C-016

ディザスタリカバリ構成におけるコピー機能操作のための アクセス権限管理方式

岡田　渡†　　江丸　裕教†　　木原 健一†
Wataru Okada　Hironori Emaru　Kenichi Kihara

1．はじめに

IT 普及により企業情報システムの重要性は高まる一方である．ところが，テロ，災害等によるシステム停止やデータ損失のリスクをゼロにすることはできない．長時間のシステム停止や業務データの損失が発生すると，企業収益に影響を与えるばかりでなく，信用の失墜により企業の存続すら危ぶまれる．このため，上記災害等への対策は必要不可欠である[1].

長時間のシステム停止やデータ損失のリスクを回避するため，ディザスタリカバリ構成が採られる．ディザスタリカバリ構成は，通常運用時に遠隔地にデータの複製を作成することで，障害発生時に複製を用いた迅速な業務復旧を可能にする．近年ではデータを保管するストレージシステムに搭載されるコピー機能を用いたディザスタリカバリ構成が注目されている（以降，この構成をディザスタリカバリ構成とよぶ）．

この構成においてコピー機能の誤操作等による複製作成の失敗や復旧作業の失敗は致命的である．また，ストレージシステムには，一般的に，数千に上る記憶領域が存在しており，複数の業務がこれらの記憶領域を利用している．各業務にとって適切なコピー機能の操作を行うために，業務に合わせて各管理者のコピー機能操作可能な範囲に企業情報システム全体を分割すると共に，悪意のある操作を防ぐセキュリティが必要となる．

本報告では，コピー構成に従い，各管理者のコピー機能操作可能な範囲を動的に決定するための操作権限管理方式を提案する．

2．ディザスタリカバリ構成と課題

2.1．ディザスタリカバリ構成

図１にディザスタリカバリ構成の一例を示す．本構成では，リモートコピー機能を用い正サイトの業務データを副サイトへミラーリングし，さらに，ローカルコピー機能を用い定期的なバックアップを取得する[2].

正サイトには，ストレージシステムと複数の運用系業務計算機が配置される．副サイトにはストレージシステムと複数の待機系業務計算機が配置される．また，配置場所を選ばない管理サーバが存在する．

各業務計算機はそれぞれのサイトに配置されたストレージシステムの記憶領域を利用する．また，管理サーバは，業務の管理者やストレージシステムの管理者の指示に従い，各サイトのストレージシステムと業務計算機を管理する．

ストレージシステム間にはリモートコピー機能が動作する．また，ストレージシステム内部では，ローカルコピー機能が動作する．コピー元の記憶領域とコピー先の記憶領域の組を「ペア」とよぶ．また，ペアのコピー機能を操作することを単に「ペアを操作する」とよぶ．

障害発生時には，副サイトに作成されたデータのミラーまたはバックアップを用いて業務を復旧する．

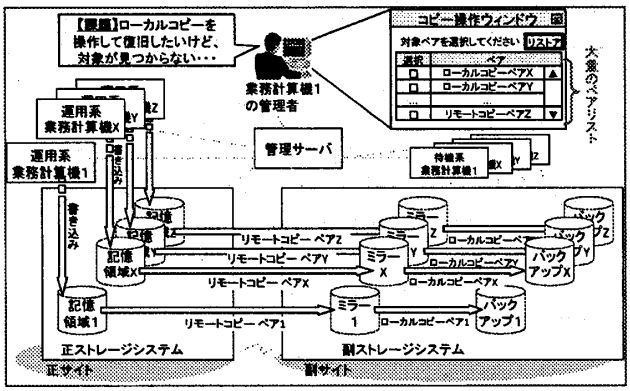

図１　ディザスタリカバリ構成とその課題

2.2．コピー機能操作に係る課題

一般にバックアップのタイミングや業務復旧手順は業務形態に依るため，業務の管理者が業務に適したペア操作を行う必要がある．これを実現するため，従来は，業務の管理者へ，ストレージシステム全体のペアの操作権限を付与していた．

しかし，前述のとおり，ストレージシステムには他の業務用のペアも存在するため，無関係な業務用のペアも操作可能となってしまう．また，ストレージシステムには，全体で数千にも上る記憶領域とそれに係るペアが存在する場合，操作すべきペアの特定には手間がかかり，業務の管理者の負担となる可能性がある（図１）．

3．コピー機能操作権限管理方式の検討

3.1．課題解決とコピー機能操作権限管理方式

上記課題は，業務管理者に付与する操作権限の粒度を，ストレージシステム単位からペア単位へと細分化し，各業務管理者へ業務にあわせて操作権限を付与することで解決できる．

具体的には，業務管理者がペア操作を指示する画面に，操作権限を持つペアのみを表示する．これにより，限られた数のペアのみ表示されるため，操作すべきペアの特定が容易になる．また，同様に，無関係のペアが表示されないため，悪意を持った操作を防ぐことができる．

この操作権限を管理する方式として次の２つの方法を検討した．

(1) 業務計算機指定での管理（図２）

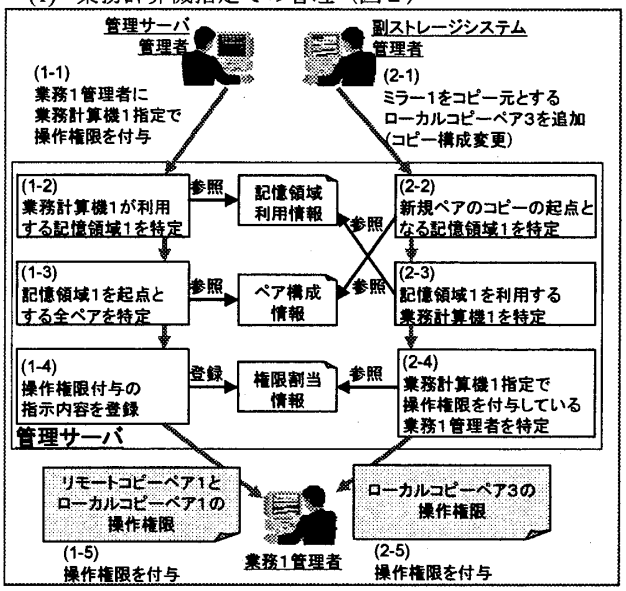

図２　業務計算機指定での管理

本管理方式では，業務計算機を指定して業務の管理者にペアの操作権限の付与を行う．

管理サーバは，ストレージシステムから，各記憶領域とそれを利用する業務計算機の対応情報(表１)，ペアの構成情報（表２）を取得・管理する．また，以下で説明する処理により作成される操作権限の割当情報（表３）も管理する．

計算機	記憶領域
業務計算機1	記憶領域1
業務計算機2	記憶領域2
...	...

表1 記憶領域利用情報

ペア	コピー元	コピー先
リモートコピーペア1	記憶領域1	ミラー1
ローカルコピーペア1	ミラー1	バックアップ1
...	...	...

表2 ペア構成情報

ユーザ	割当計算機
業務1管理者	業務計算機1
業務2管理者	業務計算機2
...	...

表3権限割当情報

ペアの操作権限付与の指示を受け付けると(図２(1-1))，管理サーバは，記憶領域利用情報から，指定された業務計算機が使用する記憶領域を特定する．そして，ペア構成情報からその記憶領域をコピー元とするペアを特定する．そして，特定したペアのコピー先がコピー元となるペアを再帰的に探索し，指定された業務計算機に係る全ペアを特定する（図２(1-2)）．次に管理サーバは権限付与の指示内容(どの業務の管理者にどの業務計算機を指定してペア操作権限を付与したか)を記憶しておく(図２(1-3))．そして，特定したペアの操作権限を業務の管理者へ付与する(図２(1-4))．ペアの操作権限を剥奪する場合も同様の処理で行う．

また，本管理方式では，管理サーバがコピー構成の変更指示を受け付けると，変更内容に応じて動的にペアの操作権限を業務の管理者へ付与する．たとえば、ペアの追加指示を受け付けると(図２(2-1))，管理サーバは，ペア構成情報から，追加するペアのコピー元がコピー先となるペアを探索し，再帰的にコピーの起点となる記憶領域を特定する．そして，特定した記憶領域がどの業務計算機に利用されているかを記憶領域利用情報から特定する(図２(2-2))．次に，その業務計算機を指定してペアの操作権限を付与された業務の管理者を権限割当情報から特定し(図２(2-3))，追加したペアの操作権限を自動的に付与する(図２(2-4))．

(2) ペア指定での管理

本管理方式では，ペアを指定して業務の管理者にペアの操作権限の付与を行う．

操作権限付与の指示を受け付けると，管理サーバは，指定されたペアの操作権限を業務の管理者へ付与する．ペアの操作権限を剥奪する場合も，同様の処理で行う．

また，本管理方式では，コピー構成の変更を行った場合に，変更に応じたペアの操作権限を業務の管理者へ手動で付与する．

３．２．管理方式の比較

悪意のある操作を防ぐためには，操作権限管理に誤りがあってはならない．これを回避するためには，管理者にとってより簡単な管理方式を提供する必要がある．そこで，本検討では，管理の容易性を観点に各方式の比較を行った．

業務計算機指定での管理では，ペアの数に依存せずに１ステップで権限付与操作が完了する．また，ペアの追加に応じて動的に権限付与がなされるため，権限付与操作後の管理が発生しない．さらに，ある業務の管理者に対してその業務が稼動する計算機を指定するのは，直接的で単純な作業である．

一方，ペア指定での管理では，ペアの数だけの権限付与操作を行う必要がある．また，ペアの追加に応じて，手動で権限付与を行う必要があり，権限付与操作後も管理が必須となる．さらに，ある業務の管理者に対してペアを指定するには，その業務が稼動する計算機の利用する記憶領域を特定し，さらにそれに係るペアを探索する必要があり，非常に複雑な作業が必要となる．

以上のように，ペア指定での管理は複雑で難易度が高く，特にディザスタリカバリ構成のような大規模複雑な構成においては，管理の負担が高くなる．よって，より簡単で確実なペア操作の権限管理が可能な業務計算機指定での管理方式を採用する．

４．さいごに

本報告では，コピー構成に従い，管理者のコピー機能操作可能な範囲を動的に決定するための権限管理方式を提案した．なお，本提案の権限管理方式は，実際の製品に適用され，簡単で確実なコピー機能操作の権限管理を実現している．

５．参考文献

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

[2] 鴨志田 毅, "金融機関勘定系におけるディザスタリカバリシステムの構築", 日立評論, Vol 87, 67-70, March, 2005

† （株）日立製作所　システム開発研究所