資料1-3

情報処理システム

高信頼化 教訓集

（ITサービス編）

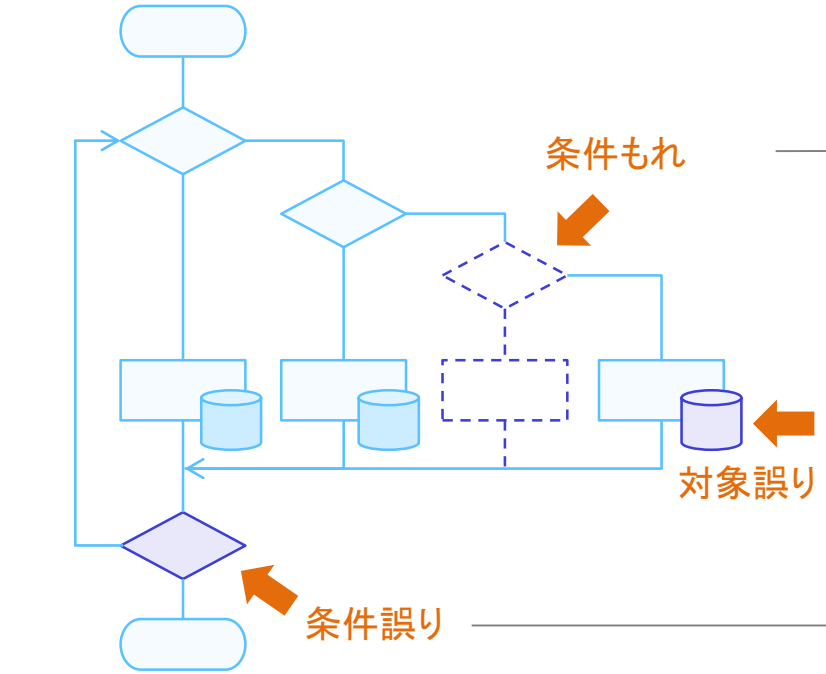
「注意すべき観点」に基づいた障害事例の分類

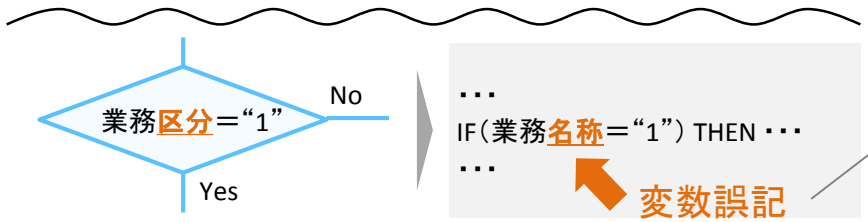
特に注意すべき障害事例

番号	注意すべき観点
①	計算処理の誤り
②	検知条件の想定もれ
③	テストによる副次作用
④	待機系への設定もれ
⑤	障害発生ケースの想定もれ
⑥	しきい値の超過
⑦	ログの肥大化
⑧	製品仕様の誤解
⑨	不完全な作業実施
⑩	作業中偶発事象への考慮不足

① 計算処理の誤り

処理条件もれ、処理対象誤り、処理条件誤り、変数名誤り





計算条件のもれ

事例 1703　事例 1704

通常外処理のもれ

加算を主体とした業務処理（使用料計算）で減算処理が発生し、誤請求を行ってしまった

教訓 T5

処理対象の時点誤り

高額療養費は診療月時点での世帯単位で計算する必要があるが、診療月後に世帯変更があった世帯に対して変更後の世帯単位で計算してしまった

事例 1425

ありえないはずの条件の実在

1,000件連続で「データなし」を処理終了とする仕様に対して実データで当該条件が発生したため、後段の送金処理が未完了となった

事例 1419

変数名の誤記

条件分岐処理において、区分を示す変数を入れるべき場所に名称を示す変数を入れてしまい、分岐が機能せず、臓器移植患者の待機日数計算を誤った

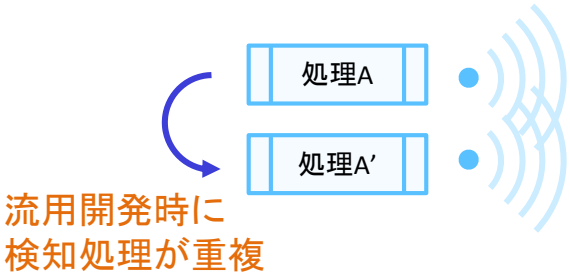
事例 1705

主要な対策方法

- **サービスの視点での変更点を見落とさない仕組みづくり （教訓T5参照）**
- 設計もれに対する社内組織間の役割分担明確化、マネジメント強化、発注側の検証テスト強化等

② 検知条件の想定もれ

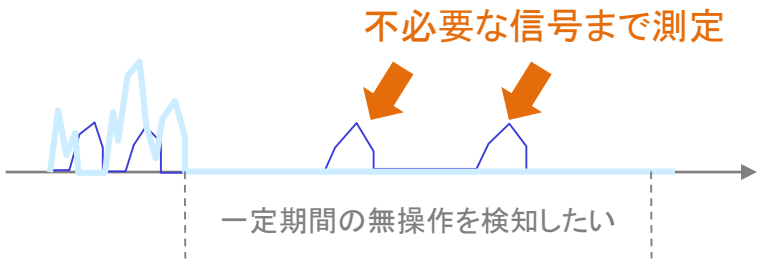
検知処理の設計誤り



メッセージ重複による誤検知

流用開発時に同一のジョブ完了メッセージを重複作成したため、ジョブ実行順序が変わりバッチ処理に論理矛盾が発生した

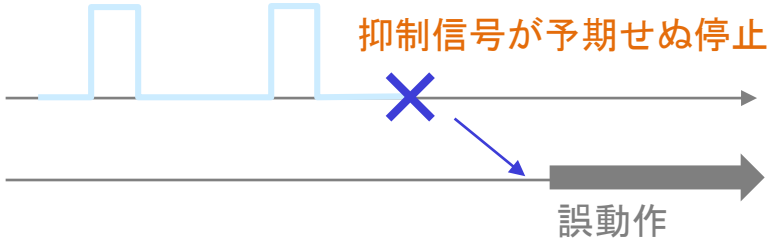
教訓 T26



無操作異常の不検知

運転士の一定時間無操作を検知する仕組みで、自動列車制御による減速を乗務員操作と誤って検知し、本来の異常検知を行えていなかった

事例 1431



抑制信号停止による誤検知

発信用サーバに定期的に受信していた通行止め情報が途切れたため、復旧したと誤判断し、通行止め解除のメールが誤って自動送信された

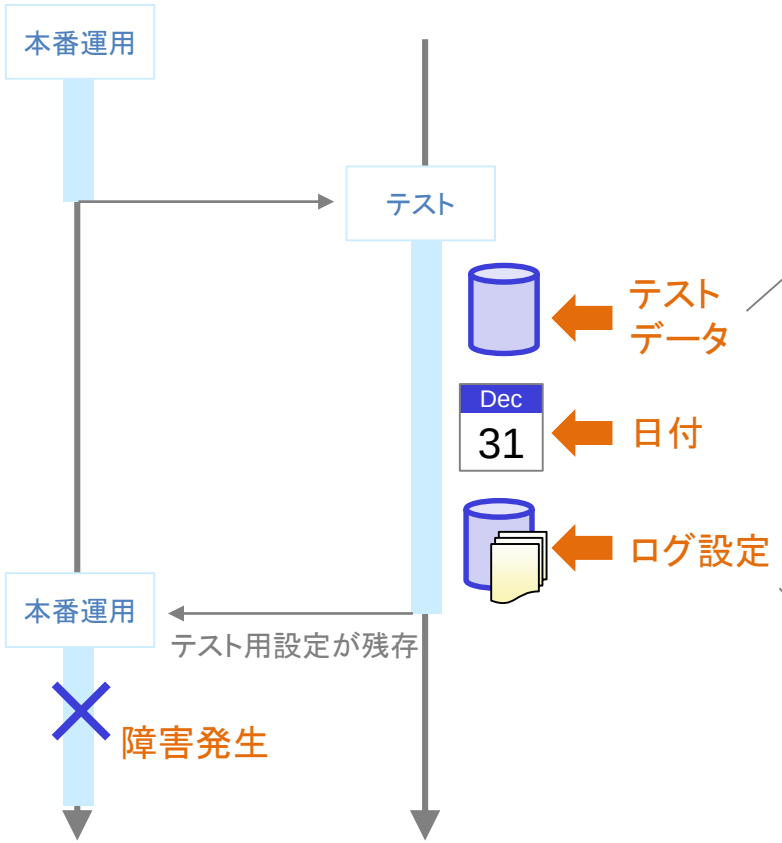
事例 1231

主要な対策方法

- **既存システムの流用開発はその前提条件を十分把握（教訓T26参照）**
- 設計でのレビューの強化、不整合や競合に対するシステム全体を俯瞰するチェック
- 信号が途切れた際に安全側へ倒すフェールセーフな設計の導入

③ テストによる副次作用

テスト用の設定の残存



テストデータの本番残存

- 改札機に対して消費税改定を想定したテストを実施後、データを戻す作業を怠り、利用者から料金を過剰に収受した — 事例1405
- テストデータの削除を忘れてバッチ処理を実行したため、残高証明書の発行手数料を二重に引き落としてしまった — 事例1013

システム日付の設定誤り

- 消費税改定を想定した切替で、1台の路線バスにのみ誤って日付を1日早くセットし、消費税改定1日前から増税後の運賃を徴収した — 事例1409

テスト時のログ出力設定の残存

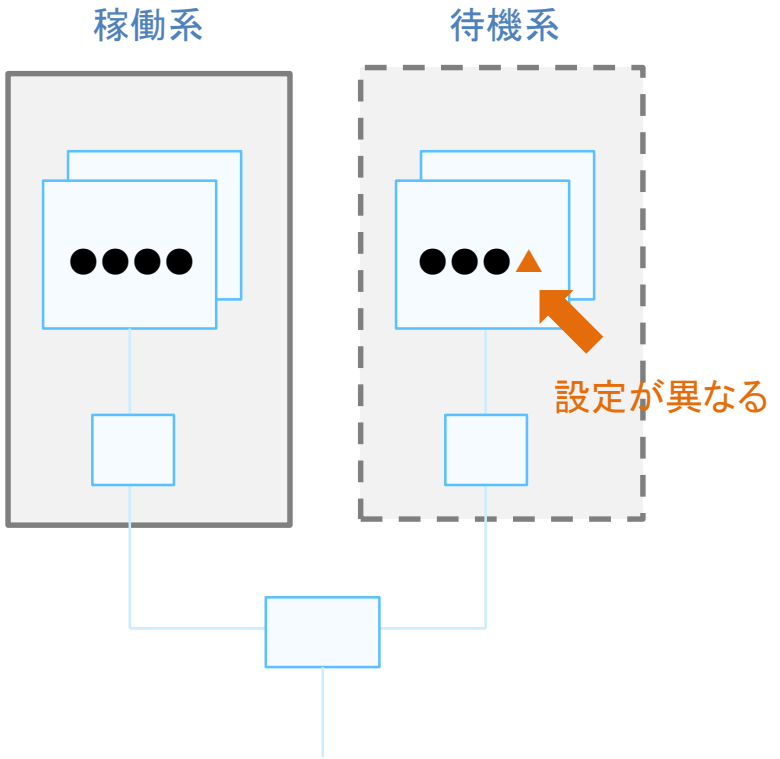
- システムテスト中にログを詳細に出力する設定としたまま、それを修正せずに本番運用を行い、カード発行処理が大幅に遅延 — 事例1215

主要な対策方法

- テスト作業内容（特に戻し作業）に対するレビューの徹底とテスト実施後の証跡チェック
- テスト時に変更する各種パラメータの把握、テスト実施前後のパラメータ突合

④ 待機系への設定もれ

待機系の設定誤り



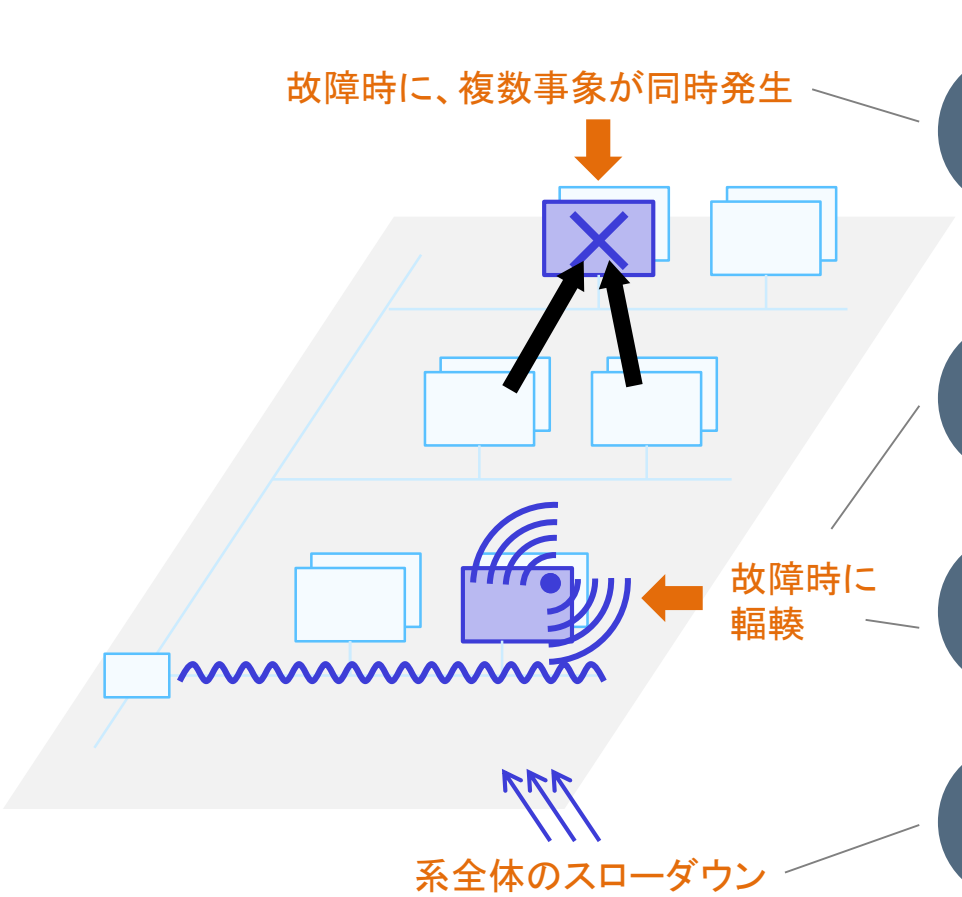
待機系での パラメータ設定誤り	稼働系と待機系の同期を取るべきソフトウェアパラメータにもかかわらず、待機系への設定を怠り、待機系が起動しなかった	教訓 T7
待機系での ファイル不足	保守作業での設定ミスで待機系側に必要ファイルが存在せず、障害時に切替失敗	教訓 G11
待機系での パスワード設定もれ	稼働系のみパスワードを変更し待機系のパスワードを変更せず、データ同期時にエラーが発生	事例 1640

主要な対策方法

- 重要なシステムは、**保守実施時に待機系への切替えテストを必須化（教訓G11参照）**
- 保守運用での稼働系と待機系のパラメータ設定の管理と作業確認、**障害訓練（教訓T7参照）**

⑤ 障害発生ケースの想定もれ

部分的な故障が発生した際に、複数の処理が競合



複数事象が同時発生するケースの想定もれ

- 2つの監視機能（DB同期、自ノード監視）が偶然重複したため、待機系切替用の最後のDBサーバまでが停止 — 教訓 T23
- 2つのtelnet接続（障害情報収集、自動監視）が競合し、無限ループが発生 — 教訓 T20

故障時のネットワーク輻輳の想定もれ

- ハードディスクの故障で「リセット通知」が出続け、処理渋滞で一部の通信が途切れ、制御監視端末からの系切替えが行えなかった — 教訓 T2

故障時のエラーメッセージ発生の想定もれ

- ディスク装置故障によりシステムがダウンした際にエラーメッセージが大量に発生し、連携先のシステムもダウンした — 事例 1007

サイレント障害（NW性能劣化の不検知）

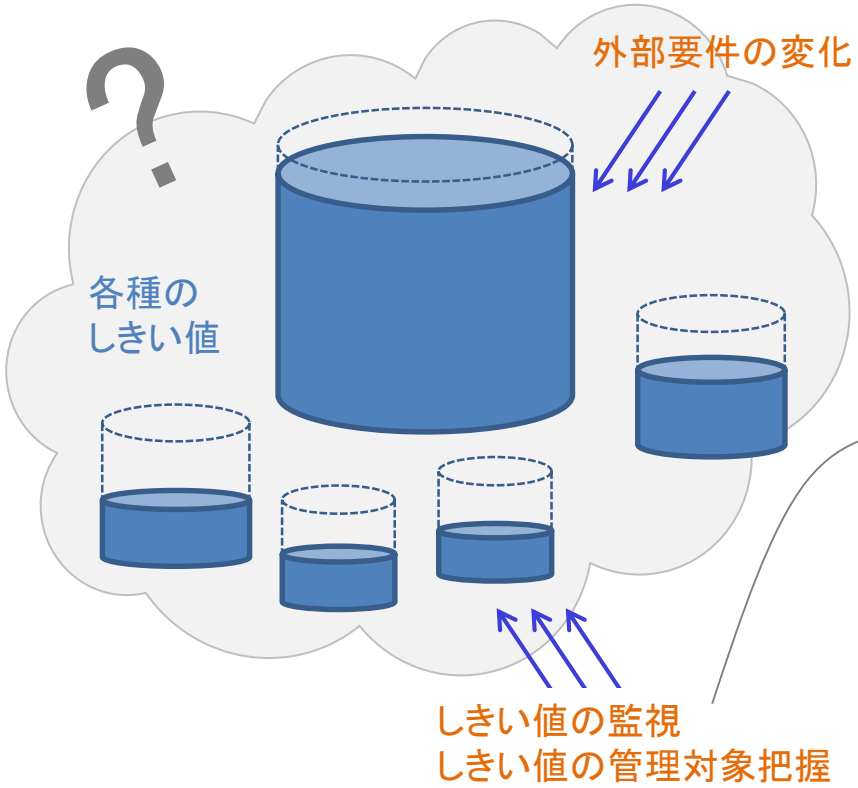
- 負荷分散装置でリクエストが廃棄されていたが、廃棄数がしきい値未満であったため検知できなかった — 教訓 T11

主要な対策方法

- 蟻の目だけでなく、<u>システム全体を俯瞰する鳥の目で総合的対策を実施（教訓T2参照）</u>
- <u>障害監視は複数の観点から実装（教訓T23参照）</u>

⑥ しきい値の超過

関係者が認識できていない暗黙のしきい値



業務要件変更時のしきい値不変更

予測可能時間を増大した際に予測対象列車数の上限値を変更せず、予測ダイヤを表示できなくなった。

教訓 T4

しきい値超過の不検知

スローダウンを契機に、重要性を認識していなかった予約処理のバッファが連鎖的に満杯となり、全体機能が停止

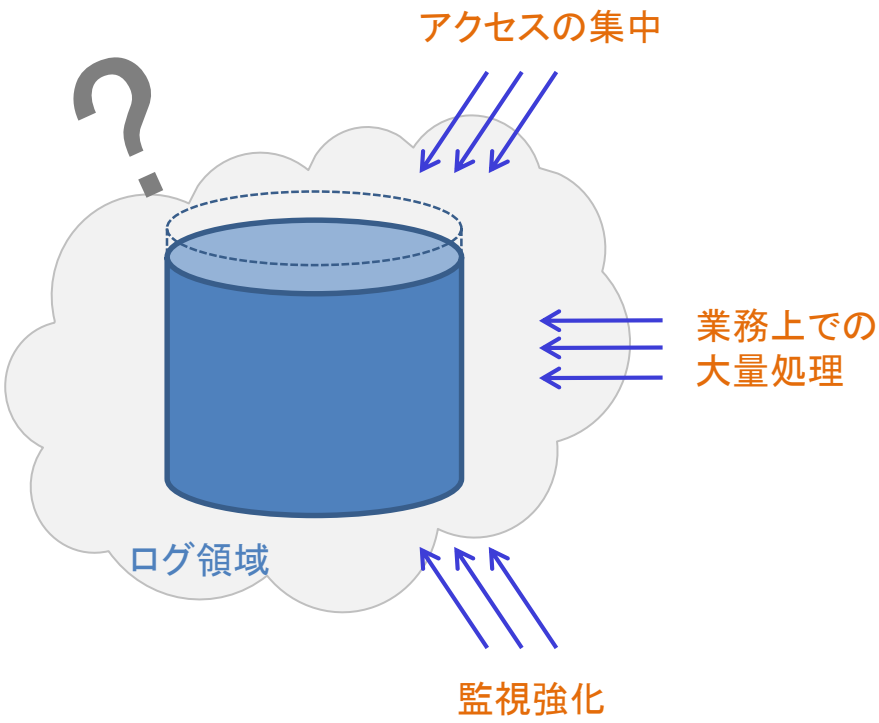
教訓 T22

主要な対策方法

- 外部要件の変化点の管理強化による上限値越えの予測と見直し（教訓T4参照）
- バッファ蓄積状況、データ滞留状況等の監視、アラート設定、しきい値として管理すべき対象の把握

⑦ ログの肥大化

ログの容量が想定以上に増加



アクセス集中時のログ肥大化

動画配信サービスでアクセス集中時にログが急増し、リソース不足により処理が滞留。配信予定のライブ中継映像が提供できなかった

事例 1710

大量業務処理時のログ肥大化

大規模マンションの住民の地番修正時に同マンションに入居する他住民もログに記録するため、ログ容量が超過し障害発生

事例 1507

監視強化によるログ肥大化

滞留プロセスを重点監視した結果、ログが大量に記録され、ログデータ転送時にメモリ不足となりATMが停止

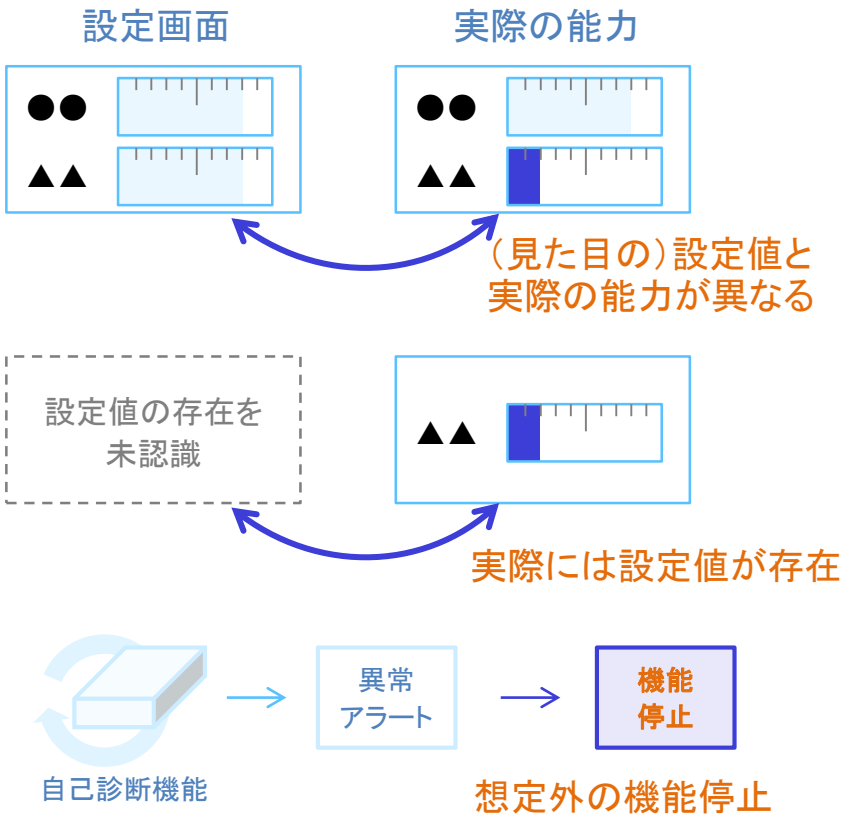
事例 1611

主要な対策方法

- 記録が必要となるログの精査、ログ容量の事前予測
- ログ領域に対する監視設定と、定期的な領域使用量確認

⑧ 製品仕様の誤解

製品独自の制約事項や仕様条件



感覚と異なる設定値

負荷分散装置のセッション数が設定値の1/4となる「仕様」のため、応答速度が低下した

教訓 T11

隠れた設定値

帳票作成用パッケージの仕様を把握しておらず、同時に実行できる印刷命令数の設定を誤り、証明書発行システムで障害発生

事例 1501

異常検知のみで機能停止

ディスクモジュールの自己診断機能で、異常検知のみで機能停止する仕様となっていた

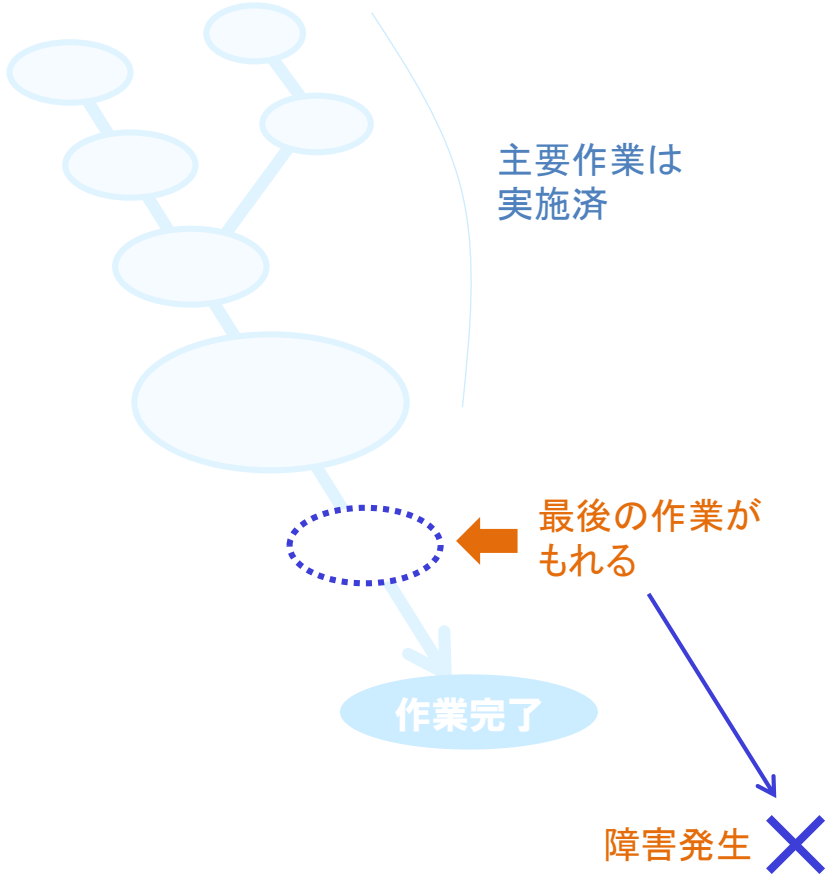
教訓 G11

主要な対策方法

- **サービス視点からの適切な監視（教訓T11参照）**
- ファームウェアのバージョンアップ内容を含めた、製品仕様の確認

⑨ 不完全な作業実施

作業完了の誤認や作業の確認もれ



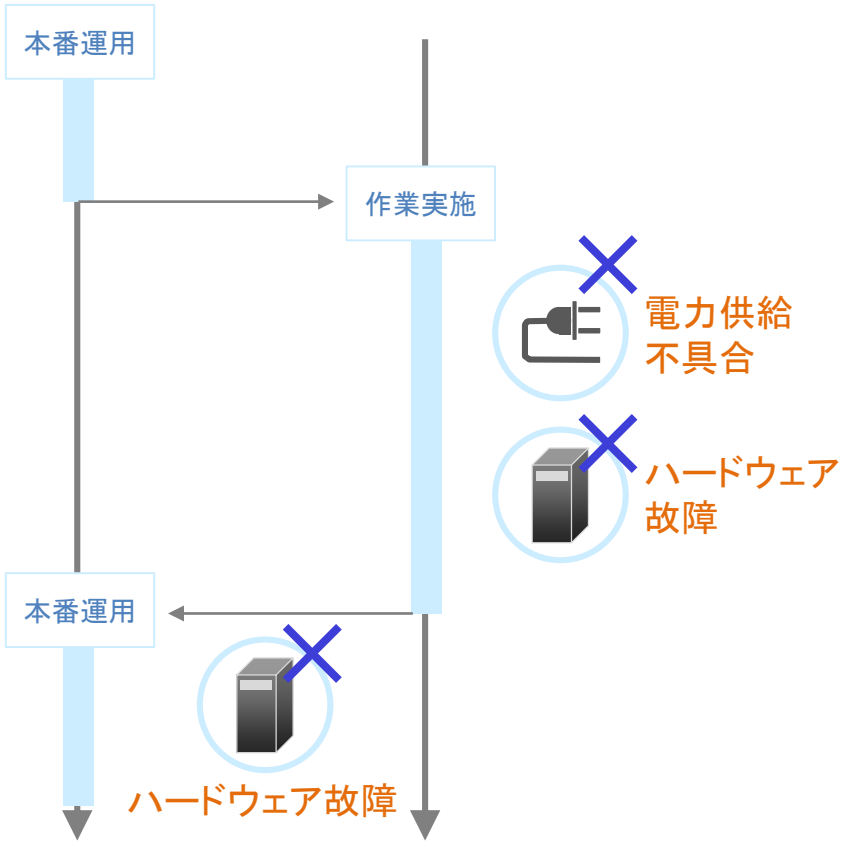
作業完了の誤認	動作確認が完了したと誤認してプロシージャを強制終了してしまい、未完了の書込み機能が繰り返し起動してディスクを一杯にした	教訓 G16
再起動もれによる作業未反映	運賃切替のためのシステム更新時に、駅員が券売機1台の電源を切り忘れたため更新できず、切符の販売金額を誤った	事例 1411
緊急作業と定期作業の競合で更新漏れ	顧客データの定期修正時に、緊急作業更新前のデータを対象としたため、緊急作業結果が反映されなかった	教訓 T15

主要な対策方法

- 本番環境に適用する資産に対する**動作環境の確認徹底（教訓G16参照）**
- **緊急時こそ、データの一貫性を確保するように注意（教訓T15参照）**

⑩ 作業中偶発事象への考慮不足

偶発的な電力供給不具合やハードウェアの故障



作業時の電力供給不具合

- 電源設備の定期点検中に、システムへの電力供給に不具合が発生し、システムがダウンした — 事例 1305
- 列車指令所内の電源装置のバッテリー交換時に不具合が発生し、運行管理システムへの電力供給が止まり、列車が約1時間運休した — 事例 1708

作業時のハードウェア故障

- 保守作業のため自動切替を解除した時にハードウェア故障が発生し、サービスが10分間停止 — 教訓 G15

切戻し時のハードウェア故障

- 新設備へのバージョンアップに失敗し、現行設備への切戻し中に新設備の片系でハード障害が発生し、残りの片系も過負荷でサービスがダウン — 事例 1314

主要な対策方法

- 「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（教訓G15参照）**
- **業務特性レベルに応じた保守作業時の不測事態発生への備えの設定（教訓G15参照）**