6H-7

ディザスタリカバリにおける運用設計の簡略化に向けた検討

丸山 直子†, 古橋 亮慈‡, 田口 雄一†, 山本 政行†, 兼田 泰典†
†(株)日立製作所システム開発研究所 ‡(株)日立製作所SANソリューション事業部

1. はじめに

近年, 多発するテロや自然災害の脅威を背景に, 情報システムの災害対策であるディザスタリカバリの重要性が高まっている[1]. ディザスタリカバリは, 企業の重要なデータ資産を, 距離を隔てた二つ以上の拠点に保管し, 一つの拠点が損害を受けた場合にも, もう一方の拠点において業務を再開可能とする方法である.

ディザスタリカバリには, 許容される業務停止時間, 要求されるデータ復元時点, システム導入コストなどに応じて様々な実施形態がある. 例えば, データを記録した光ディスクや磁気テープ等の可搬メディアを遠隔地に輸送する形態や, クラスタソフトウェアやストレージ装置のデータ転送(リモートコピー)機能を用いて, ネットワーク経由でデータを遠隔地に転送する形態がある.

ストレージのリモートコピー機能を用いると, ホストの性能に影響を与えることなく, 高速にデータを遠隔地へ転送することができる. そのため, このようなストレージシステムを用いてディザスタリカバリを実施する企業が増加している.

2. 本研究の課題と目的

2.1. 本研究の対象システム構成

リモートコピーを用いたストレージシステム(以降, リモートコピーシステム)を導入する際には, リモートコピーに関わるシステム構成設計及び運用設計が必要となる.

システム構成設計では, 図1に示すようなリモートコピーシステムを設計する. リモートコピーシステムは, 通常の業務拠点である正サイトと, 正サイトから距離を隔てた場所に用意した副サイトから構成される. また, 各サイトは, それぞれストレージ, 業務サーバ, ネットワークなどから構成され, サイト間はリモートコピー用回線により接続される.

また, 運用設計では, 災害・障害発生時の切替え処理を設計する. リモートコピーシステムでは, 正サイトにおいて重大な障害や災害が発生すると, リモートコピー制御を伴う切替え処理を実施することにより, 副サイトに業務拠点を切替え(正⇒副切替え), 業務を継続する. また, 正サイトが復旧したときには, 業務拠点を副サイトから正サイトに戻すよう切替える(副⇒正切替え).

Study for Simplification of Disaster Recovery System Operation Planning
Naoko Maruyama†, Ryoji Furuhashi‡, Yuichi Taguchi†, Masayuki Yamamoto†, Yasunori Kaneda†
†Systems Development Laboratory, HITACHI, Ltd
‡Storage Area Network Systems Solution Division, HITACHI, Ltd

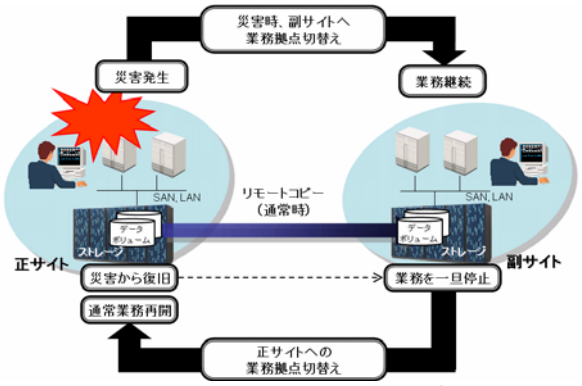

図 1 リモートコピーシステムの概要

2.2.本研究の課題

リモートコピーシステムの切替え処理では, アプリケーション操作やリモートコピー操作等, 幾つもの操作を実施しなければならない. 切替え処理時間を短縮するには, これらの手順を事前に設計しておく必要がある. 切替え処理手順の設計においては, (a) 想定すべき障害部位や障害の発生の起こり方(障害イベント)と, (b)障害イベントが発生した場合に必要な切替え処理手順の二つの観点から設計を行う必要がある.

(a) 想定すべき障害イベントの検討では, 対象システムの運用中に発生し得る障害イベントを網羅する必要がある. 本検討では, 機器や業務への影響など, 様々な観点から洗い出しが必要である.

また, (b) 障害イベントが発生した場合に必要な切替え処理手順の設計では, リモートコピー機能に対する操作, ファイルシステムに対する操作, バックアップ機能に対する操作など, 様々な操作の組み合わせと順序を設計する必要があるため, 設計者の高度な専門技術が要求される.

このように, リモートコピーシステムの切替え処理手順設計は複雑であり, 設計者の負担となっている.

2.3. 本研究の目的

本研究では, リモートコピーシステムの切替え処理手順の事前設計を簡略化し, 運用設計の負担を軽減する方法を提案する.

3. 運用設計の簡略化に向けた検討

3.1. 運用設計の共通化

リモートコピーシステムの切替え処理手順設計の簡略化に向け, 以下に示す方針に基づき, 検討を行った。

SAN: Storage Area Network
LAN:Local Area Network
RC: Remote Copy

(1) リモートコピーシステムにおいて発生し得る障害イベントを集約する
(2) 集約した障害イベントに対する対策方針を検討し，対策時の処理手順を共通化する

まず，(1)では，図1に示したリモートコピーシステムにおいて発生し得る障害イベントを洗い出す．これらを，復旧処理にリモートコピー制御を伴うものについて整理すると，これらの障害は表 1に太枠で示す 5 つの部位の障害イベントとして集約することができる．このように，多数の障害イベントを集約することで，対策方針である切り替え処理手順の設計が簡略化される．

次に，(2)では，障害発生時の正サイトから副サイトへの切換え処理手順及び，正サイト復旧後の副サイトから正サイトへの切換え処理手順を設計する．

これらの切替え処理手順は，データの損害状況によって異なる．データ損害状況とは，各々のイベントが発生した時のデータの利用可否である．損害状況には，以下に示す3つの種類がある．

① データ損害が有り，正サイトで業務継続不可能
② データ損害は無く，正サイトで業務継続不可能
③ データ損害は無く，正サイトで業務継続可能

例えば，正サイト被災の場合，正サイトでデータ損害が発生し，正サイトでの業務継続も不可能であるため，①となる．一方，リモートコピー回線の障害では，データそのものに損害は無く，正サイトにおいて業務継続は可能であるため，③となる．

切替え処理手順を，データの損害状況の観点から分類すると，表 1に示すように，5 種類の切換え処理手順(A～D)を設計すればよいことがわかる．

表 1:切替え処理手順の分類

#	障害イベント	正⇒副 切替え処理	副⇒正 切替え処理	
1	業務サーバ障害	切替え処理 A	切替え処理 C	
2	RC 回線障害	ー(*)	不要	
3	RC バッファ溢れ	ー(*)	不要	
4	データボリューム障害	切替え処理 B	切替え処理 D	切替え処理 E
5	サイト被災			

(*)切替え処理は無いが，サイト内での回復処理が発生する．

ただし，表 1の#4, 5 においては，正サイト復旧後に，データ損害が無かった場合のことを想定し，2通りの切換え処理手順(D及びE)を用意しておく必要がある．

このように，想定イベントを整理し，それに対応する切替え処理手順を事前に共通化することで，切替え処理手順の設計作業を簡略化することができる．

3.2. 共通化後の切替え処理手順の例

正サイトの災害復旧を例に切替え処理手順を解説する．正サイトが災害から復旧すると，副サイトから正サイトに業務拠点を切替える処理(表 1の切替え処理D又はE)を行う．

切替え処理D及びEは，正サイトにおけるデータの損害状況により選択する必要がある．切替え処理D(表 2)は「災害により正サイトのデータが利用不可」である場合，切替え処理E(表 3)は「正サイトのデータが利用可能」である場合の手順である．

表 2:正サイト復旧後の切替え処理 D

順序	処理内容
1	副サイトにてサービスを停止
2	副サイトのアプリケーションを停止
3	副サイトのデータボリュームをアンマウント
4	リモートコピーのペア関係を一旦解除
5	副サイトから正サイトへリモートコピーを開始(全データのコピー)
6	コピー終了後，コピー方向を反転
7	正サイトのデータボリュームをマウント
8	正サイトのアプリケーションを開始
9	正サイトにてサービスを開始

表 3:正サイト復旧後の切替え処理 E

順序	処理内容
1	副サイトにてサービスを停止
2	副サイトのアプリケーションを停止
3	副サイトのデータボリュームをアンマウント
4	副サイトから正サイトへリモートコピーを再開(差分データのみコピー)
5	コピー終了後，コピー方向を反転
6	正サイトのデータボリュームをマウント
7	正サイトのアプリケーションを開始
8	正サイトにてサービスを開始

3.3.運用設計の簡略化による効果

本研究において検討した切替え処理手順を実際の運用設計に適用した結果，運用設計に費やす作業時間を低減した．

4. まとめ

本報告では，ディザスタリカバリを目的としたリモートコピーシステムの切替え処理手順設計の一部を共通化することにより，運用設計作業を簡略化する設計技術を提案した．また，本検討結果を実際の運用設計に適用し，設計効率向上に貢献した．

参考文献

[1] Rudolph, C.G, "Business continuation planning/disaster recovery", Communications Magazine, IEEE, Volume 28, Issue 6,PP.25-28, June 1990