ディザスタリカバリの適用拡大による ビジネスコンティニュイティの実現

－リカバリ段取り時間を短縮－

第２事業部
基盤システム第２開発部
基盤第１チーム
ITスペシャリスト
佐野　泰之
Yasuyuki　Sano
yasuyuki-sano@exa-corp.co.jp

ビジネスコンティニュイティ（ビジネス継続性、以下BC）を高いレベルで実現するため、災害時回復の観点をデータ損失による障害発生に拡大適用し、復旧までの目標時間（Recovery Time Objective　以下RTO）の性質を明らかにし、その短縮を図った。関連してデータ保護、リカバリとリストアについて最新のストレージ基盤技術を紹介した。

RTO短縮にはシステム系と人間系の両面から検討する必要があることを示した。本稿では特に人間系であるリカバリ段取り時間に着目して議論を進め、担当者と手順の二つの観点から各種の問題点にアプローチし、その時間短縮方法を提案した。

また、本方法を実際に稼動しているシステムに適用し、適用前には13.5時間あったRTOを4時間に短縮した例を紹介した。

1. はじめに

業務システムのIT化に伴い、高度なビジネスコンティニュイティ（ビジネス継続性、以下BC）を実現するには、ITの高可用性・高信頼性が不可欠なものとなっている。その中でも、データを蓄積し供給するストレージ基盤は、高度BC実現のための根幹的な技術である。

BCを実現するストレージ基盤技術には、ディスク・コントローラ・電源などのハードウェアコンポーネントの故障に備え、それらを２重化した構成にてシステムの高可用性を実現するものがある。また、万が一災害が発生した場合のシステムダウンタイムを短くする災害時回復の技術として、最新のデータ通信機能を駆使し、遠隔地へデータを転送・コピーするディザスタリカバリ（Disaster Recovery：災害対策、以下DR）がある。

しかし、DRは大規模地震や火災など、発生確率が低いものを対象としており、身近な発生確率の高いデータ損失障害を対象としているものではない。そのため、DRの目標値として設定する、RPO（Recovery Point Objective：目標復旧時点）やRTO（Recovery Time Objective：目標復旧時間）を、データ損失障害の回復について適用し、RPOの最新化やRTOの短縮化について議論することはあまりなかった。

本稿では、BCを実現するために必要な災害時回復の観点を、極めて発生確率が高い、データ損失による障害発生に拡大適用する。そこでのデータ保護とストレージ基盤の最新技術を活用したRTO短縮方法を紹介する。さらに、RTO短縮をシステム系と人間系の両面から検討する。特に人間系ではリカバリ段取りに着目したRTO短縮方案について述べる。これにより当社のお客様にて、データ損失による障害発生時のRTOを短縮した実例を紹介する。

2. BC（ビジネス継続性）とデータ保護

本章ではBC実現のためのデータ保護の重要性とストレージ基盤の最新技術動向について述べる。

2.1. データ保護の重要性

BCとはコアオペレーションの持続であり、IT化された業務システムのダウンタイムを短くすることが課題である。ダウンタイムが発生することは、業務の停止によるお客様の信頼消失や、ブランドイメージの破壊につながりかねない。このため、多くの企業ではBCの実現に取り組んでおり、システムのダウンタイムを発生させないための、高可用性システムを検討し既に導入している。さらに、万が一災害や障害が発生した場合のダウンタイムを抑えるため、DRシステムの構築の検討にも着手している。特に最近は、予防対策となる前者よりも、発生対策となる後者について議論されることが多くなってきている。実際に、メーカやベンダなどのセミナーでも、BCの対策としてDRシステムを提案していることが多い。

一方、DRを実現するためにストレージ基盤に求められることは、蓄積した重要なデータを損失から守ること、つまりデータ保護である。図１に示すように、データ損失の要因は、「人為的ミス」・「ソフトウェア障害」・「ウィルス」によるものが、要因全体の半分以上を占めている。これは、「自然災害」による要因と比較して、発生確率が圧倒的に高い。

このことから、DRシステムを構築してBCを実現するためには、これら全体の半分以上を占める要因からデータを保護する方策の検討が極めて重要であることが分かる。

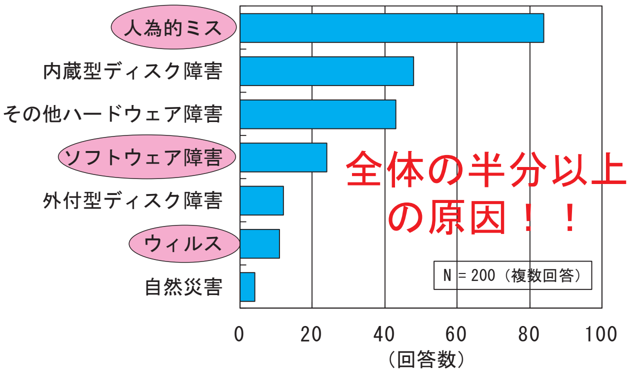

図１　データ損失の要因[1)]

2.2. データ保護とストレージ基盤の最新技術動向

データ損失には、災害などによりストレージ機器が破壊される物理的なデータ損失と、磁気ディスク上の電子記録が失われる論理的なデータ損失がある。発生確率が高い、「人為的ミス」・「ソフトウェア障害」・「ウィルス」によるデータ損失は、後者の論理的なデータ損失である。これを保護する手段はバックアップしかない。[2)]　つまり、

論理的に意味が保たれた静的で安定した状態、いわゆる一貫性のあるデータを常に用意しておき、万が一の場合に元に戻すバックアップシステムが論理的なデータ損失の対策に必須である。

そこで、ストレージ基盤には効率的にバックアップを行い、障害時のリストアを高速に行うことでダウンタイムを短くすることが求められる。最近では、業務システムに影響を与えることなくバックアップが取得でき、また高速にリストアできる機能を持ったディスク装置がバックアップシステムに多く採用されている。

図２は、複数のDB（Data Base）サーバがSAN（Storage Area Network）を経由して、一つの外部ディスクを共有する、最新かつ典型的なシステム構成の一例である。

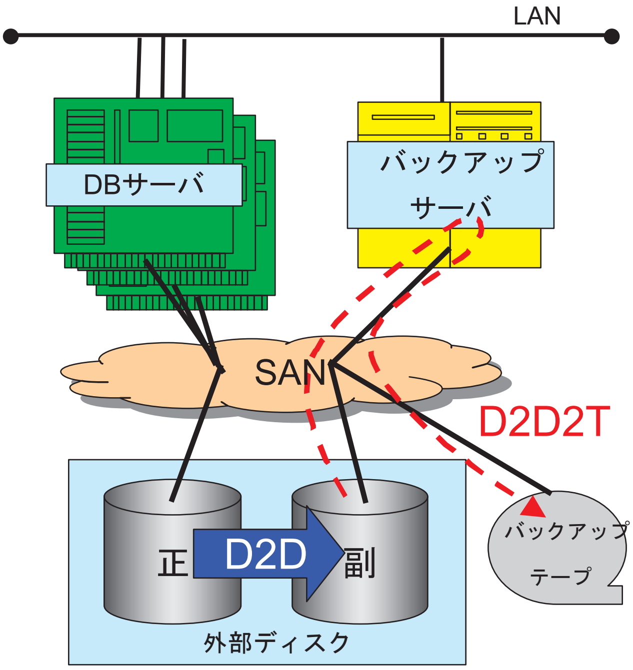

図２　SANを中核に据えたストレージシステム

このシステムでは、ディスクからディスクへのバックアップを瞬時に行う、D2D（Disk to Disk）というバックアップ方式を適用している。このD2D方式には筐体内ボリュームコピー機能と、変更箇所のコピーのみを実施する差分機能を装備している。 D2D方式の機能は外部ディスクシステムに集約しているため、業務システムを担うDBサーバに負荷をかけないのが特徴である。また、DBがユーティリティで装備している、オンラインバックアップモジュールと組み合わせれば、業務を止めることなく一貫性のあるデータを取得できる。

さらに、バックアップソフトを導入したバックアップサーバを設置し、ディスク上にあるバックアップデータをテープへ保管することもできる。これを、D2T（Disk to Tape）方式といい、バックアップデータの複数世代の確保や、テープの可搬性を生かし災害時対策のテープ外部保管を可能とする。

上記のD2DとD2Tを組み合わせて、D2D2T（Disk to Disk to Tape）方式という。

一方、高速リストアはバックアップ同様、D2D方式で実現する。なお、リストアを行うバックアップデータは、外部ディスクの副ディスクに保管する。それは、DBサーバが直接アクセスする外部ディスクの正ディスクが、論理的に破損した場合のバックアップになる。バックアップの副ディスクから見て、異なる箇所のみを正ディスクにコピーする差分機能が使えるため、高速なリストアが可能となる。具体的には250GBのデータを約５分でリストア完了した事例3)がある。この方式は、テープを使ってリストアを行っていた旧来に比べ、１桁以上の時間短縮ができる。

以上、BCを実現するためのDRシステムの最新技術動向として、効率的なバックアップと、障害発生時の高速リストアを実現している先端的なストレージシステムを紹介した。

3. DRと目標復旧時間（RTO）

本章では、DRにおけるRTOの意味とその内訳および、リカバリとリストアを整理して述べる。

3. 1. 目標復旧時点（RPO）と目標復旧時間（RTO）

業務システムのDRを計画・検討する上で、定量的な目標としてRPOとRTOを設定することが一般的である。図3で示すとおり、RPOは災害発生時点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。一方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経過である。RPOとRTOは、業務それぞれの業種・企業・部門やサービス内容に応じ、災害対策コストと被災損害コストのバランスを検討した上で設定する。しかし、これらは大規模地震や火災などの広域災害を対象とすることが多く、発生確率の高い、論理的なデータ損失の対策に適用されることは少なかった。

そこで、本稿では論理的なデータ損失の対策の目標とし

てRPOとRTOを適用する。すると､RPOはデータ損失によるシステムダウン発生時から、どの時点のデータまで復旧するか、つまりどの程度までデータ損失を許容するかの目標となる。一方、RTOは障害発生時からどのくらいでデータ復元ができ、システム復旧できるかの時間、つまりダウンタイムの目標となる。これらの目標を持って、許容できるデータ損失とダウンタイムをあらかじめ要件として明確に決めておけば、要件にあったバックアップシステムを設計・構築することができる。

RPOの短縮は、できるだけ頻繁にバックアップを実施し、データの保護ができない期間を縮めることである。一方、RTOの短縮にはバックアップデータのリストアを高速に行う技術を採用し、リストア時間を短くすることが有効である。そのため､ストレージベンダやソフトウェアベンダは高速リストア機能を持った製品を数多く開発・発表している。

しかし、それらを採用するだけでRTOが短縮できると考えがちであるが、製品の技術だけでは解決できない要因が潜んでおり、それが足かせとなっているのが現状である。コストをかけて高速リストア機能を持った非常に高価な製品を採用しても、効果を発揮しない場合もある。そこで、足かせとなる要因を明らかにすべくRTOの内訳を分析することから始める。

3.2. RTOの内訳

データ損失による障害が発生した場合のRTOを短縮するために、まずはその内訳を洗い出し、それぞれの要因について検討していく。図４にRTOの内訳を示す。

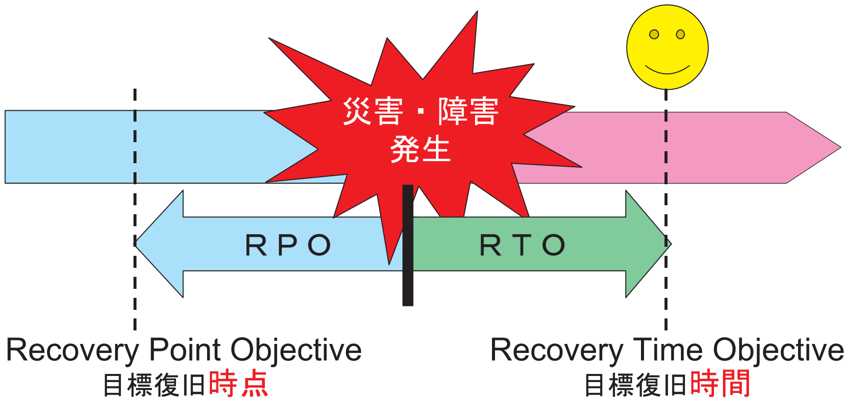

図３　目標復旧時点（RPO）と目標復旧時間（RTO）

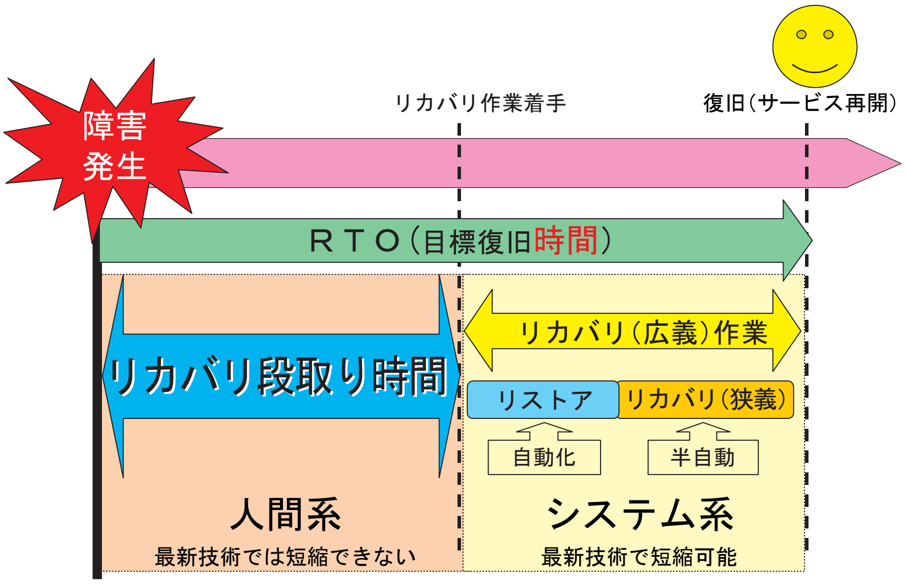

図４　RTOの内訳

時間の経過に基づいたRTOの内訳は以下のとおりである。

(1) 障害が発生してから、障害が発覚するまで
(2) 障害が発覚してから、リカバリ作業に着手するまで
(3) リカバリ作業に着手してから、リカバリが完了しシステムが復旧するまで

まず、(1)の"障害が発生してから障害が発覚するまで"の時間には、厳密には多少の時間差が存在する。実際、運用監視システムで異常を検知する場合や、システムのユーザがサービスの停止に気がつく場合など、障害を発覚する手段はシステムごとに異なり、その状況に応じて発生から発覚までの時間は伸縮する。しかし、システムダウンとはサービスダウンと定義すれば、ユーザがシステムを使用できなくなった時点をもって、障害が発生した時間とすることができる。ここでは、障害発覚時を障害発生時と定義し、障害発生と障害発覚の間には時間差がないものとする。

次に、(2)の"障害が発覚してからリカバリ作業に着手するまで"の時間については人間系の対応であり、今まではあまり着目されることがなく、議論されることもほとんどなかった。しかし、この時間がRTOの内訳の大半を占める事例もあり、決して無視できるものではない。本稿では、この時間をリカバリ段取り時間と定義して、その内容と短縮のための方案を４章で詳しく述べる。

(3)の"リカバリ作業に着手してから、リカバリが完了しシステムが復旧するまで"の時間は、前節2.2で紹介したストレージ基盤をはじめとする、システム系の最新技術に依存するところが大きい。ここで対象としているデータ損失による障害の場合、データ復元をできる限り早く終えることが課題となる。

以上を整理すると次の式で表せる(図４参照)。

目標復旧時間（RTO）＝ リカバリ段取り時間 ＋
リカバリ（広義）作業時間

3.3. リカバリとリストア

データ損失障害のリカバリとは、バックアップデータを使用してデータの復元を行い、システム稼動のための作業と確認を行うことである。データの復元はリストア、システム稼動のための作業と確認は狭義のリカバリ、そしてその二つをあわせて広義のリカバリと定義する(図４参照)。

リカバリ（広義）作業 ＝ リストア作業 ＋ リカバリ（狭義）作業

リストアとは、保存した一貫性のあるバックアップデータを元の箇所に配置することである。自動化が可能なため、判断や操作ミスを防ぐことができる。システム系のRTO短縮方案として、2.2項で述べたストレージ最新技術を用いた、リストア時間の短縮が可能である。

一方、狭義のリカバリはリストアしたデータをもって、システムを障害発生前の状態に復旧する作業である。リストアとは異なり、人間による高度な判断が必要な場合が多く、自動化は極めて難しい。そこで、狭義のリカバリはシステムが用意したリカバリ機能を、あらかじめ用意した手順書にのっとって人が作業することになる。したがって、厳密にはこれは人間とシステムの複合系による半自動の作業となる。ただ、この複合系に内在する人間的要素への対策は、次の４章で詳しく述べる人間系への対策の中で十分にカバーしている。そこで、ここでは狭義のリカバリに対する対策を改めて議論することはしない。また簡便のため、狭義のリカバリ時間は、図4では複合系とはせずにシステム系に含めて示すことにした。

なお、本稿でのリカバリは特に断りのない限り、リストアと狭義のリカバリをあわせた広義のリカバリを表すものとする。

4. 人間系のRTO短縮方案

本章では人間系の対応策として、リカバリ段取り時間の短縮について述べる。

4.1. リカバリ段取り時間

リカバリ段取り時間とは、障害が発生してからリカバリ作業に着手するまでの時間を表現した筆者の造語である。この時間の長短は、後続のリカバリ作業を行うための、意思決定の体制に大きく依存する。そもそもリカバリ作業は、障害発生時にのみ実施、つまり不定期に発生し、かつ緊急を要することが多い。また、破損状態の確認・解析、復旧方針の判定、現状確保、リストア作業、確認作業、動作検証というように、人間の高度な判断が不可欠となる。場合によっては、システムの管理者権限、ネットワークスキル、データベーススキル、システム全体のアーキテクチャや業務への影響度の判断など、より高いスキルを持ったエキスパートでなければ対処できない場合もある。[4] したがって、リカバリ段取り時間を短縮して速やかにリカバリ作業に入るには、上記の要件を満たすエキスパートの確保を含

め、リカバリ体制を整備しておく必要がある。

次に、リカバリ段取り時間を担当者と手順の二つの観点で分類し、それぞれの問題要因と改善方案について述べる。

4.2. リカバリ担当者の観点

担当者の役割は、実際にリカバリ作業を実施することである。システムの構築が完了し運用フェーズに入れば、運用担当者はシステムの起動確認・監視・バックアップなど、あらかじめ決まった定常業務を行う。しかし、リカバリ作業は計画のできない非定常業務のため、役割分担が不明確になりがちである。いざ、障害が発生しリカバリ作業が必要となっても、実施する人を決めていない、決めていたとしても当日その場にいない、異動により引き継ぎが行われていないなど、なかなか作業に着手できない。また、リカバリ作業はバックアップシステムを構築し、納入したベンダやSI会社の役割であるとの思い込みから、担当者に当事者意識が欠如している場合もある。さらに、運よく作業を実施できる人がみつかったとしても、その人が到着するまで待つことで、作業着手ひいては復旧までの時間を無駄に引き延ばしてしまうこともある。

これらを改善するためには、リカバリを役割分担が必要なイベントとして位置づけ、その責任者を決めておき、複数の作業者を明確にアサインする必要がある。そして、複数の作業者によるローテーションにより、いつでも対応できるようにしておくことが望ましい。また、作業者の異動による引き継ぎは、責任者の指示の下引き継ぎ先と内容を明確にしておく。これは一見当たり前のようであるが、リカバリのような非定常業務ではついあいまいになりがちなので、徹底しておく必要がある。さらに、バックアップシステムのベンダやSI会社の支援が必要であれば、依頼する支援内容と対応時間を決めておき、システム納入時から契約を締結しておくと、役割分担が明確になる。これらにより、いつでも対応できる体制を作っておけば、作業者を待つことに浪費される時間を極力短縮できる。

4.3. リカバリ手順の観点

二つ目の観点は手順である。リカバリ作業を行う手順の有無だけでなく、その内容によっても、リカバリ段取り時間は大きく伸縮する。上述のとおり、リカバリ作業は不定期かつ、緊急を要するため、その作業内容は慎重かつ正確に行う必要がある。手順書がないと、作業担当者の経験や力量とその場限りの判断となるため、時間を要するだけではなく、ミスによる二次障害に発展する可能性もある。一方、手順書があったとしても、作業担当者が滞りなく作業できる内容になっていない場合もある。例えば、サーバにログインする方法や、画面・メニューの開き方などの初期動作方法の記述が省略されている、用語が統一されていない、また理解できない専門用語があるなど、分かりにくい手順書のために作業が進まないこともある。

さらに、リカバリ作業の中で使用する、バックアップデータの有効性の判断も必要である。日々バックアップはとっているものの、そのデータをリカバリするために一貫性がとれているか、また不足がないかなど、判断がつかない場合がある。以上のように、手順書の有無やその内容、さらにバックアップデータの有効性の判断など、リカバリ段取り時間が大きく伸長する要因は数々ある。

手順に対する改善は、作業者がミスなく落ち着いて作業ができる、完成度の高いリカバリ手順書を作成することが基本である。そこで、完成度を上げるための効果的な方法は、リカバリの責任者と作業者であるリカバリ担当者が、手順書を自ら作成することである。リカバリ担当者ではなく、バックアップシステムを開発・構築した担当者が手順書を作成し、それをもってリカバリ担当者に対し一方的にスキルトランスファーをする方法では、両者にはスキルや視点のずれがあるため、役に立たない手順書となりやすい。また、リカバリ担当者の当事者意識が薄れてしまうこともある。これらを防ぐためにも，手順書の読者であるリカバリ担当者が自ら作成することを強く勧める。

一方、先に述べたとおり、リカバリ作業には多岐にわたる知識や情報が必要なため、リカバリ担当者が独力で手順書を作成することは難しい。そのために、業務システム・インフラ・バックアップシステムなどの開発・構築担当者が、リカバリに必要な技術情報をもれなく提供し支援することが必須である。その上で、リカバリ担当者が手順書を作成し、そのあとはそれぞれの開発・構築担当者とレビューを繰り返すことで、完成度を上げていくことが必要である。

もう一つ、日々のバックアップデータの有効性を、いざリカバリ作業時に判断することは非常に難しい。たとえ、システム構築前に実施するリカバリテストにて、先に作成した手順書を基に、バックアップデータを使ったリカバリ動作と確認を行っていたとしても、構築後の運用フェーズ

の中で、バックアップデータの有効性が保証できるものではない。これは、運用フェーズでデータの容量やその内容が変化すること、OSやアプリケーションのパッチ適用など、システムの変更により構築前のテストの状態と、徐々にかけ離れていくためである。

この問題を解決するには、定期的にリカバリテストを予行演習として実施することが有効である。この予行演習により、日々のデータの変化によるリカバリ時間の確認をはじめ、手順の再確認や見直しをすることができる。ひいては、万が一のリカバリ作業の精度向上と、判断の迅速化による時間短縮が期待できる。

5. RTO短縮の実例

以上述べてきた方案を用いて、当社がお客様に納入したシステムで発生したデータ損失障害にて、RTOを短縮した実例を紹介する。このシステムは、リレーショナルデータベース（Relational Data Base ：以下、RDB）を実装したパッケージツールに、当社が開発したアプリケーションをアドオンした設計・開発支援システムで、お客様社内でサービス展開されている。バックアップは、2.2項で紹介したD2D2T方式を採用している。

ある日、ユーザがこのシステムを使用中に原因不明のサービス停止が発生した。お客様からの連絡を受け、当社の開発担当者が現地に駆けつけ調査を行った。状況の確認後、アプリケーションの再起動を試みたが、最初に起動すべきRDBのプロセスが起動しないことが判明した。RDBが出力したエラーコードやログの解析の結果、RDBに論理障害が発生し復旧にはバックアップを使ったデータ復元しかないと判断した。その後、データ復元作業を行いアプリケーションの正常起動を確認し無事サービス再開に至ったが、復旧までの時間（RTO）は13.5時間も要しており、その間サービスは停止した。

お客様からは本障害の原因追及・再発防止とあわせ、サービス時間の停止つまりRTOを1日の業務時間の半分に相当する４時間以内にするよう要請があった。そこで、RTO短縮のための本方案を適用し、以下の具体的な対策を検討した。

(1) 改善前のRTO確認

障害が発生してから当社の開発担当者が現地入りするまでの時間・解析する時間・手順方法を決定して、リカバリ作業を着手するまでの時間を合計したリカバリ段取り時間が９時間、さらにリカバリ時間が4.5時間で、あわせて13.5時間であった。

(2) リカバリ段取り時間の短縮検討

改善前は、障害発生から当社の開発担当者が現地入りするまでの数時間は何も行われていなかった。 お客様と当社との間で、障害発生時のリカバリ作業に関する取り決めがなかったため、お客様は当社の開発担当者を待ち続ける必要があった。

改善後は、お客様と当社との役割分担を明確にし、両社にてリカバリ作業体制を確立した。障害発生後はまずお客

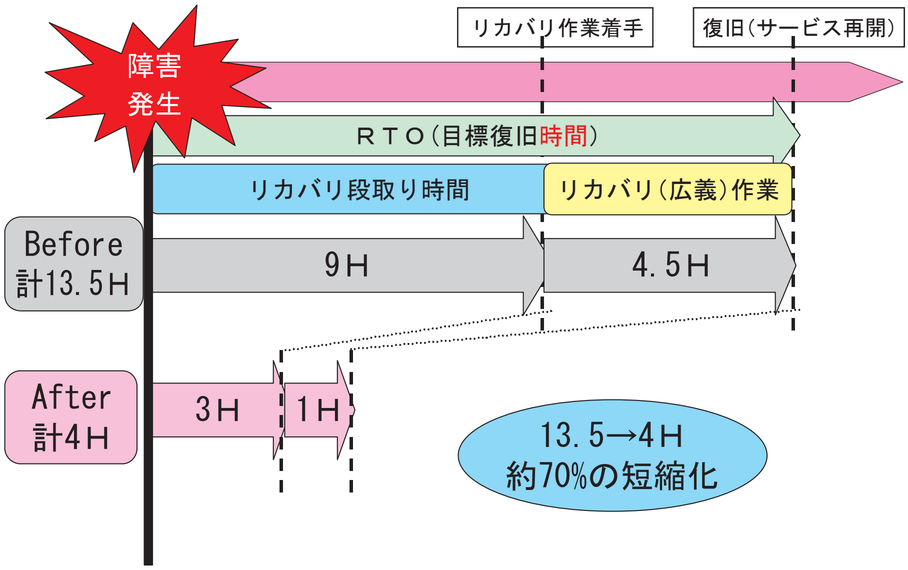

図５　RTO短縮具体例

様にて、手順に基づき障害の一次切り分けと原因解析のためのログやデータの収集を実施していただくことにした。その間に当社担当者が現地入りし、それらの結果を基にリカバリ作業を行うこととした。この結果、試算では従来のリカバリ段取り時間の９時間を３時間に短縮できた。

(3) リカバリ時間の検討

改善前は、構築前のテストで実施したリカバリテストが不足していたことが分かった。

つまり、本システムで導入しているD2D2T方式のバックアップのリストアテストでは、D2Tによるテープからのリストアのみ実施し、D2Dによるディスクからのリストアは実施していなかった。また、手順書にもその手順がなく、今回のリカバリ作業ではD2Dリストアによる高速リストアを実施できなかった。

改善後は、特別に機会を設けD2Dによるリストアテストを行い、手順を確立して手順書に反映した。この結果、従来のリカバリ時間の4.5時間を１時間に短縮することができた

以上の対策検討により、図５で示すとおり改善前のRTO13.5時間を、改善後はリカバリ段取り時間の３時間とリカバリ時間の１時間の合計４時間と大幅に短縮でき、お客様の要請にこたえた。

この実例からRTOの内訳の中で、リカバリ段取り時間がリカバリ時間に比べ長くかかっていることから、人間系のRTO短縮方案であるリカバリ段取り時間短縮の検討が、RTO全体の短縮のために極めて有効であると実証できた。

6. おわりに

本稿では、BCの実現をストレージ基盤の視点から見て、データ損失によるダウンタイムの短縮、つまりRTOを短縮するための方案と実例を紹介した。特に、今まで着目されていなかった、障害発生からリカバリ作業に着手するまでに要する時間を、リカバリ段取り時間と定義し、その内訳とそれを短縮する方案について述べた。これが、後続のリカバリ時間を短縮するため導入した高速リストア機能などの最新技術と組み合わさって、RTO全体を短縮するために有効なことが分かった。

一方、BCの実現は本稿で取り上げた障害回復のほかに、高可用性からのアプローチも必要である。高可用性とは、計画的なシステムダウンだけでなく、不慮の障害発生時にもサービス提供を継続することである。一般的に、クラスタリングソフトや負荷分散装置などを導入し、システムの高可用性を確保している。

当社では、本稿で議論した障害回復のためのデータ保護システムだけでなく、高可用性のためのクラスタリングシステムの提案・設計・構築と保守についても、永年行ってきている。これからも、それら培ってきた技術と経験を柱とし、継続かつ発展的な活動によりお客様のシステムのBC実現に貢献する、IT基盤の技術・サービスを提供していく。

これを新たに、"エクサのBCインフラソリューション"と称し、技術・サービス領域を拡大しつつ、お客様のニーズにこたえるシステムを提供していく所存である。

参考文献

（図書、論文、出所）

1) IDC Japan, (2006)

2) 喜連川優"ストレージネットワーキング技術"オーム社
P.99 (2005.7)

3) 伊藤幸司"先進ストレージ管理ソリューション　～初導入にチャレンジ～"
exa review No.5 P.61 (2005.12)

4) 喜連川優"ストレージネットワーキング技術"オーム社
P.101 (2005.7)