ストレージシステムによる災害対策の現実解

さの　　やすゆき
佐野　　泰之

株式会社エクサ　基盤イノベーション技術部
ＩＴプロフェッショナル

’

原稿量
本文　　８，０００字
要約　　１，１００字
図表　　６枚

＜要　約＞

日本における過去の災害発生及び今後の発生予測を踏まえ、システムの災害対策の強化による、企業の事業継続性確保への関心は極めて高い。

事業継続をＩＴで実現するものに、災害対策、緊急時対応計画、そしてバックアップの確保がある。バックアップの確保とは、電子データの正確なコピーを作ることであり、通常はストレージシステムで実現している。つまり、災害対策とストレージシステムには密接な関係がある。そのストレージシステムには、機能、性能、信頼性、そしてコストにおいてさまざまなものがある。だが、災害対策システムの中では中心的な立場であるにもかかわらず、単にコストだけを注目し、また機能や性能などの技術的要素が極めて複雑なため、その理解が周知されず適切なものが選択されていないのが現状である。

そこで本稿では、現時点で構築及び運用可能なストレージステムをわかりやすくカテゴライズすることで、専門家以外の方でも災害対策の実現レベルに応じたシステムを選択できることを目的とした。

更に、災害対策システムの計画と運用フェーズにおける課題にも着目することで、より効果の高い災害対策システムの構築及び運用ができることを目的とした。

まず、システム選定前の検討にて、対象システムを選定し、イニシャルコスト、ランニングコスト、ＲＴＯ（Recovery Time Objective、目標復旧時間）、ＲＰＯ（Recovery Point Objective、目標復旧時点）など、具体的に数値で比較できる目標を設定する。

そして、その目標に応じてストレージシステムを選定する。カテゴライズには、データのコピー対象、データの転送方法がある。更に、そのデータの転送方法として、テープの搬送及びサーバー型レプリケーションとストレージ型レプリケーションがある。それらをＲＴＯ／ＲＰＯ、コスト、設計・構築工数、管理性、拡張性で評価し、選択のポイントとした。

また、災害対策システムの計画と運用フェーズの課題として、本番システムが稼働中の箇所（本番サイト）の運用に加え、災害時の切替え先の箇所（災対サイト）の維持の必要性についても紹介した。

以上の内容をもとに、災害対策システムが成り立つための数式を以下のとおり提示した。

災害対策システム＝明確な目標×正しいシステム構成×災対サイトの維持

この数式は掛け算であるため、どれかひとつが「ゼロ」になってしまえば、システムの価値が、「ゼロ」になってしまうことを提言した。

本稿が、災害対策システムに携わる担当者だけでなく、システムに関連するすべての方々の参考となり、そのシステムの品質向上に少しでも寄与できれば幸いである。

目　次

1. はじめに

日本における過去の災害発生及び今後の発生予測を踏まえ、システムの災害対策の強化による企業の事業継続性確保への関心は極めて高い。

まず、事業継続をマネジメントレベルから業務レベルまで掘り下げると、事業継続管理（ＢＣＭ）、事業継続計画（ＢＣＰ）を経て、ＩＴで実現する、災害対策、緊急時対応計画、そしてバックアップの確保となる。バックアップの確保とは、電子データの正確なコピーを作ることであり、通常はストレージシステムで実現している。

つまり、災害対策とストレージシステムには密接な関係がある。

そのストレージシステムには、機能、性能、信頼性、そしてコストにてさまざまなものがあり、災害対策の実現レベルに応じて、適切なものを選択する必要がある。本来ストレージシステムは、災害対策システムの中では中心的な立場であるにもかかわらず、単にコストだけを注目し、また機能や性能などの技術的要素が極めて複雑なため、その理解が周知されず適切なものが選択されていないのが現状である。

そこで本稿では、現時点で構築及び運用が可能なストレージステムをわかりやすくカテゴライズすることで、専門家以外の方でも災害対策の実現レベルに応じたシステムを選択できることを目的とした。

更に、災害対策システムの計画と運用フェーズにおける課題にも着目することで、より効果の高い災害対策システムの構築及び運用ができることを目的とした。

本稿が、災害対策システムに携わる担当者だけでなく、システムに関連するすべての方々の参考となり、そのシステムの品質向上に少しでも寄与できれば幸いである。

2. システム選定前の検討

まず、ストレージシステムを選定する前に、検討すべき災害対策システムとしての対象の絞り込み、コストの検討及び目標の設定について述べる。

2.1 対象の絞り込み

本番システムが稼働中の箇所（以下、本番サイト）の周辺で局所災害が発生し、システムが稼働できなくなることを想定し、災害時の切替え先（災害対策サイト　以下、災対サイト）を設置する災害対策システムを計画する場合、まずは対象となるシステムを選定する必要がある。それには、システムの必要性や目的を明確にし、費用対効果や社会的信用にも踏み込んだ提案が必要だが、ＩＴだけで検討できることには限界がある。そこで、ＩＴからのアプローチとして、イニシャルコスト、ランニングコスト、ＲＴＯ（Recovery Time Objective、目標復旧時間）、ＲＰＯ（Recovery Point Objective、目標復旧時点）などの具体的に数値で比較できる目標を設定する。それら、具体的に数値で比較し、レベルの高いものからＡ・Ｂ・Ｃのように、少なくとも３つのレベルに分割し対象をグループ化する。災害対策システムは、保険的な役割が高いため、なるべくコストを抑えることを念頭においたスモールスタートによるアプローチがふさわしいと考える。よって、まずはレベルの高いＡだけを対象にするなど、対象の絞り込みを最初に行うことを推奨する。[1)]

2.2 コストの検討

災害対策システムにおけるストレージシステムのコストを、イニシャルコスト及びランニングコストに分けて検討する。

イニシャルコストには、ハードウェア装置の購入費、ソフトウェアのライセンス費用、システムの構築費がある。一方、ランニングコストには、ハードウェア装置の保守費、ソフトウェアのライセンス保守費、ネットワーク回線の使用料、サイトの使用料、保守要員の人件費がある。あらかじめ、それぞれの費用がどれくらいのかを算定する必要がある。特に、ソフトウェアの保守ライセンス費用やネットワーク回線の使用料は忘れがちなので、留意が必要である。

2.3 目標の設定

災害対策システムを計画・検討する上で、定量的な目標としてＲＴＯ／ＲＰＯを設定する必要がある。図 2.1 で示すとおり、ＲＴＯは、災害発生時点からどの時点で復旧するかの目標時間指標である。また、ＲＰＯは災害発生時からどの時点の状態に復旧するかの、目標時間指標である。

これらは３章で述べるシステム選定に直接かかわるものなので、必ず明確にしておく必要がある。

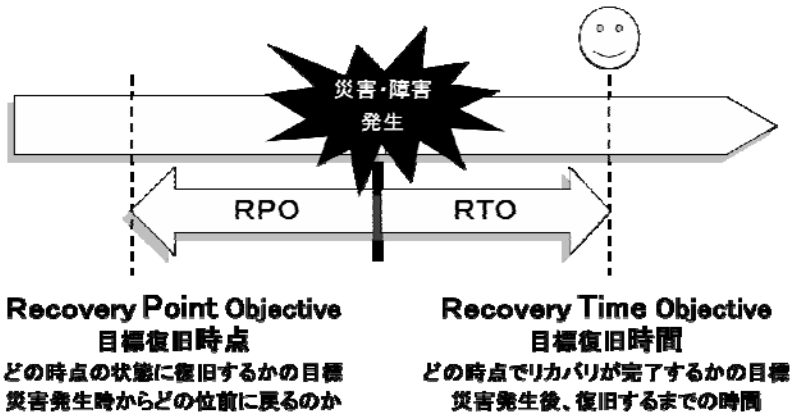

図 2.1　ＲＴＯとＲＰＯ

3. システム選定

ストレージシステムの選定にあたり、コピーするデータの対象とコピーの方法について述べる。

3.1 データのコピー対象

災害対策システムで中心的な役割であるバックアップの確保、つまり電子データの正確なコピーの作成する対象について検討する。これは、本番サイトのデータを災対サイトにコピーする際に、どのデータを対象とするかを決めることであり、大まかに二つに区別できる。

一つ目は、実際に利用されているデータであり、ここでは「プライマリデータ」と呼ぶ。そのプライマリデータのコピーを作成し、災対サイトでそのまま使用する。

二つ目は、プライマリデータを一度本番サイトでコピーしたデータ、つまり「バックアップデータ」を作成し、そのデータ更にコピーして災対サイトで使用する。

これらを以下の図で示す。また、コピーの具体的な方法については、次節で述べる。

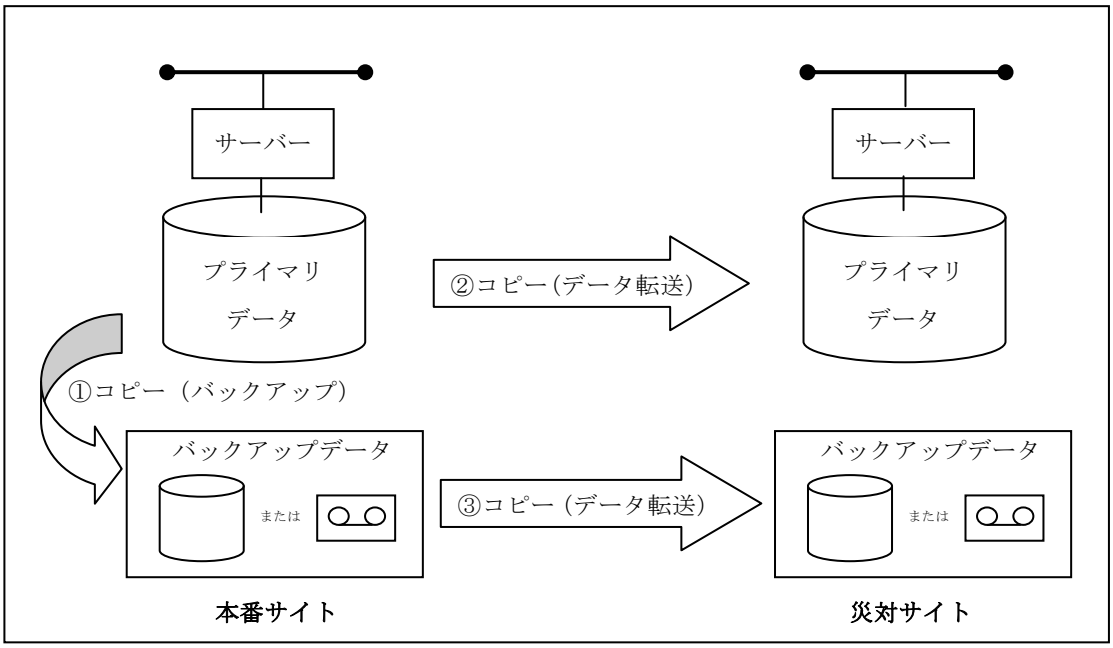

図 3.1　データのコピー対象

3.2 データコピーの方法

図 3.1 で示したとおり、データのコピーには本番サイト内で実施するプライマリデータのコピー（図中の①バックアップ）と、本番サイトのプライマリデータまたはバックアップデータの災対サイトへのコピー（図中の②及び③のデータ転送）がある。

3.2.1 バックアップ

バックアップは、本番サイトのプライマリデータが消失した場合の復旧を目的として取得する。一般的には、専用のバックアップソフトを使用して、ディスクまたはテープに取得する。バックアップデータは、復旧の際のリストアに使用できるよう、整合性のあるものを取得する。

3.2.2 データ転送

本番サイトから災対サイトへのデータ転送は、テープの搬送またはレプリケーション機能が多く利用される。テープの場合は、本番サイトから災対サイトに定期的にバックアップデータが格納されたテープを物理的に搬送する。

一方、ディスクを使用するレプリケーションには、本番サイトと災対サイトのデータを常に同じ状態にしておく同期方式と、決めた時間に同じ状態にする非同期方式がある。

同期方式は非同期方式に比べ、データ転送に使用する回線への負荷が高くなることと、使用可能な距離に制限があるため、ＲＴＯをゼロにしなくてはならないミッションクリティカルなシステム以外は、非同期方式が多く採用されている。

また、レプリケーションにはサーバーに専用のソフトウェアを導入して機能を実現する「サーバー型」と、ディスクの機能で実現する「ストレージ型」がある。詳細については、次節で述べる。

3.3 レプリケーションの種類

データを転送するレプリケーションの種類として、二つの方法について述べる。

3.3.1 サーバー型

サーバー型レプリケーションでは、サーバーにインストールしたソフトウェアでデータ転送を行う。レプリケーション機能に特化したソフトウェア、またはメールシステムやデータベースなどのミドルウェアのオプションを利用する。図 3.2 で示すとおり、本番サイトのプライマリデータはサーバーとネットワーク回線及び、災対サイトのサーバーとディスクを経由してデータを転送する。

サーバー型では、レプリケーションソフトウェアはサーバー上で実行されるので、後述するストレージ型とは異なり、ストレージディスクなどのハードウェアの追加コンポーネントは必要としない。そのため、サーバー型はより安価に導入できる方式である。一方、サーバーに新たな処理のオーバーヘッドがかかること、そしてインストールしたソフトウェアに万が一不具合が発生した場合など、本来サーバー上で稼働するアプリケーションに影響を与えることがある。更に、ソフトウェアのライセンス費用とシステム管理業務がサーバー数に比例して増えていくので、サーバー数の多い環境にはストレージ型の方が有利である。実際には、サーバー数が多い場合や、重要な役割を担うハイエンドサーバーについては、サーバー型ではなくストレージ型が多く採用されている。

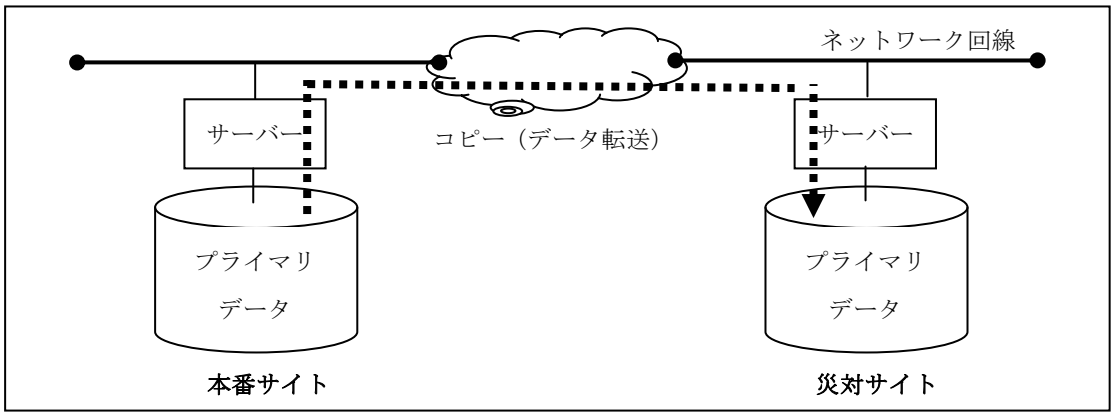

図 3.2　サーバー型レプリケーション

3.3.2 ストレージ型

ストレージ型レプリケーションでは、レプリケーションソフトウェアはストレージディスクに実装されているコントローラー上で実行される。つまり、サーバー型とは異なりサーバー及びサーバー上で稼働するアプリケーションには影響を与えない。

ストレージ型の歴史は長く、当初はハイエンドレベルのディスクを中心に実装され、極めてミッションクリティカルなシステムに限り導入されていたが、現在ではスモールからミッドレンジレベルにも実装され、信頼性のみならず価格的にも安定している。

サーバーのＯＳに依存しないこと、ライセンス料がサーバー数ではなくストレージの容量で決まることからみて、サーバーを多数備える環境にふさわしい。レプリケーションの負荷はストレージコントローラーに移されるので、サーバーに処理オーバーヘッドは発生しない。

一方、混在したストレージ環境をサポートしないため、本番サイトと同一機種のストレージディスクを災対サイトにも導入する必要があるため、サーバー型に比べ初期費用は高くなる。

図 3.3 で示すとおり、ストレージ型ではプライマリデータだけでなく、バックアップデータのデータ転送が可能である。ただし、プライマリデータかバックアップデータかにより、ストレージディスクを選択する必要がある。プライマリデータ用は、文書ファイルなどの非構造化データを格納するシステムに向いている。一方、データベースなどの構造化データを格納するシステムでは、直接プライマリデータをコピーするのではなく、一旦本番サイトで整合性のあるバックアップを取得し、そのバックアップデータを災対サイトに転送する方法が多く採用されている。バックアップ用には､データ重複排除などの追加機能を備えたものがあり､転送するデータを最小限にすることで、ネットワーク回線の負荷及び回線使用料などのランニングコストを抑えることが可能である。

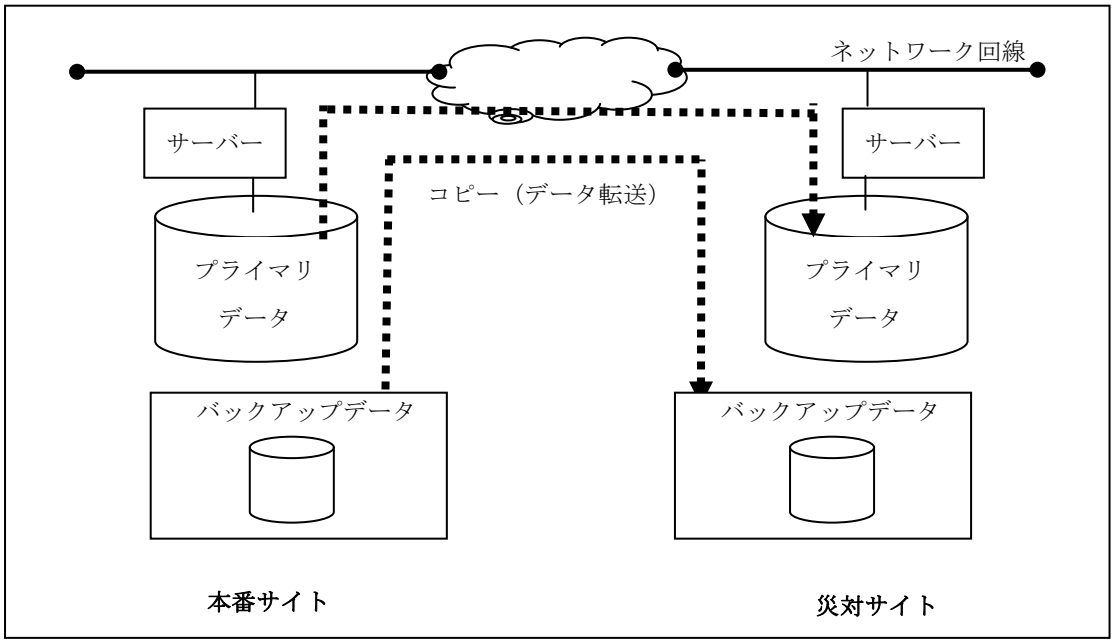

図 3.3 ストレージ型レプリケーション

3.4 選定のポイント

選定のポイントとして、目標とするＲＴＯ／ＲＰＯの設定及び、その実現性について述べる。

3.4.1 ＲＴＯ／ＲＰＯの設定

選定の第一歩は、ＲＴＯ（目標復旧時間）とＲＰＯ（目標復旧時点）を決めることである。陥りやすい例として、「本番サイトで稼働中にシステムはすべて重要なので、災害発生時には即すべてのシステムを災対サイトで稼働可能とする」、という完璧なシステム検討をしてしまうことである。つまり、ＲＴＯとＲＰＯを「ゼロ」に近づけることから始めてしまう。前述のとおり、これは技術的にはじゅうぶん可能ではあるが、それ相応の技術構成・運用・コストが必要で、実現するには数々の課題を解決しなければならなくなる。しかし、技術や運用の課題の解決に時間をとられ、コスト面など経営層の合意がとれないうちに時間だけが進み、計画が頓挫することがある。[2)]

災害対策システムは、保険的な役割が高いため、なるべくコストを抑える、つまりＲＴＯ／ＲＰＯはある程度余裕を持ったものを設定することを推奨する。具体的には、ＲＴＯ／ＲＰＯは時間単位ではなく日数単位で設定する、いわゆるスモールスタートで取り組む方が、より現実解に近いシステムになると筆者は判断している。

3.4.2 目標の実現性

ＲＴＯ／ＲＰＯが決まれば、あとはどの方式を選択してその目標が実現するかを考える。

例えば、本番サイトのバックアップデータを災対サイトに転送するためにテープを選択した場合は、そのテープを災対サイトのプライマリデータ領域にリストアするのにどのくらい時間を要するのかを検討する。それが、目標以内の時間または日数であれば、まずはテープ搬送によるシステムを選択してみる。テープ搬送による災害対策は、手軽に開始でき最も典型的且つ確実な手段である。

次に、テープ搬送では目標が達成できないのであれば、そこで初めてレプリケーションを検討する。前述のとおり、ＲＴＯをゼロにしなくてはならないミッションクリティカルなシステム以外は非同期方式で検討する。そして、サーバー型、ストレージ型のどちらかにするかについては、対象となるサーバー台数の数から決めてみる。具体的に、サーバー台数が 2～3 ケタレベルであれば、ストレージ型を推奨する。

更に、バックアップデータ用かプライマリデータ用かのどちらかを選定するかについては、バックアップ用であれば、稼働中の現行システムに追加対応できるのでまずは候補とする。

一方、プライマリデータ用の場合は、稼働中の現行システムの変更ならびにデータ移行が必要となるため、本番サイトの初期構築時から災害サイトを見据えて設計する必要がある。

また、バックアップ用の場合は、テープ搬送と同様に災対サイトのプライマリデータ領域にリストアするのにどのくらい時間を要するのかを検討する。これは、意外と見落とされがちなことである。つまり、レプリケーションしているデータが、バックアップデータなのか、プライマリデータなのかを常に留意しておかなければならない。レプリケーションさえ実行していれば、災対サイトで即データが使用可能であるという思い込みは意外と多いためである。

いままで述べたことを踏まえ、現時点で筆者が考える現実解として、方式と検討項目と見解を表 4.1 にまとめた。これは一例であり、最終的には検討する方自身で作成することを強く推奨する。

表 4.1　方式と検討項目

検討項目	バックアップデータ			プライマリデータ	
	テープ搬送	サーバー型レプリケーション	ストレージ型レプリケーション	サーバー型レプリケーション	ストレージ型レプリケーション
ＲＴＯ／ＲＰＯ	数日から数週間	数日	数日	１日以内	１日以内
イニシャルコスト	低い	中	高い	高い	極めて高い
ランニングコスト	低い	中	中	高い	高い
設計工数	低い	中	中	高い	高い
構築工数	低い	高い	中	極めて高い	極めて高い
管理性	テープの搬送に伴う管理がやや複雑	サーバー台数が増えると管理性が劣る	専用機（アプライアンス）が多く管理は簡素	サーバー台数が増えると管理性が劣る	極めて簡素
拡張性	テープを増やすことで容量拡張可能	サーバー増設で可能も管理性が落ちる	専用機の台数を増やすことで可能	サーバー増設で可能も管理性が落ちる	ディスク増設で可能
留意点	災対サイトにて、バックアップデータをリストアする必要があるため、その時間分ＲＴＯが加算される			プライマリデータを転送しているため、災対サイトにてデータがそのまま使用できるため、ＲＴＯが短縮できる	
総評	スモールスタート向き 最も実績のある方式	サーバーのアプリケーションに影響ありサーバー総台数が２ケタ以上には向かない	専用機により構築が簡素化できる 重複排除などの追加機能が享受できる	ＲＴＯ／ＲＰＯが厳しい、メールシステムやデータベース向き	ＲＴＯ／ＲＰＯが厳しい、ミットレンジからハイエンド向き メールシステム、データベースに加え、ファイルサーバーにも向く

4. 災対サイトの維持

設定した目標に応じて、災害対策システムとして災対サイトを構築した場合、従来、実施している本番サイトの運用以外に考慮すべきことを紹介する。これらは、一見当たり前なことではあるが、筆者が数々の事例をみてきた限り、意外と見逃されているようである。これらを実施しない限り、時間とコストをかけて構築した災対サイト、つまり災害対策システム全体が機能しなくなるので、じゅうぶんに留意願いたい。

4.1 データ以外のコピー

３章では、本番サイトのプライマリデータ及び、バックアップデータつまり、データのコピーについて紹介した。これらのデータは、前述のレプリケーションやバックアップにて、自動的にコピーできる。一方、サーバー内にあるＯＳやソフトウェアについては、コピーの対象外である。

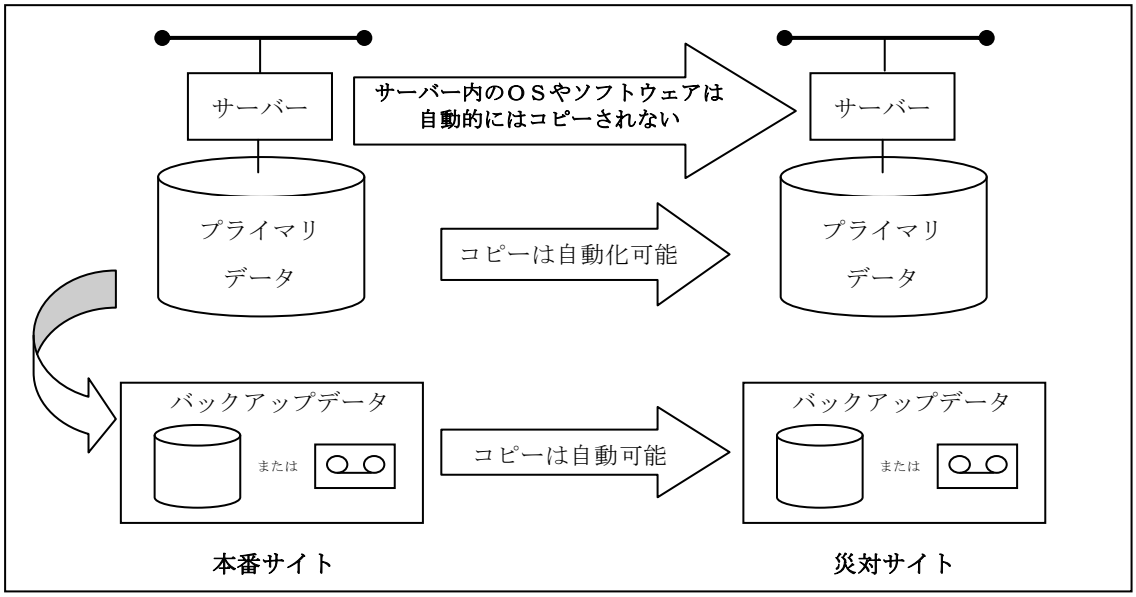

図 4.1 自動化コピーが可能なデータと、できないサーバー内のＯＳやソフトウェア

本番サイトのサーバーに、ＯＳやソフトウェアのＰＴＦ（Program Temporary Fix）を適用した場合、自動的には災対サイドのサーバーには適用されない。つまり、本番サイトのサーバーに変更を実施した場合は、即時に災対サイトにも適用する必要がある。万が一、本番サイトと災対サイトに差異がある状態で、災害が発生した場合は、災対サイトへの切替えができなくなる可能性が高くなる。これを防ぐためには、従来の本番サイトにおける運用の作業項目に、災対サイトへの適用作業を追加しておくのが望ましい。なお、適用もれを防ぐためにも、本番サイトに適用する前に、災対サイトから適用する方法がある。これにより、作業の手順やシステムの影響を、ふだん待機中の災対サイトを使用して事前に確認できる。

よって、災対サイトへの適用もれを防ぐだけでなく、本番サイトで稼働中のシステムに対する、変更作業によるリスクを軽減する効果が期待できる。[3)]

4.2 予行演習

万が一災害が発生して、本番サイトから災害サイトに切替えが必要となった場合、スムースに切り替わるかどうかを定期的に確認しておく必要がある。これは、本番及び災対の両サイトにおける日々の運用での、ＯＳやソフトウェアのＰＴＦの適用、更にデータ増加などにより、システム構築前の切替えテストでは確認できないことがある。できれば、年に１回の予行演習を実施するルールを策定していただきたい。もし、本番サイトのシステム稼働の重要度から、どうしても定期的な予行演習が難しい場合は、次節で述べる手順書の見直しだけでも定期的に実施することを推奨する。

4.3 手順書の見直し

災害対策システム構築中に作成した、本番サイトから災害サイトへの切替えに関する手順書は、常に内容を確認し見直す必要がある。これは、切替え作業は日常業務ではないため、担当者のスキルを維持できないためである。更に、本番及び災対の両サイトのシステム変更内容を反映した手順に更新することも必要である。そして、運用担当者が配置換えになった場合も、新しい担当者が操作できる内容かどうかも確認が必要である。見直しや整備を怠った手順書では、せっかくの災対サイトの価値が発揮できなくなることもあるので、常に留意していただきたい。

5. まとめ

本稿では、災害対策システムの中で中心的な構成のひとつである、ストレージシステムの選択のポイントを、データのコピーの方法を中心に紹介した。これらは、すべて筆者がいままで携わってきたシステム構築のプロジェクトで経験してきた実績のある方法であり、決してストレージベンダーがプロモーションする最新技術ではない。つまり、現在でもすぐに適用できるものが現実解といえる。一方、災害対策システムは、サーバー、ストレージ、ネットワークなどのシステム構成だけで成り立っているわけではなく、以下のとおりの数式で成り立つと筆者は考える。

災害対策システム＝明確な目標×正しいシステム構成×災対サイトの維持

明確な目標とは、２章で紹介したＲＴＯ／ＲＰＯをはじめとする時間や日数の数字で示した、会社の経営の立場で合意がとれたものである。決して後から簡単に変更できるものではない。特に、システム構成が決まってからこの目標を見直すことがあるが、このような場合は必ずといっていいほどシステムが成立しないように見受けられる。

更に、４章で紹介した災対サイトを維持する仕組みも重要である。災対サイトの運用・維持を後回しにして、予算を組まなかったため、システムが成立しないこともありうる。

なお、この数式は掛け算であるため、どれかひとつでも「ゼロ」になってしまえば、システムの価値は「ゼロ」になってしまうことを付け加えておく。

最後に、本稿で紹介したことが災害対策システムに携わる担当者だけでなく、システムにかかわるすべての方々に賛同いただき、システムの品質向上に少しでも寄与できれば幸いである。

参考文献

1. 佐野泰之、第 47 回 IBM ユーザー・シンポジウム論文／「災害対策システムの５つの落とし穴」、2009 年 5 月発行、5 ページ
2. 佐野泰之、第 47 回 IBM ユーザー・シンポジウム論文／「災害対策システムの５つの落とし穴」、2009 年 5 月発行、5 ページ
3. 佐野泰之、第 47 回 IBM ユーザー・シンポジウム論文／「災害対策システムの５つの落とし穴」、2009 年 5 月発行、8 ページ