利用、遠隔地保管）		○		○		○
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ（相互切り替え；Active-Active型、本番-開発型など）			●		●	
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ						
				差分バックアップ						
				増分バックアップ（基本）		○	○	○	○	○
				継続的データ保護利用の増分バックアップ（CDP）		○	○	○	○	○
				ブロックレベルの増分バックアップ（重複除外技術）		○	○	○	○	○
		バックアップ先種別（クラウド利用含む）	ﾊﾞｯｸｱｯﾌﾟ先	自社方式						
				データセンタ事業者利用		●	●			
				クラウド事業者利用				●	●	●
			多重バックアップ			●	●	●	●	●
		バックアップデータの保護強化策	機密分散データ保管					●	●	●
			暗号化							
		オンライン/オフライン型	オンラインバックアップ			●	●	●	●	●
			オフラインバックアップ							
監視・監査技術	監視	リカバリ制御	制御の自動化			●	●	●	●	●
			手動制御							
		バックアップ状態の可視化	リアルタイム監視			●	●	●	●	●
			定期監視							
	監査	検査/動作検証				●	●	●	●	●
		教育・訓練				●	●	●	●	●

図 5-2　モデルケースⅠの該当するバックアップシステムオプション

5.1.3 DR 対策策定の検討結果

モデルケースⅠの該当バックアップシステムオプションをランク値(点数付け)による評価を行い、各 IT システムに最も適合するバックアップシステムを決定する。

なお、モデルケースⅠのおいては、特にユーザ固有の利用者組織固有の要望・嗜好がないことから、重み付けについては全て標準的な重み：１とする。

図 5-3 に評価結果を示す。

バックアップ構築/監視・監査技術					決定因子の重み	システム候補				
対応DRクラス⇒						A B	A B	B C	B C	B C
バックアップシステムオプション番号⇒						⑤-3	⑤-4	⑥-1	⑥-2	⑦-1
構築技術	バックアップ/リカバリシステム（手段・構成）	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース						
				②レプリケーション						
				③クラウド利用リストア型データバックアップ						
				④クラウド利用リストア型システムバックアップ						
			切替型	⑤サイト間フェイルオーバ（クラスタリング機能利用）		●	●			
				⑥クラウド利用切替型バックアップ（自社ークラウド間）				●	●	
				⑦クラウド利用切替型バックアップ（クラウド内センタ間）						●
		バックアップ/リカバリシステム構成		ローカルバックアップ（サイト内保管）						
				ネットワークバックアップ（遠隔地保管）		○		○		○
				LANフリーバックアップ（専用ネット利用、遠隔地保管）		○		○		○
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ（相互切り替え；Active-Active型、本番-開発型など）			●		●	
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ						
				差分バックアップ						
				増分バックアップ（基本）		○	○	○	○	○
				継続的データ保護利用の増分バックアップ（CDP）		○	○	○	○	○
				ブロックレベルの増分バックアップ（重複除外技術）		○	○	○	○	○
		バックアップ先種別（クラウド利用含む）	バックアップ先	自社方式						
				データセンタ事業者利用		●	●			
				クラウド事業者利用				●	●	●
			多重バックアップ			●	●	●	●	●
		バックアップデータの保護強化策	機密分散データ保管					●	●	●
			暗号化							
		オンライン/オフライン型	オンラインバックアップ			●	●	●	●	●
			オフラインバックアップ							
監視・監査技術	監視	リカバリ制御	制御の自動化			●	●	●	●	●
			手動制御							
		バックアップ状態の可視化	リアルタイム監視			●	●	●	●	●
			定期監視							
	監査	検査/動作検証				●	●	●	●	●
		教育・訓練				●	●	●	●	●
評価項目（DRクラス決定因子）										
バックアップ対象の特性（レジリエンス）		業務（データ/システム）の重要度				10	10	10	10	10
		業務のリアルタイム性				8	10	2	4	6
前提・制約条件（コスト・効率・運用負荷・信頼性）		コスト			1	2	4	6	8	10
		1回のバックアップデータ転送量			1	8	8	6	6	6
		取扱いデータの最高機密レベル			1	10	8	6	4	2
		運用/管理負荷			1	4	2	8	6	10
		既存資産の活用性			1	10	10	6	6	2
		バックアップシステムの信頼性			1	10	8	6	4	2
対象リスクの範囲						10	10	10	10	10
バックアップ対象の特性（レジリエンス）：小計						9	10	6	7	8
前提・制約条件（コスト・効率・運用負荷・信頼性）：小計						7.333	6.667	6.333	5.667	5.333
対象リスクの範囲：小計						10	10	10	10	10
合計						8.778	8.889	7.444	7.556	7.778

図 5-3　モデルケース I のシステムオプション評価結果

以上の評価結果からモデルケース I における対象 IT システムのバックアップシステムとして⑤-4 のシステムオプションを選択する。このとき、⑤-4 では「構築技術-バックアップ方式-バックアップデータの範囲」の「増分バックアップ(基本)」、「継続的データ保護利用の増分バックアップ(CDP)」、「ブロックレベルの増分バックアップ(重複除外技術)」のいずれかの技術を選択することとなるが、RPO ; 5 分間隔でバックアップデータ転送量;最大約 300MB は一般的なネットワーク技術で実現することが可能であるため「増分バックアップ(基本)」を選択することとする。

また、既存のバックアップシステムとして、自社のバックアップサイトを構築しているが、バックアップサイト運用費が重み、現在海外の DC 利用も視野に入れた相互バックアップ構築を構想しているため、⑤-4 の DC 事業者を利用する相互バックアップシステムは現実的に実現・実装可能なものである。このような観点踏まえ、決定したバックアップシステムと既存のバックアップシステムとのギャップ評価を行い、評価結果の差分要件に関して移行性を考慮した新システムへの移行計画を検討するが、本事例においては割愛する。

その他、対象組織における DR 対策が必要な全 IT システムに対して、IT システムごとに決定したバックアップシステムの対策コストを見積り、その合計と、IT-BCP からの入力情報である許容総コストをもとに比較・調

整を行うが、本計画策定事例ではモデルケースの対象 IT システムの１つを事例として示しているため、IT システムごとの見積り、許容総コストをもとに比較・調整などは割愛する。

5.1.4 決定したバックアップシステム

以上の検討結果、決定したバックアップシステムの定義した要件とシステム構成を図 5-4、図 5-5 にまとめる。

モデルケースⅠ				
業種・組織概要				
業種				サービス業
業務内容				工業製品の品質、安全性検査や認証等
従業員数				約300名
対象となる業務（システム）				検査や認証等の管理業務。
決定因子				対象システムの要件
バックアップ対象の特性（レジリエンス）				-
	業務（データ/システム）の重要度			業務継続上、常に必須なシステム/データ
	業務のリアルタイム性	RPO（目標復旧時点）		5分以内
		RTO（目標復旧時間）	大規模システム障害	5分以内
			大規模災害	1日以内
		RLO（目標復旧レベル）		全てのシステム機能、災害前と同等の性能
前提・制約条件（コスト・効率・運用負荷・信頼性）				-
	コスト	導入コスト＋ランニングコ		「500万から1000万」
	1回のバックアップデータ転送量			現状データ転送量は最大約300MB
	取扱いデータの最高機密レベル			機密レベル2（関係部署内）
	運用/管理負荷			低
	既存資産の活用性			有
	バックアップシステムの信頼性			高
対象リスクの範囲				偶発的リスクor意図的リスク

図 5-4　モデルシステムⅠのバックアップシステム要件

バックアップ構築/監視・監査技術						対象システム構成
構築技術	バックアップ/リカバリシステム（手段・構成）	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース		
				②レプリケーション		
				③クラウド利用リストア型データバックアップ		
				④クラウド利用リストア型システムバックアップ		
			切替型	⑤サイト間フェイルオーバ（クラスタリング機能利用）		●
				⑥クラウド利用切替型バックアップ（自社－クラウド間）		
				⑦クラウド利用切替型バックアップ（クラウド内センタ間）		
		バックアップ/リカバリシステム構成		ローカルバックアップ（サイト内保管）		
				ネットワークバックアップ（遠隔地保管）		
				LANフリーバックアップ（専用ネット利用、遠隔地保管）		
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ（相互切り替え；Active-Active型、本番-開発型など）		●
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ		
				差分バックアップ		
				増分バックアップ（基本）		●
				継続的データ保護利用の増分バックアップ（CDP）		
				ブロックレベルの増分バックアップ（重複除外技術）		
		バックアップ先種別（クラウド利用含む）	バックアップ先	自社方式		
				データセンタ事業者利用		●
				クラウド事業者利用		
			多重バックアップ			●
		バックアップデータの保護強化策	機密分散データ保管			
			暗号化			
		オンライン/オフライン型	オンラインバックアップ			●
			オフラインバックアップ			
監視・監査技術	監視	リカバリ制御	制御の自動化			●
			手動制御			
		バックアップ状態の可視化	リアルタイム監視			●
			定期監視			
	監査	検査/動作検証				●
		教育・訓練				●

図 5-5　モデルケースⅠのバックアップシステム構成

5.2 モデルケースⅡによる計画策定事例

以下にモデルケースⅡの DR アセスメント、DR 要件定義、DR 対策策定の各プロセスの検討結果と決定したバックアップシステムを説明する。

5.2.1 DR アセスメントの検討結果

以下にモデルケースⅡにおける各決定因子の対象 IT システムのバックアップ関連パラメータ値とマッチングする DR クラス表のレンジ値を示す。

表 5-3　モデルケースⅡのバックアップ関連パラメータ値と該当 DR クラスレンジ値

<table>
<tr><td colspan="4">モデルケースⅡ</td></tr>
<tr><td colspan="4">業種・組織概要</td></tr>
<tr><td colspan="2">業種</td><td colspan="2">サービス業</td></tr>
<tr><td colspan="2">業務内容</td><td colspan="2">受託業務を中心としたサービス業の持株会社</td></tr>
<tr><td colspan="2">従業員数</td><td colspan="2">約 2000 名(グループ連結)
約 50 拠点(グループ連結/国内・海外拠点含む)</td></tr>
<tr><td colspan="2">対象となる業務(システム)</td><td colspan="2">・ERP システム(財務会計・人事管理・販売管理・ワークフロー)等で扱う基幹業務
・メール・グループウェアなどのコミュニケーション業務</td></tr>
<tr><td colspan="2">決定因子</td><td>対象システムのバックアップ関連パラメータ値</td><td>該当する DR クラスレンジ値</td></tr>
<tr><td colspan="2">バックアップ対象の特性(レジリエンス)</td><td>-</td><td>-</td></tr>
<tr><td colspan="2">業務(データ/システム)の重要度</td><td>持株会社として各事業会社を横断的に統括しているため、グループ全体として事業継続性や連結決算対象としてみた場合に影響のある業務。</td><td>グループ内向けサービスであることからレンジ値は「業務継続上、あれば良いシステム/データ」(DR クラス C、D、E)が該当</td></tr>
<tr><td rowspan="3">業務のリアルタイム性</td><td>ＲＰＯ(目標復旧時点)</td><td>日次バックアップからの復旧</td><td>「1 日以内の時点」(DR クラス C)が該当</td></tr>
<tr><td rowspan="2">ＲＴＯ(目標復旧時間)</td><td>大規模システム障害</td><td>数時間以内</td><td>「2 時間以内」(DR クラス C)が該当</td></tr>
<tr><td>大規模災害</td><td>3 日以内に再開</td><td>「1～7 日間」(DR クラス C)が該当</td></tr>
<tr><td>ＲＬＯ(目標復旧レベル)</td><td>・ERP のすべての業務
・事業会社で横断して利用するシステム機能、データを優先</td><td>「特定システム機能のみ災害前に比べ限定された性能を許容」(DR クラス B、C、D)が該当</td></tr>
<tr><td colspan="2">前提・制約条件(コスト・効率・運用負荷・信頼性)</td><td>-</td><td></td></tr>
<tr><td>コスト</td><td>導入コスト＋ランニングコスト(年間)</td><td>IT 統括部門内で検討･策定(リスク管理委員会で協議・決定)</td><td>経営者への判断を仰がず IT 部門内判断するためレンジ値は中程度の「500 万から 1000 万」(DR クラス B)相当</td></tr>
</table>

1 回のバックアップデータ転送量	現状データ転送量は最大約 100GB	「GB オーダ」(DR クラス C、D、E)が該当
取扱いデータの最高機密レベル	各事業会社で作成する税務・人事などの管理データを持株会社として各事業会社を横断して管理	各事業会社で作成する情報ため「機密レベル２(関係部署内)」(DR クラス B)が該当
運用/管理負荷	待機系システムの切り替えは経営判断を伴うため手動での切り替えを実施。	手動での切り替えが可能なため「中」(DR クラス C、D、E)が該当
既存資産の活用性	遠隔地への手動での切り替え型。本番系、待機系ともの DC 事業者を利用。DC 事業者の 100Mb/s の専用回線を利用して日次オンラインデータバックアップ。	有
バックアップシステムの信頼性	バックアップシステムに切替後グループ内で継続利用するため対象システムと同レベルの信頼性が必要(メインサイト復旧後も、戻すリスクの方が大きいと判断しバックアップサイトでそのまま業務を継続することとしている。)	グループ内向けサービスのため、「中」(DR クラス C、D、E)が該当
対象リスクの範囲	・大規模災害対応。 ・計画停電対応。	偶発的リスク

以下にモデルケースⅡにおける各決定因子の対象 IT システムのバックアップ関連パラメータ値とマッチングする DR クラス表のレンジ値を示す。

以上から「取扱いデータの最高機密レベル」は DR クラス B 相当のパラメータ値となり、それ以外は DR クラス C のレンジ値が該当することから、DR クラス C をベースに「取扱いデータの最高機密レベル」を機密レベル 1(組織内)⇒機密レベル 2(関係部署内)としたカスタム DR クラス C´を作成する。

5.2.2 DR 要件定義の検討結果

上記の結果、DR クラス C のバックアップ技術をカスタム DR クラス C´を満たすバックアップ技術を選択し、そのバックアップ技術から候補となるバックアップシステムオプションを作成する。

図 5-6 に「バックアップ技術選択表」(図 4-4)からモデルケースⅡが最も近い DR クラス C で対象リスク範囲が「偶発的リスク」となるバックアップ技術を参照し、カスタム DR クラス C´を満たすバックアップ技術を選択した結果を示す。

カスタム DR クラス C´は、「取扱いデータの最高機密レベル」を機密レベル 1(組織内)⇒機密レベル 2(関係

部署内)に変更したもので、この因子を実現する技術は「構築技術-バックアップ方式-バックアップデータの保護強化策」を「暗号化」⇒「機密分散データ保管」に変更すれば対応可能である。

バックアップ構築/監視・監査技術						カスタムC´
					DR選択表の決定因子；対象リスクの範囲⇒	偶発的リスク
構築技術	バックアップ/リカバリシステム（手段・構成）	バックアップ/リカバリ手段	リストア型	テープ/ディスクベース		
				レプリケーション		○
				クラウド利用リストア型データバックアップ		
				クラウド利用リストア型システムバックアップ		○
			切替型	サイト間フェイルオーバ（クラスタリング機能利用）		
				クラウド利用切替型バックアップ（自社－クラウド間）		○
				クラウド利用切替型バックアップ（クラウド内センタ間）		○
		バックアップ/リカバリシステム構成		ローカルバックアップ（サイト内保管）		
				ネットワークバックアップ（遠隔地保管）		○
				LANフリーバックアップ（専用ネット利用、遠隔地保管）		○
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ（相互切り替え；Active-Active型、本番-開発型など）		○
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ		
				差分バックアップ		
				増分バックアップ（基本）		○
				継続的データ保護利用の増分バックアップ（CDP）		○
				ブロックレベルの増分バックアップ（重複除外技術）		○
		バックアップ先種別（クラウド利用含む）	ﾊﾞｯｸｱｯﾌﾟ先	自社方式		○
				データセンタ事業者利用		○
				クラウド事業者利用		○
			多重バックアップ			○
		バックアップデータの保護強化策	機密分散データ保管			
			暗号化			
		オンライン/オフライン型	オンラインバックアップ			○
			オフラインバックアップ			
監視・監査技術	監視	リカバリ制御	制御の自動化			
			手動制御			○
		バックアップ状態の可視化	リアルタイム監視			
			定期監視			○
	監査	検査/動作検証				○
		教育・訓練				○

図 5-6　モデルケースⅡの該当するバックアップ技術

次に、バックアップシステムオプション選択表(図 4-5)から、DR クラス C のバックアップシステムオプションを参照し、カスタム DR クラス C′を満たすバックアップシステムオプションをシステム候補として作成した結果を図 5-7 に示す。

カスタムDRクラスC′を実現する技術として「構築技術-バックアップ方式-バックアップデータの保護強化策」を「暗号化」⇒「機密分散データ保管」に変更したが、この変更に伴い、クラウドを利用する⑥-3、⑥-4、⑦-2、④-1、④-2 のシステムオプションについては、クラウド利用における追加データ保護強化策として「構築技術-バックアップ方式-バックアップデータの保護強化策」を「暗号化」から「機密分散データ保管」に変更した⑥-3′、⑥-4′、⑦-2′、④-1′、④-2′を作成した。

なお、モデルケースⅡは、「対象リスク範囲」として偶発的リスクに対応するため、意図的リスクで選択されている「構築技術-バックアップ/リカバリシステム構成」の「ローカルバックアップ（サイト内保管)」を含むシステムオプション(②-1)を削除したシステムオプションをシステム候補として選択している。

バックアップ構築/監視・監査技術						バックアップシステムオプション ※●：システムオプション必須技術 ○システムオプション内で1つ選択する技術								
						C	C	C	C	C	C	C	C	C
					バックアップシステムオプション番号⇒	⑥-3′	⑥-4′	⑦-2′	②-2	②-3	②-4	②-5	④-1′	④-2′
構築技術	バックアップ/リカバリシステム（手段・構成）	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース										
				②レプリケーション					●	●	●	●		
				③クラウド利用リストア型データバックアップ										
				④クラウド利用リストア型システムバックアップ									●	●
			切替型	⑤サイト間フェイルオーバ（クラスタリング機能利用）										
				⑥クラウド利用切替型バックアップ（自社－クラウド間）		●	●							
				⑦クラウド利用切替型バックアップ（クラウド内センタ間）				●						
		バックアップ/リカバリシステム構成		ローカルバックアップ（サイト内保管）										
				ネットワークバックアップ（遠隔地保管）		○		○	○		○		○	
				LANフリーバックアップ（専用ネット利用、遠隔地保管）		○		○	○		○		○	
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ（相互切り替え：Active-Active型、本番-開発型など）			●			●		●		●
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ										
				差分バックアップ										
				増分バックアップ（基本）		○	○	○	○	○	○	○	○	○
				継続的データ保護利用の増分バックアップ（CDP）		○	○	○	○	○	○	○	○	○
				ブロックレベルの増分バックアップ（重複除外技術）		○	○	○	○	○	○	○	○	○
		バックアップ先種別（クラウド利用含む）	ﾊﾞｯｸｱｯﾌﾟ先	自社方式					●	●				
				データセンタ事業者利用							●	●		
				クラウド事業者利用		●	●	●					●	●
				多重バックアップ		●	●	●	●	●	●	●	●	●
		バックアップデータの保護強化策		機密分散データ保管		■●	■●	■●					■●	■●
				暗号化		●	●	●					●	●
		オンライン/オフライン型		オンラインバックアップ		●	●	●	●	●	●	●	●	●
				オフラインバックアップ										
監視・監査技術	監視	リカバリ制御		制御の自動化		●	●	●						
				手動制御					●	●	●	●	●	●
		バックアップ状態の可視化		リアルタイム監視		●	●	●	●	●	●	●	●	●
				定期監視										
	監査	検査/動作検証				●	●	●	●	●	●	●	●	●
		教育・訓練				●	●	●	●	●	●	●	●	●

図 5-7　モデルケースⅡの該当するバックアップシステムオプション

5.2.3 DR 対策策定の検討結果

モデルケースⅡの該当バックアップシステムオプションをランク値(点数付け)による評価を行い、各 IT システムに最も適合するバックアップシステムを決定する。

なお、モデルケースⅡのおいては、特にユーザ固有の利用者組織固有の要望・嗜好がないことから、重み付けについては全て標準的な重み：1 とする。また、カスタム DR クラスを作成したため、「バックアップシステムオプション評価表」のシステム候補を⑥-3、⑥-4、⑦-2、④-1、④-2 から⑥-3´、⑥-4´、⑦-2´、④-1´、④-2´に差し替えている。(各システム候補の相対比較による点数付けは差し替えたシステム候補においても変更は無い。)

図 5-8 に評価結果を示す。

バックアップ構築/監視・監査技術					決定因子の重み	システム候補								
対応DRクラス⇒						BC	BC	BC	C	C	C	C	C	C
バックアップシステムオプション番号⇒						⑥-3´	⑥-4´	⑦-2´	②-2	②-3	②-4	②-5	④-1´	④-2´
構築技術	バックアップ/リカバリシステム（手段・構成）	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース										
				②レプリケーション					●	●	●	●		
				③クラウド利用リストア型データバックアップ										
				④クラウド利用リストア型システムバックアップ									●	●
			切替型	⑤サイト間フェイルオーバ（クラスタリング機能利用）										
				⑥クラウド利用切替型バックアップ（自社ークラウド間）		●	●							
				⑦クラウド利用切替型バックアップ（クラウド内センタ間）				●						
		バックアップ/リカバリシステム構成		ローカルバックアップ（サイト内保管）										
				ネットワークバックアップ（遠隔地保管）		○		○	○		○		○	
				LANフリーバックアップ（専用ネット利用、遠隔地保管）		○		○	○		○		○	
				センタバックアップ（相互切り替え：Active-Active型、本番-開発型など）			●			●		●		●
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ										
				差分バックアップ										
				増分バックアップ（基本）		○	○	○	○	○	○	○	○	○
				継続的データ保護利用の増分バックアップ（CDP）		○	○	○	○	○	○	○	○	○
				ブロックレベルの増分バックアップ（重複除外技術）		○	○	○	○	○	○	○	○	○
		バックアップ先種別（クラウド利用含む）	バックアップ先	自社方式					●	●				
				データセンタ事業者利用							●	●		
				クラウド事業者利用		●	●	●					●	●
			多重バックアップ			●	●	●	●	●	●	●	●	●
		バックアップデータの保護強化策	機密分散データ保管			●	●	●					●	●
			暗号化											
		オンライン/オフライン型	オンラインバックアップ			●	●	●	●	●	●	●	●	●
			オフラインバックアップ											
監視・監査技術	監視	リカバリ制御	制御の自動化			●	●	●						
			手動制御						●	●	●	●	●	●
		バックアップ状態の可視化	リアルタイム監視			●	●	●	●	●	●	●	●	●
			定期監視											
	監査	検査/動作検証				●	●	●	●	●	●	●	●	●
		教育・訓練				●	●	●	●	●	●	●	●	●
評価項目（DRクラス決定因子）														
バックアップ対象の特性（レジリエンス）		業務（データ/システム）の重要度				10	10	10	10	10	10	10	10	10
		業務のリアルタイム性				8	9	10	3	4	1	2	6	7
前提・制約条件（コスト・効率・運用負荷・信頼性）		コスト			1	1	2	3	4	5	6	7	10	9
		1回のバックアップデータ転送量			1	6	6	6	8	8	8	8	6	6
		取扱いデータの最高機密レベル			1	2	2	2	8	8	6	6	4	4
		運用/管理負荷			1	8	9	10	1	2	4	5	6	7
		既存資産の活用性			1	2	2	1	8	8	6	6	4	4
		バックアップシステムの信頼性			1	2	2	1	8	8	6	6	4	4
対象リスクの範囲						10	10	10	10	10	10	10	10	10
バックアップ対象の特性（レジリエンス）：小計						9	9.5	10	6.5	7	5.5	6	8	8.5
前提・制約条件（コスト・効率・運用負荷・信頼性）：小計						3.5	3.833	3.833	6.167	6.5	6	6.333	5.667	5.667
対象リスクの範囲：小計						10	10	10	10	10	10	10	10	10
合計						7.5	7.778	7.944	7.556	7.833	7.167	7.444	7.889	8.056

図 5-8　モデルケースⅡのシステムオプション評価結果

以上の評価結果からモデルケースⅡにおける対象 IT システムのバックアップシステムとして④-2´のシステムオプションを選択する。このとき、④-2´では「構築技術-バックアップ方式-バックアップデータの範囲」の「増分バックアップ(基本)」、「継続的データ保護利用の増分バックアップ(CDP)」、「ブロックレベルの増分バックアップ(重複除外技術)」のいずれかの技術を選択することとなるが、RPO；日次でバックアップデータ転送量；最大約 100GB はデータ転送時間をどの程度確保できるかが不明で、クラウドを利用することもあり安全サイドに考え転送データ量を削減可能な「ブロックレベルの増分バックアップ(重複除外技術)」を選択することとする。

また、既存のシステムとして、オンサイトとバックアップサイトの両方にデータセンタ事業者の商用データセンタを利用しており、例えばそのデータセンタ事業者と連携可能なクラウドバックアップサービスを利用するなど行えば、④-2´は現実的に実現・実装可能なものである。このような観点を踏まえ、決定したバックアップシステムと既存のバックアップシステムとのギャップ評価を行い、評価結果の差分要件に関して移行性を考慮した新システムへの移行計画を検討するが、本事例においては割愛する。

その他、対象組織における DR 対策が必要な全 IT システムに対して、IT システムごとに決定したバックアップシステムの対策コストを見積り、その合計と、IT-BCP からの入力情報である許容総コストをもとに比較・調整を行うが、本計画策定事例ではモデルケースの対象 IT システムの１つを事例として示しているため、IT システムごとの見積り、許容総コストをもとに比較・調整などは割愛する。

5.2.4 決定したバックアップシステム

以上の検討結果、決定したバックアップシステムの定義した要件とシステム構成を、図 5-9、図 5-10 にまとめる。

モデルケースⅡ				
業種・組織概要				
業種				サービス業
業務内容				受託業務を中心としたサービス業の持株会社
従業員数				約2000名（グループ連結） 約50拠点（グループ連結/国内・海外拠点含む）
対象となる業務（システム）				・ERPシステム（財務会計・人事管理・販売管理・ワークフロー）等で扱う基幹業務 ・メール・グループウェアなどのコミュニケーション業務
決定因子				対象システムの要件
バックアップ対象の特性（レジリエンス）				-
	業務（データ/システム）の重要度			業務継続上、あれば良いシステム/データ
	業務のリアルタイム性	RPO（目標復旧時点）		日次バックアップからの復旧
		RTO（目標復旧時間）	大規模システム障害	数時間以内
			大規模災害	3日以内に再開
		RLO（目標復旧レベル）		特定システム機能のみ 災害前に比べ限定された性能を許容
前提・制約条件（コスト・効率・運用負荷・信頼性）				-
	コスト	導入コスト＋ランニングコ		「500万から1000万」
	1回のバックアップデータ転送量			現状データ転送量は最大約100GB
	取扱いデータの最高機密レベル			機密レベル2（関係部署内）
	運用/管理負荷			中
	既存資産の活用性			有
	バックアップシステムの信頼性			中
対象リスクの範囲				偶発的リスク

図 5-9　モデルシステムⅡのバックアップシステム要件

バックアップ構築/監視・監査技術						対象システム構成
構築技術	バックアップ/リカバリシステム（手段・構成）	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース		
				②レプリケーション		
				③クラウド利用リストア型データバックアップ		
				④クラウド利用リストア型システムバックアップ		●
			切替型	⑤サイト間フェイルオーバ（クラスタリング機能利用）		
				⑥クラウド利用切替型バックアップ（自社－クラウド間）		
				⑦クラウド利用切替型バックアップ（クラウド内センタ間）		
		バックアップ/リカバリシステム構成		ローカルバックアップ（サイト内保管）		
				ネットワークバックアップ（遠隔地保管）		
				LANフリーバックアップ（専用ネット利用、遠隔地保管）		
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ（相互切り替え；Active-Active型、本番-開発型など）		●
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ		
				差分バックアップ		
				増分バックアップ（基本）		
				継続的データ保護利用の増分バックアップ（CDP）		
				ブロックレベルの増分バックアップ（重複除外技術）		●
		バックアップ先種別（クラウド利用含む）	バックアップ先	自社方式		
				データセンタ事業者利用		
				クラウド事業者利用		●
			多重バックアップ			●
		バックアップデータの保護強化策	機密分散データ保管			●
			暗号化			
		オンライン/オフライン型	オンラインバックアップ			●
			オフラインバックアップ			
監視・監査技術	監視	リカバリ制御	制御の自動化			
			手動制御			●
		バックアップ状態の可視化	リアルタイム監視			●
			定期監視			
	監査	検査/動作検証				●
		教育・訓練				●

図 5-10　モデルケースⅡのバックアップシステム構成

5.3 モデルケースⅢによる計画策定事例

以下にモデルケースⅢの DR アセスメント、DR 要件定義、DR 対策策定の各プロセスの検討結果と決定したバックアップシステムを説明する。

5.3.1 DR アセスメントの検討結果

以下にモデルケースⅢにおける各決定因子の対象 IT システムのバックアップ関連パラメータ値とマッチングする DR クラス表のレンジ値を示す。

表 5-4　モデルケースⅢのバックアップ関連パラメータ値と該当 DR クラスレンジ値

モデルケースⅢ				
業種・組織概要				
業種			製造業	
業務内容			機械製造業	
従業員数			約 300 名	
対象となる業務(システム)			生産管理業務	
決定因子			対象システムのバックアップ関連パラメータ値	該当する DR クラスレンジ値
バックアップ対象の特性(レジリエンス)			-	-
	業務(データ/システム)の重要度		日々の製造作業を管理するシステムであり、半日程度の停止であれば業務に大きな影響は与えない	社内向けサービスであり、半日程度ならば業務に支障が無いことからレンジ値は「業務継続上、あれば良いシステム/データ」(DR クラス C、D、E)が該当
	業務のリアルタイム性	ＲＰＯ(目標復旧時点)	日次バックアップからの復旧	「1 日以内の時点」(DR クラス C)、「数日」(DR クラス D)が該当
		ＲＴＯ(目標復旧時間) 大規模システム障害	半日程度	「12 時間以内」(DR クラス D)が該当
		大規模災害	2 週間	「数週間」(DR クラス D)が該当
		ＲＬＯ(目標復旧レベル)	全ての業務(システムのレスポンスが平常時より低下することは許容)	「特定システム機能のみ 災害前に比べ限定された性能を許容」(DR クラス B、C、D)が該当
前提・制約条件(コスト・効率・運用負荷・信頼性)			-	
	コスト	導入コスト＋ランニングコスト(年間)	IT 運営委員会で検討、情報システム部門で具体化	経営者への判断を仰がず IT 部門内判断するためレンジ値は中程度の「500 万から 1000 万」(DR クラス B、C、D)相当
	1 回のバックアップデータ転送量		現状データ転送量は最大約 100GB	「GB オーダ」(DR クラス C、D、E)が該当

取扱いデータの最高機密レベル	工場の生産管理データ	工場内で作成し、組織内で共有する情報ため「機密レベル 1 (組織内)」(DR クラス C、D、E、F)が該当
運用/管理負荷	現状手作業でのバックアップ媒体へデータ転送やシステム障害時の復旧をしており、管理負担などは問題になっていない。	手動での切り替えが可能なため「中」(DR クラス C、D、E)が該当
既存資産の活用性	別ビルの施錠キャビネットへのバックアップ媒体によるテープ/ディスクバックアップ (3 週間分保管)	有
バックアップシステムの信頼性	バックアップシステムに切替後工場で継続利用するため対象システムと同レベルの信頼性が必要	社内向けサービスのため、「中」(DR クラス C、D、E)が該当
対象リスクの範囲	・ハードウェアの故障 ・大規模災害対応	偶発的リスク

以上から全ての決定因子において DR クラス D のレンジ値が該当することから、モデルケースⅢでは DR クラス D を選択する。

5.3.2 DR 要件定義の検討結果

上記の選択結果、DR クラス D をもとに、バックアップ技術を選択し、そのバックアップ技術から候補となるバックアップシステムオプションを選択する。

図 5-11 に「バックアップ技術選択表」(図 4-4)からモデルケースⅢが該当する DR クラス D で対象リスク範囲が「偶発的リスク」となるバックアップ技術を選択した結果を示す。

バックアップ構築/監視・監査技術						D
				DR選択表の決定因子：対象リスクの範囲⇒		偶発的リスク
構築技術	バックアップ/リカバリシステム（手段・構成）	バックアップ/リカバリ手段	リストア型	テープ/ディスクベース		
				レプリケーション		○
				クラウド利用リストア型データバックアップ		
				クラウド利用リストア型システムバックアップ		○
			切替型	サイト間フェイルオーバ（クラスタリング機能利用）		
				クラウド利用切替型バックアップ（自社－クラウド間）		
				クラウド利用切替型バックアップ（クラウド内センタ間）		
		バックアップ/リカバリシステム構成		ローカルバックアップ（サイト内保管）		
				ネットワークバックアップ（遠隔地保管）		○
				LANフリーバックアップ（専用ネット利用、遠隔地保管）		○
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ（相互切り替え；Active-Active型、本番-開発型など）		○
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ		
				差分バックアップ		
				増分バックアップ（基本）		○
				継続的データ保護利用の増分バックアップ（CDP）		○
				ブロックレベルの増分バックアップ（重複除外技術）		○
		バックアップ先種別（クラウド利用含む）	ﾊﾞｯｸｱｯﾌﾟ先	自社方式		
				データセンタ事業者利用		○
				クラウド事業者利用		○
			多重バックアップ			
		バックアップデータの保護強化策	機密分散データ保管			
			暗号化			○
		オンライン/オフライン型	オンラインバックアップ			○
			オフラインバックアップ			
監視・監査技術	監視	リカバリ制御	制御の自動化			
			手動制御			○
		バックアップ状態の可視化	リアルタイム監視			
			定期監視			○
	監査	検査/動作検証				○
		教育・訓練				○

図 5-11　モデルケースⅢの該当するバックアップ技術

次に、バックアップシステムオプション選択表(図 4-5)から、モデルケースⅢが該当する DR クラス D のバックアップシステムオプションをシステム候補として選択した結果を図 5-12 に示す。

バックアップ構築/監視・監査技術						バックアップシステムオプション ※●：システムオプション必須技術 ○システムオプション内で1つ選択する技術			
						D	D	D E	D E
					バックアップシステムオプション番号⇒	④-3	④-4	②-6	②-7
構築技術	バックアップ/リカバリシステム（手段・構成）	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース					
				②レプリケーション				●	●
				③クラウド利用リストア型データバックアップ					
				④クラウド利用リストア型システムバックアップ		●	●		
			切替型	⑤サイト間フェイルオーバ（クラスタリング機能利用）					
				⑥クラウド利用切替型バックアップ（自社ークラウド間）					
				⑦クラウド利用切替型バックアップ（クラウド内センタ間）					
		バックアップ/リカバリシステム構成		ローカルバックアップ（サイト内保管）					
				ネットワークバックアップ（遠隔地保管）		○		○	
				LANフリーバックアップ（専用ネット利用、遠隔地保管）		○		○	
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ（相互切り替え；Active-Active型、本番-開発型など）			●		●
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ					
				差分バックアップ					
				増分バックアップ（基本）		○	○	○	○
				継続的データ保護利用の増分バックアップ（CDP）		○	○	○	○
				ブロックレベルの増分バックアップ（重複除外技術）		○	○	○	○
		バックアップ先種別（クラウド利用含む）	ﾊﾞｯｸｱｯﾌﾟ先	自社方式					
				データセンタ事業者利用				●	●
				クラウド事業者利用		●	●		
			多重バックアップ						
		バックアップデータの保護強化策	機密分散データ保管						
			暗号化			●	●		
		オンライン/オフライン型	オンラインバックアップ			●	●	●	●
			オフラインバックアップ						
監視・監査技術	監視	リカバリ制御	制御の自動化						
			手動制御			●	●	●	●
		バックアップ状態の可視化	リアルタイム監視			●	●	●	●
			定期監視						
	監査	検査/動作検証				●	●	●	●
		教育・訓練				●	●	●	●

図 5-12　モデルケースⅢの該当するバックアップシステムオプション

5.3.3 DR 対策策定の検討結果

モデルケースⅢの該当バックアップシステムオプションをランク値(点数付け)による評価を行い、各 IT システムに最も適合するバックアップシステムを決定する。

なお、モデルケースⅢのおいては、特にユーザ固有の利用者組織固有の要望・嗜好がないことから、重み付けについては全て標準的な重み：1 とする。

図 5-13 に評価結果を示す。

バックアップ構築/監視・監査技術					対応DRクラス⇒	決定因子の重み	システム候補			
							D	D	DE	DE
					バックアップシステムオプション番号⇒		④-3	④-4	②-6	②-7
構築技術	バックアップ/リカバリシステム（手段・構成）	バックアップ/リカバリ手段	リストア型		①テープ/ディスクベース					
					②レプリケーション				●	●
					③クラウド利用リストア型データバックアップ					
					④クラウド利用リストア型システムバックアップ		●	●		
			切替型		⑤サイト間フェイルオーバ（クラスタリング機能利用）					
					⑥クラウド利用切替型バックアップ（自社ークラウド間）					
					⑦クラウド利用切替型バックアップ（クラウド内センタ間）					
		バックアップ/リカバリシステム構成			ローカルバックアップ（サイト内保管）					
					ネットワークバックアップ（遠隔地保管）		○		○	
					LANフリーバックアップ（専用ネット利用、遠隔地保管）		○		○	
					センタバックアップ（相互切り替え；Active-Active型、本番-開発型など）			●		●
	バックアップ方式	バックアップデータの範囲	データの範囲		フルバックアップ					
					差分バックアップ					
					増分バックアップ（基本）		○	○	○	○
					継続的データ保護利用の増分バックアップ（CDP）		○	○	○	○
					ブロックレベルの増分バックアップ（重複除外技術）		○	○	○	○
		バックアップ先種別（クラウド利用含む）	バックアップ先		自社方式					
					データセンタ事業者利用				●	●
					クラウド事業者利用		●	●		
			多重バックアップ							
		バックアップデータの保護強化策	機密分散データ保管							
			暗号化				●	●		
		オンライン/オフライン型	オンラインバックアップ				●	●	●	●
			オフラインバックアップ							
監視・監査技術	監視	リカバリ制御	制御の自動化							
			手動制御				●	●	●	●
		バックアップ状態の可視化	リアルタイム監視				●	●	●	●
			定期監視							
	監査	検査/動作検証					●	●	●	●
		教育・訓練					●	●	●	●
評価項目（DRクラス決定因子）										
バックアップ対象の特性（レジリエンス）		業務（データ/システム）の重要度					10	10	10	10
		業務のリアルタイム性					8	10	8	10
前提・制約条件（コスト・効率・運用負荷・信頼性）		コスト				1	8	10	4	6
		1回のバックアップデータ転送量				1	8	8	10	10
		取扱いデータの最高機密レベル				1	8	8	10	10
		運用/管理負荷				1	10	10	8	8
		既存資産の活用性				1	8	8	10	10
		バックアップシステムの信頼性				1	8	8	10	10
対象リスクの範囲							10	10	10	10
バックアップ対象の特性（レジリエンス）：小計							9	10	9	10
前提・制約条件（コスト・効率・運用負荷・信頼性）：小計							8.333	8.667	8.667	9
対象リスクの範囲：小計							10	10	10	10
合計							9.111	9.556	9.222	9.667

図 5-13　モデルケースⅢのシステムオプション評価結果

以上の評価結果からモデルケースⅢにおける対象 IT システムのバックアップシステムとして②-7 のシステムオプションを選択される。このとき、②-7 は、データセンタ事業者を利用した相互切り替え型のセンタバックアップ方式となるが、このモデルケースではバックアップ対象システムを自社拠点で構築しており、さらに現状データセンタ事業者を利用しているシステムも存在しないことから、②-7 を実現するためにはかなりのコストが必要となるため、実装・実現制約上現実的ではない。そこで、代替システムオプションとして、次に合計点の高い④-4 を選択し検討したところ、④-4 はクラウド事業者を利用した相互切り替え型のセンタバックアップ方式となり、これにより②-7 よりコスト低減の見込めることから④-4 をモデルケースⅢのバックアップシステムとして決定することとする。

このとき、④-4 では「構築技術-バックアップ方式-バックアップデータの範囲」の「増分バックアップ(基本)」、「継続的データ保護利用の増分バックアップ(CDP)」、「ブロックレベルの増分バックアップ(重複除外技術)」のいずれかの技術を選択することとなるが、RPO；日次でバックアップデータ転送量；最大約 100GB はデータ転送時間をどの程度確保できるかが不明で、クラウドを利用することもあり安全サイドに考え転送データ量を削

減可能な「ブロックレベルの増分バックアップ(重複除外技術)」を選択することとする。

また、既存のバックアップシステムとして、自社の別ビルの施錠付き保管庫へバックアップ媒体を保管しており、決定したバックアップシステム④-4 とはかなり異なる技術となるため、現状のバックアップシステムの廃棄などが必要になると思われる。このような観点を踏まえ、決定したバックアップシステムと既存のバックアップシステムとのギャップ評価を行い、評価結果の差分要件に関して移行性を考慮した新システムへの移行計画を検討するが、本事例においては割愛する。

その他、対象組織における DR 対策が必要な全 IT システムに対して、IT システムごとに決定したバックアップシステムの対策コストを見積り、その合計と、IT-BCP からの入力情報である許容総コストをもとに比較・調整を行うが、本計画策定事例ではモデルケースの対象 IT システムの 1 つを事例として示しているため、IT システムごとの見積り、許容総コストの比較・調整などは割愛する。

5.3.4 決定したバックアップシステム

以上の検討結果、決定したバックアップシステムの定義した要件とシステム構成を、図 5-14、図 5-15 にまとめる。

モデルケースⅢ				
業種・組織概要				
業種				製造業
業務内容				機械製造業
従業員数				約300名
対象となる業務(システム)				生産管理業務
決定因子				対象システムの要件
バックアップ対象の特性(レジリエンス)				-
	業務(データ/システム)の重要度			業務継続上、あれば良いシステム/データ
	業務のリアルタイム性	RPO(目標復旧時点)		日次バックアップからの復旧
		RTO(目標復旧時間)	大規模システム障害	半日程度内
			大規模災害	2週間以内
		RLO(目標復旧レベル)		特定システム機能のみ 災害前に比べ限定された性能を許容
前提・制約条件(コスト・効率・運用負荷・信頼性)				-
	コスト	導入コスト+ランニングコ		「500万から1000万」
	1回のバックアップデータ転送量			現状データ転送量は最大約100GB
	取扱いデータの最高機密レベル			機密レベル1(組織内)
	運用/管理負荷			中
	既存資産の活用性			有
	バックアップシステムの信頼性			中
対象リスクの範囲				偶発的リスク

図 5-14　モデルシステムⅢのバックアップシステム要件

バックアップ構築/監視・監査技術						対象システム構成
構築技術	バックアップ/リカバリシステム（手段・構成）	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース		
				②レプリケーション		
				③クラウド利用リストア型データバックアップ		
				④クラウド利用リストア型システムバックアップ		●
			切替型	⑤サイト間フェイルオーバ（クラスタリング機能利用）		
				⑥クラウド利用切替型バックアップ（自社－クラウド間）		
				⑦クラウド利用切替型バックアップ（クラウド内センタ間）		
		バックアップ/リカバリシステム構成		ローカルバックアップ（サイト内保管）		
				ネットワークバックアップ（遠隔地保管）		
				LANフリーバックアップ（専用ネット利用、遠隔地保管）		
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ（相互切り替え；Active-Active型、本番-開発型など）		●
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ		
				差分バックアップ		
				増分バックアップ（基本）		
				継続的データ保護利用の増分バックアップ（CDP）		
				ブロックレベルの増分バックアップ（重複除外技術）		●
		バックアップ先種別（クラウド利用含む）	バックアップ先	自社方式		
				データセンタ事業者利用		
				クラウド事業者利用		●
			多重バックアップ			
		バックアップデータの保護強化策	機密分散データ保管			
			暗号化			●
		オンライン/オフライン型	オンラインバックアップ			●
			オフラインバックアップ			
監視・監査技術	監視	リカバリ制御	制御の自動化			
			手動制御			●
		バックアップ状態の可視化	リアルタイム監視			●
			定期監視			
	監査	検査/動作検証				●
		教育・訓練				●

図 5-15　モデルケースⅢのバックアップシステム構成

6. おわりに

東日本大震災や昨今のクラウドサービスにおけるデータ損失事故などの大規模(広域)災害・障害の教訓より、情報システムにおけるデータ・システムのバックアップが重要視されてきていること、従来の所持・占有型のシステムに比べコスト対効果が高い利用・共有型のクラウドサービスが普及してきていることから、クラウドの利用も視野に入れたディザスタリカバリ計画(DRP)の策定、特にバックアップシステムの要件定義を支援することを目的とした、「クラウドセントリックディザスタリカバリ計画ガイドライン」を作成した。

本ガイドラインは、従来には無かった体系的・網羅的観点から対象 IT システムに適したバックアップ要件・技術を、シート群を用いて容易に選定・特定できる点を特長としたガイドラインとなっている。このため、現状、ディザスタリカバリ(DR)向けのバックアップに関する広く知られた標準的な手法やガイドラインなどが無いことにより、効果的なバックアップを行えていない、災害・障害時に役に立たないバックアップを行っている等の問題に対して、解決の一助としてご活用いただけるものと考える。

7. 参考文献

[1] 日経 BP ムック：「IT で実現する 震災・省電力 BCP 完全ガイド」(2011.6.16)

[2] JUAS(一般社団法人 日本情報システム・ユーザー協会)：「企業 IT 動向調査 2012」(2012.5.28)

[3] ファーストサーバ株式会社　第三者調査委員会：「調査報告書(最終報告書)」(2012.7.31)

8. 付録１：ガイドラインで参照利用するシート一覧

以下に、本ガイドラインで参照利用する 4 種類の定義・選択・評価シート一覧を示す。

① DR クラス定義表(図　8-1)

② バックアップ技術選択表(図　8-2)

③ バックアップシステムオプション選択表(図　8-3)

④ バックアップシステムオプション評価表

- DR クラス A 向け(図　8-4)
- DR クラス B 向け(図　8-5)
- DR クラス C 向け(図　8-6)
- DR クラス D 向け(図　8-7)
- DR クラス E 向け(図　8-8)
- DR クラス F 向け(図　8-9)
- DR クラス α 向け(図　8-10)
- DR クラス β 向け(図　8-11)

				標準形DRクラス						+	特殊形DRクラス	
DRクラス				A	B	C	D	E	F		α	β
決定因子				レンジ値							レンジ値	
バックアップ対象の特性(レジリエンス)												
	業務(データ/システム)の重要度			事業継続上、常に必須なシステム/データ	事業継続上、常に必須なシステム/データ	事業継続上、あれば良いシステム/データ	事業継続上、あれば良いシステム/データ	事業継続上、あれば良いシステム/データ	事業継続上、当面無くても支障のないシステム/データ		事業継続上、システム稼働は必須、データはあれば良い	事業継続上、当面無くても支障のないシステムだが、データ欠損は許されない
	業務のリアルタイム性	RPO(目標復旧時点)		災害・障害発生時点	1時間以内の時点	1日以内の時点	数日	1週間以内の時点	1ヶ月以内の時点		数日	災害・障害発生時点
		RTO(目標復旧時間)	大規模システム障害	数分	2時間以内	2時間以内	12時間以内	24時間以内	1～3日		数分	1～3日
			大規模災害	数分	2時間以内	1～7日間	数週間	1～6ヶ月	1～6ヶ月		数分	1～6ヶ月
		RLO(目標復旧レベル)		全てのシステム機能 災害前と同等の性能	全てのシステム機能 災害前と同等の性能	特定システム機能のみ 災害前に比べ限定された性能を許容	特定システム機能のみ 災害前に比べ限定された性能を許容	特定システム機能のみ 災害前に比べ限定された性能を許容	特定システム機能のみ 災害前に比べ限定された性能を許容		全てのシステム機能 災害前と同等の性能	特定システム機能のみ 災害前に比べ限定された性能を許容
前提・制約条件(コスト・効率・運用負荷・信頼性)												
	コスト	導入コスト+ランニングコスト(年間)		1000万～	500～1000万	500～1000万	500～1000万	～500万	～500万		500～1000万	500～1000万
	1回のバックアップデータ転送量			MBオーダ	MBオーダ	GBオーダ	GBオーダ	GBオーダ	TBオーダ		GBオーダ	MBオーダ
	取扱いデータの最高機密レベル			機密レベル3 (関係者内)	機密レベル2 (関係部署内)	機密レベル1 (組織内)	機密レベル1 (組織内)	機密レベル1 (組織内)	機密レベル1 (組織内)		機密レベル1 (組織内)	機密レベル3 (関係者内)
	運用/管理負荷			低	低	中	中	中	高		低	中
	既存資産の活用性			有or無	有or無	有or無	有or無	有or無	有or無		有or無	有or無
	バックアップシステムの信頼性			高	高	中	中	中	低		高	高
対象リスクの範囲				・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク	・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク	・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク	・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク	・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク	・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク		・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク	・偶発的リスク&意図的リスク OR・偶発的リスク OR・意図的リスク

※背景色:黄色部分は技術選択、システムオプション選択の際に活用するためにいずれかの値を指定する因子で、DRクラス選択時には利用しない因子

図　8-1　DR クラス定義表

バックアップ構築/監視・監査技術						標準形DRクラス												+	特殊形DRクラス			
						DRクラス													DRクラス			
						A		B		C		D		E		F			α		β	
					DR選択表の決定因子;対象リスクの範囲⇒	偶発的リスク	意図的リスク	偶発的リスク	意図的リスク	偶発的リスク	意図的リスク	偶発的リスク	意図的リスク	偶発的リスク	意図的リスク	偶発的リスク	意図的リスク		偶発的リスク	意図的リスク	偶発的リスク	意図的リスク
構築技術	バックアップ/リカバリシステム(手段・構成)	バックアップ/リカバリ手段	リストア型		テープ/ディスクベース											○	○					
					レプリケーション					○	○	○	○	○	○					○	○	
					クラウド利用リストア型データバックアップ									○	○	○	○					
					クラウド利用リストア型システムバックアップ					○	○	○	○									
			切替型		サイト間フェイルオーバ(クラスタリング機能利用)	○	○	○	○										○	○		
					クラウド利用切替型バックアップ(自社ークラウド間)			○	○	○	○								○	○		
					クラウド利用切替型バックアップ(クラウド内センタ間)			○	○	○	○								○	○		
		バックアップ/リカバリシステム構成			ローカルバックアップ(サイト内保管)		○		○		○		○		○		○			○		○
					ネットワークバックアップ(遠隔地保管)	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○
					LANフリーバックアップ(専用ネット利用、遠隔地保管)	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○
					ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ(相互切り替え;Active-Active型、本番-開発型など)	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ												○	○		○	○		
				差分バックアップ												○	○		○	○		
				増分バックアップ(基本)		○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○
				継続的データ保護利用の増分バックアップ(CDP)		○	○	○	○	○	○	○	○	○	○	○	○				○	○
				ブロックレベルの増分バックアップ(重複除外技術)		○	○	○	○	○	○	○	○	○	○	○	○				○	○
		バックアップ先種別(クラウド利用含む)	ﾊﾞｯｸｱｯﾌﾟ先	自社方式		○	○			○	○					○	○		○	○	○	○
				データセンタ事業者利用		○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○
				クラウド事業者利用				○	○	○	○	○	○	○	○	○	○		○	○		
			多重バックアップ			○	○	○	○	○	○								○	○	○	○
		バックアップデータの保護強化策	機密分散データ保管					○	○													
			暗号化							○	○	○	○	○	○	○	○		○	○		
		オンライン/オフライン型	オンラインバックアップ			○	○	○	○	○	○	○	○	○	○				○	○	○	○
			オフラインバックアップ													○	○					
監視・監査技術	監視	リカバリ制御	制御の自動化			○	○	○	○										○	○		
			手動制御							○	○	○	○	○	○	○	○				○	○
		バックアップ状態の可視化	リアルタイム監視			○	○	○	○										○	○	○	○
			定期監視							○	○	○	○	○	○	○	○					
	監査	検査/動作検証				○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○
		教育・訓練				○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○

図　8-2　バックアップ技術選択表

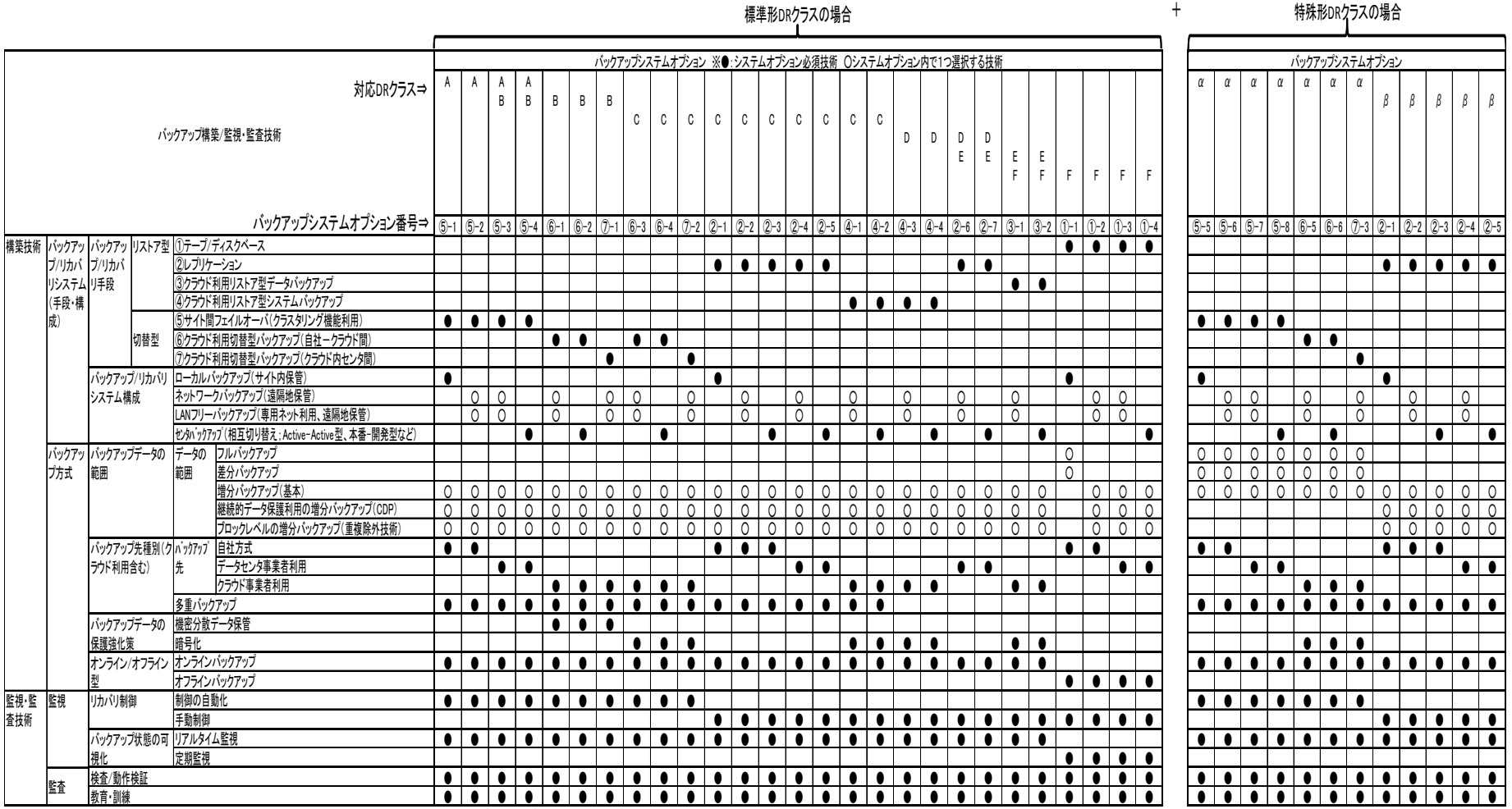

図　8-3　バックアップシステムオプション選択表

バックアップ構築/監視・監査技術						決定因子の重み	システム候補			
					対応DRクラス⇒		A	A	A B	A B
					バックアップシステムオプション番号⇒		⑤-1	⑤-2	⑤-3	⑤-4
構築技術	バックアップ/リカバリシステム(手段・構成)	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース						
				②レプリケーション						
				③クラウド利用リストア型データバックアップ						
				④クラウド利用リストア型システムバックアップ						
			切替型	⑤サイト間フェイルオーバ(クラスタリング機能利用)			●	●	●	●
				⑥クラウド利用切替型バックアップ(自社ークラウド間)						
				⑦クラウド利用切替型バックアップ(クラウド内センタ間)						
		バックアップ/リカバリシステム構成		ローカルバックアップ(サイト内保管)			●			
				ネットワークバックアップ(遠隔地保管)				○	○	
				LANフリーバックアップ(専用ネット利用、遠隔地保管)				○	○	
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ(相互切り替え;Active-Active型、本番-開発型など)						●
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ						
				差分バックアップ						
				増分バックアップ(基本)			○	○	○	○
				継続的データ保護利用の増分バックアップ(CDP)			○	○	○	○
				ブロックレベルの増分バックアップ(重複除外技術)			○	○	○	○
		バックアップ先種別(クラウド利用含む)	バックアップ先	自社方式			●	●		
				データセンタ事業者利用					●	●
				クラウド事業者利用						
			多重バックアップ				●	●	●	●
		バックアップデータの保護強化策	機密分散データ保管							
			暗号化							
		オンライン/オフライン型	オンラインバックアップ				●	●	●	●
			オフラインバックアップ							
監視・監査技術	監視	リカバリ制御	制御の自動化				●	●	●	●
			手動制御							
		バックアップ状態の可視化	リアルタイム監視				●	●	●	●
			定期監視							
	監査	検査/動作検証					●	●	●	●
		教育・訓練					●	●	●	●
評価項目(DRクラス決定因子)										
バックアップ対象の特性(レジリエンス)		業務(データ/システム)の重要度					10	10	10	10
		業務のリアルタイム性					10	6	4	8
前提・制約条件(コスト・効率・運用負荷・信頼性)		コスト				1	10	4	6	8
		1回のバックアップデータ転送量				1	10	8	8	8
		取扱いデータの最高機密レベル				1	10	8	6	6
		運用/管理負荷				1	4	6	8	10
		既存資産の活用性				1	10	10	8	6
		バックアップシステムの信頼性				1	10	8	6	4
対象リスクの範囲							10	10	10	10
バックアップ対象の特性(レジリエンス):小計							10	8	7	9
前提・制約条件(コスト・効率・運用負荷・信頼性):小計							9	7.333	7	7
対象リスクの範囲:小計							10	10	10	10
合計							9.667	8.444	8	8.667

図　8-4　バックアップシステムオプション評価表（DR クラス A 向け）

バックアップ構築/監視・監査技術						決定因子の重み	システム候補				
					対応DRクラス⇒		A B	A B	B C	B C	B C
					バックアップシステムオプション番号⇒		⑤-3	⑤-4	⑥-1	⑥-2	⑦-1
構築技術	バックアップ/リカバリシステム(手段・構成)	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース							
				②レプリケーション							
				③クラウド利用リストア型データバックアップ							
				④クラウド利用リストア型システムバックアップ							
			切替型	⑤サイト間フェイルオーバ(クラスタリング機能利用)			●	●			
				⑥クラウド利用切替型バックアップ(自社ークラウド間)					●	●	
				⑦クラウド利用切替型バックアップ(クラウド内センタ間)							●
		バックアップ/リカバリシステム構成		ローカルバックアップ(サイト内保管)							
				ネットワークバックアップ(遠隔地保管)			○		○		○
				LANフリーバックアップ(専用ネット利用、遠隔地保管)			○		○		○
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ(相互切り替え;Active-Active型、本番-開発型など)				●		●	
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ							
				差分バックアップ							
				増分バックアップ(基本)			○	○	○	○	○
				継続的データ保護利用の増分バックアップ(CDP)			○	○	○	○	○
				ブロックレベルの増分バックアップ(重複除外技術)			○	○	○	○	○
		バックアップ先種別(クラウド利用含む)	バックアップ先	自社方式							
				データセンタ事業者利用			●	●			
				クラウド事業者利用					●	●	●
			多重バックアップ				●	●	●	●	●
		バックアップデータの保護強化策	機密分散データ保管						●	●	●
			暗号化								
		オンライン/オフライン型	オンラインバックアップ				●	●	●	●	●
			オフラインバックアップ								
監視・監査技術	監視	リカバリ制御	制御の自動化				●	●	●	●	●
			手動制御								
		バックアップ状態の可視化	リアルタイム監視				●	●	●	●	●
			定期監視								
	監査	検査/動作検証					●	●	●	●	●
		教育・訓練					●	●	●	●	●
評価項目(DRクラス決定因子)											
バックアップ対象の特性(レジリエンス)		業務(データ/システム)の重要度					10	10	10	10	10
		業務のリアルタイム性					8	10	2	4	6
前提・制約条件(コスト・効率・運用負荷・信頼性)		コスト				1	2	4	6	8	10
		1回のバックアップデータ転送量				1	8	8	6	6	6
		取扱いデータの最高機密レベル				1	10	8	6	4	2
		運用/管理負荷				1	4	2	8	6	10
		既存資産の活用性				1	10	10	6	6	2
		バックアップシステムの信頼性				1	10	8	6	4	2
対象リスクの範囲							10	10	10	10	10
バックアップ対象の特性(レジリエンス):小計							9	10	6	7	8
前提・制約条件(コスト・効率・運用負荷・信頼性):小計							7.333	6.667	6.333	5.667	5.333
対象リスクの範囲:小計							10	10	10	10	10
合計							8.778	8.889	7.444	7.556	7.778

図　8-5　バックアップシステムオプション評価表（DR クラス B 向け）

バックアップ構築/監視・監査技術						決定因子の重み	システム候補									
					対応DRクラス⇒		BC	BC	BC	C	C	C	C	C	C	C
					バックアップシステムオプション番号⇒		⑥-3	⑥-4	⑦-2	②-1	②-2	②-3	②-4	②-5	④-1	④-2
構築技術	バックアップ/リカバリシステム(手段・構成)	バックアップ/リカバリ手段	リストア型		①テープ/ディスクベース											
					②レプリケーション					●	●	●	●	●		
					③クラウド利用リストア型データバックアップ											
					④クラウド利用リストア型システムバックアップ										●	●
			切替型		⑤サイト間フェイルオーバ(クラスタリング機能利用)											
					⑥クラウド利用切替型バックアップ(自社ークラウド間)		●	●								
					⑦クラウド利用切替型バックアップ(クラウド内センタ間)				●							
		バックアップ/リカバリシステム構成			ローカルバックアップ(サイト内保管)					●						
					ネットワークバックアップ(遠隔地保管)		○		○		○		○		○	
					LANフリーバックアップ(専用ネット利用、遠隔地保管)		○		○		○		○		○	
					センタバックアップ(相互切り替え;Active-Active型、本番-開発型など)			●				●		●		●
	バックアップ方式	バックアップデータの範囲	データの範囲		フルバックアップ											
					差分バックアップ											
					増分バックアップ(基本)		○	○	○	○	○	○	○	○	○	○
					継続的データ保護利用の増分バックアップ(CDP)		○	○	○	○	○	○	○	○	○	○
					ブロックレベルの増分バックアップ(重複除外技術)		○	○	○	○	○	○	○	○	○	○
		バックアップ先種別(クラウド利用含む)	バックアップ先		自社方式					●	●	●				
					データセンタ事業者利用								●	●		
					クラウド事業者利用		●	●	●						●	●
					多重バックアップ		●	●	●	●	●	●	●	●	●	●
		バックアップデータの保護強化策			機密分散データ保管											
					暗号化		●	●	●						●	●
		オンライン/オフライン型			オンラインバックアップ		●	●	●	●	●	●	●	●	●	●
					オフラインバックアップ											
監視・監査技術	監視	リカバリ制御			制御の自動化		●	●	●							
					手動制御					●	●	●	●	●	●	●
		バックアップ状態の可視化			リアルタイム監視		●	●	●	●	●	●	●	●	●	●
					定期監視											
	監査	検査/動作検証					●	●	●	●	●	●	●	●	●	●
		教育・訓練					●	●	●	●	●	●	●	●	●	●
評価項目(DRクラス決定因子)																
バックアップ対象の特性(レジリエンス)		業務(データ/システム)の重要度					10	10	10	10	10	10	10	10	10	10
		業務のリアルタイム性					8	9	10	5	3	4	1	2	6	7
前提・制約条件(コスト・効率・運用負荷・信頼性)		コスト				1	1	2	3	8	4	5	6	7	10	9
		1回のバックアップデータ転送量				1	6	6	6	10	8	8	8	8	6	6
		取扱いデータの最高機密レベル				1	2	2	2	10	8	8	6	6	4	4
		運用/管理負荷				1	8	9	10	3	1	2	4	5	6	7
		既存資産の活用性				1	2	2	1	10	8	8	6	6	4	4
		バックアップシステムの信頼性				1	2	2	1	10	8	8	6	6	4	4
対象リスクの範囲							10	10	10	10	10	10	10	10	10	10
バックアップ対象の特性(レジリエンス):小計							9	9.5	10	7.5	6.5	7	5.5	6	8	8.5
前提・制約条件(コスト・効率・運用負荷・信頼性):小計							3.5	3.833	3.833	8.5	6.167	6.5	6	6.333	5.667	5.667
対象リスクの範囲:小計							10	10	10	10	10	10	10	10	10	10
合計							7.5	7.778	7.944	8.667	7.556	7.833	7.167	7.444	7.889	8.056

図　8-6　バックアップシステムオプション評価表（DR クラス C 向け）

バックアップ構築/監視・監査技術						決定因子の重み	システム候補			
					対応DRクラス⇒		D	D	D E	D E
					バックアップシステムオプション番号⇒		④-3	④-4	②-6	②-7
構築技術	バックアップ/リカバリシステム(手段・構成)	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース						
				②レプリケーション					●	●
				③クラウド利用リストア型データバックアップ						
				④クラウド利用リストア型システムバックアップ			●	●		
			切替型	⑤サイト間フェイルオーバ(クラスタリング機能利用)						
				⑥クラウド利用切替型バックアップ(自社ークラウド間)						
				⑦クラウド利用切替型バックアップ(クラウド内センタ間)						
		バックアップ/リカバリシステム構成		ローカルバックアップ(サイト内保管)						
				ネットワークバックアップ(遠隔地保管)			○		○	
				LANフリーバックアップ(専用ネット利用、遠隔地保管)			○		○	
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ(相互切り替え;Active-Active型、本番-開発型など)				●		●
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ						
				差分バックアップ						
				増分バックアップ(基本)			○	○	○	○
				継続的データ保護利用の増分バックアップ(CDP)			○	○	○	○
				ブロックレベルの増分バックアップ(重複除外技術)			○	○	○	○
		バックアップ先種別(クラウド利用含む)	バックアップ先	自社方式						
				データセンタ事業者利用					●	●
				クラウド事業者利用			●	●		
			多重バックアップ							
		バックアップデータの保護強化策	機密分散データ保管							
			暗号化				●	●		
		オンライン/オフライン型	オンラインバックアップ				●	●	●	●
			オフラインバックアップ							
監視・監査技術	監視	リカバリ制御	制御の自動化							
			手動制御				●	●	●	●
		バックアップ状態の可視化	リアルタイム監視				●	●	●	●
			定期監視							
	監査	検査/動作検証					●	●	●	●
		教育・訓練					●	●	●	●
評価項目(DRクラス決定因子)										
バックアップ対象の特性(レジリエンス)		業務(データ/システム)の重要度					10	10	10	10
		業務のリアルタイム性					8	10	8	10
前提・制約条件(コスト・効率・運用負荷・信頼性)		コスト				1	8	10	4	6
		1回のバックアップデータ転送量				1	8	8	10	10
		取扱いデータの最高機密レベル				1	8	8	10	10
		運用/管理負荷				1	10	10	8	8
		既存資産の活用性				1	8	8	10	10
		バックアップシステムの信頼性				1	8	8	10	10
対象リスクの範囲							10	10	10	10
バックアップ対象の特性(レジリエンス):小計							9	10	9	10
前提・制約条件(コスト・効率・運用負荷・信頼性):小計							8.333	8.667	8.667	9
対象リスクの範囲:小計							10	10	10	10
合計							9.111	9.556	9.222	9.667

図　8-7　バックアップシステムオプション評価表（DR クラス D 向け）

バックアップ構築/監視・監査技術						決定因子の重み	システム候補			
					対応DRクラス⇒		D E	D E	E F	E F
					バックアップシステムオプション番号⇒		②-6	②-7	③-1	③-2
構築技術	バックアップ/リカバリシステム(手段・構成)	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース						
				②レプリケーション			●	●		
				③クラウド利用リストア型データバックアップ					●	●
				④クラウド利用リストア型システムバックアップ						
			切替型	⑤サイト間フェイルオーバ(クラスタリング機能利用)						
				⑥クラウド利用切替型バックアップ(自社ークラウド間)						
				⑦クラウド利用切替型バックアップ(クラウド内センタ間)						
		バックアップ/リカバリシステム構成		ローカルバックアップ(サイト内保管)						
				ネットワークバックアップ(遠隔地保管)			○		○	
				LANフリーバックアップ(専用ネット利用、遠隔地保管)			○		○	
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ(相互切り替え;Active-Active型、本番-開発型など)				●		●
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ						
				差分バックアップ						
				増分バックアップ(基本)			○	○	○	○
				継続的データ保護利用の増分バックアップ(CDP)			○	○	○	○
				ブロックレベルの増分バックアップ(重複除外技術)			○	○	○	○
		バックアップ先種別(クラウド利用含む)	バックアップ先	自社方式						
				データセンタ事業者利用			●	●		
				クラウド事業者利用					●	●
			多重バックアップ							
		バックアップデータの保護強化策	機密分散データ保管							
			暗号化						●	●
		オンライン/オフライン型	オンラインバックアップ				●	●	●	●
			オフラインバックアップ							
監視・監査技術	監視	リカバリ制御	制御の自動化							
			手動制御				●	●	●	●
		バックアップ状態の可視化	リアルタイム監視				●	●	●	●
			定期監視							
	監査	検査/動作検証					●	●	●	●
		教育・訓練					●	●	●	●
評価項目(DRクラス決定因子)										
バックアップ対象の特性(レジリエンス)		業務(データ/システム)の重要度					10	10	10	10
		業務のリアルタイム性					4	6	8	10
前提・制約条件(コスト・効率・運用負荷・信頼性)		コスト				1	8	10	4	6
		1回のバックアップデータ転送量				1	10	10	8	8
		取扱いデータの最高機密レベル				1	10	8	10	8
		運用/管理負荷				1	8	10	4	6
		既存資産の活用性				1	8	10	8	10
		バックアップシステムの信頼性				1	10	8	10	8
対象リスクの範囲							10	10	10	10
バックアップ対象の特性(レジリエンス):小計							7	8	9	10
前提・制約条件(コスト・効率・運用負荷・信頼性):小計							9	9.333	7.333	7.667
対象リスクの範囲:小計							10	10	10	10
合計							8.667	9.111	8.778	9.222

図　8-8　バックアップシステムオプション評価表（DR クラス E 向け）

バックアップ構築/監視・監査技術						決定因子の重み	システム候補					
					対応DRクラス⇒		E F	E F	F	F	F	F
					バックアップシステムオプション番号⇒		③-1	③-2	①-1	①-2	①-3	①-4
構築技術	バックアップ/リカバリシステム(手段・構成)	バックアップ/リカバリ手段	リストア型		①テープ/ディスクベース				●	●	●	●
					②レプリケーション							
					③クラウド利用リストア型データバックアップ		●	●				
					④クラウド利用リストア型システムバックアップ							
			切替型		⑤サイト間フェイルオーバ(クラスタリング機能利用)							
					⑥クラウド利用切替型バックアップ(自社ークラウド間)							
					⑦クラウド利用切替型バックアップ(クラウド内センタ間)							
		バックアップ/リカバリシステム構成			ローカルバックアップ(サイト内保管)				●			
					ネットワークバックアップ(遠隔地保管)		○			○	○	
					LANフリーバックアップ(専用ネット利用、遠隔地保管)		○			○	○	
					ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ(相互切り替え;Active-Active型、本番-開発型など)			●				●
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ					○			
				差分バックアップ					○			
				増分バックアップ(基本)			○	○		○	○	○
				継続的データ保護利用の増分バックアップ(CDP)			○	○		○	○	○
				ブロックレベルの増分バックアップ(重複除外技術)			○	○		○	○	○
		バックアップ先種別(クラウド利用含む)	バックアップ先	自社方式					●	●		
				データセンタ事業者利用							●	●
				クラウド事業者利用			●	●				
			多重バックアップ									
		バックアップデータの保護強化策	機密分散データ保管									
			暗号化				●	●				
		オンライン/オフライン型	オンラインバックアップ				●	●				
			オフラインバックアップ						●	●	●	●
監視・監査技術	監視	リカバリ制御	制御の自動化									
			手動制御				●	●	●	●	●	●
		バックアップ状態の可視化	リアルタイム監視				●	●				
			定期監視						●	●	●	●
	監査	検査/動作検証					●	●	●	●	●	●
		教育・訓練					●	●	●	●	●	●
評価項目(DRクラス決定因子)												
バックアップ対象の特性(レジリエンス)		業務(データ/システム)の重要度					10	10	10	10	10	10
		業務のリアルタイム性					8	10	6	1	2	4
前提・制約条件(コスト・効率・運用負荷・信頼性)		コスト				1	8	10	6	1	2	4
		1回のバックアップデータ転送量				1	6	6	10	8	8	8
		取扱いデータの最高機密レベル				1	1	2	10	8	6	4
		運用/管理負荷				1	8	10	6	1	2	4
		既存資産の活用性				1	1	2	10	4	6	8
		バックアップシステムの信頼性				1	1	2	10	4	6	8
対象リスクの範囲							10	10	10	10	10	10
バックアップ対象の特性(レジリエンス):小計							9	10	8	5.5	6	7
前提・制約条件(コスト・効率・運用負荷・信頼性):小計							4.167	5.333	8.667	4.333	5	6
対象リスクの範囲:小計							10	10	10	10	10	10
合計							7.722	8.444	8.889	6.611	7	7.667

図　8-9　バックアップシステムオプション評価表（DR クラス F 向け）

バックアップ構築/監視・監査技術						決定因子の重み	システム候補						
					対応DRクラス⇒		α	α	α	α	α	α	α
					バックアップシステムオプション番号⇒		⑤-5	⑤-6	⑤-7	⑤-8	⑥-5	⑥-6	⑦-3
構築技術	バックアップ/リカバリシステム(手段・構成)	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース									
				②レプリケーション									
				③クラウド利用リストア型データバックアップ									
				④クラウド利用リストア型システムバックアップ									
			切替型	⑤サイト間フェイルオーバ(クラスタリング機能利用)			●	●	●	●			
				⑥クラウド利用切替型バックアップ(自社ークラウド間)							●	●	
				⑦クラウド利用切替型バックアップ(クラウド内センタ間)									●
		バックアップ/リカバリシステム構成		ローカルバックアップ(サイト内保管)			●						
				ネットワークバックアップ(遠隔地保管)				○	○		○		○
				LANフリーバックアップ(専用ネット利用、遠隔地保管)				○	○		○		○
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ(相互切り替え;Active-Active型、本番-開発型など)						●		●	
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ			○	○	○	○	○	○	○
				差分バックアップ			○	○	○	○	○	○	○
				増分バックアップ(基本)			○	○	○	○	○	○	○
				継続的データ保護利用の増分バックアップ(CDP)									
				ブロックレベルの増分バックアップ(重複除外技術)									
		バックアップ先種別(クラウド利用含む)	バックアップ先	自社方式			●	●					
				データセンタ事業者利用					●	●			
				クラウド事業者利用							●	●	●
			多重バックアップ				●	●	●	●	●	●	●
		バックアップデータの保護強化策	機密分散データ保管										
			暗号化								●	●	●
		オンライン/オフライン型	オンラインバックアップ				●	●	●	●	●	●	●
			オフラインバックアップ										
監視・監査技術	監視	リカバリ制御	制御の自動化				●	●	●	●	●	●	●
			手動制御										
		バックアップ状態の可視化	リアルタイム監視				●	●	●	●	●	●	●
			定期監視										
	監査	検査/動作検証					●	●	●	●	●	●	●
		教育・訓練					●	●	●	●	●	●	●
評価項目(DRクラス決定因子)													
バックアップ対象の特性(レジリエンス)		業務(データ/システム)の重要度					10	10	10	10	10	10	10
		業務のリアルタイム性					10	7	8	9	4	5	6
前提・制約条件(コスト・効率・運用負荷・信頼性)		コスト				1	7	4	5	6	8	9	10
		1回のバックアップデータ転送量				1	10	8	6	6	2	2	4
		取扱いデータの最高機密レベル				1	10	9	8	7	6	5	4
		運用/管理負荷				1	4	5	6	7	8	9	10
		既存資産の活用性				1	10	9	8	7	6	5	4
		バックアップシステムの信頼性				1	10	9	8	7	6	5	4
対象リスクの範囲							10	10	10	10	10	10	10
バックアップ対象の特性(レジリエンス):小計							10	8.5	9	9.5	7	7.5	8
前提・制約条件(コスト・効率・運用負荷・信頼性):小計							8.5	7.333	6.833	6.667	6	5.833	6
対象リスクの範囲:小計							10	10	10	10	10	10	10
合計							9.5	8.611	8.611	8.722	7.667	7.778	8

図　8-10　バックアップシステムオプション評価表（DR クラスα向け）

バックアップ構築/監視・監査技術						決定因子の重み	システム候補				
					対応DRクラス⇒		β	β	β	β	β
					バックアップシステムオプション番号⇒		②-1	②-2	②-3	②-4	②-5
構築技術	バックアップ/リカバリシステム(手段・構成)	バックアップ/リカバリ手段	リストア型	①テープ/ディスクベース							
				②レプリケーション			●	●	●	●	●
				③クラウド利用リストア型データバックアップ							
				④クラウド利用リストア型システムバックアップ							
			切替型	⑤サイト間フェイルオーバ(クラスタリング機能利用)							
				⑥クラウド利用切替型バックアップ(自社ークラウド間)							
				⑦クラウド利用切替型バックアップ(クラウド内センタ間)							
		バックアップ/リカバリシステム構成		ローカルバックアップ(サイト内保管)			●				
				ネットワークバックアップ(遠隔地保管)				○		○	
				LANフリーバックアップ(専用ネット利用、遠隔地保管)				○		○	
				ｾﾝﾀﾊﾞｯｸｱｯﾌﾟ(相互切り替え;Active-Active型、本番-開発型など)					●		●
	バックアップ方式	バックアップデータの範囲	データの範囲	フルバックアップ							
				差分バックアップ							
				増分バックアップ(基本)			○	○	○	○	○
				継続的データ保護利用の増分バックアップ(CDP)			○	○	○	○	○
				ブロックレベルの増分バックアップ(重複除外技術)			○	○	○	○	○
		バックアップ先種別(クラウド利用含む)	バックアップ先	自社方式			●	●	●		
				データセンタ事業者利用						●	●
				クラウド事業者利用							
			多重バックアップ				●	●	●	●	●
		バックアップデータの保護強化策	機密分散データ保管								
			暗号化								
		オンライン/オフライン型	オンラインバックアップ				●	●	●	●	●
			オフラインバックアップ								
監視・監査技術	監視	リカバリ制御	制御の自動化								
			手動制御				●	●	●	●	●
		バックアップ状態の可視化	リアルタイム監視				●	●	●	●	●
			定期監視								
	監査	検査/動作検証					●	●	●	●	●
		教育・訓練					●	●	●	●	●
評価項目(DRクラス決定因子)											
バックアップ対象の特性(レジリエンス)		業務(データ/システム)の重要度					10	10	10	10	10
		業務のリアルタイム性					10	6	8	2	4
前提・制約条件(コスト・効率・運用負荷・信頼性)		コスト				1	10	2	4	6	8
		1回のバックアップデータ転送量				1	10	8	8	8	8
		取扱いデータの最高機密レベル				1	10	8	8	6	6
		運用/管理負荷				1	6	2	4	8	10
		既存資産の活用性				1	10	8	8	6	6
		バックアップシステムの信頼性				1	10	8	8	6	6
対象リスクの範囲							10	10	10	10	10
バックアップ対象の特性(レジリエンス):小計							10	8	9	6	7
前提・制約条件(コスト・効率・運用負荷・信頼性):小計							9.333	6	6.667	6.667	7.333
対象リスクの範囲:小計							10	10	10	10	10
合計							9.778	8	8.556	7.556	8.111

図　8-11　バックアップシステムオプション評価表（DR クラス β 向け）

9. 付録２：プロセス実施確認チェックリスト

本ガイドラインの各プロセスでの実施事項を実施確認するためのチェックリストを以下に示す。

プロセス	#	実施確認項目	ガイドライン関係箇所（章番号）	実施確認チェック（レ）	備考
DRアセスメント	1	入力情報となる各対象ITシステムのバックアップ関連パラメータ値を明確化しましたか？	4.1	□	
	2	上記パラメータ値に対応する各対象ITシステムのDRクラスを「DRクラス定義表」より選定しましたか？	4.1	□	
DR要件定義	3	各対象ITシステムの選定したDRクラスに該当するバックアップ技術を、対象リスク（偶発・意図的リスク）の範囲も考慮して「バックアップ技術選択表」より選択しましたか？	4.2	□	
	4	各対象ITシステムの選定したDRクラスに該当するバックアップシステムオプションを、対象リスク（偶発・意図的リスク）の範囲も考慮して「バックアップシステムオプション選択表」より選択しましたか？	4.2	□	
DR対策策定	5	各対象ITシステムの選定したDRクラスに該当するバックアップシステムオプションにつき、該当する「バックアップシステムオプション評価表」を選定しましたか？	4.3	□	
	6	各対象ITシステムにつき、上記選定の「バックアップシステムオプション評価表」の評価項目への重み付けを入力しましたか？	4.3	□	
	7	各対象ITシステムにつき、上記選定の「バックアップシステムオプション評価表」により、各システム候補の重み付け計算による評価点を算出しましたか？	4.3	□	
	8	各対象ITシステムにつき、上記評価点の最も高いシステムオプションを、選択技術の決定も含め、最適なバックアップシステムとして特定しましたか？	4.3	□	
	9	各対象ITシステムにつき、特定した最適なバックアップシステムが実現・実装制約上調整不要か確認しましたか？（調整要の場合、＃8に戻り代替システムオプションの選択あるいは＃4に戻りカスタムシステムオプション作成）	4.3	□	
	10	各対象ITシステムごとに決定した最適バックアップシステムの対策コストを見積り、その合計と、IT-BCPからの入力情報である許容総コストを比較し、合計が許容総コスト内であることを確認しましたか？	4.3	□	
	11	各対象ITシステムごとに決定した最適バックアップシステムにつき、該当DRクラス、バックアップ関連パラメータ値、選択技術の情報に基づき、バックアップシステムの要件定義としてまとめましたか？	4.3	□	