基幹業務の実運用を考慮した
リカバリ方法の実践

三菱ガス化学 株式会社　新潟工場

■ 執筆者Ｐｒｏｆｉｌｅ ■

亀　谷　和　美

1965 年　三菱ガス化学(株)新潟工場入社
1987 年　システム業務担当
1994 年　大規模Ｃ／Ｓシステムの開発
現在　　管理部システム計画グループ長

■ 論文要旨 ■

弊社，新潟工場は 10 年前に，いち早くクライアントサーバシステムを導入した．同時に業務のあり方も著しい変革を求められ，電子承認やペーパーレス化を中心としたシステムの導入を行って来た．

従来，高速・大容量のハードウェアを利用する基幹業務は，絶対的な信頼性から汎用コンピュータで行われて来た．しかしそれらの業務システムも時代の流れとともに PC サーバーシステムに移行され，性能と経済性からその依存度は増加している．

一方，システム管理者は依存度が高くなる程，万が一システムデータが破損した場合「迅速な復旧が行えるか否か」という，一抹の不安要素を抱える．

当グループでは，DLT や RAID システムに頼っているフェールセーフを見直すことにより，実用的なバックアップとリカバリ方法の実践を行った．

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　当社概要

三菱ガス化学株式会社新潟工場では，24 時間体制でケミカル原料の製造を行っており，一日あたりの総生産量は約 80 種 400 トンに及ぶ．これらの製品出荷には約 150 台のトラック及びタンクローリーが稼動している．この出荷指示や計画を一手に行っているのが自社開発の受注システムである．これは製造と同様に弊社業務の基幹となっており，弊社が 24 時間体制で操業を行う要でもある．

１．２　提案背景

昨今のコンピュータ及びネットワークシステムへの業務依存度を考えると，これらコンピュータによる基幹業務態系なくして通常の業務を滞りなく遂行することは難しい．

基幹業務以外にも ISO に則した文書保存を筆頭とするペーパーレス化の実践などにより，システムは高速・大容量・高信頼性を常に凌駕しなければならない．今後もシステムの依存度が一層高まる事は明白である．

受注システムを柱とする弊社業務システムのありかたを考えた時，システム自体が堅牢に稼動することはもっともだが，業務データの普遍的な維持及び緊急時における破損データの早急な復元という点も重要な事項となる．いくら日常業務を安全かつ確実に行えるようなソフトウェアの開発を行ったとしても，物理的要因や除去できなかったソフトウェアのバグ，又は外部からのウイルスによる被害や使用者の不注意などによるデータの損傷損壊で，システムそのものが機能しなくなるという要因はいくらでも考えられる．システムを提案提供する側としては，これらシステムの停止など，考えられる不安要因に対してさまざまな方面からシステムの正常稼動を維持する仕組みを考察しなければならない．弊社では，万一システムやデータが破損した場合でも，迅速に復旧を行うことで責任ある企業として業務停止を極力抑制するとともに，被害の対価を抑えるための実用的なバックアップ及びリカバリの再考がシステムフェールセーフの一環として重要であると考え，これを実践した．

２．旧システムの問題点

２．１　旧基幹システムの構成

旧基幹システムでは７台の個別のサーバに Microsoft WindowsNT 4.0 Server を用い，各サーバのハードウェア RAID にてデータの多重化を行うと共に，ローカル接続された DLT や他サーバの専用領域へ OS 標準のバックアップユーティリティーである NT バックアップを利用して，夜間にデータのバックアップを取るという手法を取っていた（**図１**）．

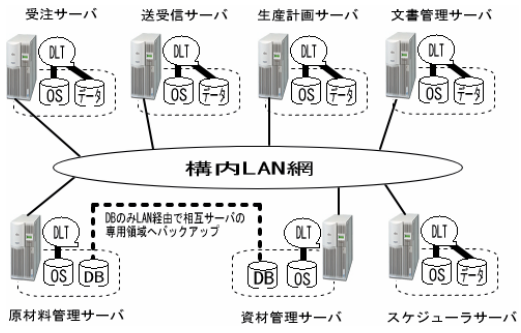


図１　旧基幹システムのバックアップ構成

２．２　旧基幹システムの問題点

図１のとおり，旧基幹システムではデータのリカバリ作業よりもデータバックアップへの傾倒がみられた．これは旧システムの設計時におけるサーバやネットワークの背景が現在とは異なっていたためであり，当初の設計思想を現状の業務においても使用できるように後々対応してきたのだが，現実には決して十分なものとは言いがたい．そこで，システムの信頼性を高め，スムーズなリカバリ作業を行なうために，これら旧基幹システムのバックアップ及びリカバリ方法の問題点を整理した．

（１）バックアップ作業の問題点

旧システムでは，各サーバにおいて OS 標準の NT バックアップを使いアプリケーションとデータファイルを DLT にバックアップしていた．しかし，NT バックアップではアクティブな状態のファイルを保存できないという理由により，システムやデータファイルを完全な状態でバックアップすることは不可能だった．修復の内容によっては OS 及びアプリケーションを再インストールした後，前日の夜間にバックアップしたファイルを DLT よりリカバリするという方法を取っていた．しかし，この方法では実際にデータをリカバリするまでに多くの作業時間を要し，データの復元ポイントが前日の夜間まで戻るため，業務データにタイムラグが発生するという大きな問題があった．特に，汎用コンピュータから移行された基幹系の業務サーバでは，頻繁な更新があり 15 分に一度という短時間間隔でのバックアップの必要性があった．書き込み速度が低速なため，実稼働時間中の DLT へのバックアップは現実的には不可能であり，これを補うための手段として別サーバに専用領域を設けてバッチ処理でデータのコピーを行う手法を取っていた．

サーバにはすべてハードウェア RAID を施し，多重化による障害の軽減を図っていたが，RAID のみでは使用者のミスや近年急増したウイルスによる被害が発生した際など，多重化されたファイル自身もダメージを受けるなどの問題をはらんでおり，ソフト的障害発生時のバックアップとしては有用ではなかった．

これらの手法は，いずれもバックアップとしては苦肉の策であり，十分なものとは言い難い．

（２）リカバリ作業の問題点

旧システムでは，多くの場合 OS やアプリケーションの再インストールからデータのリカバリまでを行う必要があり，その為の作業時間は半日から数日となる事が予想されていた．しかも，リカバリ作業には，システムの構成を熟知している必要があり，限られたシステム担当者でなければこの作業は不可能でもあった．しかし，システム開発や保守のアウトソーシング化が進み，これらの作業を行う事ができる技術者が現場に常駐する事は難しいという現状を考えると，実際のリカバリ作業開始までにはさらに空白の時間が生じる事は必至であった．これによりシステムの復旧から再稼動までに長時間を要することから，多大な損害の可能性と，企業としての信用，信頼の失墜を招くことが懸念された．

３．新基幹業務システムの考察

３．１　新基幹システムに求められるもの

これらの問題点を考慮して，新基幹システムに求められるバックアップ及びリカバリシステムの重点項目を策定した.

（1）バックアップ作業

・OS 及びアプリケーションをサーバ単位で一括イメージファイルにする（以下イメージ化という）バックアップ作業の完全自動化
・喪失データを極力少なくするため，データ領域の短時間サイクルのバックアップ
・バックアップデータを世代管理することによるリカバリポイントの選択肢拡大

（2）リカバリ作業

・最短１時間以内でのリカバリ作業による業務の復旧
・作業の簡素化で専任者以外でも容易に出来るリカバリの実現
・ハードウェアの統一や集約による代替機調達時間の短縮

これら条件を効率良くサーバシステムに用いる事で，システムの恒常的な安定稼動と，不測の事態におけるフェールセーフを実現させる事を目標とした.

３．２　新基幹システムの問題と対策

新システムに望むものは，一見簡単に実現できそうに見える．事実，限りない予算があれば，すべてを集約できるハードウェアとその為のアプリケーションを必要なだけ導入すれば済む問題である．大手金融業やデータバンク業ではこれこそが企業の要であり，その為の予算投入は当然視されるところである．しかし，弊社を含む多くの日本企業の実情を考えると，現実的ではない過大投資は事実上不可能に近い．すべてのデータに対して，起こり得るであろうすべての事象へのフェールセーフを導入するメリットがあるのかという事を考えざるを得ない．そこで，弊社では現状稼動する７台のサーバを分析し，それらのサーバが必要とするフェールセーフの形を明白にする事により，よりコストパフォーマンスの高いトータルフェールセーフの実現を図った（**表１**）.

表１　サーバの運用形態の分析と要求一覧

サーバ名称	稼　動　内　容	稼動時間	データ量（MB）	データ更新頻度	システム依存指数 *1	環境更新変更頻度 *2	データベース	リストア許容時間	要求されるサーバの選定基準 *3
受　　注	在庫管理と営業からのオーダーに対する出荷指示	早朝～22時間	3,200	高	高	低	有	60分	ＩＮＳＤＢ
送　受　信	遠隔本社とのホスト通信	早朝～22時間	400	低	高	低	無	60分	ＩＮ
原材料管理	工場内の原材料の在庫管理及び手配	早朝～22時間	2,800	高	高	低	有	60分	ＩＤＮ
文 書 管 理	ＩＳＯ文書管理	24時間	3,000	極低	中	低	無	360分	ＩＬ
生 産 計 画	製品の操業計画を管理	24時間	5,000	中	中	低	有	360分	ＩＤＬ
資 材 管 理	工場内購入品及び設備管理	24時間	16,000	高	中	低	有	360分	ＩＤＬ
スケジューラ	社内公開Ｗｅｂサーバ及びスケジュール管理	24時間	1,000	低	低	低	無	720分	ＩＬ

*1 システムが停止した場合、再稼動までに発注書発行などの業務が代替えで行えるものを依存指数（低）、業務が中断するものを依存指数（高）とする.
*2 データベース等の運用環境が変更され、環境の更新や変更が頻繁に発生するものを（高）とする.
*3 新基幹サーバとして要求される選定基準を下記の記号で分類表示.
I（Image）：OS及びアプリケーションのイメージファイル作成　N(iNtegrate)：サーバ集約　S(Short)：データの短間隔バックアップ
D（Database）：データベースエンジン　L（Long）：データの長間隔バックアップ　B（Big）：大容量データのバックアップ

３．３　新基幹システムの構成

表１を基に新基幹業務サーバ群のハードウェア選定を行なった．新構成ではシステム依存度が高い受注，送受信，原材料管理のサーバをユニット式の Fujitsu PRIMERGY BX300 ブレードサーバ（以下ブレードサーバという）とした．このブレード化は，万一のハードウェア障害時に備えて代替用のブレードユニットを用意することでハードウェア的障害を短時間で復元できると共に，ユニット単体で RAID1 の構成が成されているため，ディスクユニット単体の不良にもマージンが設けられているという点からの選択である．また，このシステムでは別途 Fujitsu PRIMERGY L100E デプロイメントサーバ（以下デプロイメントサーバという）を設け，これらブレードサーバの運用を監視すると同時に，システムイメージやデータのネットワークストレージへの転送を行う事ができるようにしてある．

ブレード化以外の４台（以下一般サーバという）については搭載メモリ量やハードディスク容量の再考察を行い，RAID5 によるハードディスク障害に対応すると共にバックアップ用の DLT をすべてに装備した．

新サーバ群のもうひとつの特徴として，大容量のネットワークストレージサーバ Fujitsu ETERNUS NR1000 F170（以下 NR1000F という）を用意した事が挙げられる．これには，DLT などのデバイスでは不可避なメディアの変更作業や，耐用時間の管理を回避する目的，年々増大するデータのバックアップ及びリカバリ時間の短縮，ネットワークを介してバックアップを行うという冗長性，また，バックアップデータの一元管理などが挙げられる．今回選択した NR1000F には，このシステムにバックアップファイルの世代管理機能が付いているという点も選択の一因になった．

３．４　バックアップの方法とタイミング

まず，OS 及びアプリケーションに関しては，全サーバの OS とアプリケーションをイメージ化し，バックアップを行う事とした．緊急時の再インストール作業をバックアップイメージからのリカバリに代替する事で，サーバ機能の復元に要する時間を大幅に短縮できる事となる．また，１時間以内に復元が求められるサーバについては，このイメージ自体を NR1000F に保存する事により，リカバリ時のデータ転送速度を向上させ，より迅速な復元を可能にできる．

すべてのデータに関して単純に NR1000F にバックアップデータを保存するという手法を取らない理由としては，限りあるネットワークインフラに対して不要なトラフィックを発生させたくないという考えがある．また，既存の DLT 装置を適所に効率よく使用することで新規ハードウェアにあてる不要な経費を削減できる．例え小規模な経費でも，削減を意識しなければ大きく膨らむものである．

データのバックアップタイミングに関しては，サーバにより幾つかの条件があるため，より細分化する事が必要であった．まず，データ更新頻度を元にしたバックアップ間隔，そしてデータベースエンジンの有無，また，リカバリの許容時間などである．例えば，受注サーバのデータは 15 分毎に受注データが更新されるため，15 分間隔でのバックアップが必要であるが，データベースエンジンを使用しているため安易な差分ファイルのバックアップという手法を取る事はできない．

一般サーバでは，データ更新のタイミングは不特定であり業務の状況及びデータの更新頻度から 30 分間隔での更新を行うのが良いという結論に達した．

これらのサーバにもデータベースエンジンが稼動しているものや，保有データ量の大小，システム依存度などの複合的条件が絡み合っており，既存のハードウェア資産やバックアップに割り当てられるネットワークトラフィック量等を考慮すると，ハードウェアは**図２**の構成で行う事が妥当であるという結論に至った．

３．５　ソフトウェアの選定

バックアップソフトウェアには，単純バックアップ（ファイルのコピー），アーカイブ及びイメージ化によるバックアップとそれぞれのバックアップファイルの世代管理が求められる．ただし，これもハードウェア同様，各サーバの構成用途により適材を適所に用いる必要がある．ここでは複数のバックアップ用ソフトウェアを使用する事とした．

また，このソフトウェア選定作業はハードウェア選定と同時に進行しているため，ハードウェアに標準で装備される（あるいは，ハードウェアとソフトウェア双方がマッチするような仕様の）ソフトウェアは，それを優先的に使用することとした．（**表２**）

表２　ソフトウェアの選定及び割り当て

使用サーバ	使用したソフトウエア	動作 *1	機能及び方法
受　注 送　受　信 原材料管理	System Cast Wizard	B	ディスクまたはパーテション単位でのイメージファイルをバックアップ バックアップ時には対象サーバは停止している必要がある
		R	イメージファイルの復元でディレクトリやファイル単位では不可能 リストア時には対象機は停止している必要がある
		S	タスクスケジューラにより処理を起動　*2
資材管理 文書管理 生産計画 スケジューラ	ARCserve Backup + Disaster Recovery Option	B	ドライブ、フォルダ、ファイルを指定してバックアップ ＤＬＴ装置に圧縮されたイメージファイルとしてバックアップ アクティブなファイルやシステムレジストリもバックアップが可能
		R	ディレクトリやファイル単位でのリストアが可能 Disaster Recovery OptionでＯＳやARCserve Backupをインストールせずに、サーバの復旧が可能
		S	ARCserve自身のスケジューラにより処理を起動
受　注 原材料管理 生産計画 資材管理	Disk Mirroring Tool	B	スケジュールによるフォルダ単位のバックアップ
		R	対象のフォルダをエクスプローラで復元
		S	タスクスケジューラにより処理を起動

*1　動作の種類別に記号表示　B:バックアップ　R:リストア　S:スケジューリング
*2　タスクスケジューラとはMicrosoft Windowsに標準添付されているプログラム起動用のスケジューラソフト

３．６　新基幹サーバシステム

これらのハードウェア，ソフトウェア選考原案を元に，フェールセーフシステムを組み込んだ新基幹サーバの構築を行なった（**図２**）．

構内ネットワークには基幹業務用のメインフレームとクライアントパソコン 350 台が接続されている．新サーバシステムの接続と同時にネットワークの接続環境もバックアップリカバリがネットワークに負荷を与えないようにネットワークトラフィックを計測しながらサーバの接続構成やネットワーク機器の選択を行った．

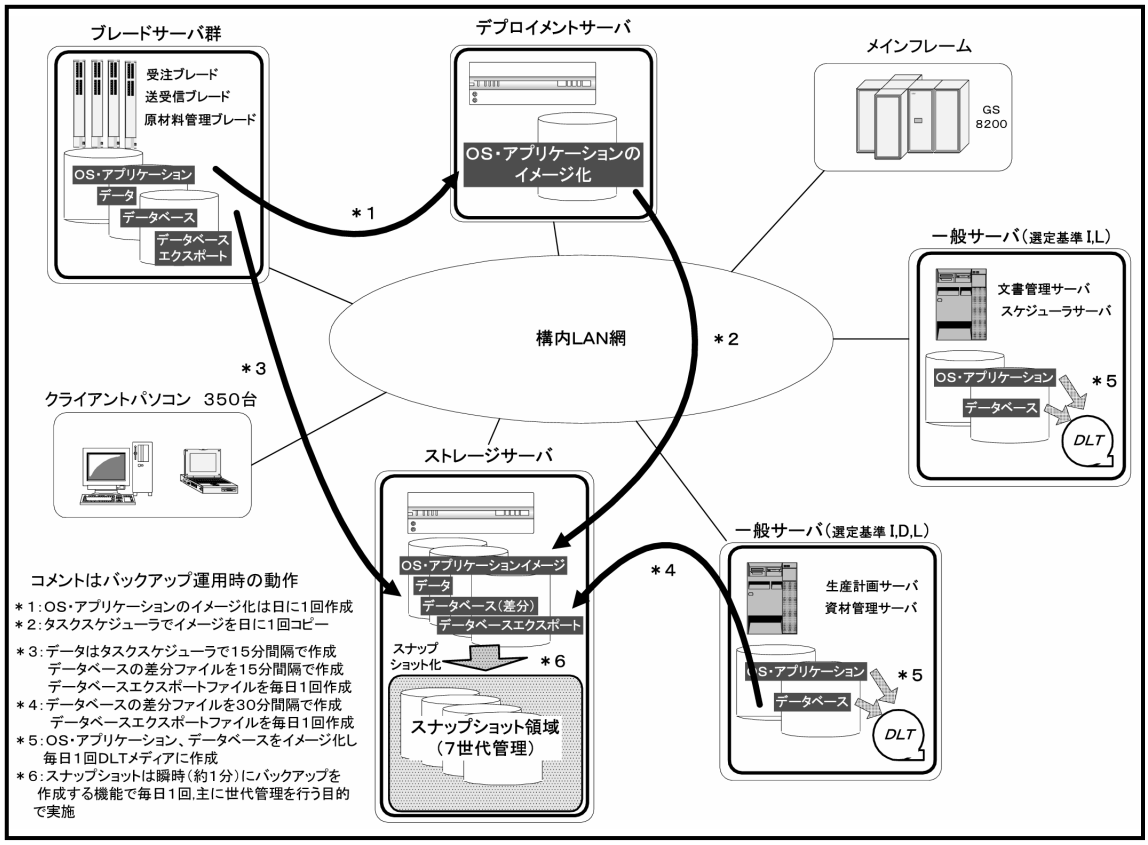


図２　バックアップリカバリ構成概要

４．運用方法

４．１　バックアップ作業

導入に際しては繰り返し仮稼動試験を行った．ここではその手順を示すとともに，試験データを元に導入効果を検証する．

バックアップ作業はすべてタスクスケジューラ又はアプリケーションのタイマ機能により自動化されており，人間が介す事により起こり得るケアレスミスを防いでいる．すべてのサーバは 1 日に 1 回 OS を含むシステム全体のイメージをバックアップする．この際，アプリケーションの仕様により一度システムをシャットダウンさせなけらばならないが，各サーバの利用状況より夜間又は早朝にこの作業を行っても支障がない事を事前に確認してある．各々のサーバはこの指定された時間に自動的にシステムデータをイメージ化し，指定されたストレージにデータを格納する．また，このイメージも世代管理されており，緊急時には最大 7 世代前のシステム状態まで戻すことが可能である．

データに関しては，稼動サーバによりバックアップ方法が異なる．大量のデータが頻繁に更新されるサーバでは更新ファイルの差分バックアップを行う事によりバックアップ所要時間及びインフラの占有縮小を図っている．また，他システム等が使用中のアクティブなファイルやデータベース関連のファイルは，ARCserve Backup + Disaster Recovery Option（以下 ARCserve という）を使用する事で，アクティブな状態のファイルも強制的にバックアップを行う．

４．２　リカバリ作業

ブレード化されたサーバにおいては System Cast Wizard でシステムデータの復元を行い，後に必要なデータをバックアップファイルよりコピーする（**図３**）．また，これらの作業はすべて GUI 上での操作が可能であり，万一運用担当者が不在の場合でも仕様書の確認や電話などで指示を仰ぐことにより，一般のシステム担当者でも簡単にリカバリ操作が可能である．さらに，万一ハードウェアの故障があってもバックアップ用のハードウェアにシステムイメージ及びデータを復元することによりシステムの回復が可能である．方法は簡単で，障害のあったブレードを予備のブレードと入れ替えた後，上記のリカバリ作業を行うだけである．また，このブレードサーバはホットスワップが可能なため，ブレードサーバ全体を停止する必要が無い．これにより，リカバリ時に他の連携サーバを停止することなく，作業ができるという利点がある．

ブレード以外の一般サーバに関しても，ハードウェア障害等の問題が解決次第，同様の方法でリカバリ作業を開始できる（**図３**）．一般サーバでは，バックアップされたシステムイメージがテープデバイスに保存される．これは一見，リカバリ作業の効率を考えると非効率的に見えるが，これらサーバの業務依存度が比較的低く，システムやデータの規模が小さい事やリカバリ許容時間が比較的長い事などによりこの方法を選択した．尚，その他データベースファイルに関してはブレードサーバ同様 GUI によるリカバリが可能であり，その操作は容易に行える．

リカバリ作業もブレードサーバと一般サーバでは上記のように方法は異なるが，その作業性は大幅に簡素化され所要時間は著しく短縮された．

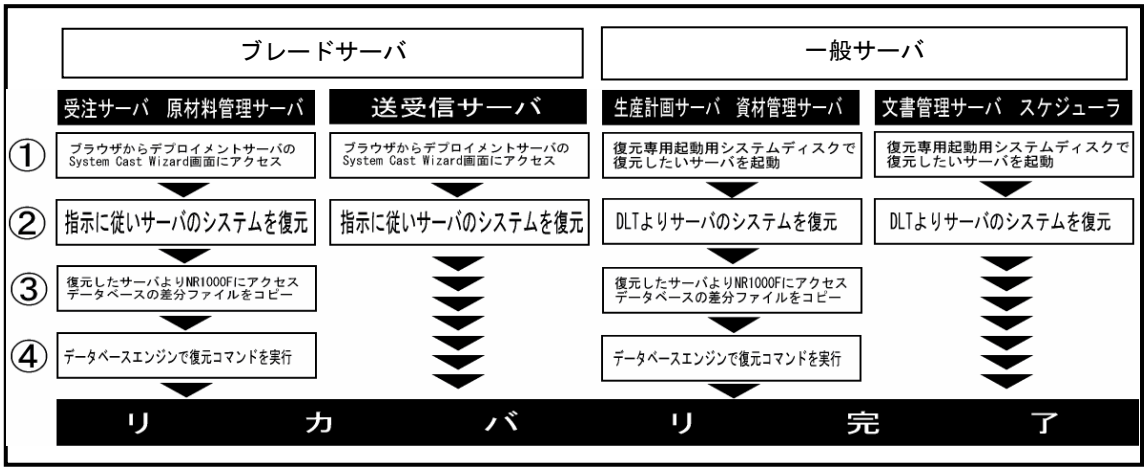


図３　各サーバのリカバリ手順

５．検証・評価

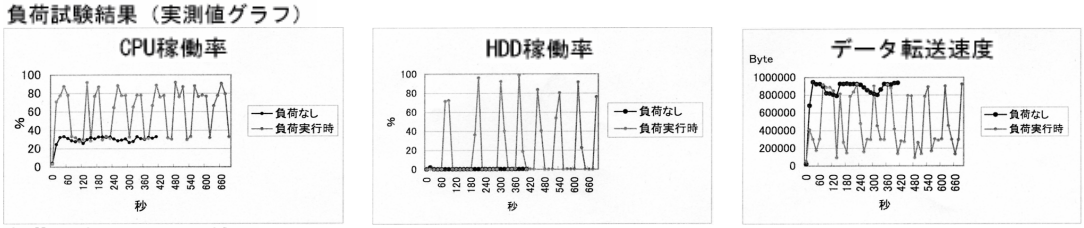
５．１　バックアップ検証と評価

各サーバとも OS 及びアプリケーションのバックアップについては，業務が終了した夜間の指定時間内に自動処理されて問題なく完了し，満足のできる結果となった．ファイルのバックアップについては，いちばん稼働率が高く 15 分ごとにバックアップを行なう受

注サーバの試験データを一例として**表３**に示す．この検証では 15 分間隔で更新される想定実務ファイルの 1.5 倍量を差分ファイルとして人為的に作り出し，ネットワークの通常負荷時と高負荷時双方において検証を行なった．通常負荷時では 6 分 30 秒で差分ファイルのバックアップが完了していることから，15 分のバックアップ許容時間が十分であることがうかがえる．また，高負荷時試験では HDBENCH を使用して高負荷状態を人為的に作って検証した結果，こちらも約 13 分ほどでバックアップは完了することが確認できた．一見，時間的マージンが乏しいと思われる結果だが，実稼動時にはこれほどのファイル量や高負荷状態が持続することは考えられないという点を踏まえると十分納得できる検証結果が得られた．

表３　受注サーバのバックアップ負荷試験表

負荷試験結果（実測値グラフ）



負荷試験結果（平均値）

負荷状態	対象ファイル	対象ファイル量	対象総データサイズ	最大 CPU 稼働率	平均 CPU 稼働率	最大ディスク稼働率	平均ディスク稼働率	最大書き込み速度	平均書き込み速度	実行時間
通常	差分	784MB	201,550	37%	31%	5%	1%	980kb/s	768kb/s	6 分 30 秒
高	差分	784MB	201,550	91%	59%	99%	39%	920kb/s	520kb/s	12 分 57 秒

※差分ファイルは 201,350 個のファイルに任意に 200 個のファイルを作成追加することにより発生させた．

５．２　リカバリ検証と評価

リカバリ作業の検証はブレードサーバと一般サーバに分けて行った．最大実務データ量と OS 及びアプリケーションの占有量を算出して，その 1.5 倍相当のダミーデータをサーバに個別にインストールして検証を行なった．これは実務における個々のサーバのデータ使用量が流動的であるため，現時点でのサーバが保有するデータ量を元に検証を行なっても，近い将来この結果の有効性が危ぶまれる可能性が高いという理由からこの手法を選択した．

検証の結果，**表４**にあるように，すべてのサーバにおいて当初目標としていたリカバリ許容時間を下回ることができた．この結果は今後の運用に大きな意味を持つもので，トータルフェールセーフという観点からも満足のいく結果が得られた．

表４　リカバリ試験表

サーバ種	ソフトウエア	リストア元	ファイル量	最大処理時間	合計処理時間	最小許容時間	許容時間－処理時間
ブレード（ＤＢ有）	System Cast Wizard	デプロイメント	4,130MB	20 分	49 分	60 分	11 分
	Disk Mirroring Tool	NR1000F	784MB	29 分			
ブレード（ＤＢ無）	System Cast Wizard	デプロイメント	4,130MB	20 分	20 分	60 分	40 分
一般（ＤＢ有）	ARCserve Backup	DLT テープ	25,000MB	120 分	149 分	360 分	211 分
	Disk Mirroring Tool	NR1000F	784MB	29 分			
一般（ＤＢ無）	ARCserve Backup	DLT テープ	25,000MB	120 分	120 分	360 分	240 分

６．残された課題

新基幹システムにおけるフェールセーフの一環であるこのシステム構成では，日々の作業が自動化されており，保守管理は定期的な監視程度で済むほど省力化された．しかし，リカバリ作業を要する事態が発生した場合，いくら復旧が楽であるとは言え，その手法を作業者が十分認知している必要がある．また，システムの根幹にかかわる変更や拡張が発生した場合には，保守管理が簡単になった反面，複雑化したシステムを熟知しておかなければ相互にリンクされたシステム全体にダメージを与えかねない．

人員やコストの省力化などシステムのアウトソーシング化が進む今日において，恒常的に安定した管理や開発を可能にするには，積極的な管理者や技術者の教育が必要である．これは省力化と相反することであり，我々はこのジレンマを回避すべく大量のマニュアルや仕様書による教育方法を見直した．これは経験や知識を効率的に引き継ぐことが容易であり，動画や音声を中心とした分かり易いDVD形式のマニュアルの作成に繋がった．

システムが完成された今，このように管理が容易で万人が扱えるシステムの真価を発揮させるには，これらヒューマンエデュケーションに対する認識の刷新も必要であると感じている．

７．おわりに

企業において，データやシステムが高いプライオリティーを有する現在，それを統括するシステム管理者がその維持管理に万全を期しているとしても，ひとたびそのシステムが停止，損壊した場合には，多額の損害や責任所在が求められるだろう．企業としては社会に対する責務を果たすという見地から，万一の事態に備え，これらを未然に防ぐために，想定されるさまざまなシーンに対応できるトータルシステムを構築することは重要な事である．また短時間でフルバックアップが可能なユーティリティーやハードウェアが存在する現在，これらを行うためには，多くの労力を費やす必要は無いとの考えもある．しかし，これら大半は，銀行等の大規模システムを考慮した高価なものであり，中小規模のシステムでは，予算，機能の両面から必ずしも妥当なものでは無いと言える．一般的にフェールセーフの形を固定化して，それ以外の方法を邪道とする事は，結果として中小規模のシステム構成を持つ企業の根本的な意識を低下させる事になるのではないだろうか．今回の試みは，弊社にとっては大きな財産となり得たが，この方法がデファクトスタンダードになる事は稀であると思っている．是非とも弊社の試みを参考に，常識にとらわれない自社独自のシステム運用というものに目を向けていただきたい．その為のテーゼ，アンチテーゼとなってくれれば幸いである．

また最後に，新基幹システムの設計構築に携わってくれたすべてのスタッフと，弊社の試みに対し執筆の機会を与えていただいた FUJITSU ファミリ会に，深く感謝を申し上げます．