4M−3

FTS(Fault Tolerant System)評価における自動検証技術

井口　祐一　　誉田　直美　　赤尾　圭昭

日本電気（株）

1．はじめに

今日の情報処理社会において、コンピュータシステムが社会の中枢を占めることになってきたことに伴い、システムの高信頼性・高運用性が高く望まれている。そこで、FTS（Fault Tolerant System）に対する期待も大きくなってきている。このフォールトトレラント性を実現する方法として、複数ホストの疎結合接続でのホットスタンバイ方式がある。最近では、大規模ネットワーク化の波を受け、フォールトの発生による業務処理ホストの切り替え時に、端末とホスト間の転送データが欠落したり、二重に処理されたりしないような機能が要求されている。今回、このような機能を自動的に検証する技術を開発したので報告する。

2．システムの概要

検証の対象となるシステムは、高信頼性・高運用性を目指し、フォールトの発生時に、迅速に業務を再開するとともに、フォールトの位置を決定し、リカバリを行う機能を備えている。システムは、複数ホストが疎結合接続されており、稼働系ホストと待機系ホストからなる。稼働系ホストでは、オンライントランザクション処理業務を、待機系ホストでは、バッチ業務、開発及びテストを行う。ホットスタンバイ方式では、稼働系におけるオンライントランザクション処理業務の継続が不可能となるようなフォールトが発生した場合、その業務を速やかに待機系で継続し、稼働系の復旧を行う。

これらを実現する為には、次の3つの重要な機能が必要である。

・業務実施ホストの高速切り替え

・運用状態の引き継ぎ

・端末からの入力データの引き継ぎ

これら3つの機能のうち、特に検証の対象とした「端末からの入力データの引き継ぎ」機能について説明する。

従来のホットスタンバイ方式では、ホストの切り替え時に、オンライントランザクション処理業務用端末のセッションの再接続を行っていた。しかし、高速切り替え機能により、待機系ホストとネットワークプロセッサ間で待機セッションを張っておくことで、セッションの切断が発生せず、端末はホスト切り替えを知る必要がなくなった。そのため、セッション再接続時に端末からデータを再投入し、業務を継続する必要もなくなった。一方、ホストが受信した入力データは、メモリ上で管理されており、ホスト切り替え時に失われてしまう。そこで、ホストでのデータ処理が終了するまで、ネットワークプロセッサ内に、端末からの入力データを保持する機能を備えている。ネットワークプロセッサは、ホスト切り替え時に、旧稼働系ホストでのデータ処理が終了していないデータを、新稼働系ホストに送出する。

図2．1にホスト切り替え前後の様子を示す。

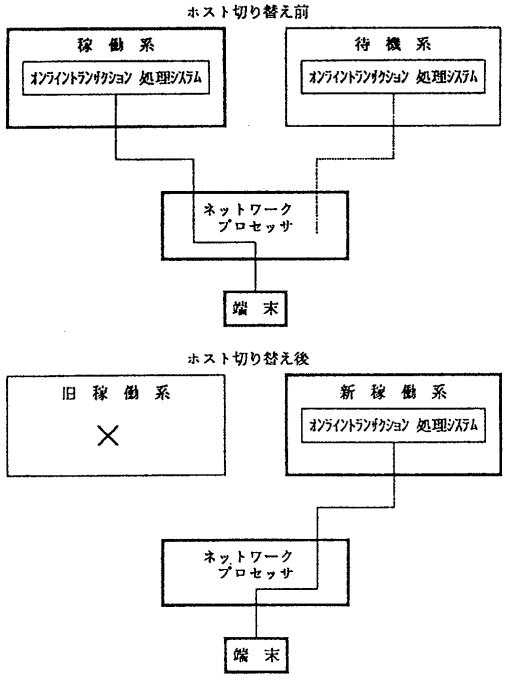

図2．1

Automatic Verification Technique
in Fault Tolerant System Quality Assurance System
Yuichi IGUCHI , Naomi HONDA , Yoshiaki AKAO
NEC Corporation

3．検証技術

検証システムの構成を図3．1に示す。

ホスト1は稼働系、ホスト2は待機系である。ホスト3には、端末シミュレータを配置する。

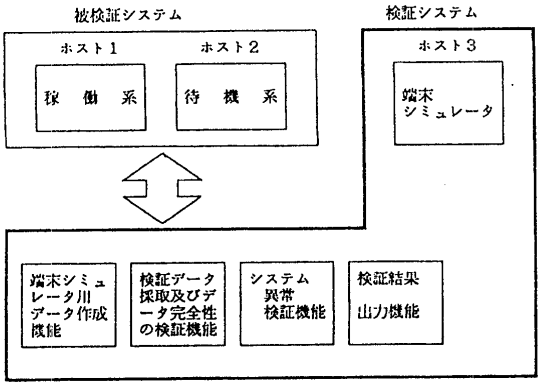

図3．1

検証システムにおける処理の流れと、被検証システムにおけるイベントの発生状況を図3．2に示す。

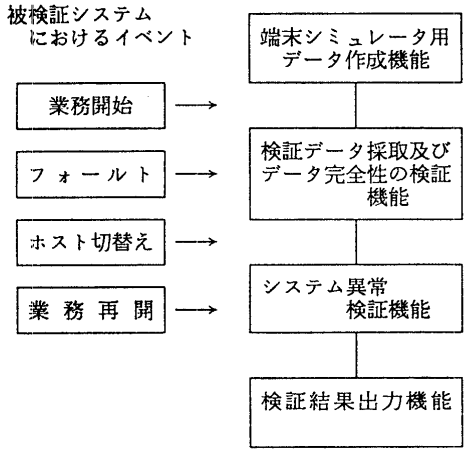

図3．2

検証システムが有する4つの機能について、詳細に説明する。

（1）端末シミュレータ用データ作成機能

端末シミュレータ用ファイルには、検証に使用するトランザクションへの入力データが、端末シミュレータ用に編集されて格納されている。端末シミュレータ用データ作成プログラムは、端末シミュレータ用ファイルのデータの中で、端末からの入力に当たる部分に、端末ごとに順次番号を付加する。端末シミュレータは、端末シミュレータ用のデータを読み込み、稼働系のオンライントランザクション処理システムにデータを送出する。

（2）検証データ採取及びデータ完全性の検証機能

被検証システムのオンライントランザクション処理システムは、端末シミュレータからのデータを受信後、指示された処理（該当トランザクションの起動等）を行う。起動されたトランザクションは、通常のデータ処理（ユーザDBの検索・更新等）に加えて、データ処理の完了を記録するために、検証システムのサブロードモジュールを呼び出す。サブロードモジュールでは、処理済みデータ管理ファイルを、端末IDをキーにして、更新を行うことで、検証に必要なデータを採取するとともにデータの完全性を検証する。トランザクションは、全ての処理が終了した時点で、必要なデータを端末シミュレータに対して送り返す。

データの完全性の検証は、以下のように行う。

①端末からホストへの送信データの欠落

検証システムのサブロードモジュールは、各トランザクションが受信した入力データの順次番号が、処理済みデータ管理ファイルの該端末の順次番号より2以上大きい場合、データの欠落が発生した旨、トラブル状況一覧ファイルに記録する。

②データの二重処理

フォールトの発生によるホスト切り替え時に、ネットワークプロセッサからホストへ送られたデータが、トランザクションで完全に処理される前に消失した可能性がある場合、データは再処理される。その際、該データが二重処理されていないか確認する。すなわち、トランザクションが受け取った入力データの順次番号が、処理済みデータ管理ファイルの該端末の順次番号と等しいかどうかを検証システムのサブロードモジュールが検証する。二重処理が発生した場合、トラブル状況一覧ファイルに記録する。

（3）システム異常検証機能

被検証システムの処理が終了した時点で、以下のような検証データの分析を行うため、検証プログラムを実行する。その結果、異常を発見した場合、トラブル状況一覧ファイルに記録する。

①通信トレースの検証

各ホストの通信トレースを突き合わせることにより、ホストと端末間の転送データの欠落、二重転送等の異常が発生していないか検証を行う。

②端末シミュレータのモニタ情報

端末シミュレータのモニタ情報をもとに、通信トレースをチェックすることで、端末からの入力データの内容が誤って転送されていないか検証を行う。

③稼働情報

被検証システムのシステム関係（メモリ管理、入出力管理等）、オンライントランザクション処理システム、通信管理等のサブシステムの動作結果について検証を行う。

④オンライントランザクション処理システムのモニタ情報

トランザクションの終了状態、CPU／ELAP時間、データ送受信及びデータ処理結果に異常がないか検証を行う。

（4）検証結果出力機能

トラブル状況一覧ファイルを入力として、トラブル内容の分析を行い、その結果を編集出力する。

4．おわりに

この自動検証技術により、ホットスタンバイ方式における端末とホスト間のデータの完全性について、効率的な検証が可能になる。また、あらゆる面からのデータをチェックすることで、システムの矛盾を確実に発見することができる。今後は、検証のみでなく、自動評価システムとして、評価環境の設定機能、フォールト発生のタイミングを指定可能にする実行制御を開発することで、さらに効率的に確実な検証を実施可能にする。

参考文献：

相澤、川西、山元；
「高信頼性を追及した〔ACOS−4／XVP〕」
NEC技法 Vol45 No.1 PP60〜63

相澤、富山、今井；
「ACOS−4／XVPによる高運用性／高稼働性」
NEC技法 Vol45 No.1 PP64〜66