3.4 システム環境の変化への対応に関する教訓（その 1）（T4）

教訓 T4

システムに影響する変化点を明確にし、その管理ルールを策定せよ！

問題

制御系システムは、監視・制御を行う上位システム（以下、上位）とそれぞれが独立した制御装置・移動装置を持つ下位システム（以下、下位）とで役割分担をしている。

列車制御システムも同様な構成になっており、列車の運転は上位の指令センターと呼ばれる所で集中監視を行っている。さらに、事故などがあって列車が乱れた場合に対処するために、数時間先までの運転がどのようになるかの予測をシステムで行い、その結果を予測ダイヤとして画面に表示している。

ある日、雪によるポイント不具合が早朝に複数の駅で発生した。駅間停車防止のため複数列車に列車抑止（列車に対して駅にとどまるよう指示）を入力したところ、画面表示がすべて消えてしまい、予測ダイヤを見ることができなくなった（図 3.4－1）。

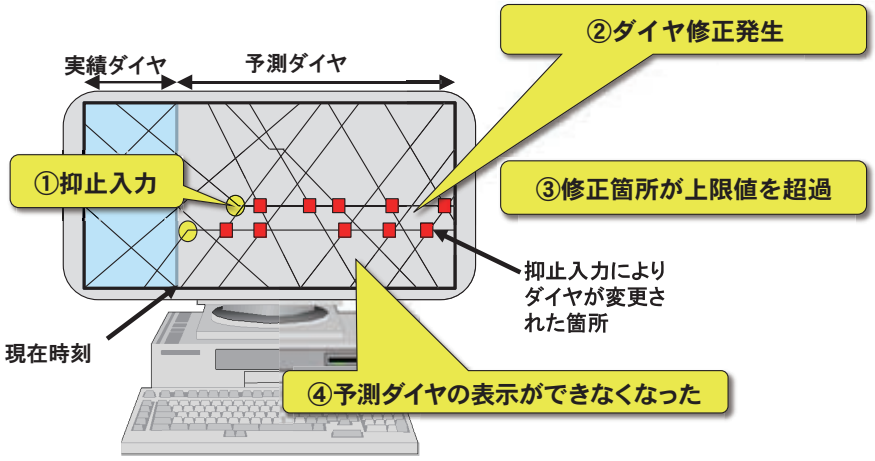

図 3.4－1　障害発生状況とモニター画面

原因

直接原因は、駅間に列車が停車するのを防止するため、複数列車に対し「列車抑止」入力を行ったことである。「抑止」入力を行うと、対象となる列車ごとに予測ダイヤの修正個所がシステムの画面に表示されることになっている。この入力が早朝であったため、変更入力に基づく予測ダイヤ上の「修正

個所」がほぼ 1 日分発生した結果、システムの上限値（修正個所：600 件）を超えてしまい、予測ダイヤを表示できなくなった。（上限値を超えた場合には画面を消すという仕様になっていた）

この上限値はシステム構築当初から決まっていたものであった。

システムは、長期間の使用にともない変化が生ずる。その変化は、新サービス開始や法改正等のようにある一点で起こるものと、利用者の増減や装置の劣化のように徐々に緩やかに変わっていくものある。そのような変化によってシステムの要件（ここでは上限値）変更が必要となる要因を変化点という。また、変化点管理とは、変化点を監視することによって未然に対策を取る管理のことである。

根本原因は、システムに大きな変化点があったにも関わらず、それを見逃していたことである。具体的には、以下のように、変化点の見逃しが 3 つ存在していた。

【原因 1】予測時間の延長

列車ダイヤの予測時間を 4 時間先から 24 時間先までに変更した際、「修正個所数」の上限値の増加などシステム全体の機能要件変更を行わなかった。

【原因 2】列車本数の増加

列車の本数が年々増加しており、本来ならば（運転本数の増加の都度、）上限値を超えた際のシステムの動作を見直す必要があったにも関わらず、行わなかった。

【原因 3】「抑止」機能の使い方の変化

システム導入当初、「抑止」機能は、指定駅区間に指示を行う「駅抑止」を使っていた。その後、今回の障害のトリガである「列車抑止」が、年月とともに徐々に、かつ優先的に使われ出した。「列車抑止」は「駅抑止」に比べ、予測ダイヤの「修正個所数」が多い。このような傾向にも関わらず、「抑止」機能の使い方の変化を監視し、それにともなう「修正個所数」への影響を確認することを怠っていた。

まとめると、根本原因は、全体に影響する変化点（この場合、予測時間、列車運転本数、使い方の変化）が管理されていなかったことである。

このように、予測時間、列車運転本数といったハード的（物理面）な観点だけでなく、使い方の変化（利用形態の変更）といったソフト的（運用面）な観点も含めた変化点を監視し、そこから、システム障害に結びつく上限値超えを事前に察知し、対策を打つことが必要であった（図 3.4－2）。

事例では、上限値超えを取り上げているが、システム的には、リソース不足、性能不足などの非機能要件に影響する変化点を監視することといえる。

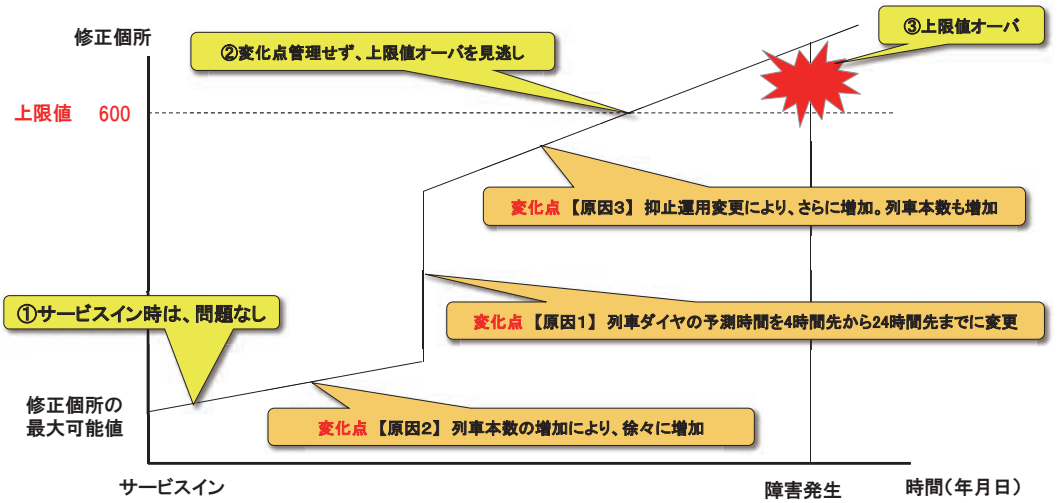

図 3.4－2　上限値超えに至る「修正個所の最大可能値」の変化

対策

予測ダイヤの処理（1 分おき）のたびに修正個所のクリアを行うとともに、修正個所 600 件までは予測ダイヤの演算処理を継続し、予測ダイヤを描画するようにプログラムを改修した。

また、システムの変化点を管理するルールを設け、要件の変更につながるような案件に対しては、システムの見直しを行うようにした。

過去においては、制御系システムは、上位と下位とで役割分担をしているため、上位が変更されても、下位（それぞれ独立した制御装置・移動装置）には影響がなかった。しかし、上位によって下位が管理されるようなソフトウェア構成になってきている現在ではシステム全体での変化点の管理が必要になる。

制御系システムでの変化点は、一般的なシステムの仕様変更の他に、運用形態の変化、対象時間、対象機器の動き、機器数の変化なども含む。障害を事前に防止するためには、この変化点を見逃さない仕組みを構築することがポイントになる。

特に、機能の拡張（制限値に影響する場合）時は、変化点を見逃してはならない。この事例のようにアプリケーションプログラムの中でテーブル内のデータ件数の制限を持っているパターンは非常に多い。制限値に対する上記のような変化点が管理指標のひとつである。

今回の障害では、ある開発時に決定した上限値が、ユーザの取扱い方や輸送形態等の変化、システムの改良などでシステムにかかわる諸元の変動により上限値を超えることがないよう変化点を適切に管理することになる。

今回の問題については、以下の 3 つの変化点管理を行った。

- 上位における仕様変更（予測時間の変更等）　→　【原因 1】の対応
- 下位における列車制御装置の変更（列車本数の増加等）　→　【原因 2】の対応
- （オペレーション、運用）項目表を作成し、使い方の変化を常時チェック　→　【原因 3】の対応

制御系システムの変化点管理ルールを明確にし、そのルールを守る仕組みを構築するために、次の 4 点を行う。

- システムが監視・制御する対象と仕様の変化点を洗い出し、管理項目とする。
- 変化点管理のルールとそれを守る仕組みを構築する。
- 上限／下限値の設定された管理項目の物理的な変化、特に重要データの「見える化」を検討し、モニタリング機能の強化を行う。
- 変化点管理で使用する管理指標を関係部門で共有し、また定期的な会議でその管理指標を確認しあい、「変化点の見落とし」を防ぐ。

これらの対策により、現場環境の変化、システム要件に変化があった時点を可視化することができる。

効果

制御系システムの変化点管理を行うことにより、システム要件の変更の時期が明確になる。その結果、システムの更新を行うことにより、システム障害を防ぐことができる。

制御系システムは、列車運転に限らず、工場における生産ライン制御、電力の供給ライン管理制御、通信の交換機制御など、世の中に数多く存在している。これらのシステムにおいても変化点管理を応用し、社会インフラの混乱を防ぐことができる。

教訓

制御システムのような長期的に使うシステムは、様々な内的（運用の変化）、外的要因（機器などの物理的増加）から、当初設定した上限値や機能の使い方に大きな変化が起きていることがある。また、新サービス開始や法改正等のような一点の変化点だけでなく、利用者の増減等長期的な変化でとらえなければならない変化点もある。

それらの変化点を見逃すと、後日重大な障害を起こすことになる。システム全体に影響する変化点を明確にし、その管理ルールに基づいた変化点管理を行うことが、システムの改修を促す要件変更のときを逃さず、システム障害を未然に防ぐ対策である。