3.12 互換部品の入れ替えに関する教訓（T12）

教訓 T12

新製品は、旧製品と同一仕様と言われても、必ず差異を確認！

問題

ユーザ X 社の制御系システム（24 時間稼働）には、2 重化されている制御装置（CPU とディスク装置を含む）が組み込まれている。

その制御装置の A 系の LAN ボードに不具合が生じた。そこで、制御装置の A 系のみを停止させて LAN ボードを交換することとした。

先ず A 系を停止させる自動シーケンスを実行した。A 系 CPU が切り離された（図 3.12－1 ①）後、B 系 CPU から両系のシステムディスク装置へのリセットが行われた（図 3.12－1 ②）。この処理において、両系のシステムディスク装置ともタイムアウトが発生し、制御装置全体が動作を停止した（図 3.12－1 ③④）。

A 系、B 系ともに再立上げを続けたが、復旧できなかった。原因究明中に、開発環境の制御装置が本番機として使用できることが分かり、急遽代用機として使用した（図 3.12－1 ⑤）。

このサービスの利用者は、1 日中影響を受けた。

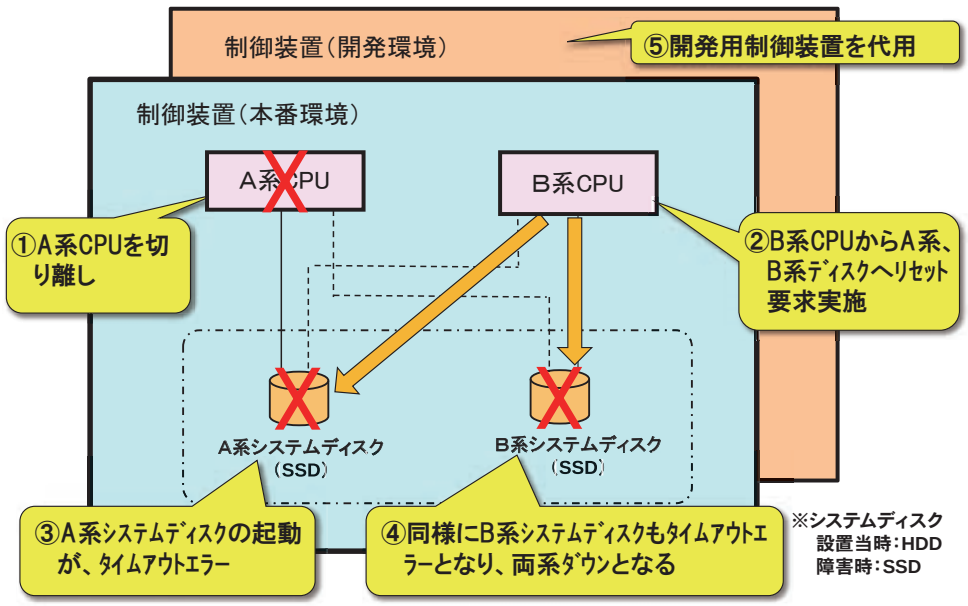

図 3.12－1　障害状況

原因

システム導入当初、制御装置のシステムディスク装置は，HDD を使用していた。

保守運用フェーズに入り、数年前に HDD から SSD に交換した。

しかし、今回の障害では、制御装置の片系 CPU 停止時の OS のタイマ監視時間と SSD のリセット完了時間とに不整合があった。直接の原因は、ベンダが、SSD は、標準として規定されているコマンド・インターフェースで HDD と互換性があると認識していたため、HDD と SSD の起動時性能（標準の規定外の事項）での差異を見逃してしまったことによる（図 3.12－2）。

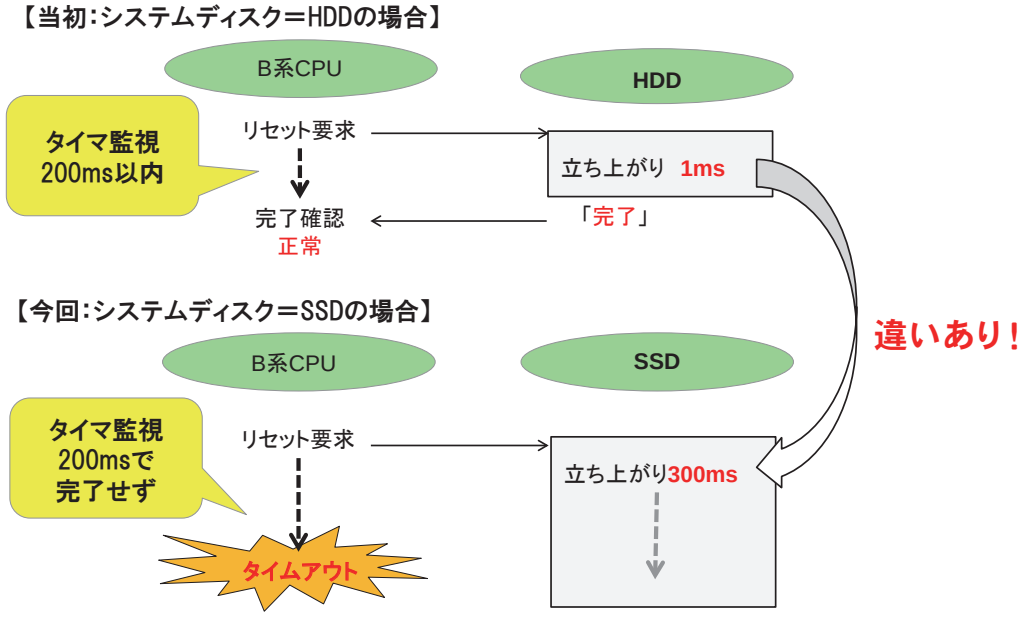

図 3.12－2　HDD と SSD の立ち上がり時間の相違

また、根本原因は、今回の障害を防ぐことができた（事前に不具合を発見できた）時点が 2 カ所あったが、以下のようにそれを見逃してしまったことである。

① 数年前、ベンダが、システムディスクを HDD から SSD に交換したとき

ベンダは、交換する新部品がシステムと整合しているかについて、SSD は、HDD と互換性がある仕様になっていると判断してしまい、以下のような視点からの確認を怠ってしまった。

- 機能やインターフェースが一部異なる。また、新機能が追加されている。
- 異なる部品、製品の場合には，設計思想そのものが異なっている。
- 機能仕様は同じであっても、性能等の非機能仕様が異なる。

また、テストの中でも、先の観点から、2 重化されている制御装置の片系を交互に停止させる動作確認を行うべきであったが、テストの必要なしと判断してしまったため、不具合を発見することができなかった。

② 今回の本番作業前に行った事前確認のとき

ベンダは、自工場での手順書確認で制御装置の片系を止めて LAN ボードの交換を実施していたが、HDD で動作確認しただけで「問題なし」と報告し、本番環境と同じ SSD での動作確認を行っていなかった。そのため、ここでも不具合を発見することができなかった。

対策

直接の対策として、ベンダは、プログラムの更改（制御装置 OS のタイマー監視時間を SSD のリセット処理完了までに延長）を行った。さらに、部品の更新時に確認不足を起こさないために社内ルールを見直し、作業手順を自工場内で確認するときは、工場内の装置は現地と同一構成で行うようにした。

また、ユーザは、制御装置に関する作業準備について、影響範囲を関係部署と共有し、事前に開発環境の制御装置にて動作確認を行った上で、本番環境の部品交換を行うようにした。

制御系システムは、保守運用が非常に長期になる場合が多い。そのため、途中で部品の供給が中止となったり、ソフトウェアの保守契約が切れてしまったりなどの理由により、新製品（HW、SW）に交換せざるを得ない事態が起こる。

予防対策では、今回の事例のように、新製品と従来製品との差異を見逃さないためのルールを作ることが重要となる。その場合、従来と異なる新装置、新ソフトウェアがシステムに組み込まれるときは、どんなに互換性があると言われているものであっても、変更部分と非変更部分との整合性を確認することが重要である。

そのためには、ベンダ、ユーザ双方が、相手の役割分担を支援し合うことが重要である。特にユーザがベンダの障害予防対策の実施状況を確認する、つまり、ベンダの確認の見落としを補完することがより有効である。ユーザは、ベンダからの報告を鵜呑みにせず、リスク、ハザード分析などを行い、システムの重要度に応じてテスト範囲を明確にし、受け入れテスト（デグレードテスト）を行うなど、ベンダ側に一歩踏み込んだ対応が重要である。

ベンダとユーザ双方が新製品をシステムに組み込む場合のそれぞれの対策例を一覧で示す。さらに、本編の他の参照すべき教訓（T6, T7）を加えた（表 3.12－1）。

一覧の作業項目は、対象となるシステムや役割分担の決め方によって異なるので、ベンダとユーザで十分話し合って決める必要がある。

表 3.12－1　対策例一覧

	ベンダ	ユーザ
予防対策	①部品の機能仕様、非機能仕様の相違点の洗出し ②部品の更新時に確認不足を起こさないための社内ルールの見直し ③作業手順を工場内で確認する時、工場内の装置は現地と同一構成とし、実施 ④機能停止を伴う部品交換作業は、制御装置の機能に影響しないよう開発用の装置にてオフラインで動作確認を行い、その結果を確認した上で部品交換を実施	①ハザード分析の実施　→　リスク対策 ②関係者ベンダを交え、新製品と従来製品との差異をチェック ③ベンダの工場内でのテスト内容、結果を確認した上で、ユーザの受入テスト内容の確認 ④開発環境での事前確認 ・相違点に関する動作確認の実施 ・デグレードテストの実施 （活用できる他の教訓） 教訓T6：テスト環境と本番環境の差異を体系的に整理し、障害のリスク対策を練る。
実行時対策	①本番作業実施前にバックアップを準備する。 （活用できる他の教訓） 教訓T7：バックアップ切替が失敗する場合を考慮すべし	①ハザード分析によるリスク対策の策定と実施 ②上記リスク対策として、作業に因るシステム停止の影響範囲を関係部署と共有し、これを想定した作業計画を立案し、実施

効果

制御系システムを長期間保守運用する場合、今までと異なる新装置、新ソフトウェアをシステムに組み込まざるを得ない事態が生ずる。その場合、ユーザとベンダが役割分担の上、連携し、補完しあいながら、変更部分と非変更部分との整合性を確認することにより、障害を減らすことができる。

教訓

新旧製品の差異に因る障害は、互換性があると言われても、変更部分と非変更部分との整合性を確認することが重要である。

特に、ユーザは、ベンダの予防対策に踏み込みことにより、ベンダの予防対策をより効果のあるものにする。

つまり、ユーザとベンダは、既存製品から新製品に交換するときは、同じ物と言われても別物に交換するものとして対策を考え、連携し補完し合いながら、従来製品と新製品との整合性を確認することになる。