大容量オンライン・ファイルシステムにおける ファイル，メッセージの安全管理について

竹井大輔† 井上　健†

1. まえがき

座席予約システム，銀行システムに代表される大容量のオンライン・ファイルシステムは，そのファイルに収容される情報量が膨大なこと，その取扱い対象が社会生活と密着していること，さらに，全国規模のサービスエリアを持つこと等の理由により，ひとたびサービス停止の状態に至ると，一般利用者に大きな支障を与えることになる．

ここでは，それらのシステムの安全対策として，ファイル，トランザクション，メッセージの保護，管理，および障害時の回復方式について述べるものである．

2. ファイルの管理

ここで述べるファイルシステムのモデルは，図1に示す構成からなるものとする．すなわち，データファイル (DF) は一般に端末からの情報により更新される在庫管理形のファイルである．また端末ファイル(AF)は，端末毎に出力情報を管理し，障害時の情報の再送等に供するためのファイルである．さらに，端末からの入出力情報，および処理結果を記録するのにトランザクションファイル (TF) がある．

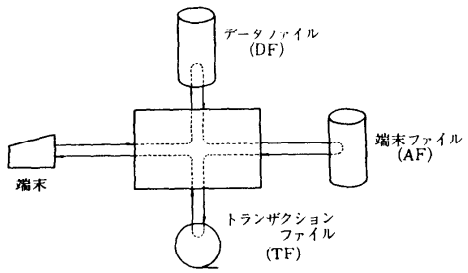


図 1　ファイルシステムのモデル

† 日本国有鉄道電気局通信課

一般に，データファイル，端末ファイルは，高いトラフィックに対処するためランダムアクセスファイルが用いられ，トランザクションファイルは，その量が多く，かつブロッキングが可能なため磁気テープが用いられるのが通例である．

2.1 ファイルデータの作成・変更

一般にデータファイルに収容される被更新データおよびそれに付属するコントロールデータは，それ自身独立して存在するものは少なく，他の種々のテーブル，ファイルとリンクしているものが大部分を占める．

したがって，データファイル等を新規作成，変更する場合は，当然これら関係するテーブル，ファイルとの相互の論理性を厳重にチェックしなければならないが，このような場合，これらの作成・変更作業を個々に行うことは，オペレーションの繁雑さ，それに伴なうエラーの増加，また結果の確認に手数を要することに通じるので，できるだけソースデータの一元化を行い，ソースデータの追加，変更のみにより，すべての関係するファイルへの追加，変更が行えるようにすべきであろう．

また，ソースデータより，実際にファイルへデータの書込みを行う場合は，一般にオンラインサービス時間外に行なう方が，種々のエラーに対する対策上，安全であることは明白であるが，現実の問題としては，オンラインサービス時間の延長とそれに伴なうオフラインメンテナンス時間の短縮，ファイルメンテナンスの緊急性等の理由により，オンラインサービス時間帯でそれらのファイルメンナンス作業を行うことが不可避となってきている．

したがって，オンラインサービス時間帯にファイルメンテナンスを行なうための安全対策として，端末からの要求とメンテナンス作業とが競合した場合，同一データの更新を避けるため，該当データへの端末からのアクセスを一時禁止すること，および，ファイルメ

ンテナンス中にシステムダウンが発生した場合にそなえて，該当データを復元し，再試行するために必要なデータの磁気テープ等への事前退避の手段を講じておくことが必要であろう．この場合，端末からのアクセス禁止が連続して行われると，オンラインサービスの低下となるので，大量のデータによるファイルメンテナンスの場合は，連続してアクセス禁止の処置をとらぬよう，きめ細かな制御が必要となる．

また，中央のファイルデータに対する変更が，中央のみでなく，端末側からも要請される場合は，一般端末のうち，特定なものに，データメンテナンス機能を許し，中央におけるデータメーテナンス作業を軽減することができる．この場合，その特定端末の番号，操作コード等をキーとして，それ以外の端末からの操作を禁止する処置をとる必要がある．

2.2 ファイル処理方式

オンライン・リアルタイムシステムの基本条件は，想定されるトラフィックを，定められた応答時間内に処理することである．この基本条件を満足し，かつ信頼性，可用性，拡張性，経済性を併わせ考慮して，処理方式が決められるわけである．

ファイル処理に関しても，処理中に生じた障害をいかに検出し，被害の範囲を最小限にくいとめるか，また障害発生後は，いかに，速く，確実に，そして簡単に元の状態に戻すか，の二点を安全対策の中心として考えながら，一般の処理を考えていかねばならない．そして，これら処理方式は，単純なものから複雑なものまで，多岐にわたるが，いずれにせよ，業務の重要性，処理能力，異常時対策のバランスを考えながら設計していかねばならない．

まず，ファイル方式として，シングルファイル，デュアルファイルの各方式がある．

（1） シングルファイル

一般に，そのファイルに障害が起こると，オンラインで更新されているファイルの場合は，すぐに回復することが困難である．ファイルをある時点にダンプされた状態に戻し，その時点から，障害時点までのトランザクションによって，ファイルを再製していく方法が一般的だが，長時間を要する．したがって，リードオンリーのファイル，または，サービス停止時間がある程度長くなっても差しつかえないシステムでは，この方式で十分であるが，端末側を長時間停止させることのできないシステムでは，運用上，大きな支障があろう．

（2） デュアルファイル

長時間のサービス停止が許されないシステムでは，前述のトランザクションをもとにしたファイル回復を日常的な手段とすることは，運用上支障するので，迅速なファイル回復のためには，この方式をとるべきである．すなわち，この方式では，障害時には，正常な系のファイルの内容を，予備の系に移して，短時間でデュアルファイルを構成することができるし，緊急の場合には，そのまま，正常系のみをシングルファイルとして，構成することもできる．もちろん，この場合も，両系ファイルの同時障害にそなえて，トランザクションによるファイル回復の手段を残しておかねばならないが，その使用確率は，きわめて低いものとなろう．

正常時におけるファイル処理方式は，データの読出し，書込み時におけるチェックをどの程度行なうかによって異なる．

まず，データ書込み時に，他のトランザクションよりアクセスされないよう，該当デバイスにホールドする必要が出てくる．デュアルファイルの場合，そのホールドが両系にわたるため，その間，他のトランザクションは待たされることになる．回復処理の段階においては，このホールド期間が十分長い方が安全ではあるが，ここが処理能力を上げていく上でのネックになる場合があり，やはり，必要最小限におさえるべきであろう．

つぎに，データが正常に書かれたことをチェックするための方法として，リードアフタライトチェック，デュアルファイルにおける両系の照合チェックなどが一般的だが，これらのうち，どれを採用するかは，その後の異常処理をいかに変えるか，それが失敗した場合に，安全側の処置がとれるか，また，ファイルへのアクセス回数の増加によって，どの程度，全体の処理能力に影響を与えるか，により決るものと考えられる．

たとえば，国鉄の座席予約システム・マルス 105 にては，デュアルファイル方式で，更新するファイルに対しては，上記のチェックは一切していないが，読出し，書込みが正常にできておれば，そのデータの内容については，サイクリックチェック等により，ほとんど信頼できるという実績がある．

2.3 異常時のファイル回復方式

異常時におけるファイルの状態としては，大別して次の二つの状態が考えられる．すなわち，ファイルの

読出し，書込み時の異常の場合に，ファイルをいかに保護し，元のレベルのサービスを維持するかという場合と，ファイル処理途中に，システムダウンとなった場合，処理中のトランザクションの紛失，重複を防ぎファイルを回復する場合である．いずれの場合にも，これらのファイル回復処置は，システムの回復処置を含めて，できるだけ単純明快にする必要がある．複雑高級な処理は，いざというとき不安がともなうからである．

（1） デバイス異常の場合

一般に，デバイス異常のため，データの読出し，書込みが一定回数の再試行を行なっても不能の場合は，そのトランザクションは，処理不能として端末に返される．それと同時に，デバイス管理テーブルの該当デバイスのところには，アクセス禁止のフラグが立てられる．この場合，無条件にアクセス禁止とするのではなく，そのファイルの重要性等を考慮して，基準値を設け，その値を越えた場合，アクセス禁止の処置をとり，オペレータにその旨を通知する．

その後の処置としては，デュアルファイルでは，残った正常系の内容を，予備のデバイスに移しかえ，その後，アクセス禁止のフラグを消して，回復させる．

シングルファイルの場合は，まず，最新の該当ファイルの内容をダンプしたものをつかって，ある時点の状態にファイルを戻す．このファイル内容のダンプはその周期が短ければ短いほど，ファイル回復に要する時間が短くてすむが，ダンプの回数が多くなる．したがって，これらの障害が実際発生した場合，どの程度，システムに影響を与えるか，で回数をきめるべきだが，毎日の運転作業に定例的に組込み，1日1回ダンプしている所が多い．

つぎに，ダンプした時点からのトランザクションファイルから，逐次情報を読出し，データファイルを更新していく．この場合，処理時間をできるだけ短縮するため，メモリの許すかぎりマルチ処理を行うべきであり，かつ，データファイルへのアクセスも，多種のテーブル，ファイルをたどらずに，直接行えるようトランザクションファイルの内容も，データファイルのアドレスを含むようにしたい．

また，回復処理中に，何らかの異常により，トランザクションファイル内の情報と，それに対応するデータファイルの情報が，論理的に矛盾する場合が生ずることがある．このような場合は，その旨，オペレータに通告し，オペレータが安全側に処置できるよう，その情報を，打出す等の処置を行なわせる必要がある．

（2） システムダウンの場合

システムダウン時において，トランザクション，ファイルの回復を行う場合，そのトランザクションが，その時，どんな処理状態にあったかで，回復処理が大いに異なる．すなわち，更新をともなうファイルシステムでは，まだファイルを更新しないトランザクションはシステムに何ら影響を及ぼさないと同じなので，システムダウン時には，捨て去っても差しつかえない．

そこで，トランザクションがどの処理状態にあるかを示す処理状態フラグを各トランザクション毎に設け，システムダウン時に，そのフラグの状態によって回復を行う．特に，ファイルの状態を中心に考えれば，図2に示すように，フラグの表示を変化させればよい．このフラグを利用して，ファイル回復処理を行う前提として，処理途中のトランザクションの内容が正常であることが必要である．したがって，回復処理に先立って，ダウン時，処理バッファに残されたトランザクションの一部のサムをチェックすることによりそのトランザクションの有効性を確認する．

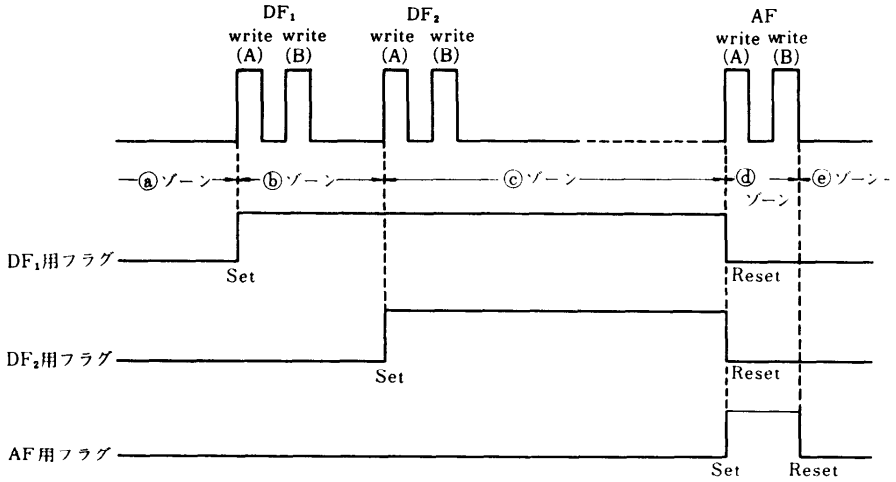
このトランザクションが信頼できない場合は，内部における回復は不能となるので，その対策として，そのトランザクションをラインプリンタ等に打出し，オペレータにその装置を委ねるか，または，そのトランザクションを捨てた場合，システムとしてつねに安全側の処置をとるようにするを考えねばならない．

トランザクションが有効な場合は，フラグ表示に従って，表1に示すような回復処理を行う．ここで関係ファイルについて，A→B を行うのは，デュアルファイルの場合，A処理済，B未処理の場合があるので，両系を一致させるためである．

また，フラグのセット，リセットの微妙なタイミングでダウンすると，ファイルを更新しているのにフラ

表1 ダウン時のファイル回復処置

ダウン発生個所	フラグ表示 DF_1	DF_2	AF	処置
ⓐゾーン	0	0	0	何もしない　トランザクションは無効
ⓑゾーン	1	0	0	$DF_1(A)\rightarrow DF_1(B)$, トランザクションから $DF_1(A)(B)$ を元に戻す
ⓒゾーン	1	1	0	$DF_2(A)\rightarrow DF_2(B)$, トランザクションから $DF_1(A)(B)$, $DF_2(A)(B)$ を元に戻す
ⓓゾーン	0	0	1	$AF(A)\rightarrow AF(B)$　トランザクションは有効
ⓔゾーン	0	0	0	何もしない　トランザクションは有効



DF_1, DF_2, AFはデュアルファイルである.

図 2 ファイル処理手順とファイル用フラグ表示

グがセットされない場合（図 2, ⓒゾーンとⓓゾーンの境界）や，フラグをセットして，ファイルアクセスする前にダウンした場合のようなことが生じる.

この場合は，トランザクションが正常であるにもかかわらず，捨ててしまう可能性もあり，その確率は非常に低いが，やはり安全側に処理することを考えねばならない.

さらに，AF（端末ファイル）書込み後のダウンは，送信中のエラー等を含めて，後述する端末からの申告方式を採用し，いたずらに，微妙なタイミングのファイル回復を複雑にせずに，端末オペレータの簡単な判断に委ねることも可能である.

3. メッセージの管理

中央装置におけるファイル処理，およびその回復処理が正常に行えても，端末に正常なメッセージが返されるという保証はない. そこで，端末までを含めたメッセージの管理を考えねばならない.

3.1 前提

（1） 端末オペレータ

ここで取り上げているシステムでは，端末からの要求メッセージに応じて中央がファイル処理をして，その結果回答メッセージを端末が受信するという Inquiry 形のメッセージを扱っている. そこで端末には常時オペレータが居ると考えてよい.

（2） メッセージの紛失・重複

ファイルシステムでは一般に端末の受取るメッセージについては，

（a） 紛失してはならないし，

（b） 重複してもいけない

場合が基本である. もちろんメッセージの種類によっては（例えばファイル内容の照会など），(a), (b)を考えなくてよいであろう. (a), (b) の管理をするために中央の行なったファイル処理の結果は必らず端末に出力されなければならない. つまり端末が正常に回答メッセージを受信できない場合，中央では更新後のファイルを更新前の状態に戻すことを考える必要がある.

（3） 端末の操作

端末オペレータは，正常に回答メッセージが受信できなければ，再度同一操作することを原則とする.

3.2 障害の発生

（1） 障害発生のタイミング

障害の発生するタイミングとして端末からの要求メッセージに対する中央の処理が，

（a） ファイル更新前か，

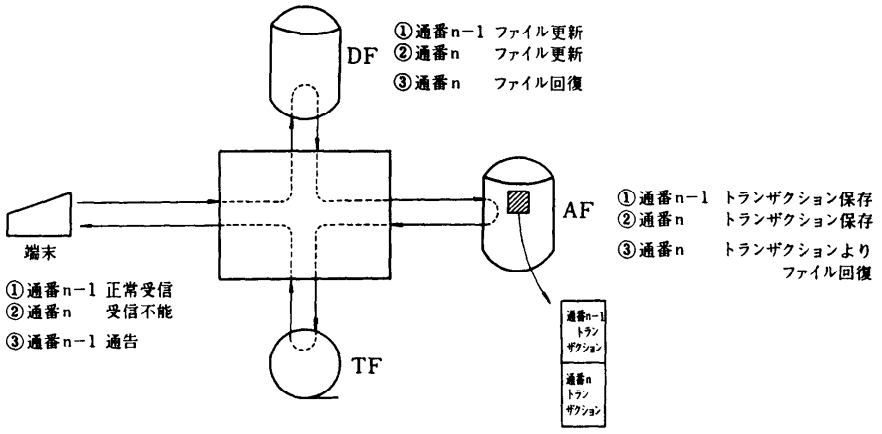
（b） ファイル更新後か

の 2 通りがある. (b)の場合，何らかの方法でファイル回復をすべきである.

（2） 障害原因

原因として 3 種類ある.

（a） 中央側の障害でシステム停止に到るときと部分的な異常がある. システム停止時のファイル回復については，2.3 (2)に述べた.



解　説

① 端末からのファイル更新要求に対して通番 n−1 を付与した．

② 端末からのファイル更新要求に対して通番 n を付与したが端末で受信できなかった．

③ そこで，端末から，通番 n−1 までは有効な旨を通告し AF よりトランザクションを参照してファイル回復を行なう．

④ その後，端末では，②の操作を再度行なう．

図 3　端末ファイルによるメッセージの管理

（b） オンラインシステムであるので伝送路においてフェージング，端局の障害，集線装置交換機等の障害が考えられる．

（c） 端末において，紙づまり，紙切れ，プリンタ不良等による障害があろう．

3.3 処理方式

ファイル更新後ある条件により更新前の状態に戻すためには一時的にそのトランザクション情報を保存しておかなければならない．そこで保存箇所として，つぎの，三つの場合が考えられる．

（1） 磁気テープに保存した場合

オンライン中の障害時に磁気テープよりトランザクション情報を見つけ出すことは困難であろう．

（2） メモリに保存した場合

伝送制御手順上，端末から回答メッセージに対する肯定応答のないとき保存箇所に記録されてトランザクション情報を参照してファイル回復を行う．

回線用バッファを使用すると肯定応答のないときファイル処理のタスクを起動する必要がある．

タスク処理バッファを使用すると中央と端末のデータリンク解放までタスクを専有してしまい処理能力に影響を与える．またマルチタスク化してもコア容量が問題となろう．

この方式では端末のオペレータには負担をかけないが，手順上肯定応答を受けても端末が正常受信できない事態のときファイル回復が困難となる．

（3） ランダムアクセスファイルに保存した場合

端末と中央とで通番管理をすると都合が良いと思われる．端末ごとのトランザクションに中央が通番を与える．端末オペレータは期待した回答を受信できないときには通番通告することにより中央がメッセージの管理をする．

この方式は端末のオペレータに負担をかけるが訓練されたオペレータであれば困難でないし，(2)の欠点である肯定応答を受けても端末が正常受信できない事態でも矛盾がおきない．さらに端末から肯定応答のないとき端末オペレータに次の操作として通番通告を行なわないと，端末操作をロックさせるようにプログラムを作っておけば通番抜け（メッセージの紛失）が避けられる．

端末ファイルを持つことにより次の利点が生じる．

（a） 端末の通番通告時にメッセージの再送を要求すれば端末ファイルを参照して再送できる．

（b） 端末対応にオンライン中に保存しておきたい情報（例えば端末の取扱い件数など）をもてる．

3.4 コンピュータ結合への応用

ファイル処理を行なうコンピュータに他コンピュータを結合させる場合ファイル回復のやり方として 3.3

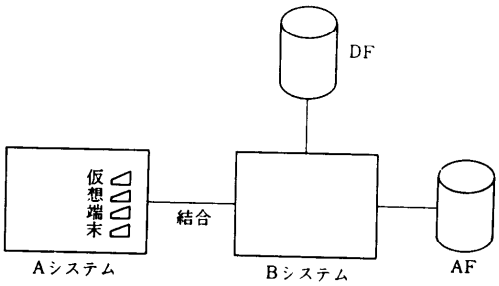


図 4 コンピュータ結合のモデル

に述べた方式を応用できると思われる．図4に簡単なモデルを示す．

Aシステムに仮想端末という概念を導入して仮想端末とBシステムとの間で通番管理を行なう．端末の場合通番通告を端末オペレータに任せたが，仮想端末の場合同じことをAシステムのプログラムがサポートすれば良い．Aシステムの仮想端末の数はトラヒック量から決定されよう．

4. おわりに

社会生活の高度化に従って，ますます大型化するオンラインファイルシステムは，今後，いっそう日常生活と密着したものとなっていくであろうが，その期待に応える意味からも，システムにおける安全管理をさらに高めなければならないと感ずる次第である．

(昭和48年8月28日受付)