## ３．２　システム全体を俯瞰した対策に関する教訓（Ｔ２）

**[教訓 T2]**
**蟻の目だけでなく、**
**システム全体を俯瞰する鳥の目で総合的な対策を行うべし！**

### 問題

Ａ 社の制御系システムの下位システム（以下、下位）にある制御装置の稼働系に故障が発生した。自動的に待機系に切り替わるところが、切り替わらなかった。さらに、上位システム（以下、上位）の監視端末からの指示による系切替えを実施したが、切り替わらなかった（図３．２－１）。

一般的に制御系システムは、制御システムの監視・制御を行う上位と、それぞれが独立した制御装置で構成された下位にグループ分けされた構成になっている。

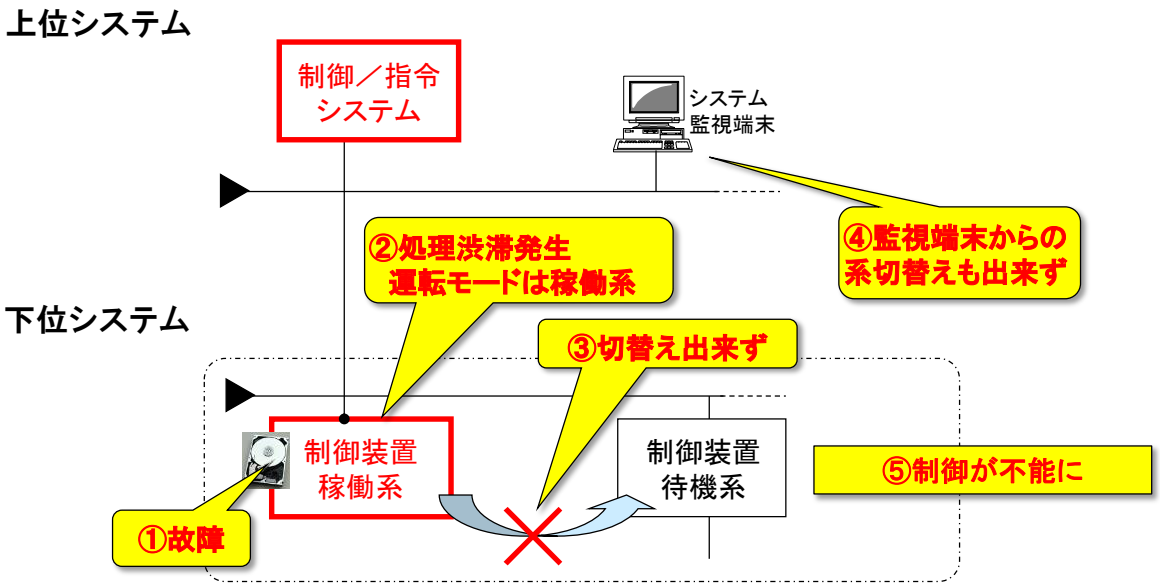


図３．２－１　システム全体図と障害発生状況

### 原因

直接の原因は、下位の制御装置の稼働系のハードディスクの機器故障である。通常初めに 1 回だけ行う「リセット通知」が故障のため出続けた。そのため処理が渋滞した。ところが稼働系は自分が処理中であると認識していたため、処理継続状態を続け、待機系への切替えは行われなかった。また、処理の渋滞のため上位との通信が途絶えたため、上位の制御監視端末からの系切替えもできなかった。

今回の事象を分析すると、以下のような根本原因があることが分かる。

【原因１】稼働系が 1 回だけ行う「リセット通知」が出続けていることを、待機系は「稼働系の障害」と判断する機能が無かった。そのため、系の切替えが下位だけで完結せず、下位が、十分な自律機能（下位の中で障害対策を行う）を有していなかった。

【原因２】上位が、下位からの出続けている「リセット通知」を障害と判断する機能が考慮されていなかった。そのため、系の切替えなど、下位を制御することが十分できなかった。

制御系システムを正常に稼働させるためには、下位の中で自律した動きをまず実施することが重要だが、下位での障害が生じた場合は、上位が下位の監視・制御を行う必要があった。今回の障害は、そのいずれにも不具合があった。

## 対策

制御系システムの系切替えの対策として、以下の 3 つの対策を行った。

【対策 A-1】　待機系装置からの停止制御機能を追加し確実に系切替えができるようにした（図３．２－２①）。

【対策 A-2】　上位の制御装置から下位の制御装置の停止を確実にできるようにした（図３．２－２②）。

【対策 B】　さらに、上位の制御装置の監視機能の強化を図った（図３．２－２③）。

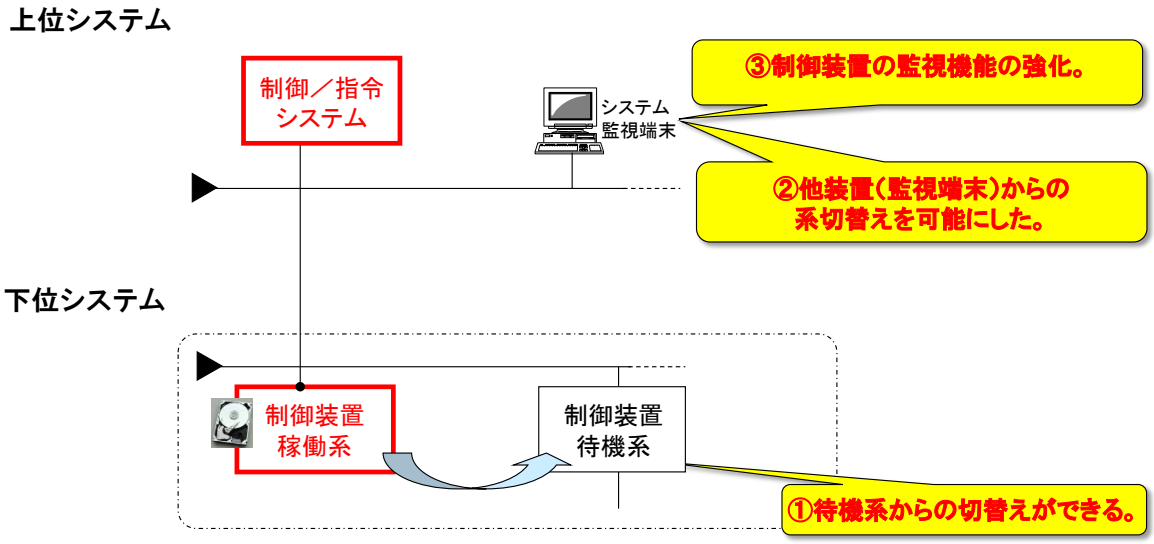


図３．２－２　対策

この系切替えの基本的な考え方は以下の 3 項目に整理できる。

【対策Ａ】システムで検知（上位、下位の制御装置）

【対策Ｂ】ソフトで検知（上位）

【対策Ｃ】手動による系切替え

今回の対策を当てはめると図３．２－３のようになる。

下位だけでの対策（対策 A-1）では、「蟻の目」対策であり、それだけでは制御系システムの対策として不十分である。そこで、「システム全体を俯瞰した鳥の目」対策として、上位からの対策（対策 A-2、対策 B）を行うことにより、システム全体の信頼性が向上する。また、対策の順序としては、対策 A から対策 C に向かっていくほど障害復旧の時間が長くなるので、対策 A から順番に行った。

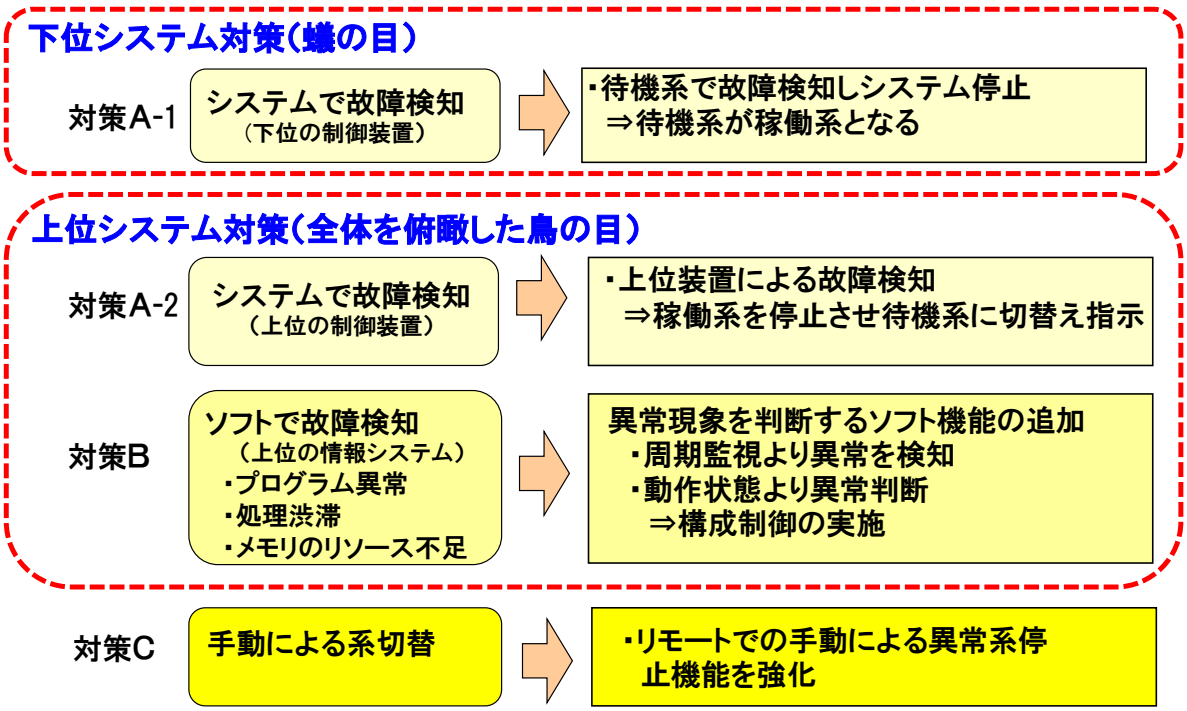


図３．２－３　信頼性向上のための系切替えの対策

## 効果

障害対策は、障害を起こした下位の制御装置だけの対策を考えがちであるが、蟻の目の対策だけでなく、システム全体を俯瞰する鳥の目対策を活用することで障害発生時の復旧時間の短縮が可能であり、システムの安定稼働（障害発生頻度の減少）が保たれる。

例えば、停電、列車運行停止などが起こらなくなり、復旧が早まる。今回の事例では、2～3 時間かかっていたのが、瞬時に復旧することができた。

## 教訓

上位システムと下位システムとで構成されている制御系システムの障害対策は、障害の発生した制御機器の対策（蟻の目）だけでなく、システム全体を俯瞰する鳥の目で総合的な対策を行うことが重要である。