2.15 保守作業時のリスク管理に関する教訓（G15）

教訓 G15　保守作業は「予期せぬ事態の発生」を想定し、サービス継続を最優先として保守作業前への戻しを常に考慮すること

問題

（システムの概要）

X 社のシステムは 24 時間稼働のオンラインシステムであり、業務の特性から高度な耐障害性を要求されている。システムは制御サーバ 1 号機と 2 号機で稼働系と交代系に二重化され、さらに各制御サーバ内で A 系システム／ B 系システムによるホットスタンバイ構成となっており、全体で 4 重化構成をとって運用している。

運用中の A 系システムと待機中の B 系システムはリアルタイムでトランザクションデータの系間同期が行われ、さらに 1 号機と 2 号機の間でもサーバ間同期が行われている。

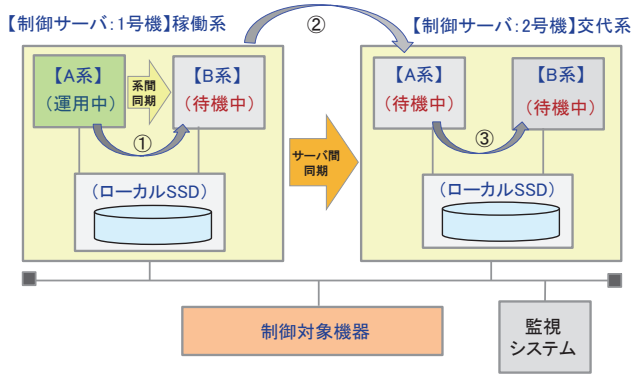

図 2.15－1　4 重化構成の概要

監視システムが A 系システムの障害状態を検知すると、以下のように自動的に切り替わり、トランザクション状態を引き継いでオンライン処理が継続される。

① 運用中の A 系システムが障害状態となると、同一制御サーバ内で待機している B 系システムに瞬時に自動で切り替わりサービスを継続する。この後、A 系システムはトランザクションデータを一旦リセットし、新たに運用中となった B 系システムからトランザクションデータの系間同期が開始され、数分後にホットスタンバイ待機状態となる。

② 稼働系制御サーバ 1 号機が障害状態（待機中のシステムがない場合も含む）となると、交代系制御サーバ 2 号機に瞬時に自動で切り替わり待機中の A 系システムが運用中となりサービスを継続する。この際もサーバ間同期が一旦リセットされ、新たに稼働系となった制御サーバ 2 号機から交代系となった制御サーバ 1 号機にサーバ間同期が開始され数分後にホットスタンバイ待機状態となる。

③ 交代系制御サーバが稼働系となり、サーバ内のA系システムが運用中となり、系間同期・サーバ間同期が再確立されホットスタンバイ待機構成となる。

④ 系間切替えやサーバ間切替えが実施された直後から同期処理が再確立するまでの数分間は瞬時の切替えが出来ない状態になっている。

（保守作業の実施）

ソフトウェア保守を行う場合は、自動切替え制御を解除した上で稼働中の制御サーバ1号機のB系システムに対してソフトウェア更新を実施し、作業完了後A系システムから保守作業後のB系システムに手動切替えをすることにより24時間オンラインシステムを中断することなく新たなサービスが開始される。この際、新たなソフトウェアによる不具合が発見された場合は、保守作業前の状態であるA系システムに手動で切り戻すこととしている。正常にサービスを開始できた場合は、残りのA系システム及び交代系の制御サーバ2号機に対し保守作業を行い、完了後に自動切替え制御を開始する。

（障害発生の状況）

障害発生の状況は以下の通りであった。（図 2.15－2）

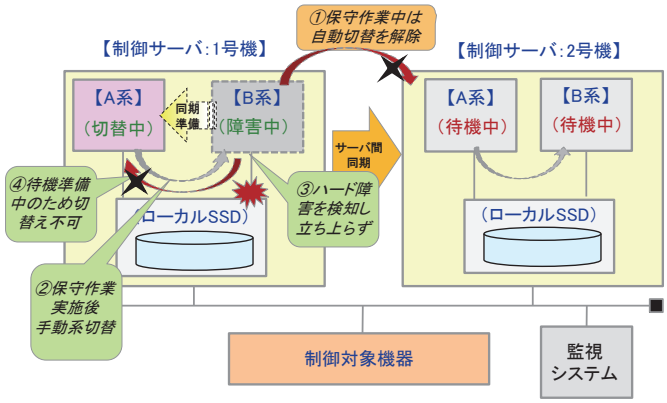

図 2.15－2　障害状況

自動切替え制御を解除（図 2.15－2 ①）しB系システムに保守作業を実施後、手動切替えを実施（図 2.15－2 ②）したところB系システムが立ち上がった直後にB系システムのハードウェアに故障が発生し停止（図 2.15－2 ③）してしまった。A系システムは新たな同期処理の開始中でありまだホットスタンバイ待機状態となっておらず（図 2.15－2 ④）切り戻すことができなかった。

通常運用であれば、ホットスタンバイ待機状態である制御サーバ2号機に瞬時に自動切替えが行われ保守作業前の状態でサービスを継続できるが、自動切替え制御を解除していたため、自動切替えが行われず、手動で制御サーバ2号機に切り替えて運用を開始するまで10分程度オンラインサービスが停止する状況となった。

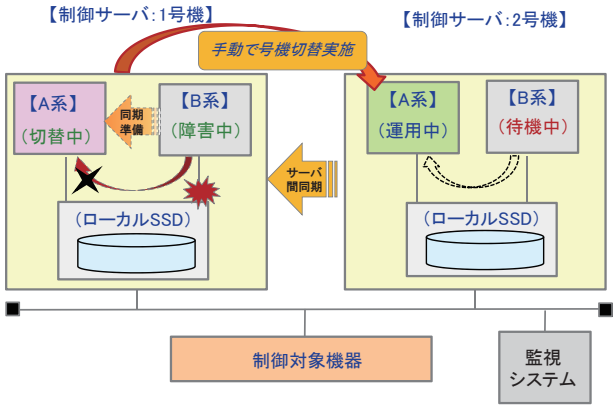

図 2.15－3　障害状況

原因

障害の直接の原因は制御サーバ１号機内のハードウェア故障であるが、ハードウェア故障への高度な耐障害性を確保したシステムであったにもかかわらず、サービスが停止となったのは保守作業時の自動切替え制御を解除していたことが原因である。保守作業時に自動切替えが発生すると予期しない事態となり保守作業自体が混乱することを危惧し、保守作業マニュアルで自動切替え制御の解除が手順化されていたものである。

また、一般的には保守作業は稼働中の制御サーバ１号機ではなく、交代系の制御サーバ２号機で実施し完了後切り替えるという手順がとられる。しかし、本システムでは保守作業完了後に切替えを行うとサーバ間同期が一旦リセットされ制御サーバ１号機がホットスタンバイ待機状態になるまでの数分間の間に障害が発生した場合に、保守作業前の状態である制御サーバ１号機への瞬時の切り戻しができないため採用していなかった。

対策

ハードウェア故障等は予期せず発生するものであり、保守作業時にも発生確率はゼロではない。再発防止対策として、サービス継続を最優先とし、自動切替えを解除しない状態で保守作業を実施することとし、万が一ハードウェア故障が発生した場合は、制御サーバの自動切替えが行われることを前提に保守マニュアルに対応手順を追加した。なお、稼働中の制御サーバでの保守作業にはリスクがともなうが、上記の理由から、保守マニュアル改訂後も従来通り稼働中サーバで保守作業を行うこととした。

効果

保守作業中に予期しない事態の発生があってもサービスが停止するリスクは解消され、改訂された保守マニュアルに基づいて継続的に実施されている。

教訓

保守作業は時間との戦いである。システムの保守作業を実施する場合、サービス継続を最優先とし、「予期せぬ事態の発生」を想定してシステム切替え時間・保守作業前の状態への戻し時間を考慮した保守計画を策定し実施することが重要である。

保守計画はサービス継続の業務特性レベルに応じて例えば以下のように策定することが考えられる。なお、実務では保守作業の内容等によりサービス継続と比較した上で策定する場合もあるであろう。

●サービス停止が許されない重要なシステムの場合：（ホットスタンバイ）

自動切替え制御を有効にしたままホットスタンバイ環境で保守を実施し作業完了後に切り替える。切り替え後障害発生時は自動切替えにより保守作業前の状態でサービス継続、保守作業は中止判断をする。

●数分間のサービス停止が許容できるシステムの場合：（コールドスタンバイ）

交代系で保守作業を実施し、作業完了後切り替える。切替え後、障害発生時は手動で保守作業前の状態を保持しているシステムに切り戻しを行うとともに、交代系も保守作業前の状態に戻してコールドスタンバイ環境を確保し、保守作業は中止判断をする。

●夜間・休日などサービスを停止可能な時間帯枠が確保可能（通常はこのケースが多い）な場合：

その場合でも翌日のオンラインサービス開始を最優先し予期せぬ事態が発生する場合を想定して、保守作業前の状態への戻し時間を確保しチェックポイントと戻し判断のタイミング等を必ず盛り込んだ保守計画を策定し作業を実施する。

また、保守作業計画書は上記業務特性レベルに関わらず例えば以下のような内容を明確にして作業をマネジメントする。

（保守作業計画書の内容）

- 各作業の所要時間見積もり、タイムチャートを作成
- 作業人員の確保と役割分担
- バックアップの取得と戻し手順の準備
- チェックポイントを複数設定
- チェックポイントでの計画と実施状況の差異確認と今後の作業予測
- 作業続行／中止の判断、緊急時の意思決定体制

など