社団法人 情報処理学会　研究報告
IPSJ SIG Technical Report

2004－EVA－11　(1)
2004／11／4

災害対策システムのリニューアルにおける現実的災害対策レベルの評価

加倉井 宏一*　荻田 光一郎*

データを有事の際に影響のない範囲の遠隔地にコピーして保存をする災害対策システムをリカバリーポイントの短縮とリカバリー目標時間の短縮を目標に回線のＴＣＰ／ＩＰ化とディスク装置の遠隔コピー機能を利用して再構築を行った．対策時間の短縮やサービスレベルの向上についての評価を行う．

ディスク装置の高速コピー機能や，高速回線を利用したＴＣＰ／ＩＰファイル転送機能により，災害時のデータ回復点時刻を大幅に改善することが可能になった．

The evaluation of disaster recovery level on a renewal project

Hirokazu Kakurai*　Kohichiro Ogita*

This paper describes that a renewal project shorten recovery point objective and recovery time objective of a disaster recovery system. The system uses a disk remote copy function and high-speed wide aria TCP/IP ftp. It able to improve recover point objective. I compare the disaster recovery system which was designed ten years ago and the system which is renewed in 2004.

１．はじめに

保険業や銀行業の様に社会的に影響度の高いシステムであればあるほど，災害による長期的なコンピュータ・システムの停止が一般消費者にも直接に大きな影響を及ぼす. 単に長期間の停止だけであれば, 問題はまだ軽い. もし，災害によって契約内容や預金残高等のデータのほとんどが失われてしまったとすれば，これは大きな社会問題と発展するのは必至である．

災害に対応したシステムの設計には，サイト計画に始まり，復旧メカニズムの選定，システム形態の設計，準備資源量設計，復旧時間の予測，整合性の維持方法，等など，実に沢山の項目が存在する．

そして，災害対策システムの構築上忘れてはならない重要な項目として，バッチ処理の取扱いが挙げられる．しかし，これは通常，扱いの難しい内容であることが多い．オンライン時間帯の被災にはバックアップ・センターでのデータベースのトラッキングにてデータのロストを最小限にすることが可能となるが，バッチ時間帯での被災では処理のリラン／リスタートのタイミングをどう選ぶか，所要入力データのバックアップ・センター側での確保をどうするかと言った課題に必ず突き当たる．

バッチ処理時間帯といえども，ＤＢ関連の処理が全てトランザクション形態で処理されていれば単純にＤＢのトラッキングにより被災時にもセンターを切り替えた時点でのバッチ処理のリスタートポイントを認識し，リスタート出来るようシステムを造っておくことは可能である．しかしながら，入出力を多用した規模が大きい従来の稼働中のシステムを，おいそれとそのようなシステムに作り替えることは簡単に出来ない．

バッチ処理の災害対策を難しくしている要因は主に次のような理由によるものである．

① バッチ処理の入力・出力が順次ファイルであるものが大量に存在する
② バッチ処理の実行環境が日々変わる可能性が大きい(ジョブ・ネットワーク／ＪＣＬ／パラメータ／所要スペース等)
③ バッチ処理中の障害回復方法は通常リスタートではなく，リランである

従って，多くの場合，最小限の変更で災害対策システムとしてこのような環境で有効な仕組みをデザインする必要が出てくる．こうした仕組みの検討は次のような項目に関して行われる．

① バッチ処理の規模を絞るか否か
② バッチジョブ・ネットワーク中でリスタート可能にするか否か
③ ＤＢのアンロード・リロードのオフライン処理の最少化

バッチ処理の災害対策の検討に当たってまず以下のような制約を満足させることも重要なポイントである．

*日本アイ・ビー・エム・システムズ・エンジニアリング(株)
*IBM Japan Systems Engineering Co., Ltd.

① 被災後，バックアップ・センター側でのバッチ処理のリラン／リスタートの影響がオンライン・サービスの再開可能目標時間内であること
② 次業務日開始時間迄に最低限の所要バッチ処理が完了すること

本論文では，損害保険会社様の事例を元に，１０年ほど前に作成されて災害対策システムが，２００４年となった今に改修を行い，どのようにサービスレベルを向上させ，対策時間の短縮を図ったのか，評価するものである．

２．ある損害保険会社様での災害対策の方式

事例として取り上げるお客様は損害保険業を営まれている．その取り扱うデータの重要性から，災害対策に対しては，かなり前から取り組まれていた．

１０年前の１９９４年に本格的な災害対策システムを構築される事となった以前から，データの定期的なテープへの吸い上げと，地方への退避という作業を行われていた．これは，災害時に契約情報等が喪失しないように，データの保全を目的とした災害対策であり，災害時にコンピューターセンターが稼動不能となった場合のサービスの再開といった部分には注意が払われていなかった．

一方，東京側データセンターの業務が実施できないほどの災禍に見舞われたような時は，損害保険会社というビジネスの性格上，その災害自体に起因する業務処理が発生し，社会的責任として業務を遂行していかなければならないという要請がある．そのため，罹災後，短時間のうちに業務を再開しえるシステムを整えるべく，１０年程前に東京ー大阪間の災害対策システムを構築されたのである．

業務として，オンラインが最重要業務であるが，保険アプリケーションの一般的性格としてバッチ処理に多くの資源を費やしている．昼間のオンライン処理に加え夜間のバッチ処理という処理特性であるため，災害対策の重要な項目としてバッチ処理の扱いが挙げられている．

３．１９９４年度での災害対策システムの仕様

１９９４年8月より要件定義を行い１９９６年1月にサービスインした災害対策システムは，広域災害が発生した場合に，災害の影響のない場所で，それまでの処理を継続することの目的を持ったシステムである．通常，処理を継続するためには，処理のためのプログラムとデータをそろえる必要がある．災害の影響を受けない場所にそれらを移動することが災害対策システムの内の「平時システム」と呼ばれる部分の目的となる．災害の影響範囲をどのように想定するかで平時システムの実現方法が大きく変化する．例えば東京にセンターがあってその代替センターが川崎であるように，災害の影響を受けない場所へのデータおよびプログラムの移動に時間がかからないと想定した場合，データは発送直後に到着し，時間差なくシステムの復元に着手できると想定できる．しかし，代替センターを近畿地方や九州地方に置かなければならないと想定すると，プログラムとデータの移動に１日程度の時間差が発生することが想定される．

送付されるプログラムやデータは，常に変化があり，一定であることはない．データは，日中のオンラインや夜間のバッチ処理で更新されるし，プログラムは新規機能追加やエラー修正で内容が更新されていく．このように連続して変化していくプログラムとデータを他の場所に移動し，処理を継続するためには，いくつかの要件を設定する必要がある．すなわち，次のような3つの要件を災害対策要件として，システムの要件定義を行う前に設定された．

① 再開対象業務：オンライン業務
② 再開状態：災害発生前日の朝の状態
③ 再開猶予期間：災害発生より２日間以内

他，設計で考慮されたシステム上の制約とその影響は次の通りとなる．

１）オンラインＤＢの総量が多い

オンラインＤＢをイメージコピーの形式で送付すると想定すると，テープ８００本以上を毎日送付しなければならなくなり，当時の運用ではデータの送付ができなかった．このために夜間のＤＢバッチも含めて，ログを集約し，送付量を削減した．

２）災害発生後に稼働するシステムは大阪のセンターを使用する

伝送で送付されるデータは，即時に大阪に到着する．しかし，量が多いために伝送の対象とできないデータはテープ上に作成し，トラック便で陸送する．このために，発送から到着までに１日の時間のずれが発生する．

３）東京側と大阪側の運用スケジュールが異なる

東京側は，２４時間の稼動と，土曜日にも通常の運用を行っている．大阪側は，朝９時から夜２４時までの稼動であり，土曜日にはシステムは停止する．このために土曜日の伝送および陸送分の受領，データの復元は行われない．従って，各週の月曜日には東京側が２日分の処理を行い，火曜日には大阪側で２日分の処理を行う．

このように設計された災害対策システムの平時運用は以下のように行われる．

1）東京側
①オンラインとバッチより出力されるＤＢログを集約して陸送する.
②プログラムの変更分を抽出して変更差分として伝送する.
③毎月一回,決められた日にバックアップをテープに作成し陸送する.

2）大阪側
①伝送分を受信する.
②陸送分を受領する.
③ある日の朝の状態を復元するための全データがそろったところで復元する.
④不要となったテープを東京に返却する.

３.１.　復元管理データベース

大阪側でプログラムとデータを復元するためには，ある日の朝の状態に必要なプログラムとデータがすべてそろっていなければならない．復元の対象となるプログラムやデータの作成に支障がなく，送付での時間の遅れもなく，また送付中の障害もなければ，大阪側では受領したものを全て復元の対象として取り扱うができる．しかし，常にこのような前提をおくことは災害対策システム要件を満たせない．データやプログラムに何らかの欠落が発生した場合，業務としての不整合が内在することになるからである．これを解決するために，大阪側でその日に復元すべきデータがどのような状況になっているかを監視できる情報を提供する必要があり，これを「復元管理データベース」と呼ぶデータベースで管理した.

大阪側で復元開始直前に復元対象のプログラムとデータが全て到着していることを照会できるようにするために，到着までの以下のような情報を蓄積する.

- 作成情報:送付対象のデータが送付用に作成されたことをあらわす.
- 発送情報:送付対象のデータが発送されたことをあらわす.
- 到着情報:送付対象のデータが到着したことをあらわす.
- 復元情報:送付対象のデータが復元されたことをあらわす.

上述の情報の組み合わせで次のような送付データの状態を表すことができる.

1）作成情報が完成されていない状態
送付予定のプログラムやデータが未だ作成されていないことを表す．この場合には，作成し送付するか，作成をあきらめ，別の方法で回復する.

2）作成情報は完成されているが発送情報が完成されていない
未発送の状態を表す．陸送で他のデータが発送済みであるにもかかわらずこの状態である場合には，テープの紛失が予想できる.

3）発送情報までは完成されたが到着情報が完成されていない
未到着の状態を表す．陸送分では運送業者での問題発生が予想される.

4）復元情報が完了されている
該当データセットの復元が完了していることを表し,関連するテープがある場合には，それを返却対象とする事を表す.

３.２.　東京側処理

オンラインの静止点を朝９時に取り，そこからＤＢログの集約を始める．ログの集約が済み，集約ログを一旦テープにバックアップした後，トラックでの陸送の開始を行う．トラックによる陸送の東京出発が夜２１時頃となる.

ＤＢログの集約と同時に，ＤＢ以外のファイルで災害時必要となるデータ・プログラムは７６８ｋｂｐｓの回線を利用したＳＮＡファイル転送で伝送を行う．この伝送は，その日の１５時頃に終了する.

３.３.　大阪側処理

陸送となったテープは翌朝９時に到着する．そこからテープのバックアップを取得した後，１５時に復元判定を行う.

復元判定は，大阪側に伝送経由や陸送経由で到着したデータに漏れがないことを確認して，ある期日の状態のデータ（通常は前日の朝９時の状態）を大阪側の災害対策システムに復元開始を指示する処理である．この後の復元処理を経ると，大阪側で災害対策対象の業務データを使用することができる状態となる.

これら東京側の処理および大阪側の処理を図示すると,図1，図2となる.

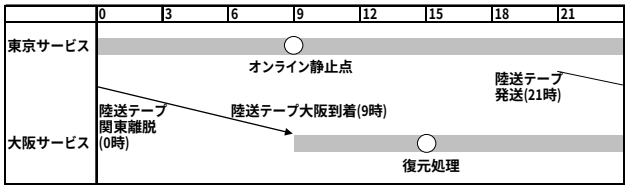

図１　１９９４年災害対策サービス

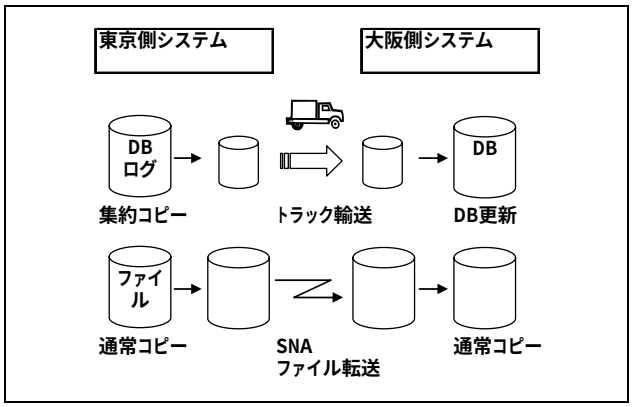

図2 １９９４年災害対策システム

４．２００４年度での災害対策の変更

２００４年になり，オンラインプログラムのバージョンアップの必要性により，お客様でＤＢの運用変更が計画された．１９９４年時の災害対策システムは当初よりＤＢのデータ維持を主眼として設計されていたため，この運用変更に伴い，大幅な改修を行う必要が出てきた．具体的には，機能上の制限により，ＤＢログ集約の機能が利用不能となり，何らかの代替手段を講じる必要が発生した．また，災害への対応の重要性が改めて認識される中，災害対策対象とすべきデータの範囲拡大や災害対策対象となっていないデータの復旧に対する要求を満たす必要が出てきた．

以下に，２００４年度の災害対策システムの改修の目的を分類する．

１）オンラインバージョンアップに対応するためのＤＢ関連送付方法の改修

災害対策対象のＤＢは，総量で約１ＴＢである．しかし，東京－大阪間の回線容量の制約によりその内容をすべて毎日大阪側に送付することはできない．このため，東京側での災害対策対象ＤＢの更新処理では，更新ログを取得し，そのログを圧縮して大阪側に送付することで，回線容量の制約を回避している．大阪側では，受け取ったログを使用してＤＢ回復機能を流用することで，特定の日時の状態を維持している．

オンラインプログラムのバージョンアップに伴い，東京側でのログの圧縮（ログ集約）が事実上不可能になるため，ＤＢの更新差分のみを大阪側に送付し，回線の効率的使用を行うことができなくなる．

２００４年の改修では，ＤＢの変更差分送付をログによらず，ディスク装置のハードウェア機能で実現することとなった．

２）災害対策対象外データの災害復旧後の回復支援機能追加

１９９４年の災害対策システムでは，災害対策対象のデータを大阪側で利用可能にするだけではなく，大阪側での更新処理の結果を東京側復旧時にそのまま継続使用できるように，「戻し」機能を提供している．

しかし，災害対策対象以外のデータは，災害時に東京側に置き去りにされるため，災害復旧時に災害対策対象データとの間で整合性の合わないものがでてくる．また，東京側の被災状況によっては，災害対象データ以外は東京側の設備が復旧しても，回復できない可能性もある．

このため，２００４年の改修の目的は，災害対策対象外のデータを大阪側で保管し，災害復旧時に災害対策対象データと整合性を持って回復できるようにするものである．

３）災害復旧のための東京側でのデータ復旧支援の充実

１９９４年の災害対策システムの「戻し」機能では，大阪側で更新された災害対策対象データを災害復旧後に東京側で回復できるように設計されている．しかし，設計当初の伝送経路等の設備の制約から復旧の作業を伝送ではなく陸送を用いて行うようになっている．

２００４年の改修では，高速回線の導入，同期管理ディスクの利用等性能面での大幅な改善を前提とした新たな「戻し」機能と運用イメージを作成しなければならない．

４）遠隔ディスクコピー機能によるボリューム単位の送付

ボリューム上のデータセットをそのまま伝送し，大阪側ではそのまま使用することになる．これを「ボリューム送付」と呼んでいる．

いくつかのケースに分け，それぞれの送付対象をどの方式で送付するかを検討した．

①災害対策対象ＤＢ

災害対策対象ＤＢは，ボリューム送付対象とする．東京側でのバックアップ作業と大阪側での復元作業の負荷削減が図れる．ただし，送付もれ管理の対象とするためにデータセット単位の管理を必ず行う．

②ＤＢ以外のファイル

伝送対象とする．カタログの管理や送付対象の東京側での配置等，現行運用の変更負荷を最小限にする．ただし，伝送には１００Ｍｂｐｓの広域イーサーネット回線を利用したＴＣＰ／ＩＰファイル転送として転送の速度を速める．

③災害対策対象外ＤＢ／ファイルの送付

災害対策対象外ＤＢ／ファイルは，ボリューム送付対象とする．東京側でのバックアップ作業の負荷削減が図れる．送付もれ対応を行わないので，データセッ

ト単位の管理は行わない.

４.１.　東京側の処理

朝９時のオンライン静止点後，ＤＢのディスクをハードウェアの機能によって高速にコピーを行う．このハードウェアの機能は,ディスクの更新部分にフラグを持ち,コピー実行によって更新部分のみをコピーして高速化を図る機能である．また，制御装置内で完結した処理であり，制御装置のプロセッサー速度で処理を行うことができる.

高速コピーが終了した後，大阪側に対して遠隔コピーを実行する．この遠隔コピーも，やはり，ディスクの更新部分のみをコピーし，処理の高速化と通信データ量の削減を図っている.

遠隔コピーには，１００Ｍｂｐｓの広域イーサーネット回線を用い，１２時頃に伝送は完了する.

同時に,伝送処理をＴＣＰ／ＩＰファイル転送で行う.ファイル転送処理は遠隔コピーで利用する１００Ｍｂｐｓ広域イーサーネット回線に相乗りする.

４.２.　大阪側処理

伝送されたディスクを，高速コピー機能を用いて，災害対策ＤＢにコピーを行う．この高速コピー機能は東京側と同じく，ハードウェアの機能として実現されている機能である.

これら東京側の処理および大阪側の処理を図示すると,図3，図４となる

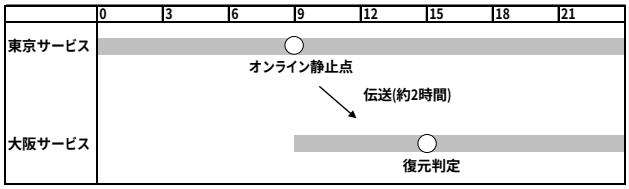

図3　２００４年災害対策サービス

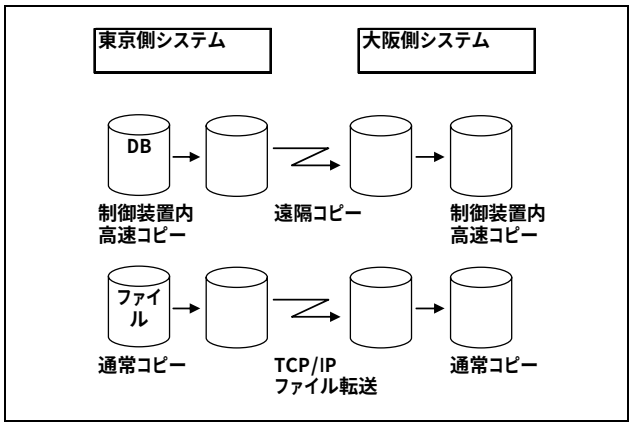

図４　２００４年災害対策システム

５．災害後業務再開時の運用

災害が発生した場合，大阪側システムでは朝の９時から業務を開始することとなっている．朝９時から夜２４時までのサービス時間と決まっており，災害時システムとして完結したつくりとなっている.

災害時の業務開始日の判断は次のように行われる．災害後システムの業務開始前処理が３時間程度でできることから，朝６時を分岐点として，当日の朝９時に業務再開を行うか,翌日の朝９時に業務再開を行うか決定する.すなわち，０時から６時までに災害が発生した場合は,当日の９時に業務を開始し,朝６時以降の災害の場合は,翌日の９時から業務を開始する.

ただし，１９９４年のシステムでは，なるべく最新データが必要な場合を考慮して，０時から６時までの災害であっても,翌日の９時からの業務再開の可能性もある.

６．新システムの評価

災害対策システムの評価の指標にＲＰＯ（Recovery Point Objective），ＲＴＯ（Recovery Time Objective）がある.

ＲＰＯは，災害発生後，どの時点のデータまで戻っての業務の再開が可能かを示す．つまり，この時間が短ければ短いほど，データの喪失が少ないといえる．この時間のデータの回復には，例えばデータの再入力等，アプリケーションでの対応や運用での対応が必要となる.

ＲＴＯは，災害発生後，どのくらいの所要時間で業務の再開が可能かを示す．この時間が短ければ短いほど,災害後の業務開始が早く，サービスが良いといえる.

この二つの指標を元に新旧の災害対策システムの仕様を比較検討する.

図５は，１９９４年のシステムでの災害発生時刻と,対応する業務再開時間，回復データの時間を図示したものである．災害時の運用によって２つの場合に分かれる（運用①と運用②).違いは０時から６時までに災害が発生した場合の対応である．運用①では，当日の朝９時からサービスを開始するが，運用②では，翌日の朝９時からサービスを開始する．それによって，回復されるデータの時刻が異なる．０時を過ぎたところで，災害対象データの陸送が関東圏を越えるため，関東全域の災害を考慮した場合，再開日を１日遅らせることで，最新の業務データを利用することができるのである．この決定は実際に被災した際にその時の状況に応じてお客様の運用責任者が決定することになっている.

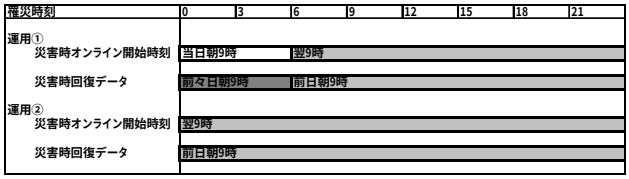

図5 1994 年の業務再開時刻と復旧データ

一方，２００４年システムでの災害発生時刻と，対応する業務再開時間，回復データの時間は図６の通りである．伝送を利用したリモートコピーが１２時で終了することから，１２時を過ぎれば当日朝９時の段階の業務データを大阪側システムのそろえることができる．

図6 2004 年の業務再開時刻と復旧データ

現行の災害対策システムは,陸送を使用しているため,データの到着までに２４時間待たなければならない．改修後では，有事稼動分の陸送は廃止されるためデータの到着までの時間が短縮される.一般的な再開要件である,「災害発生日の翌日」には変化はないが，災害発生を特定の時刻に設定した場合には，改修後の要件は陸送の影響を受けず，再開状態を改善することができる．

データの到着が早まることで,復元判定が一日早まる．具体的には，月曜日の朝の状態のデータは，月曜日の昼までに到着し，その日の復元判定の対象となる．これにより，災害発生日の朝の状態の復元が早期に行われ，現行災害対策システムに比べ改修後は再開日が一日早まる場合がある．

現行システムでは，伝送終了が１８時，陸送分の関東地方離脱が２４時となっているので，災害発生が２４時以降で翌朝陸送分が大阪側システムに到着した場合には,災害発生当日の朝の状態で再開が可能となる．改修後の想定される運用では，陸送はなく伝送の終了がボリューム送付分も含め１１時となっているので，当日１１時以降の災害発生では，当日中に災害発生日の朝の状態が復元可能となる．

ＲＰＯおよびＲＴＯを最悪の場合，最良の場合，それぞれにまとめると表１のようになる．

		旧システム	新システム
RPO	最悪	45時間 (運用①の6時)	27時間 (12時)
	最良	15時 (運用②の0時)	3時間 (12時)
RTO	最悪	33時間 (運用②の0時)	27時間 (6時)
	最良	3時間 (運用①の6時)	3時間 (6時)

表1 RPO と RTO のまとめ

ＲＴＯに関しては，特に運用①と比較すると大きな違いはないが,ＲＰＯに関しては大きな改善が見て取れる．

ＲＰＯが改善することは，それだけ災害に対するアプリケーション側や運用側の考慮を減らすことができることを示す．例えば，災害時のデータ喪失に対応する運用として,窓口でのトランザクション情報の保管があるが,契約内容の変更情報等を窓口で保存しておく日数というもの削減することができる．

ＲＴＯに関していえば,損害保険という業務の性格上,おそらく災害の発生した直後に，契約内容の照会や，保険金の払い戻し，災害発生地域外での通常業務というのが考えられ，そういった意味では，災害発生後即業務を開始しなくとも，翌日朝からの業務開始で機能的に問題ないと考える．

７．おわりに

２００４年の改修により、災害対策システムの仕組みにハードウェア機能によるディスク伝送が加わったが基本的な運用はすべて，１９９４年の災害対策システムが元となっており，オペレーター訓練も最小限で済み、サービスイン後の混乱もなかった点は成功といえる．

災害対策システムとして重要な要件であるデータの復元に関しても，既存の仕組みを最大限に活用することで運用コストを増加させることなく実現することが出来た.改修の対象となった業務は１００Ｍｂｐｓの通信回線による伝送で要件を満たすことが出来たが今後さらに多くのデータが災害対策の対象として追加された場合は通信回線の増強も考える必要が生じる．最近は広域ＬＡＮなどのテクノロジーにより大容量かつ長距離の通信のコストも下がってきているので次回の機能拡張の際には検討したい。

また，オープン系システムの災害対策として，この仕組みに追加したいという将来構想もある．そうなった場合は災害対策システムとしての価値は更に高まるために是非チャレンジしてみたい内容である．

８．参考文献

[1] 加藤礼基，遠隔コピー機能による災害対策システム構築に関する考察，情報処理学会，システム評価研究報告，No.6，2003

[2] Cathy Warrick，IBM TotalStorage Solutions for Disaster Recovery，IBM Redbook，http://www.ibm.com/redbooks，SG24-6547，2004

[3] Gregor Neaga，Continuous Availability S/390 Technology Guide，IBM Redbook，http://www.ibm.com/redbooks，SG24-2086，1998