7K−8

連続運転システム SURE SYSTEM 2000のOS SXO (7)
− 遠隔監視・保守サービスの基盤技術 −

山口 正人
富士通愛知エンジニアリング(株)

1. はじめに

SURE SYSTEM 2000は，複数CPU構成，DISKの二重化により，ハード／ソフト障害（以降，単に障害と略す）が発生しても障害部品を切り離してシステムを停止することなく稼働し続けることができる．

しかし，全く問題が無い訳では無く，システム運用や業務に対して次に示すような影響を及ぼすことがある．

また，24時間運転のため，無人化で運転する場合が多く，従来の保守手法では適用できなくなって来ている．

CPU 障害：正常状態のCPUに負荷がかかるため，業務のレスポンスが悪化する．

DISK障害：一時的に二重化から一重化に切り替え運用するが，修復までの間にさらにDISK障害が発生すると，システムが停止する可能性がある．早急に二重化に復元する必要がある．

このように，連続運転システムにおいても，障害を迅速に対応する必要があり，次のような課題を解決して行かなければならない．

- 障害の早期検出
システムの障害を早期に検出し，対処できるようにする必要がある．
- メーカでの迅速な対応
連続運転システムでは無人運転する場合が多いため，システム障害をユーザ経由では無く，メーカに直接通知して迅速に修復できる方法が望まれる．

2. 従来の問題点

2. 1 障害の検出

従来，計算機の利用者が障害を知る方法は大きく分けると次の2つであった．

1) システムの停止
従来のシステムでは，システムが停止したことで，障害発生を知る場合も多かったが，連続運転が可能でかつ無人運転を可能とするSURE SYSTEM 2000ではこの方法は適用できない．

2) コンソールの利用
従来のシステムではコンソールに表示されるメッセージから，障害発生を知る方法が一般的てある．

しかしコンソールメッセージはオペレータの介入要求などに広く利用されており，操作者がコンソールに表示される障害発生メッセージを見逃す可能性が高いことや常時コンソールを監視していなければならないという問題があった．

上記を解決する目的でプログラムによりメッセージを解析する手法も実現されている．しかし，メッセージの追加，変更への柔軟な対応が困難なことやメッセージは「資源種別」と「障害内容」の組み合わせの数（従来システムでは数百個のメッセージ）だけあることから，解析するために大量のメッセージと比較が必要であり，処理STEP数が増大するという問題があった．

Operating System SXO for Continuously Operable SURE SYSTEM 2000 (7) - The Technique for Remote Maintenance and Supervisory Service
Masato YAMAGUCHI
FUJITSU Aichi Engeneering Ltd.

2. 2 メーカへの連絡と対処

障害を検出したユーザからメーカに電話連絡が入り，その時点で初めてメーカはユーザシステムで障害が発生したことをを認識できる．

このため，人手の介入による通知の遅れと適切な障害情報の入手が難しいく，障害の解決時間（MTTR）が長くなるという問題がある．

3. システム障害管理の方式

当レポートでは次の問題を解決する方式を論ずる．

− 漏れの無い障害の検出
− メッセージの追加や変更への容易な対応
− 少ない処理Stepで障害分析
− メーカへの迅速な通知と障害の解決

3. 1 漏れの無い障害の検出

コンソール画面を見て目視によって障害を検出する方式では無く，プログラムで障害を検出することにより漏れを無くす．

3. 2 メッセージの追加や変更への容易な対応

メッセージはコンソール画面に表示してオペレータに各種介入要求を表示することを目的とし，障害を検出するためには別途，障害発生事象として体系化することにより，両者を完全に分離する．

3. 3 少ない処理Stepで障害分析

障害発生事象を「資源種別」と「障害内容」としてコード化することにより，障害が発生した資源が重要資源（CPU,共用メモリ，DISK，IO-BUS，IOアダプタ）かどうか，および障害内容が永久障害か間欠障害かを分析しやすくする．

3. 4 メーカへの迅速な通知と対応

装置の永久障害などメーカが対処しなければならない障害は，直接，当該システムからメーカの保守センタへ障害の発生と発生原因（例えば，どの装置のどの部品が故障したなど）を自動通知し，直ちに保守部品を持参したカスタマエンジニアが出動できるようにする．

4. 実現方式

ここでは，上記の様々な問題を解決すべく，SURE SYSTEM 2000において実現した遠隔監視・保守サービスの基盤技術について論ずる．

4. 1 障害事象の体系化

1) メッセージと障害事象の分離
システムの内部では全て障害事象で処理を実施する．コンソールへメッセージを表示する場合，障害事象と対応したメッセージへ変換する方式とした．
図1にメッセージと障害事象の分離を示す．

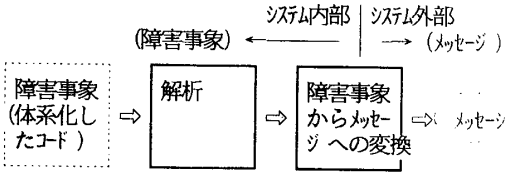


図1　メッセージと障害事象の分離

2）障害事象のコード化
「資源種別」と「障害内容」で障害事象を体系化した．その概要を図2に示す．
体系化にあたっては次の考慮をしている．
－ 資源種別については重要度の高いものから順に数値化している．
－ 障害内容については，影響度の高いものから順に数値化している．

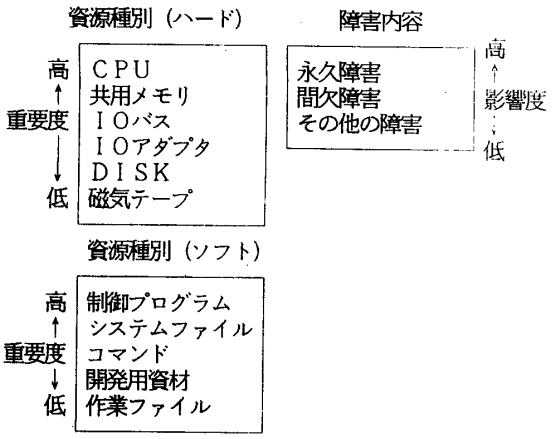


図2　障害事象のコード化

3）重大障害の検出方法
次に，障害事象からシステム運用に重大な影響を与える障害の検出例を示す．

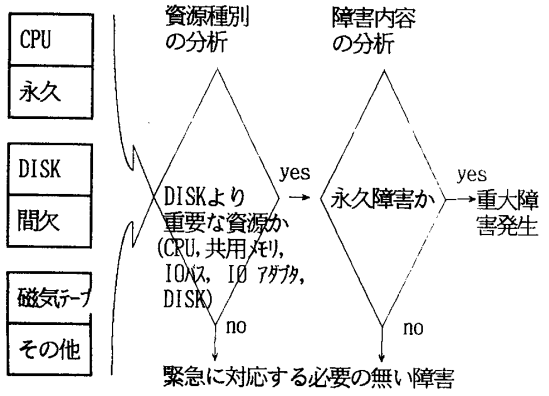
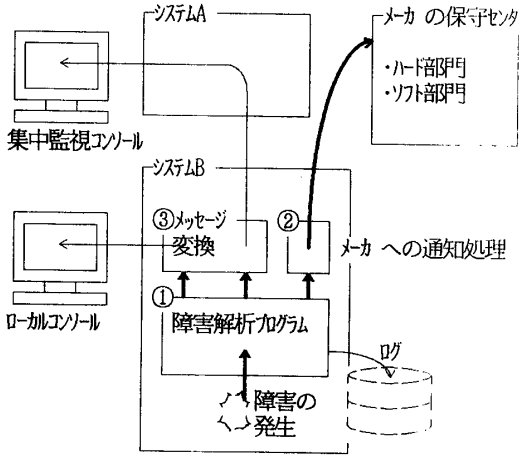


図3　重大障害の検出方法

4．2　メーカへの通知と対応

システムの運用に重大な影響を及ぼす障害が発生した場合は，コンソールにメッセージを表示するとともに，自動的にメーカの保守センタに通知する．図4にメーカへの障害通知方法を示す．



① 障害解析プログラム
障害の発生をロギングすると共に，障害事象の「資源種別」「障害内容」から，運用に影響を及ぼす重大障害かどうかを分析する．重大障害はメーカへの通知処理へ伝達する．

② メーカへの通知
障害が，どの装置のどの部品で発生したか特定し，メーカの保守センタにカストマエンジニアの緊急出動を要求する．

③ メッセージ変換
障害事象を対応するメッセージに変換し，コンソールへ表示する．

図4　メーカへの通知方法

5．今後の課題
現在，障害事象のコード化はOSが管理している資源を全て体系化し，メーカへの障害自動通知などに利用できるようになった．
今後は，コード化の範囲をユーザアプリケーションが管理する資源まで広げ，ユーザ業務に影響を与える資源全てに適用できるように拡張する予定である．