3.7 バックアップ切替え失敗に関する教訓（T7）

教訓 T7　バックアップ切替えが失敗する場合を考慮すべし

問題

冗長化構成を取っていても、障害時、バックアップ切替えが正常に機能しなかったり、障害機器の切離しによる縮退運転が正常に機能しなかったりと、システム稼働の継続ができない事例が後を絶たない。

A社の基幹システムは、デュプレックスシステムでのホットスタンバイ構成をとっている。稼働系システムのハードウェア障害が発生し稼働系がダウンした（図3.7－1①）。障害検知にともない自動的にバックアップ切替え処理が駆動され（図3.7－1②）、待機系システムを稼働させようとしたが、待機系が立ち上がった後のオンライン処理が障害となり、待機系もダウンした（図3.7－1③）。このとき、現場が混乱し、後の対処方法の決定まで多くの時間を要した。最終的に、稼働系のハードウェア故障の部品を交換し、再度、稼働系を立ち上げて処理を再開させた。

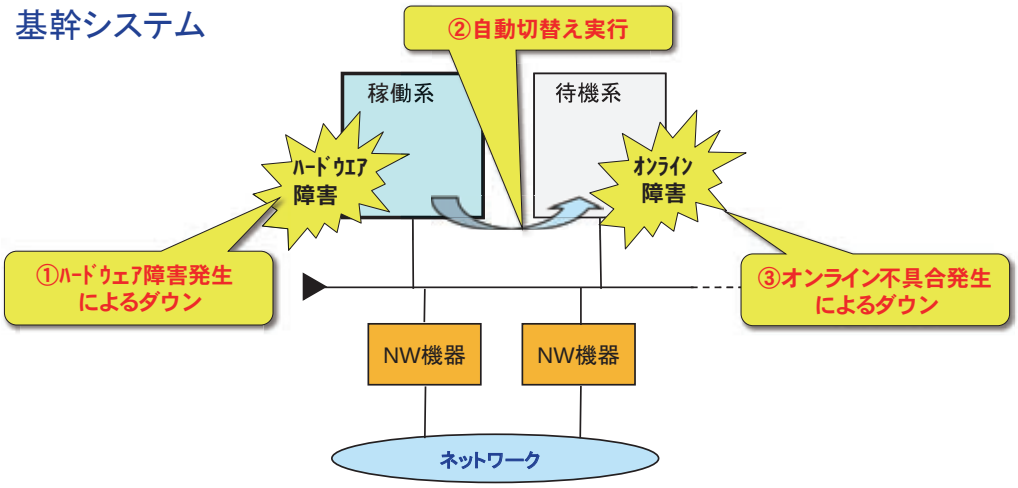

図3.7－1　障害状況

原因

バックアップ切替え時障害の直接原因は、以下の 2 点であることが分かった。

【原因 1】切替え失敗の直接原因

以前、障害が起きた際の緊急対応時に、稼働系へのソフトウェアのパラメータ設定変更を行った後、同様に待機系にもこの対応をする必要があったにも関わらず、これを怠った。さらに、稼働系と待機系の同期を取るべきソフトウェアパラメータと、それぞれの系で独自に設定するソフトウェアパラメータがあるが、それらの管理を怠った。

【原因2】復旧時失敗の直接原因

稼働系のパラメータを基に、待機系のパラメータを最新化しようとしたが、稼働系と待機系で独自に設定するパラメータが分からなかったため、修正を素早く実施することができず、待機系からのオンライン再立ち上げをあきらめざるを得なかった。稼働系のハードウェア復旧を行ってから、稼働系で再立ち上げを行ったため、復旧に大幅な遅れが出てしまった。

稼働系システムは変化するため、それに合わせて待機系システムも同期を取る必要があるが、日常の運用で検証していく仕組み（切替え実施、同期チェック、手動切替え手順書の更新等）を作らないと待機系システムは取り残されていく。

根本原因は、待機系システムを本番運用の重要な機能であるとの観点が不足しているため、日常の運用で待機系システムの検証が十分行われていないために起きている。

対策

バックアップ切替えは、本番運用であることを認識し、稼働系と同じ運用を待機系でも行うことを考えた運用計画、リスク対策を立てる。

この事例を通して、以下の対策を立てた。

- バックアップ切替え対策　（原因 1 →対策 1、2）
- 切替え失敗時の復旧対策　（原因 2 →対策 3、4）

＜対策 1＞通常保守運用において、稼働系、待機系のソフトウェアパラメータの確認、プログラムバージョン管理を徹底する。

通常運用のプロセスの中で、冗長構成を定義したソフトウェアパラメータに矛盾がないことを確認する。チェックプログラムを作成し、日常バッチ処理で、稼働系、待機系の構成定義、各サーバの構成定義のチェックを行う。さらに、システムが正しく動作するかどうか、実機のテストを行う。切替えが成功したことを確認するだけでなく、待機系でも業務が正常に稼働することまで確認する。そのため、確認事項／チェック項目（サービスはすべて稼働したか、すべての接続端末は稼働するか、等の動作確認）を明確にする。

＜対策 2＞定期的にサービス停止時間帯を設け、障害訓練を行う。

バックアップ切替えの運用を理解するために、待機系への切替えの障害訓練を行う。

なお、障害訓練で、待機系に切り替えたために本番処理が稼働してしまい、システム障害を引き起こす事例が過去にあった。この事例では、業務処理を稼働系、待機系でそれぞれ実行してしまい、二重処理になった。本番環境で実施するので、事前準備（本番環境のデータ保存、手順書の作成、訓練終了後の戻し手順、確認手順等）をしっかり行うことが必要である。

＜対策 3＞切替え失敗を想定し、復旧のための手順を明確にする。

待機系への切替えができなかったときを考え、手動で障害から復旧する場合（復旧は、バックアップ切替え方法も含めた処理継続の確立を言う）も考慮し、様々なシナリオ（目標所要時間を含む）を想定した手順書を作成しておく。また、障害復旧テストを行い、各シナリオについての所要時間を計測し、手順書の確認を行う。

＜対策 4＞障害復旧訓練を行い、実際に使える手順書を作成しておく。

障害復旧訓練を行い、シナリオに定めた時間内に復旧できるかどうかを確認する。また、実際の人の動きや判断基準等を考慮して、手順書に反映する。

効果

「バックアップ切替え失敗」になる事例を理解し、対策を実施することにより、バックアップ切替えが失敗し、障害の復旧に多大な時間を要するリスクを減らすことが期待できる。

教訓

バックアップ切替えが失敗する場合を考慮し、設計時、運用保守時、予防対策を行うことが重要である。

ここで示した障害事例に加えて、過去に起きたバックアップ切替えにかかわる障害事例を調査し、分類したところ、11 パターンあることが分かった。

“4.2　バックアップ切替え失敗の問題と対策（詳細説明）”では、それらの事例を発生原因の主な要因である「切替え失敗」、「性能不足」、「切替え無効」、「ネットワークの切替え失敗」、「設備の切替え失敗」を問題と対策として説明している。この資料を利用して、発生した障害と同じ問題に対応する対策を実施することで、再発を防止することができる。また、切替処理に関する対策を網羅的に確認・実施することができる。