「注意すべき観点」に基づいた
障害事例の分類

障害事例を分類する狙い

全体像の理解

- 詳細な事例内容を読込まなくても、短い時間で障害事例のポイントや全体像を理解できるようにしたい
- 障害発生パターンの全体像を一覧できるようにして、読者が詳細を確認したいと考えた事象に、すぐにたどり着くようにしたい

読者の追体験

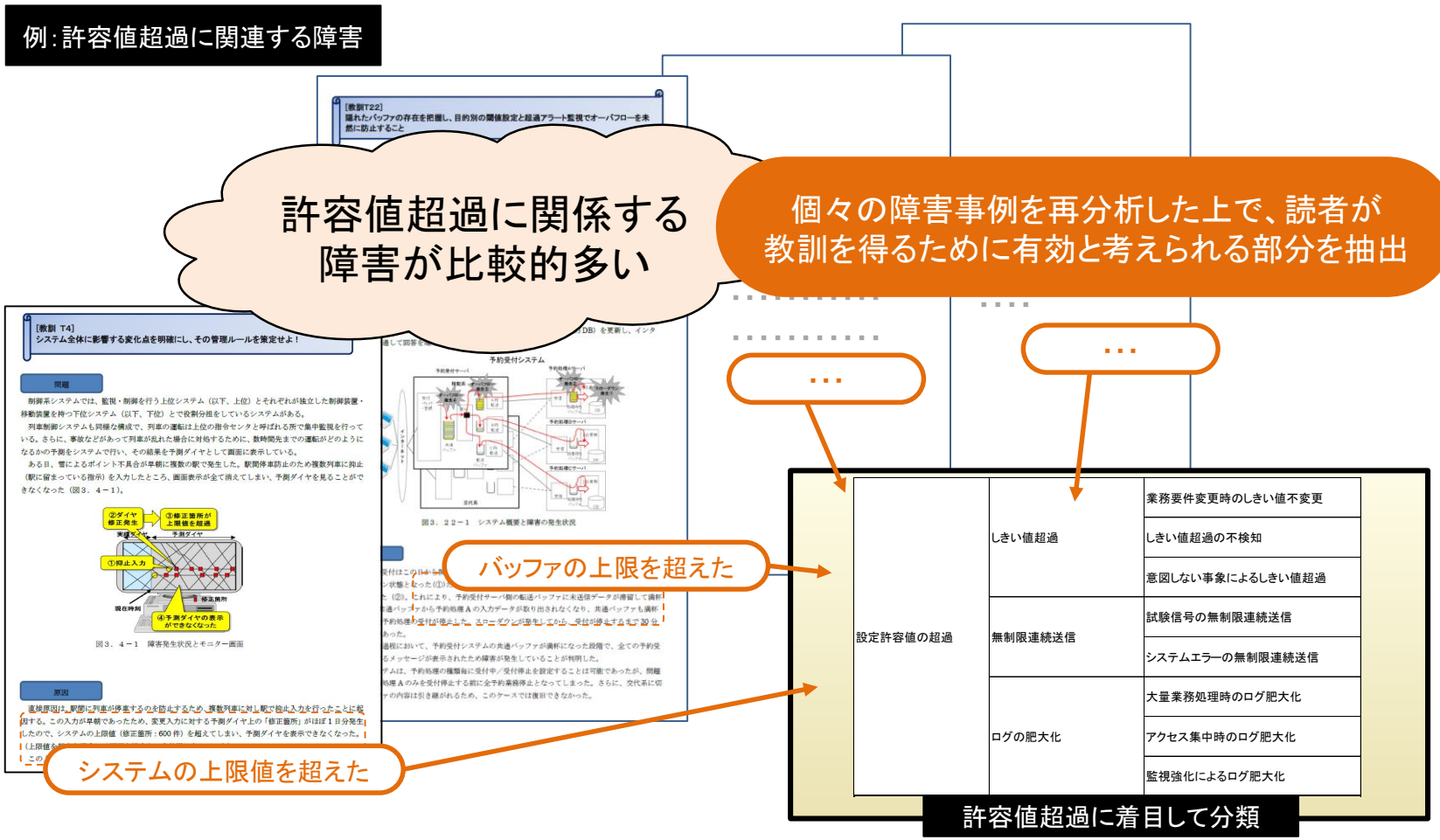
- 障害の表面的な発生原因や発生影響ではなく、「注意すべき点」を強調することで、読者自身が過去事例を追体験できるようにしたい
- 「注意すべき点」の体系に沿って教訓を提示することで、教訓の真意をより深く理解し、様々な現場に応用できるようにしたい

「注意すべき観点」に基づく分類で、過去の事例を再整理

分類の特徴　① 注意すべき観点に基づいた分類

障害内容には多種多様な分類方法（業種別、工程別、発生箇所別、原因別、影響別等）が考えられますが、読者に気づきを与える「注意すべき観点」に基づいて分類しました。

例：許容値超過に関連する障害



分類の特徴　② 分類名称のキーワード化

分類名称を短い単語に集約しつつ、読者が「なるほど」、「ありうる」と問題を追体験できるようなキーワードを選定しました。

例1
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

？　「負荷分散装置の性能不足」

○　「**感覚と異なる設定値**」

例2
ゲートウェイ設定の指示書でパラメータをローマ字で記載しており、これを誤読した結果、電話コールが異なる拠点へ転送された

？　「入力ミス」

○　「**誤解を生む作業指示**」

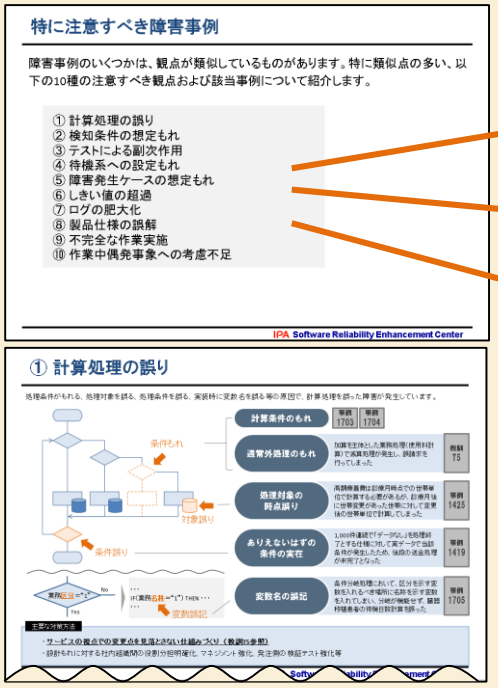
なお、それぞれの事例については、キーワードだけでなく発生事象の概況を短文（50文字程度）で解説しています。

成果物の全体構成

従来の成果物（教訓集、情報システムの障害状況一覧）へリンクする形で、事例を再整理しました。

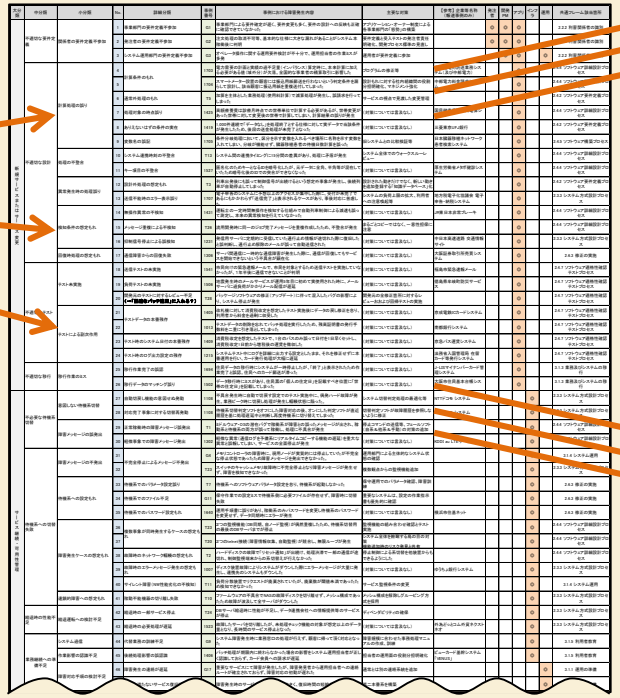
概要版
（特に注意すべき障害事例）

一覧表で整理した事例の中でも、特に注意すべき事例を解説した資料



一覧表
（「注意すべき観点」を中心とした障害事例の分類）

教訓事例、情報システムの障害状況一覧から、特に「注意すべき観点」を中心として分類をまとめ直したもの



教訓集

詳細な解説
教訓の導出

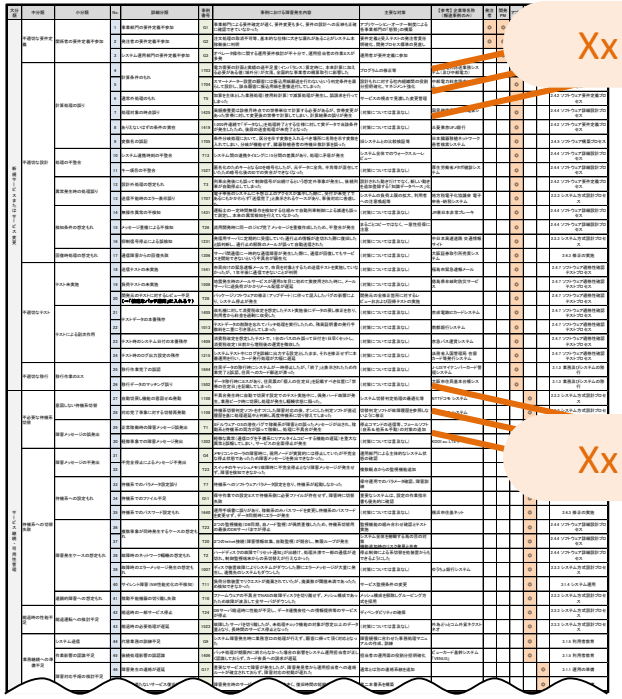
情報システムの障害状況一覧

報道事例の
概況整理

対象とした障害情報の範囲

再整理した事例の対象範囲は、以下のとおりです。

一覧表
（「注意すべき観点」を中心とした障害事例の分類）



Xx 事例

Xx 事例

教訓集

- 全ての教訓事例が対象
- 1つの教訓事例から複数の「注意すべき観点」を導出した例も存在

情報システムの障害状況一覧

- 「情報システムの障害状況」のうち、「詳細原因が理解できて教訓を得られるもの」を抽出

分類の構成

障害事例は以下の構成で分類されています。

■ 大分類

サービスマネジメントシステムの規格である JIS Q 20000-1:2012 に基づいて分類されています。

■ 中分類／小分類／詳細分類

各大分類のサービスマネジメントの範囲において、注意すべき観点に基づいて分類されています。

大分類	中分類	小分類	No.	詳細分類	事例番号	事例における障害発生
	不適切な要件定義	関係者の要件定義不参加	1	事業部門の要件定義不参加	G1	事業部門による要件確定が遅く、要件変更も多く、確認できていなかった
			2	発注者の要件定義不参加	G2	注文処理の取消不可等、基本的な仕様に大きな漏後に判明
			3	システム運用部門の要件定義不参加	G3	オペレータ操作に関する運用要件検討が不十分で
			4		1703	電力需要の計画と実績の過不足量(インバランス)要がある値(域外分)が欠落。全国的な事業者の精
					1704	スマートメーター設置の顧客には振込用紙郵送を

注意すべき観点

・事例番号のうち、GまたはTで始まるものは高信頼化教訓集、数字4桁は「情報システムの障害状況」のものである。

成果物の利用方法　① 対象者視点

障害発生内容に特に関係の深い「対象者」の視点で、区分しています。

る障害発生内容	主要な対策	【参考】企業等名称（報道事例のみ）	発注者	PM	アプリ	インフラ	運用	共通フレーム該当箇所
件変更も多く、要件の設計への反映も正確	アプリケーション・オーナー制度による各事業部門の「態勢」の構築		◎	◎	◎			2.2.2 利害関係者の識別
仕様に大きな漏れがあることがシステム本	要件定義と受入テストの発注者責任明確化、開発プロセス標準の見直し		◎	◎	◎			2.2.2 利害関係者の識別
検討が不十分で、運用担当者の作業ミスが	運用者が要件定義に参加			◎	◎		◎	
インバランス）算定時に、本来計算に加え全国的な事業者の精算取引に影響した	プログラムの修正等	北海道電力託送業務システム（及び中部電力）			◎			2.4
送用紙郵送を行わないという判定条件を漏を重複送付してしまった	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	中部電力料金請求システム			◎			2.4
算）で減算処理が発生し、誤請求を行って	サービスの視点で見渡した変更管理				◎			2.4
単位で計算する必要があるが、世帯変更が計算してしまい、計算結果の誤りが発生	（対策については言及なし）	国民健康保険共同電算システム			◎			2.4
了とする仕様に対して実データで当該条件が未完了となった	（対策については言及なし）	三菱東京UFJ銀行			◎			2.4
変数を入れるべき場所に名称を示す変数を移植患者の待機日数計算を誤った	旧システムとの比較検証等	日本臓器移植ネットワーク患者検索システム			◎			2.4
間の差異があり、処理に矛盾が発生	システム全体でのウォークスルーレビュー				◎			2.4
たが、元データに全角、半角等が混在してきなくなった	（対策については言及なし）	厚生労働省メタボ健診システム			◎			2.4
出続けるという想定外事象が発生し、後続列	設計された動きだけでなく、新しい動きを追加登録する「知識データベース」化				◎			2.4
クセスが集中した際に、受付が未完了で示されるケースがあり、事後対応に苦慮し	システムの負荷上限の拡大、利用者への注意喚起等	地方税電子化協議会 電子申告・納税システム			◎			2.5

対象者の区分

発注者	情報システムを**発注する立場の人**が、特に注意すべき観点
PM	情報システムの開発チームの中で、特に**PM（プロジェクトマネージャ）**が注意すべき観点
アプリ	情報システムの開発チームの中で、特に**アプリケーションSE**が注意すべき観点
インフラ	情報システムの開発チームの中で、特に**インフラSE**が注意すべき観点
運用	情報システムの運用チームの中で、特に**運用SE**が注意すべき観点

成果物の利用方法　② 工程視点

障害発生の原因が発生した「工程」の視点でも、区分しています。

ける障害発生内容	主要な対策	【参考】企業等名称（報道事例のみ）	発注者	PM	アプリ	インフラ	運用	共通フレーム該当箇所
件変更も多く、要件の設計への反映も正確	アプリケーション・オーナー制度による各事業部門の「態勢」の構築		◎	◎	◎			2.2.2 利害関係者の識別
仕様に大きな漏れがあることがシステム本	要件定義と受入テストの発注者責任明確化、開発プロセス標準の見直し		◎	◎	◎			2.2.2 利害関係者の識別
討が不十分で、運用担当者の作業ミスが	運用者が要件定義に参加			◎	◎		◎	2.2.2 利害関係者の識別
増えた注文が殺到し、サービス時間を短縮し	業務部門がキャパシティ管理に責任を持ち、管理項目と閾値を設定		◎			◎		2.2.3 要件の識別
受け為替相場が大きく変動し、全商品の取	（対策については言及なし）	東京商品取引所	◎			◎		2.2.3 要件の識別
アクセスを想定できず、発売開始直後から想システムが停止	チケット販売期間を前半と後半に分ける等、処理の分散化	東京国際映画祭電子チケット販売システム	◎			◎		2.3.2 システム要件定義プロセス
アクセスが集中した影響で、既存の切符購入	（対策については言及なし）	JR東日本モバイルSuica	◎			◎		2.3.2 システム要件定義プロセス
受信したところ、メールから参照したWebサイウンした	暫定的には、Webサーバから容量の大きい地図データを削除	横浜市Webサイト	◎	◎	◎	◎		2.3.2 システム要件定義プロセス
4倍になり、レスポンスが低下	業務部門作業をIT部門が確認することを一ルール化						◎	2.3.2 システム要件定義プロセス
象列車数の上限値を変更せず、予測ダイ	変化点の管理指標化				◎			2.3.2 システム要件定義プロセス
識していなかった予約処理のバッファが連鎖	各バッファの蓄積状況監視、アラート設定				◎			2.3.2 システム要件定義プロセス
に不要データが蓄積し、重量管理システム	データ滞留の監視、ソフトウェアの改修	JAL機体重量管理システム			◎			2.3.2 システム要件定義プロセス
処理量を責任をもって予測せず、システム	利用各社による運営協議会を立上げ		◎	◎				2.3.2 システム要件定義プロセス
アクセスが集中した際に、受付が未完了で示されるケースがあり、事後対応に苦慮し	システムの負荷上限の拡大、利用者への注意喚起等	地方税電子化協議会 電子申告・納税システム			◎			2.3.3 システム方式設計プロセス
いた通行止め情報が途切れた際に復旧した が誤って自動送信された	（対策については言及なし）	中日本高速道路 交通情報サイト			◎			2.3.3 システム方式設計プロセス
でのテスト実施中に、偶発ハード故障が発住し輻輳状態に陥った。	システム切替判定処理の最適化等	NTTドコモ システム				◎		2.3.3 システム方式設計プロセス
害対応の後、オンにした判定ソフトが直近待機	切替判定ソフトが故障履歴を参照しないように	NTTドコモ システム				◎		2.3.3 システム方式設計プロセス

工程区分（SLCPに準拠）

2.2.2 利害関係者の識別
2.2.3 要件の識別
2.3.2 システム要件定義プロセス
2.3.3 システム方式設計プロセス
2.3.5 システム結合プロセス
2.4.2 ソフトウェア要件定義プロセス
2.4.4 ソフトウェア詳細設計プロセス
2.4.5 ソフトウェア構築プロセス
2.4.7 ソフトウェア適格性確認テストプロセス
2.6.3 修正の実施
2.6.4 保守レビュー及び／又は受入れ
3.1.1 運用の準備
3.1.3 業務及びシステムの移行
3.1.4 システム運用
3.1.5 利用者教育
3.1.7 システム運用の評価
3.3.4 統合的制御管理
5.5.2 構成管理の実行

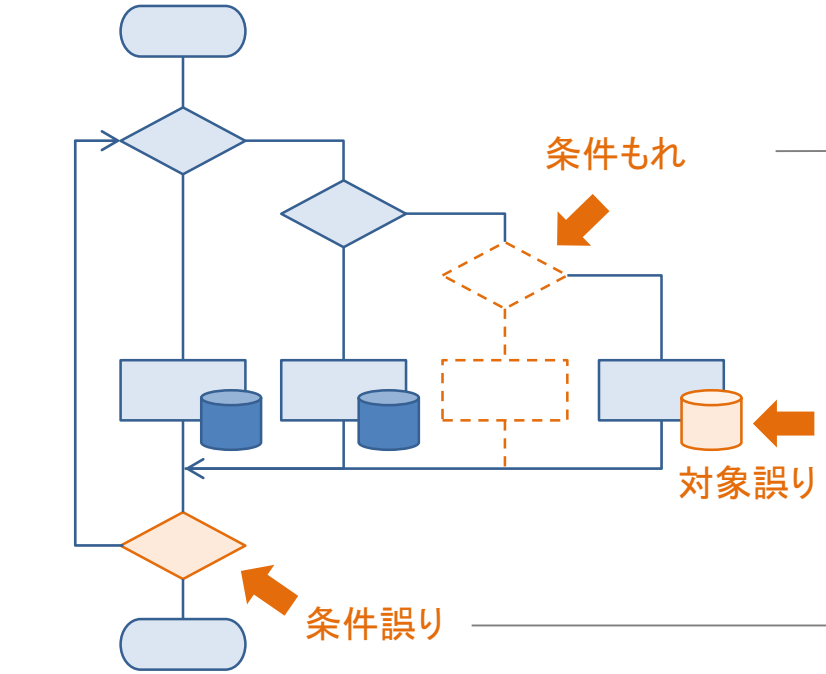
特に注意すべき障害事例

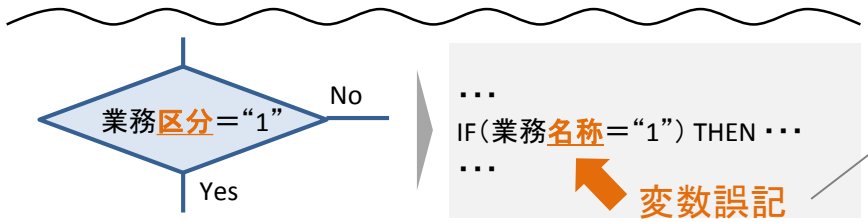
障害事例のいくつかは、観点が類似しているものがあります。特に類似点の多い、以下の10種の注意すべき観点および該当事例について紹介します。

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

処理条件がもれる、処理対象を誤る、処理条件を誤る、実装時に変数名を誤る等の原因で、計算処理を誤った障害が発生しています。





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

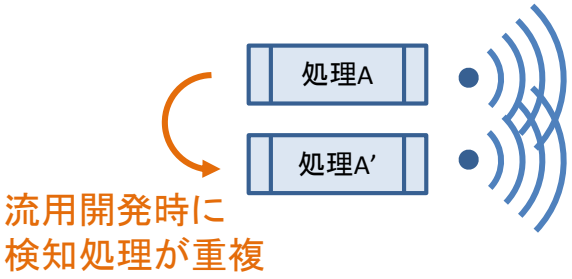
事例 1705

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

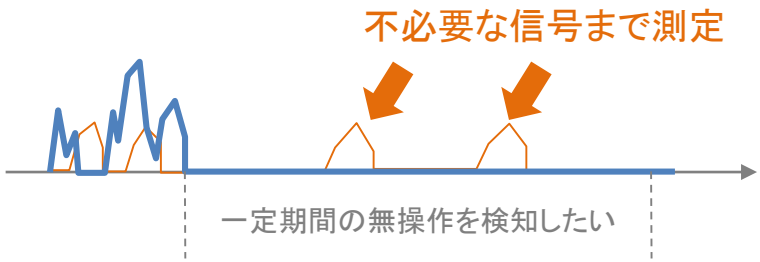
業務上の様々なイベントをシステムが検知する際に、検知処理の設計に誤りが埋め込まれやすく、これを原因とした障害が発生しています。



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

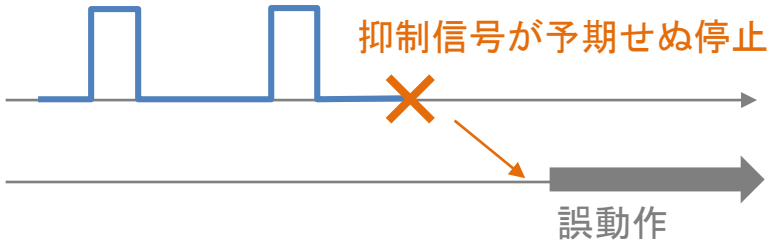
教訓 T26



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

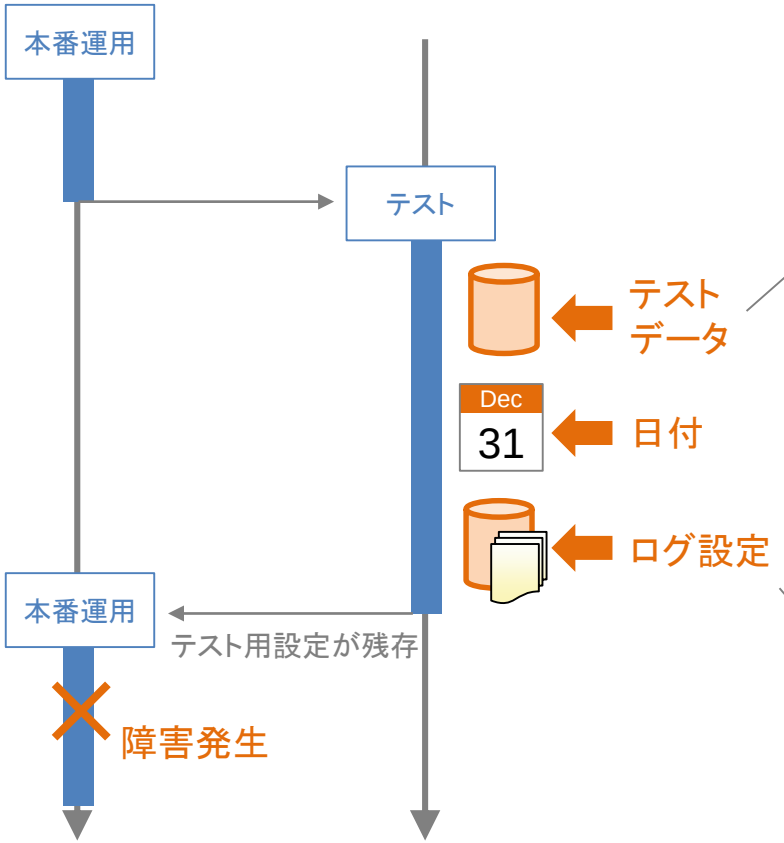
事例 1231

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

本番環境を用いたテストや切替実施時に、テスト用の設定を残存させてしまったこと等を原因とする障害が発生しています。



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

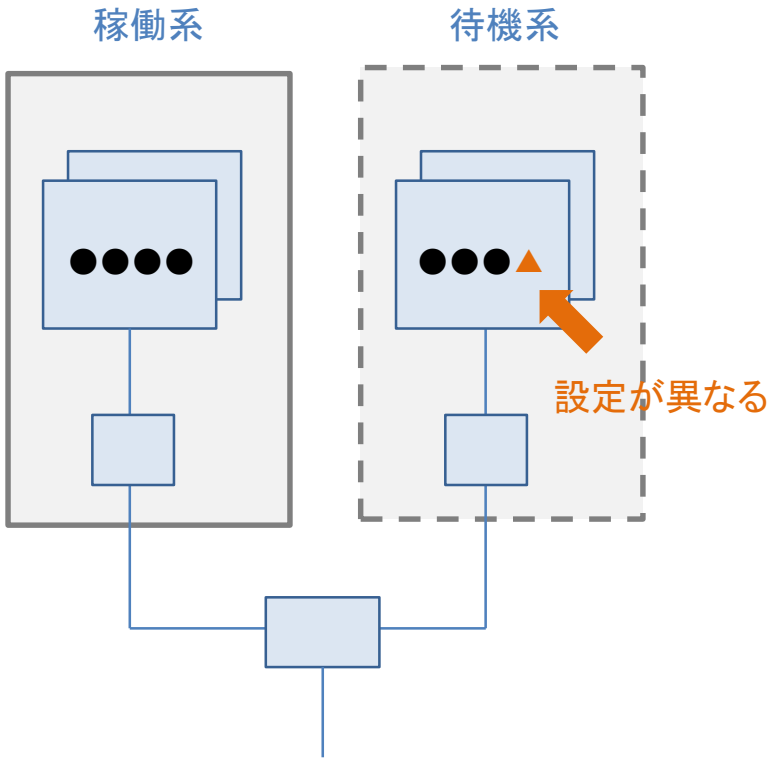
- システムテスト中にログを詳細に出力する設定としたまま、それを修正せずに本番運用を行い、カード発行処理が大幅に遅延 — 事例 1215

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

稼働系と待機系は基本的に同じ設定内容に保つ必要がありますが、待機系での設定を誤ったために、稼働系への障害発生時に待機系も起動できなかったという障害が発生しています。



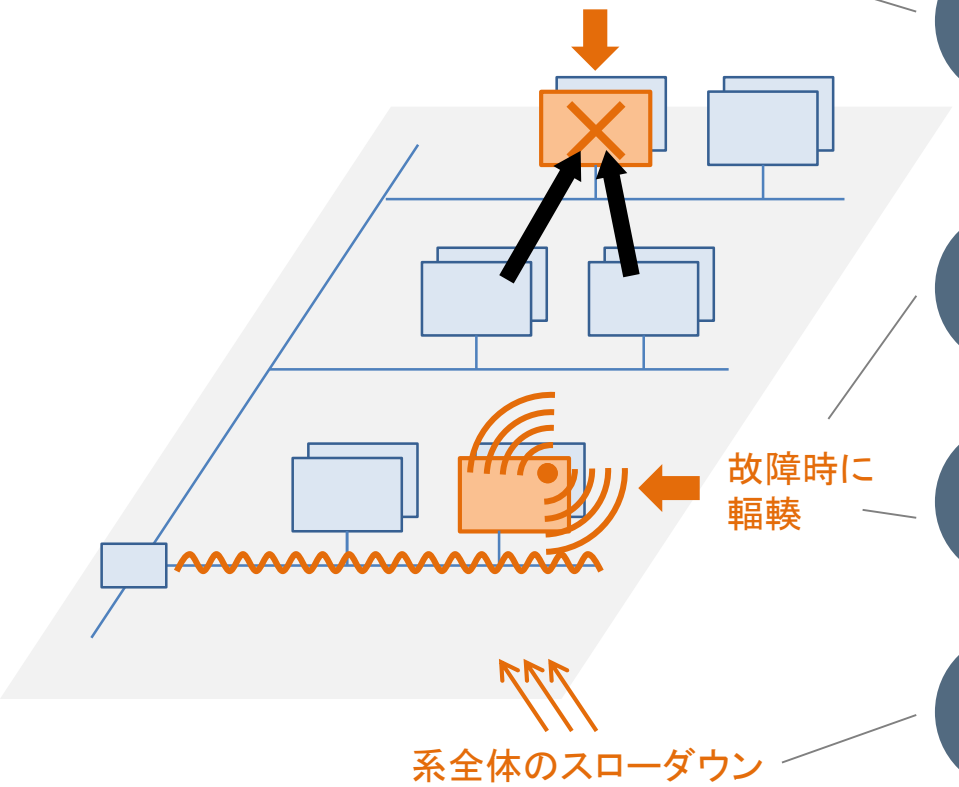
待機系でのパラメータ設定誤り	稼働系と待機系の同期を取るべきソフトウェアパラメータにもかかわらず、待機系への設定を怠り、待機系が起動しなかった	教訓 T7
待機系でのファイル不足	保守作業での設定ミスで待機系側に必要ファイルが存在せず、障害時に切替失敗	教訓 G11
待機系でのパスワード設定もれ	稼働系のみパスワードを変更し待機系のパスワードを変更せず、データ同期時にエラーが発生	事例 1640

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、複数の処理が競合して障害が拡大したり、エラーメッセージが大量に出続けることで二次障害を誘発する事例が発生しています。



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）

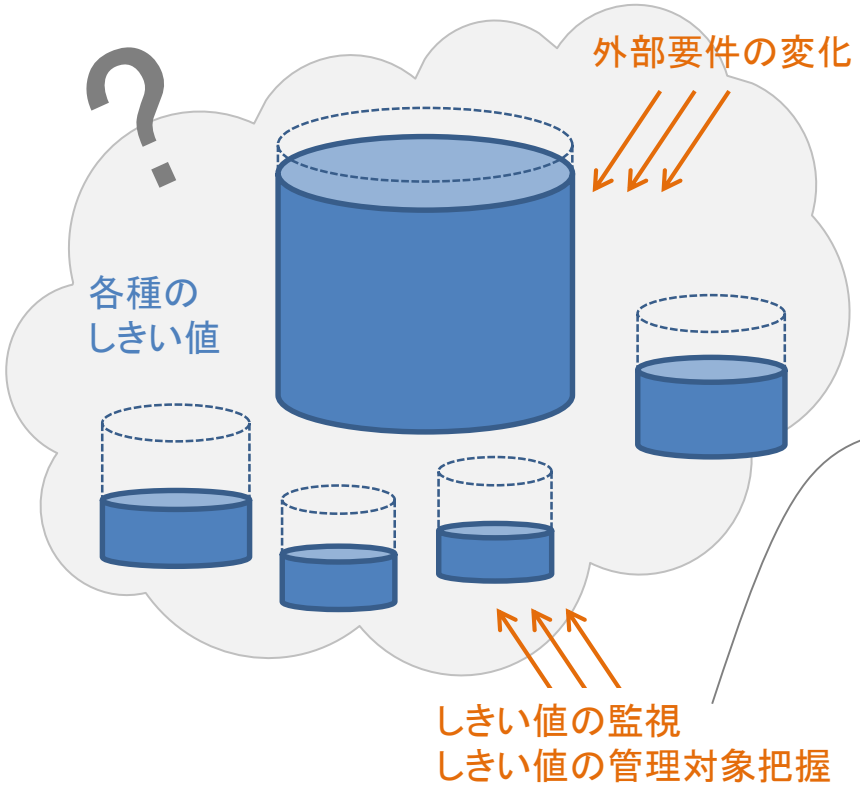
- 負荷分散装置でリクエストが廃棄されていたが、廃棄数がしきい値未満であったため検知できなかった — 教訓 T11

主要な対策方法

- 蟻の目だけでなく、**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）**
- **障害監視は複数の観点から実装（教訓T23参照）**

⑥ しきい値の超過

システム内部には、関係者が認識している明示的なしきい値もあれば、関係者が認識できていない暗黙のしきい値もあります。外部環境の変化や、長期の継続運用の結果、これらのしきい値を超過したことによる障害が発生しています。



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

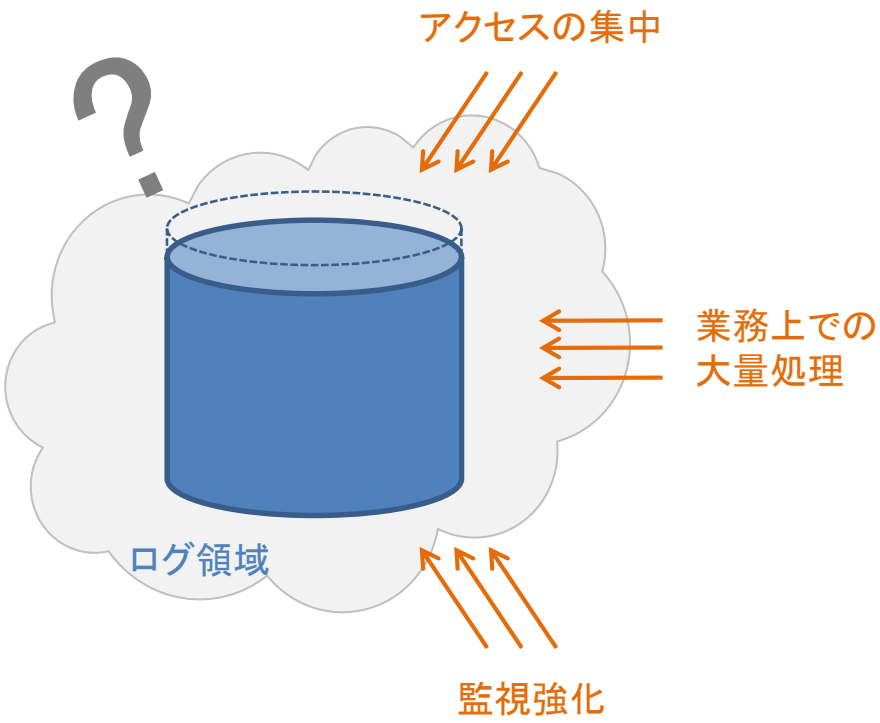
教訓 T22

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

前述のしきい値の一種でもありますが、ログの容量が想定以上に増加したことによる障害が数多く発生しています。



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

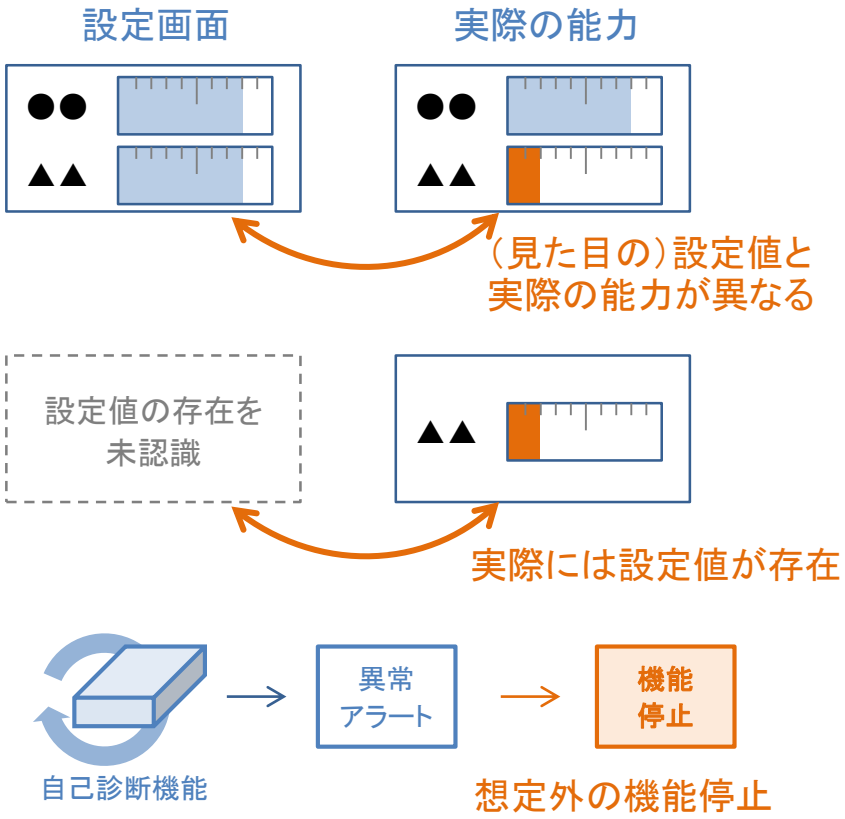
監視強化によるログ肥大化
滞留プロセスを重点監視した結果、ログが大量に記録され、ログデータ転送時にメモリ不足となりATMが停止
事例 1611

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

ハードウェア、ソフトウェア等の各製品には、独自の制約事項や仕様条件が存在することがあります。この点を熟知せずに製品を利用したことによって、障害が発生しています。



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

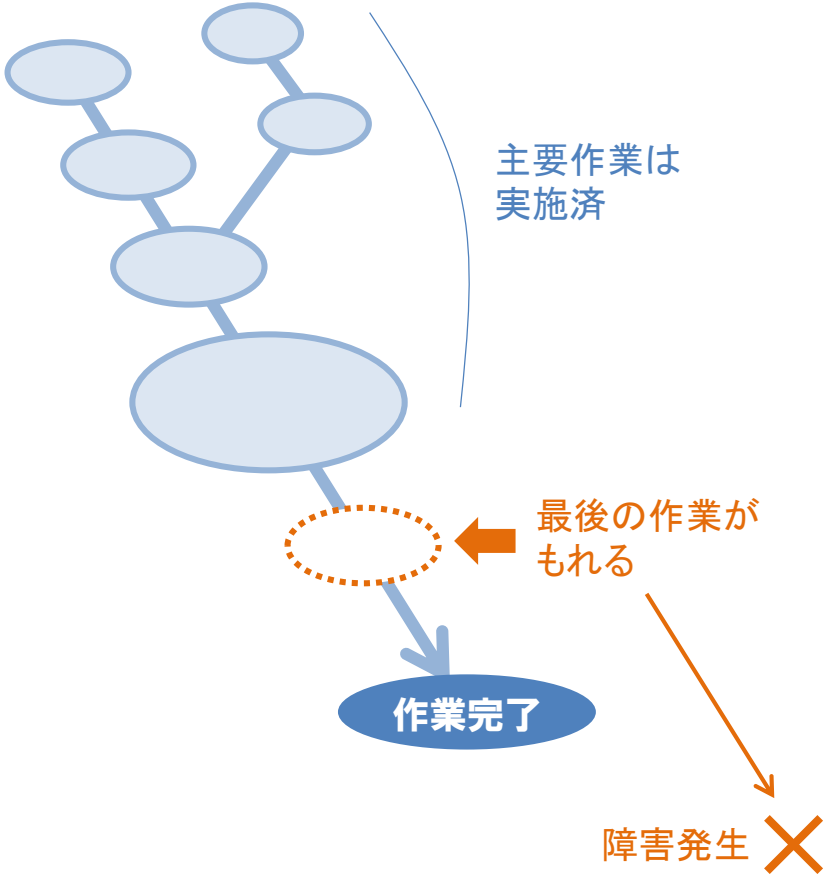
教訓 G11

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

システムの運用作業の中で、主要となる作業は確実に実施しつつも、最終的な作業や確認がもれたことによって障害が発生しています。



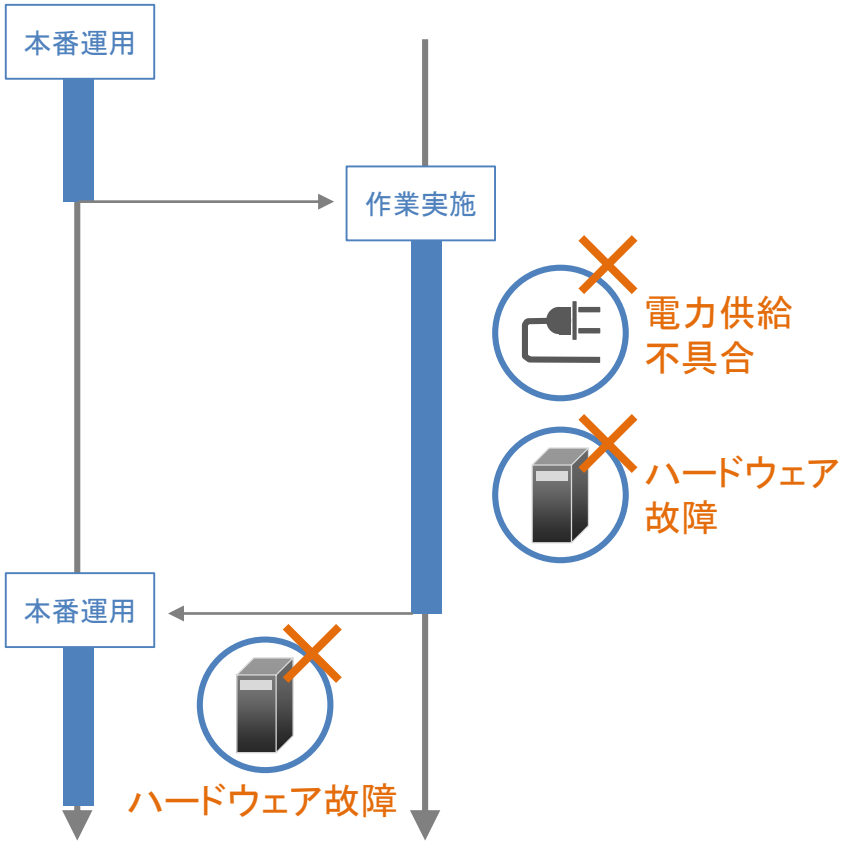
作業完了の誤認	動作確認が完了したと誤認してプロシージャを強制終了してしまい、未完了の書込み機能が繰り返し起動してディスクを一杯にした	教訓 G16
再起動もれによる作業未反映	運賃切替のためのシステム更新時に、駅員が券売機1台の電源を切り忘れたため更新できず、切符の販売金額を誤った	事例 1411
緊急作業と定期作業の競合で更新漏れ	顧客データの定期修正時に、緊急作業更新前のデータを対象としたため、緊急作業結果が反映されなかった	教訓 T15

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

システムの一時的な運用作業の中で、偶発的に電力供給やハードウェアの故障が発生したことによって障害が発生しています。



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）**