5D-6

高信頼ディザスタリカバリシステムの研究

丸山哲也† 山本康友† 荒川敬史† 二瀬健太† 川村俊二† 岩村卓成†

(株)日立製作所システム開発研究所†

1.はじめに

業務サイト(正サイト)のデータを遠隔地にバックアップすることで、テロや天災等によるシステム障害が発生しても業務復旧が可能となるディザスタリカバリシステム(DR システム)が注目されている。

金融機関等では、大規模災害にも速やかに対応するために、遠隔地にバックアップサイト(副サイト)を構築することが要求される[1]。一方で、副サイトの記憶領域(ボリューム)にバックアップされてないデータがある場合、そのデータを回復する作業が必要となり、業務復旧に要する時間が長くなる。また、データの回復が不可能な場合、多大な損害が発生する。そのため、副サイトに最新のデータを確保することが要求される。

前述の２要求を満たす方法として、３サイト DR システムがある。

本稿では、３サイト DR システムの従来方式の課題を解決する新方式を検討し、業務復旧時間の比較検証を行う。

2.目的と課題

2.1.目的

DR システムを構築する目的は、業務サイトに障害が発生した場合に、業務を短時間で復旧することである。

正サイトと同様の機能を持った副サイトを用いた２サイト DR システムの実現方法として、ネットワーク経由で副サイトへデータを転送(リモートコピー)し、正サイトに障害が発生した場合、副サイトのデータを用いて業務を復旧するものがある。

リモートコピーには、同期コピーと非同期コピーがあり、それぞれに長所・短所を持つ。同期コピーは、正サイトがホストから更新要求を受けると同時に副サイトへ更新を転送し、副サイトから更新完了の応答を受け取った後にホストへ更新完了の応答を返すことで、正サイトと副サイトのボリューム内のデータが同一である事を保証する。反面、更新完了の応答時間がサイト間の距離に依存するため、遠距離では正サイト業務の性能に悪影響を及ぼす可能性がある。

一方、非同期コピーは、正サイトがホストからの更新要求を受けると、ホストへ更新完了の応答を返した後に、副サイトへ更新を転送するため、遠距離のデータ転送でも正サイト業務の性能への影響が少ない。反面、正サイトで障害が発生した場合に、副サイトへ未到達なデータが失われる可能性がある。

なお、非同期コピーでは性能向上のため、データ転送を多重で行う。そのため、副サイトのボリュームにデータが届く順序は保証されず、データに不整合が生じる可能性がある。これを防ぐため、転送データに番号を付与する方法などで副サイトでの更新順序を保証し、データの整合性を確保する。

A study of High-Reliability Disaster Recovery System

Tetsuya Manryama†, Yasutomo Yamamoto†, Hiroshi Arakawa†, Kenta Ninose†, Shunji Kawamura†, Takashige Iwamura†,

†Hitachi, Ltd., System Development Laboratory

前述のように、同期または非同期コピーを用いた２サイト DR システムでは、正サイト業務の性能に影響を与えることなく、遠距離にある副サイトに最新のデータを確保することが出来ない。

2.2.３サイトＤＲシステム(従来方式)

２サイト DR システムが抱える問題を解決するシステムとして、正サイトの近距離に中間サイトを配し、同期コピーと非同期コピーを組み合わせてデータ転送する３サイト DR システムがある。

従来方式は、正サイトから同期コピーで中間サイトへデータを転送し、そのデータを静止化して順次副サイトへ非同期コピーにより転送することで、副サイトへの整合性を確保したデータ複製を実現する。データ静止化のために、中間サイト内でデータ複製機能(ローカルコピー)を用いる(図１参照)。

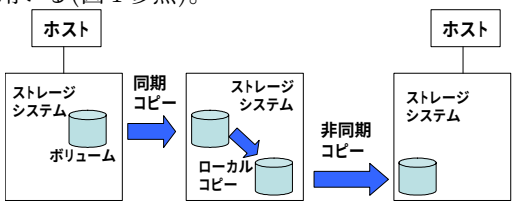

図１　３サイトＤＲシステム(従来方式)

正サイトに障害が発生した場合、中間サイトにある障害発生直前までの最新データを副サイトへ転送した後に、副サイトで業務を復旧する。

2.3.３サイトＤＲシステム(従来方式)の課題

従来方式は、静止化された複製データを更新し、副サイトへ転送するために、ローカルコピーと非同期コピーの休止・再開を以下の転送サイクルで繰り返す。

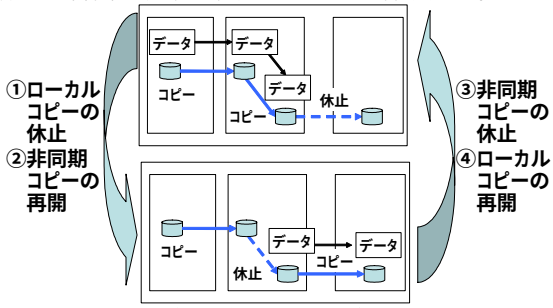

図２　従来方式での転送サイクル

ローカルコピー、非同期コピーが休止している間、各々のコピー元ボリュームで更新されたデータは、ストレージシステム内に差分データとして保管され、コピー再開後に転送される。そのため、コピーの再開後のデータ転送には、差分データ量に比例した時間が必要となる。

また、ホストからの更新要求量が単位時間当たり一定とすれば、差分データ量はコピーの休止時間に比例する。

正サイトに障害が発生した場合には、ローカルコピーと非同期コピー双方の差分データを副サイトに転送するため、更新量が多い場合、業務復旧に要する時間が長く

なる。

3.新方式の提案

新方式は、中間サイトのローカルコピーを用いず、中間サイトへ同期コピーで転送されたデータを直接非同期コピーで副サイトへ転送する(図3参照)。

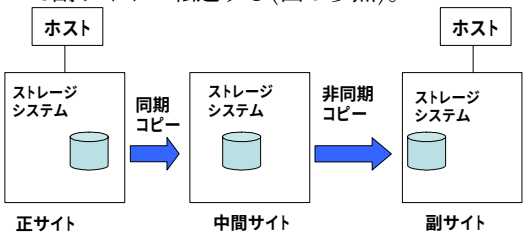

図 3　3サイトDRシステム(新方式)

新方式を実現するために、ホストからの更新要求形式(更新プロトコル)と同期コピーの転送要求形式(転送プロトコル)の差異を吸収して非同期コピーの処理を実行する機能を追加した。

転送プロトコルはオーバーヘッド削減のため、更新プロトコルとは異なる転送形式を使用している。これに対し、同期コピーの受信処理で、転送データのボリューム上のアドレスやデータ長といった情報を抽出し、更新プロトコルと同形式にすることで、非同期コピーでの転送を可能にした。

新方式では、正サイトがホストからの更新要求を受けると、中間サイトに同期コピーでデータを転送する。中間サイトは、前述した機能を追加した非同期コピーで、副サイトにデータを転送する。副サイトでは、非同期コピーの更新順序に従って、ボリュームを更新することで、整合性を確保する。

正サイトに障害が発生した場合、非同期コピーの未到達データを待って、副サイトで業務復旧を行う。

4.比較検証

従来および新方式の業務復旧手順を元に業務復旧時間を求め、比較検証を行う。

4.1.業務復旧手順

従来方式および新方式での業務復旧手順について示す。ここで言う業務復旧とは、正サイトに障害が発生した時点から、正サイトの障害直前のデータを副サイトに転送するまでとした。

従来方式では、転送サイクルのタイミングによって業務復旧手順が変化する。本稿では、最も手順が多く、復旧時間が長くなる、非同期コピーを再開した直後からの復旧手順を以下に示す。

1. 正サイトでの障害を確認する。
2. 中間サイトへの同期コピーを停止する。
3. 非同期コピーの再開後、データ転送完了を待ち、非同期コピーを休止する。
4. ローカルコピーを再開し、最新のデータが転送された後に、ローカルコピーを停止する。
5. 非同期コピーを再開し、最新のデータが転送された後に、非同期コピーを停止する。

一方、新方式の復旧手順は、従来方式で発生したコピーの休止・再開が不要となる。そのため、転送サイクルが発生せず、手順が変化しなくなり、復旧手順が簡略化される。新方式での復旧手順を以下に示す。

1. 正サイトでの障害を確認する。
2. 中間サイトへの同期コピーを停止する。
3. 非同期コピーの未到達データの到達を待ち、非同期コピーを停止する。

4.2.業務復旧時間算出方法

従来方式での業務復旧時間は、非同期コピーの再開後の差分データの転送完了を待つ時間と、ローカルコピーと非同期コピーでの最新データ転送に必要な時間の総和となる。ホストからの更新要求量が十分大きい場合、差分データ量はサイト内の全ボリュームのデータ量と等しくなる。そのため、差分データおよび最新データ転送に必要な時間は、それぞれ全ボリュームのデータ転送時間に等しくなり、業務復旧時間は以下の式で表される。

$$T = 2V/Bw + V/Cp \qquad (1)$$

表 2．パラメータ定義

パラメータ	内容
T	業務復旧時間
V	全ボリュームの容量
Bw	ネットワーク帯域
Cp	ローカルコピー速度

一方、新方式では、コピーの休止・再開を行わないため、コピー休止で発生した差分データの再転送は発生しない。そのため、非同期コピーの未到達データの到達を待つ時間だけとなり、数分程度となる。

4.3.比較検証

従来方式と新方式との業務復旧時間の比較を行う。比較において、以下のパラメータを持つ DR システムを想定した。

表3.パラメータ表

#	パラメータ名	値(単位)
1	ボリューム容量(V)	1(TB)
2	ネットワーク帯域	100(MB/s)
3	ローカルコピー速度	350(MB/s)

この条件で復旧時間を算出すると以下の結果を得た。

表 4.従来方式と新方式の比較

方式	従来方式	新方式
時間	6.3 時間	数分

5.おわりに

本稿では，業務サイトのホスト性能への影響を抑えて、遠隔地へ最新のデータをコピーする方式として、正サイトの近距離に配した中間サイトを経由してデータを転送する3サイトディザスタリカバリシステムを検討し、中間サイトでローカルコピーを行う従来方式と、直接転送を行う新方式について、業務復旧時間の比較を行った。新方式では、従来方式で必要であったコピーの休止・再開が不要となり、業務復旧時間が短縮された。

今後も、耐障害性が高く、運用や管理が容易といった要求を満たす DR システムの検討を行っていく。

参考文献

[1] Security and Exchange Commition, “Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System”、2002/2,