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)。障害検知に伴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。

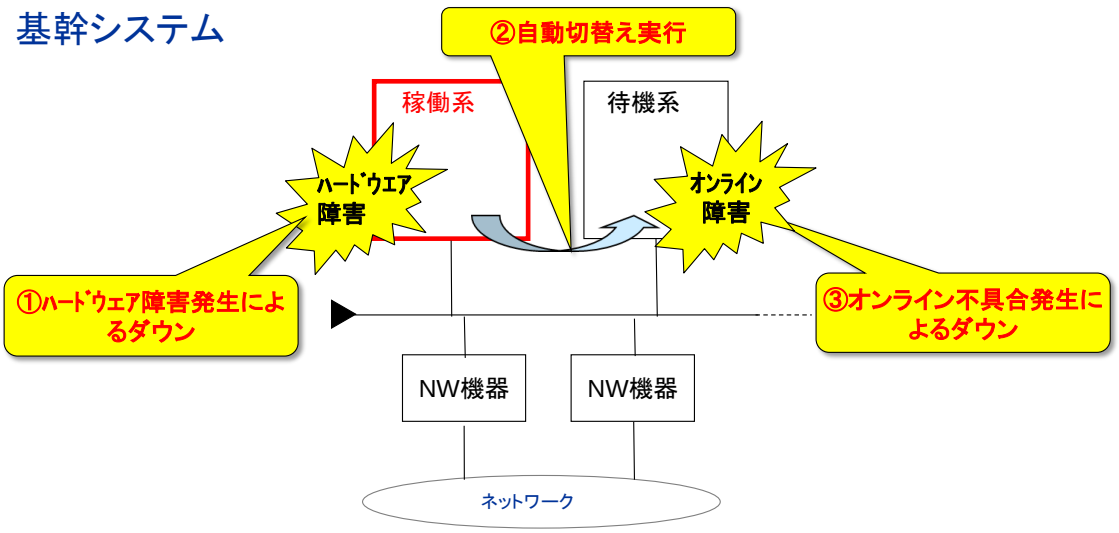

図３．７－１　障害状況

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、稼動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諦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時を考え、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関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。

“３．１９　「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。

３．１９　「バックアップ切替え失敗」の問題と対策（詳細説明）

バックアップ切替えが成功しない様々な状況を考慮して、対策を立てる。

冗長化構成を取っていても、障害時、いざバックアップ切替えや障害機器切離しによる縮退運転を行っても、システム稼働の継続ができない事例が後を絶たない。

そこで、バックアップ切替えの失敗事例を分析し、その問題と対策をまとめた。

本対策の特徴は、バックアップ切替え失敗事例を「問題」として分類、体系立てて整理している点である。過去にまとめられたもの（文献 3.19-1）に対し、重要インフラ IT サービス高信頼化部会で議論された障害事例情報等を含めて再整理したものである。

（失敗事例の問題分類）

この資料では、失敗事例を 11 パターンの問題に整理し、発生箇所に合わせてマッピングした（図１）。

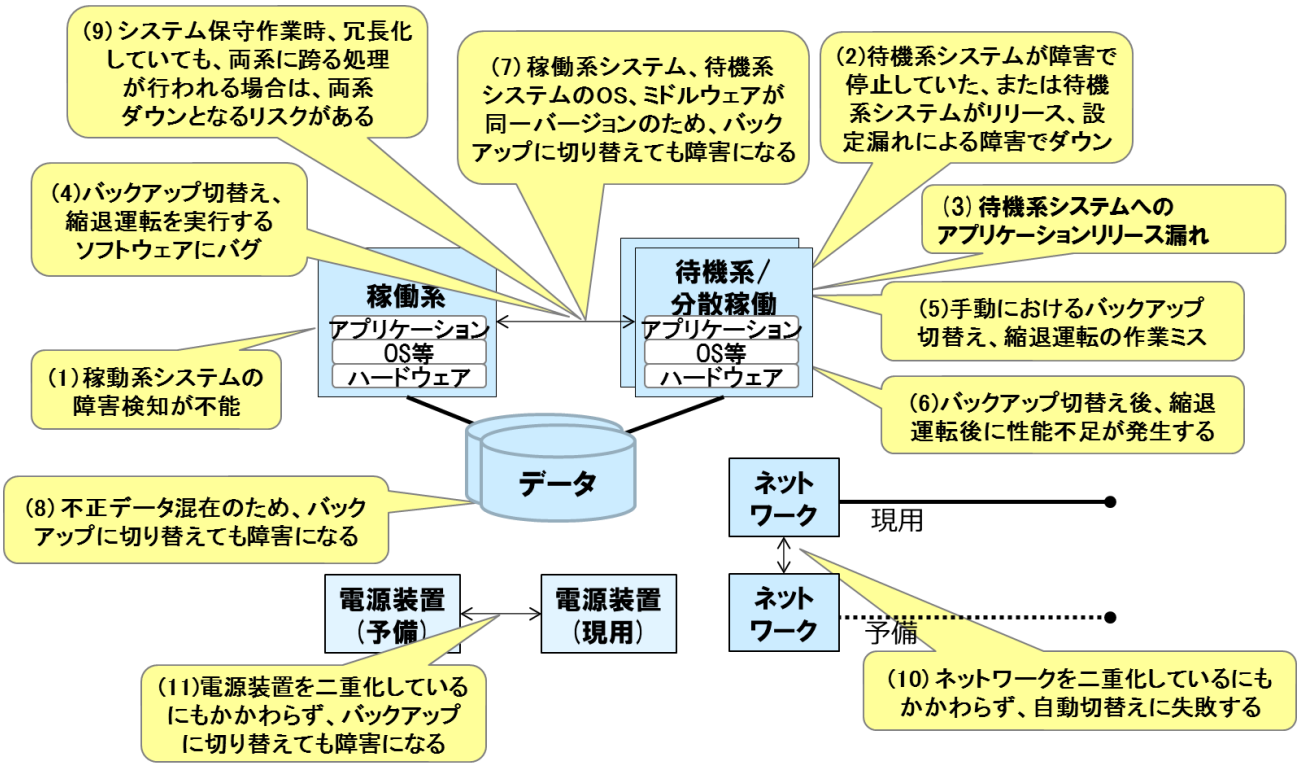

図１　問題の種類と発生箇所

※注　吹き出しの中の括弧内数字は、問題番号を示す。

（原因の分類）

この 11 パターンの問題から原因を以下の 5 つに整理した。

１．切替え失敗

２．性能不足

３．切替え無効

４．ネットワークの切替え失敗

５．設備の切替え失敗

「切替え失敗」、は、バックアップ切替え機能を管理できていないことにより起こる。

「性能不足」は、要件設計時の考慮不足、あるいは急激な情報量急増に対する対策の遅れにより起こる。

更に注意すべき点は、バックアップ切替えが正常に実行されても、処理の継続ができない「切替え無効」が起こることである。

また、「ネットワークの切替え失敗」は、ネットワークに関する切替え失敗や性能不足が起こることである。

「設備の切替え失敗」は、システム機器に重大な被害をもたらすため、決して疎かにできない。

（問題と対策）

このような点を踏まえ、対策を整理し、「問題と対策一覧」としてまとめた（表２）。

・設計時に、チェックリストとして活用することにより、バックアップ切替えの機能要件漏れや対策漏れを減らすことができる。

・運用保守時に、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、障害の再発を防止することができる。

・切替え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。

表２　「問題と対策」一覧

分類	NO	問題	対策
切替え失敗	1	稼動系システムの障害検知が不能	＜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。
	2	待機系システムが障害で停止していた、または待機系システムがリリース、設定漏れでダウンした	＜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。
	3	待機系システムへのアプリケーションリリース漏れ	＜対策3＞計画的に待機系システムを本番システムとして使用する。
	4	バックアップ切替え、縮退運転を実行するソフトウェアにバグ	＜対策4＞切替え失敗を想定し、復旧のための手順を明確にする。
	5	手動におけるバックアップ切替え、縮退運転の作業ミス	＜対策5＞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。 ＜対策6＞切替え、縮退運転の運用要件（訓練、障害時対応）は、設計時に明確にする。
性能不足	6	バックアップ切替え後、縮退運転後に性能不足が発生する	＜対策7＞バックアップ切替え後、縮退運転の場合でのピーク時性能は、日常の監視の中で想定し、必要に応じてシステムを見直す。 ＜対策8＞本番稼働に近いテスト環境を用意し、性能（負荷）確認が行えるようなツールを作成する。 ＜対策9＞切替え、縮退運転の性能要件（ピーク時）は、設計時に明確にする。
切替え無効	7	稼働系システム、待機系システムのOS、ミドルウェアが同一バージョンのため、バックアップに切り替えても障害になる	＜対策10＞OS，ミドルウェア，APのリリース時は、旧バージョンでの切戻し手順を明確にし、障害訓練 を実施する。
	8	不正データ混在のため、バックアップに切り替えても障害になる	＜対策11＞本番稼働に近いテスト環境を用意し、OS、ミドルウェアのバージョンアップ時の動作確認と性能（負荷）確認が行えるようなツールを作成する。
	9	システム保守作業時、冗長化していても、両系に跨る処理が行われる場合は、両系ダウンとなるリスクがある	＜対策12＞冗長化を実施する場合、すべての機器が冗長化されており、単体機器、または密結合の機器のような冗長化にになっていない機器、機能がないことを常に点検する。 ＜対策13＞切替え失敗のリスクを考慮し、失敗の影響を局所化する対策を立てる。 ＜対策14＞ 計画的に待機系システムを本番システムとして使用する。
ネットワーク	10	ネットワークを二重化しているにもかかわらず、自動切替えに失敗する	切替え失敗、性能不足　の対策が有効 ＜対策1＞～＜対策8＞
設備	11	電源装置を二重化しているにもかかわらず、バックアップに切り替えても障害になる	＜対策15＞電源等の設備については、 定期点検と、予備設備の稼働確認を行う。また障害訓練を定期的に行う。 ＜対策16＞電源等の設備の冗長化の運用要件は、設計時に明確にする。

切替え失敗

稼働系・待機系運用では、稼働系から待機系への「切替え失敗」の障害事例が多い。また、多重化運用でも障害機器の切離しが失敗する事例もある。最近は、切替え専用ソフトウェアの性能・品質向上、仮想化などの新技術などにより、このような障害は防げる傾向にあるが、依然として大きな課題である。

問題

（１）稼動系システムの障害検知が不能

これは、稼動系システムの障害を検知できず、バックアップ切替えや障害機器の切離しが実行されないままで、障害回復ができない問題である。

事例では、稼動系システムが停止していると判断ができない状態（サーバ間の状態監視不具合、制御信号の不具合など）であった。

また、前処理用サーバが後処理用サーバの障害を検知できずにデータのやり取りを続行したため、折角後処理用サーバの待機系があったにも関わらず、障害となった事例もあった。

他に何らかの理由（急激なデータ量増加による輻輳状態の発生、ある部分に集中したトランザクションのデッドロック多発のためロールバック多発など）で処理が大幅に遅延しながらも稼働状態のままで完全に停止しない事例もある。

※技術の教訓Ｔ１、Ｔ２，Ｔ９は、このパターンである。

（２）待機系システムが障害で停止していた、または待機系システムがリリース、設定漏れによる障害でダウンした

待機系システムに障害が発生していたが切替え時まで気付かない。稼動系システムへの基本ソフトのパッチ適用、パラメータ等の設定変更を行った後、同様に待機系システム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。このような状況で、バックアップ切替えを実行したため、待機系システムがダウンしてしまった。

※技術の教訓Ｔ７は，このパターンである。

（３）待機系システムへのアプリケーションプログラムリリース漏れ

稼動系システムへのアプリケーションプログラムリリースを行なった後、待機系システムに対しても稼動系システムと同じアプリケーションプログラムリリース作業を実施する必要があるが、これを怠った。そのため、稼動系と待機系でアプリケーションプログラムに相違が発生した。これを放置したまま、バックアップ切替えを実行したため、待機系システムで、旧バージョンのアプリケーションプログラムが動き、データベースのデータ不具合が発生した。そのため、待機系システムを止めて、データ修復を行う甚大な障害に至った。

（4）バックアップ切替え、縮退運転を実行するソフトウェアにバグ

バックアップ切替え、障害機器の切離しの縮退運転を自動的に実行するソフトウェア自体にバグがあった。そのため、障害が発生しても、バックアップ切替え、障害機器の切離しを実行できず、障害復旧ができなかった。

（5）手動におけるバックアップ切替え、縮退運転の作業ミス

上記、問題（1）から問題（4）の自動切替えが失敗した場合には、手動で切替えを実行する。また、デュプレックス構成のコールド・スタンバイやウォーム・スタンバイ、クラスタ構成の一部でも手動切替えを行う場合がある。そのような状態の場合、マニュアルの不備や障害訓練不足、オペレーションミスなどにより、手動での切替えに失敗することがあった。

原因

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など）を作らないと待機系システムは取り残されていく。多重化構成についても、同様に検証する仕組みが必要である。

根本的な原因は、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

＜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。

また、プログラムライブラリは、DISK ミラーリングで同期取りをする。それができない場合は、各サーバ上のバージョン管理をチェックする。（文献 3.19-2）

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／チェック事項（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。

さらに、ネットワーク機器の切替え訓練も行うようにする。

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＞ 計画的に待機系システムを本番システムとして使用する。

定期的に本番稼働するシステムを交互に使うことにより、「稼働系と待機系システムの同期が取れている」確証が得られる。更に、障害で切り替っても日常運用の一環であり、運用部門に負担とならない。また、急な保守作業が入って、片系を止めるような運用にも対応することが容易となる。

さらに、ネットワーク機器も交互に切り替えて使用する。

＜対策４＞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時を考え、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５＞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。

＜対策６＞切替え、縮退運転の運用要件（訓練、障害時対応）は、設計時に明確にする。

バックアップ切替えの成功のためには、その対策を設計時に明確にしておく。

運用に関する「原理原則」を活用し、冗長化対策として設計時に活用する。（文献 3.19-3）

- システム化の方針として、バックアップ切替え、縮退運転の稼働運用を定義する。
- システム要件として、バックアップ切替え、縮退運転の稼働運用を定義する。そして、受入テストとして記述する。また、障害訓練も日常運用として定義する。
- バックアップ切替え時間を定義するとともに、障害時の復旧時間、災害時の復旧時間を定義する。

性能不足

稼働系システムから待機系システムへの切替え時、障害機器の切離し（縮退運転）時に起きた性能不足の問題と対策を述べる。

問題

（６）バックアップ切替え後、縮退運転後に性能不足が発生する

バックアップ切替え時は、切替えが完了するまでに新規のトランザクションを滞留させることになる。そのため、切替え後、滞留したトランザクションが待機系システムに一気に入るため、高負荷がかかりシステムが処理できなくなる。

また、多重化運転の場合、縮退運転時には通常より性能が落ちた状態で処理することになる。縮退運転時のトランザクション処理性能を十分に確認していなかったため、縮退運転に切り替えた後、たまたまピークのトランザクションが発生した結果、処理しきれずにシステムが停止する。この縮退運転切替え時にトランザクションを滞留させる事態が発生すると、更にピーク時処理性能を高く考慮する必要がある。

また、縮退運転は、障害時以外にも保守作業時に実施することもある。その時に性能不足が発生した事例もある。

原因

多重化運用では、縮退運転直後の「性能不足」が最大の原因である。複数サーバで負荷分散を兼ねた多重系システムで、年々処理件数が増え、処理負荷の増加が進んでいるのを見逃したため、障害時に縮退運転を行った時に当初の設計時の要件を超えてしまい、性能不足が起きてしまう。

また、稼働系・待機系運用でも切替え時間が長くなってしまった場合は、その間処理の滞留が生じるため、切替え直後に性能不足が起こる。

根本的な原因は、日常の運用で、縮退時運転、バックアップ切替え時の負荷を想定した対策を怠ったためである。

対策

＜対策７＞バックアップ切替え後、縮退運転の場合でのピーク時性能は、日常の監視の中で想定し、必要に応じてシステムを見直す。

バックアップに切替える場合、切替え時間中は仕掛中のトランザクションの復旧作業を優先するため、新規のトランザクションはキューに溜められる。このため、バックアップ切替え後に、キューに滞留したトランザクションを一気に処理するため高負荷がかかることが多い。性能監視を日常の運用で監視することにより、切替え後のピーク稼働時での必要性能要件を明確にし、システムの見直し（性能向上）を実施する。

多重化運用（負荷分散クラスタ構成など）で稼働しているシステムの障害時は、障害機器を切り離す縮退運転になる。性能監視を日常の運用で監視することにより、縮退運転時での必要性能要件を明確にし、システムの見直し（性能向上）を実施する。

また、保守作業時でも縮退運転が行われることも考慮する。特に緊急対応を行う保守作業は、システム障害発生後の縮退運転時に行うことになる。よって同様に縮退運転時での必要性能要件を明確にする。

これらの対策を、常に日常運用で監視、分析し、必要に応じて性能要件の見直しを行う。

＜対策８＞本番稼働に近いテスト環境を用意し、性能（負荷）確認が行えるようなツールを作成する。

性能（負荷）確認は、本番稼働に近いテスト環境で、自動的に大量のトランザクションを発生させることができるツールを用意し、性能（負荷）確認が行えるようにする。

＜対策９＞切替え、縮退運転の性能要件（ピーク時）は、設計時に明確にする。

切替え時、縮退運転時の性能不足を起こさないためには、その対策を設計時に明確にしておく。

運用に関する「原理原則」を活用し、冗長化対策として設計時に活用する。（文献 3.19-3）

・システム要件として、バックアップ切替え、縮退運転の稼働運用を定義する。

・バックアップ切替え時、縮退運転時の性能要件にピーク時の負荷要件を明記する。

切替え無効

ここで提示した問題は、バックアップ切替えが正常に機能しても処理の継続ができない「切替え無効」事例である。

問題

（７）稼働系システム、待機系システムの OS、ミドルウェアが同一バージョンのため、バックアップに切り替えても障害になる

バージョンアップした OS、ミドルウェアそのものにバグがあり、バックアップ切替えを実行しても、待機系もそのバグで障害となってしまった。更に、切戻し手順が明確になっていなかったため、復旧に大幅な遅れが出てしまった事例もある。

また、稼動系が、ファームウェアのバグでメモリー不足エラーを起こして待機系に切り替わったが、待機系も同様にメモリー不足エラーを起こしたといった事例もある。

※技術の教訓Ｔ１０、Ｔ１６は、このパターンである。

（８）不正データ混在のため、バックアップに切り替えても障害になる

アプリケーションプログラムにバグがあり、不正なデータがデータベースに混在したため、バックアップ切替えを実行しても、待機系もその不正データの処理で障害となってしまった。

（９）システム保守作業時、冗長化していても、両系に跨る処理が行われる場合は、両系ダウンとなるリスクがある

冗長化しているにも関わらず、一方の系のシステムの処理が他方の系のシステムにも影響が及ぶような仕様になっている場合、その処理が両系に跨り両系ともシステム障害となってしまった。

※技術の教訓Ｔ１２は、このパターンである。

原因

ここで提示した問題は、結果として「切替え失敗」の事例であるが、本質は、切替えがうまく行けば問題が無くなる訳ではなく、冗長化の前に対策を行うべき問題である。このようなバックアップ切替えが正常に機能しても処理の継続ができない「切替え無効」の事例では、冗長化していても防げないことがある。

このような障害事例があることを理解し、その対策を立てることが重要となる。

対策

＜対策１０＞OS、ミドルウェア、AP のリリース時は、旧バージョンでの切戻し手順を明確にし、障害訓練を実施する。

OS、ミドルウェア、AP のリリース時は、そのソフトウェアにバグがあった場合、待機系に切替えても、稼働系と同様に待機系も障害になる。

よって、旧バージョンの手動での切り戻し手順を考え、その手順書を作成しておく。当然、障害訓練をおこない、手順書の確認を行う。

＜対策１１＞本番稼働に近いテスト環境を用意し、OS、ミドルウェアのバージョンアップ時の動作確認と性能（負荷）確認が行えるようなツールを作成する。

本番稼働に近いテスト環境で、新バージョンでの動作確認と性能（負荷）確認が行えるツールがあれば、本番稼働が正常に行えるかどうかの検証ができる。それにより、システム障害を未然に防ぐ手立てとなる。

＜対策１２＞冗長化を実施する場合、すべての機器が冗長化されており、単体機器、または密結合の機器のような冗長化になっていない機器、機能がないことを常に点検する。

冗長化をしていると思っていたところが、厳密には冗長化と言えない構成が存在する。製品特性をよく理解し、障害発生時に影響の生じない構成になっていることを常に点検する。冗長化された一つ一つの機器を確認し、一方が障害になっても問題が無いことを確認する。

※技術の教訓Ｔ１２は、この対策も有効である事例である。

＜対策１３＞切替え失敗のリスクを考慮し、失敗の影響を局所化する対策を立てる。

例えば、サーバが複数台あり冗長化構成のグループを複数作ることができるならば、グルーピングすることによって、障害のあったグループだけが停止し、他グループは正常に稼働を続けるようなシステム構成を取ることもできる。

これは、サーバだけでなく、ネットワーク、ストレージ（ＮＡＳ）でも同様にグルーピングを考慮することによってシステム全体が止まるようなリスクを軽減できる場合がある。一般には、フルメッシュ構成を取る場合が多いが、このような対策も検討に値すると考える。

※技術の教訓Ｔ１０は、この対策をとった事例である。

＜対策１４＞ 計画的に待機系システムを本番システムとして使用する。

定期的に本番稼働するシステムを交互に使う。そのことで、一方を止める（電源断）ことになり、長期間連続運転によって引き起こされるＯＳ，ミドルウェアなどの潜在バグを未然に防止することができる。併せて、「稼働系と待機系システムの同期が取れている」確証を得ることができる。

また、ネットワーク機器にもこのような対策は、効果があると考える。

※技術の教訓Ｔ１６は、この対策をとった事例である。

ネットワーク

ネットワークでの待機系への切替え時、障害機器の切離し（縮退運転）時の失敗について、問題と対策を述べる。

問題

（１０）ネットワークを二重化しているにも関わらず、自動切替えに失敗する

ネットワークの機能向上により、ネットワーク機器のソフトウェアも複雑になってきている。そのため、ネットワークの切替えや、機器切離しの設定ミス、オペレーションミス、切替え後の性能問題など、ホスト／サーバで起きている障害が、ネットワーク機器でも発生している。

- ネットワークで相互監視をおこなっている装置（ルータ等）が相手の障害を検知できずに、自動切替えが実施されずに障害が発生した。
- ネットワーク障害時、ネットワーク機器の設定パラメータが誤っていたため、正しく切替えができなかった。
- ネットワークの切替え時にも端末側の再接続要求が集中したりして輻輳状態が発生し、性能問題が生じた。

原因

ネットワークの切替え失敗、縮退運用での性能問題の原因は、ホスト／サーバで起きている原因と同じものがある。近年、ネットワーク機器の機能が向上しているため、ホスト／サーバと同様に管理しなければならないが、現場の体制、技術が追い付いていないことも考えられる。

対策

対策についても、ホスト／サーバで立てた対策を活用することができる。

＜対策１＞から＜対策９＞までを参照。

設備

設備の冗長化失敗について、問題と対策を述べる。設備の障害は、結果として甚大な被害になることがあるので、対策は重要である。

問題

（１１）電源装置を二重化しているにも関わらず、バックアップに切り替えても障害になる

無停電電源装置（UPS）や、自家発電機を準備しているにも関わらず、日常の点検漏れで動作確認が行われず、いざ商用電源の供給が止まった時、それらの装置が予定通り稼働しないために、システム障害となった。また、自家発電機を複数台用意していたが、センサーが冗長化されておらず、なおかつセンサーの障害に気づかなかったため、燃料切れを認識できなかったなどの事例もあった。

原因

運用管理者にとって設備については、やや専門外でもあり、注意が回らない場合がある。しかし、一旦電源などの障害が起きた場合、すべてのシステム機器が故障する可能性を持つため被害は甚大である。更に近年クラウドの普及により、データセンターの設立が相次いでおり、設備での不具合が多数のシステム障害を一気に発生させる原因になっている。

対策

＜対策１５＞電源等の設備については、定期点検と、予備設備の稼働確認を行う。また障害訓練を定期的に行う。

電源等の設備は、定期点検を行っている中で、予備設備に切り替えたりして稼働確認を行う。また、設備担当の点検内容をヒアリングし、システムからの以下の観点も考慮する。

・冗長化されていない設備や周辺機器があるか。
・故障している設備や周辺機器があるか。
・無停電電源装置（UPS）などの充電は十分か、自家発電の燃料は充分あるか。　等

また、電源等についても、障害訓練で予備設備の本番稼働での使用を確認する。障害訓練中に障害になる可能性もあるので、実施計画は慎重に立てる。例えば、一旦本体機器の電源を落とした後、切替え後に順次本体機器の電源を入れるなどの工夫が必要である。

＜対策１６＞電源等の設備の冗長化の運用要件は、設計時に明確にする。

電源等の設備においても、切替え時の不具合を起こさないように、多重化になっている箇所、多重化されていない箇所の洗い出しを明確にし、対策を設計時に立てておく。