システム安定稼働のためのインシデント対応計画と運用体制

Incident Response Plan and Management Structure for the Stable Operation of the System

中　尾　茂　文

要　約　システムの本番稼働後に発生するインシデントに対し，迅速かつ確実に対応するための準備が必要である．取引管理システム（後続稼働）プロジェクトでは，インシデント対応に備えたルール，作業プロセス，手順を特別体制計画として定義した．さらに，プロジェクトメンバーは本番稼働まで手順の訓練を繰り返した．

特別体制期間中は，約 4,900 件のインシデントが発生したが，特別体制に向けた準備と訓練により，発生したインシデントに対し効率よく迅速に対応し，安定稼働に繋げることができた．

Abstract　To deal quickly and reliably with the incidents that occur after the cutover of a system, it is necessary to plan the scheme to manage the incidents. On the project of JAPAN POST Trade Management System development, we defined the rules, work processes and procedures, and planned scrupulously how we would respond the incidents. Furthermore, the project's members repeated the training to respond the incidents in accordance with those definitions.

Although about 4,900 incidents occurred in the several months after the cutover of the system, we handled the incidents promptly and efficiently. Thus, we accomplished the stable operation.

1. は　じ　め　に

システムの本番稼働後に発生するシステム利用者からの問い合わせ，データ抽出などの作業依頼，障害，変更要求などのインシデントに迅速かつ確実に対応し，顧客の業務への影響を最小限に留めるために，体制の整備が必要である．

取引管理システム（後続稼働）プロジェクト[*1]（以降，本プロジェクト．取引管理システムは以降，本システム，または単にシステム）では，インシデント対応に備えた本番稼働後の特別体制計画を策定し，特別体制を解除するクライテリア，発生するインシデント数の予測，体制と役割の定義，インシデント対応フローとインシデント管理ツールの整備，システムの正常/異常稼働の早期検出を目的とした特別監視運用の定義，および会議体/情報共有手段など，ルールや手順を準備した．

本番稼働の 1 ヶ月前から特別体制計画の訓練を実施し，訓練で挙げられた課題を次回の訓練で是正することを繰り返し，本番稼働に臨んだ結果，安定稼働に繋げることができた．

本稿では本プロジェクトの事例を紹介し，本番稼働後のインシデント対応に向けて準備すべき事項について論じる．2 章で特別体制，3 章で訓練を説明し，4 章にて結果と考察を述べる．

2. 特別体制に向けた準備

本章では，特別体制計画で策定すべき事項と，本プロジェクトでの適用について述べる．

2.1 特別体制解除クライテリアの設定

まず，特別体制を終了して通常保守体制へ切り替える基準を明確にするため，特別体制を解除するクライテリアを表1のように設定し，顧客との間で合意した．

表1 特別体制解除クライテリア

評価の観点	評価対象	クライテリア
インシデントの収束	インシデント数	週間あたりのインシデント発生が予測の件数以内であり収束傾向があること
重大障害の発生	重大障害の発生間隔	直近2週間で重大障害が発生していないこと
積み残し作業量	残障害件数	残障害件数が以下のとおりであること 極大＝0件，大＝0件，中＜20件 （極大，大，中は業務影響度を示す）
バッチ安定性	バッチ処理の運用状況	バッチが自動運行可能であること 休日夜間オンコール体制が確立していること

本プロジェクトでは，本番稼働日から1ヶ月後と2ヶ月後にクライテリアの仮評価を，3ヶ月後に本評価を実施する計画とした．

2.2 インシデント数予測と要員数の算出

本番稼働後の体制を検討する際，その時にアサインが可能な要員で各チームを編成してしまうことがあるが，そうすると後になって要員不足や要員過剰に陥りやすい．

本プロジェクトでは，顧客の業務サイクルから，発生するであろうインシデント数を日次で予測し，インシデント受付とインシデント解析を担当する要員数を以下のステップにより算出した．

1）月次の顧客業務イベントカレンダーを作成
2）日次の顧客業務イベントカレンダーを作成
3）月間のインシデント発生数合計を予測
4）月次の顧客業務イベントカレンダーを考慮し，月間のインシデント発生数合計に占める日次のインシデント発生割合を設定
5）日次の顧客業務イベントカレンダーを考慮し，日中帯（9時～21時），夜間帯（21時～9時）のインシデント発生割合を設定
6）インシデント区分をシステム操作方法などの問い合わせ，データ抽出などの作業依頼，障害，および変更要求の4区分に分け，各インシデントの発生割合を設定
7）インシデント1件あたりのインシデント受付，一次切り分け，回答作業の生産性を設定（1.0h/件）
8）インシデント1件あたりのインシデント解析作業の生産性を設定（4.0h/件）

月次の顧客業務イベントカレンダーを作成する際に顧客へヒアリングし，月末・月初，五十日（ごとおび．毎月 5 日，10 日，15 日，20 日，25 日，30 日）とその翌日，顧客業務における締め日など，特異日が見えるように作成した．日次の顧客業務イベントカレンダーでは一日の顧客業務の流れを表し，どの時間帯でシステム利用が多くなるかを見えるように作成した．夜間帯では重要なバッチ処理の起動時刻，終了時刻を表した．

2. 3　体制/役割

特別体制解除クライテリアの設定，インシデント数予測における必要要員数の検討結果などを踏まえ，図 1 に示す特別体制を構築した．

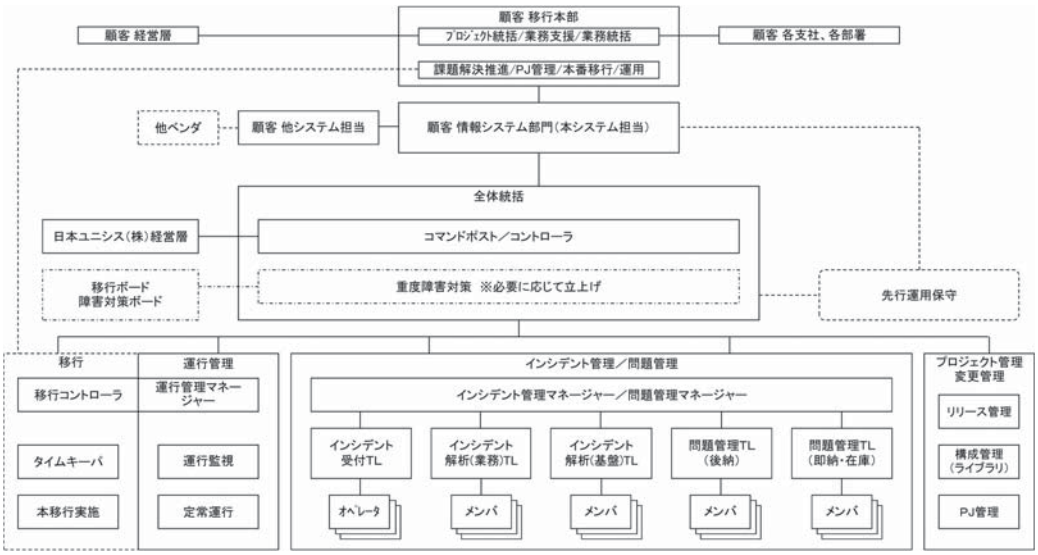

図 1　特別体制図

IT 運用に関する業務を全般的に体系化し，再構築するための指針として利用できるのが ITIL（Information Technology Infrastructure Library）であり，本プロジェクトでは ITIL のサービスサポートとして定義されている「インシデント管理」「問題管理」「変更管理」「リリース管理」「構成管理」を主要な役割として体制を組むこととした（表 2）．特にインシデント管理マネージャー，インシデント解析チームリーダ，問題管理マネージャー，問題管理チームリーダには，顧客の業務内容やシステム仕様を熟知した要員を，主要なサブシステムごとに配置した．これにより各役割内での担当業務領域のムラをなくし，迅速かつ確実なインシデント対応を可能とした．

2. 4　インシデント対応フローとインシデント管理ツール

インシデントに対応する際，プロジェクトメンバーが同じ作業プロセス，ルールの下で作業を実施することが重要である．本プロジェクトでは，顧客からの問い合わせや障害連絡などのインシデント受付，インシデント解析，暫定対応，恒久対応，顧客への回答，本番環境へのリリースなどの一連の流れを迅速かつ効率的にできるよう，図 2 に示すインシデント対応フローとして整理した．また，受付からリリースまでの作業履歴を管理するために，大規模システム

表 2　特別体制内の役割表

体　　制		主な役割
全体統括	コマンドポスト	・作業全体に関する最終的な承認 ・経営層への報告
	コントローラ	・全体的なリソースコントロール ・チェックポイント会議開催，重度障害対策ボード招集 ・リリース案件に対する品質データ管理と評価 ・稼働実績の週次モニタリング，稼働調整
	重度障害対策	・重度障害の管理（対策者の割付，状況確認など）
移行ボード・障害対策ボード		・移行作業の遅延，障害発生時に全体統括が開催
移行チーム	移行コントローラ	・移行作業全体管理 ・顧客への状況報告
	タイムキーパー	・移行作業タイムキーパー，進捗状況の把握
	本移行実施	・移行作業実施
インシデント管理	インシデント管理マネージャー	・インシデント受付窓口からの障害申告の受付 ・インシデント解析チームリーダへの解析指示，業務影響度判定 ・暫定/恒久対応の実施時期を判断・指示
	インシデント受付チームリーダ	・インシデント管理ツールへ事象登録 ・インシデントの定期的な棚卸
	インシデント受付オペレータ	・インシデント受付（メール，電話） ・インシデント管理マネージャー/インシデントチームとの連携 ・問合わせ元への回答
	インシデント解析チームリーダ（サブシステムごとに配置）	・業務影響，回避方法検討，運用制限事項，対応方針，パッチ適用，コード修正，要件整理などのインシデント解析 ・暫定対応（運用検討，パッチ作成）の指示，内部レビュ ・問題管理チームとの連携・調整
	インシデント解析担当（サブシステムごとに配置）	・インシデント解析 ・暫定対応（運用回避，暫定スクリプト） ・検証環境でのリグレッションテスト
問題管理	問題管理マネージャー	・障害の解析/対応状況全体管理 ・各問題管理チームへの対応指示，進捗管理，要員割り当て管理 ・リリース判定会議での報告
	問題管理チームリーダ（サブシステムごとに配置）	・顧客対応方針レビュおよびテスト結果報告対応 ・インシデント解析チーム，リリース管理チームとの連携 ・顧客リリース判定会議での報告 ・リグレッション結果検証レビュ
	問題管理担当（サブシステムごとに配置）	・担当障害に対する原因追及，恒久対応 ・顧客対応方針レビュおよびテスト結果報告対応
運行管理	運行管理マネージャー	・運行業務の全体管理，担当者への指示 ・顧客への稼働状況報告 ・問題管理チームから依頼された運用作業の受付
	定常運行担当	・定常，定型の AP 運用作業実施，非定常作業実施 ・新規/更新済み定型作業の受入，運用一覧管理 ・非定型作業の実施
	運行監視担当	・バッチステータス監視，運行管理マネージャーへの報告 ・運行管理マネージャーへの稼働状況報告，リリース後の状況注視報告 ・統合監視ソフトウェアによるアラート受付/管理
変更管理	リリース管理	・リリース計画策定 ・リリース内容，作業の承認 ・検証環境/本番環境へのリリース作業実施
	構成管理	・リリース申請受付，リリース資材作成 ・リグレッションテスト全体管理
プロジェクト管理	プロジェクト管理	・進捗管理，品質管理，コスト管理

向けの自社製インシデント管理ツールを採用した（図3）．インシデント対応フローおよびインシデント管理ツールは，より効率的なインシデント対応を実現するために，特別体制期間中でもプロジェクトメンバーからの要望を受け入れ，随時機能向上を可能とした．

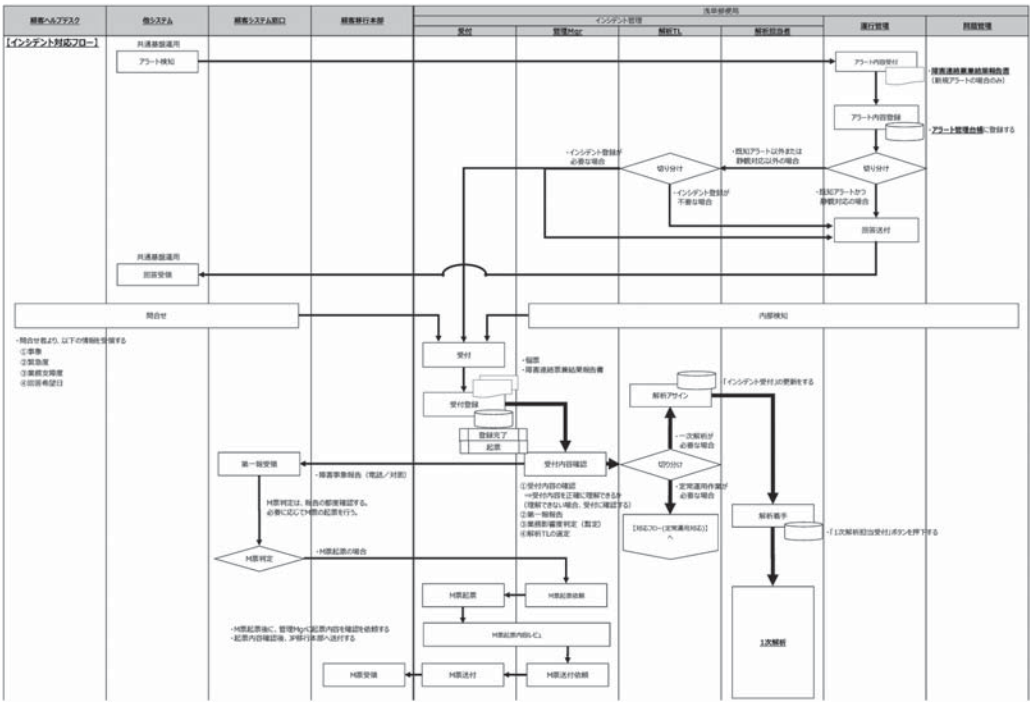

図2　インシデント対応フロー（一部抜粋）

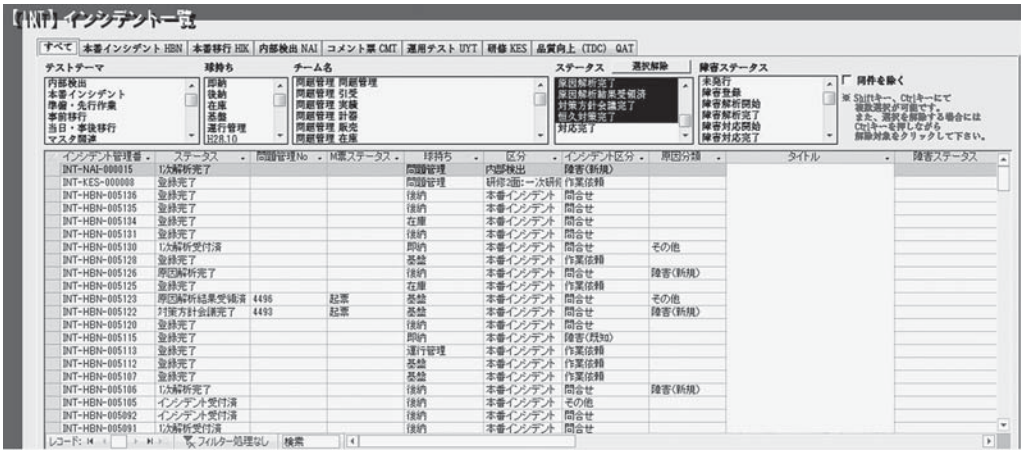

図3　インシデント管理ツール

2.5　特別監視運用

本番稼働後のシステムの正常稼働の確認と，システム稼働における問題点の早期検知を目的として，統合監視ソフトウェアによるシステム監視運用に加え，特別監視運用を定義した．本

システムの基本的な業務サイクルは1ヶ月サイクルであるため，本番稼働後1ヶ月間を特別監視運用期間と定義し，業務処理量から見たシステムの稼働状況を監視することを目的として，業務処理状況や他システムとの連携状況を重点的に定期監視した（表3）．

表3　特別監視運用

分　類	確認項目	集計単位	確認時点と確認対象								
			0時	3時	6時	9時	12時	15時	18時	21時	24時
業務処理状況監視	OLTP取込状況	件数	○	○	○	○	○	○	○	○	○
	在庫・精算関連処理状況	件数	○	○	○	○	○	○	○	○	○
	業務アラート発生状況	件数	○	○	○	○	○	○	○	○	○
	取引登録/修正状況	件数	○	○	○	○	○	○	○	○	○
	担当者締め/日締め状況	件数	○	○	○	○	○	○	○	○	○
	債務管理連携状況	件数	○	○	○	○	○	○	○	○	○
	社外Web利用状況	件数	○	○	○	○	○	○	○	○	○
他シス連携監視	滞留監視	滞留レコード件数	○	○	○	○	○	○	○	○	○
	取込エラー監視	エラーレコード件数	○	○	○	○	○	○	○	○	○

2.6　インシデント対応状況の把握

本番稼働後にマネジメント間で最新のインシデント対応状況を把握するため，定期的にチェックポイント会議を開催し，特別監視運用の状況報告，インシデント発生状況，重大障害の対応状況，直近のリリース準備状況などの共有を図った（表4）．特別体制期間中は24時間のシフト体制であり，マネージャー同士が顔を合わせない日もあるため，チェックポイント会議がコミュニケーションロスを補完するための有効な手段である．

表4　チェックポイント会議における報告内容

報告者	報告内容
運行管理マネージャー	特別監視運用の状況報告
インシデント受付チームリーダ	インシデント発生状況（問合せ件数，障害件数，未解決件数）
インシデント管理マネージャー	重大障害の対応状況（業務影響，回復見込み，作業状況）
プロジェクト管理チームリーダ	直近の緊急リリース対象件数とその準備状況

3.　特別体制訓練

前章で述べた特別体制に向けた準備が十分であるかを検証すると共に，プロジェクトメンバー自身が特別体制計画の内容を具体的に理解し，各自に与えられた役割の行動要領に従い業務遂行できるよう，特別体制訓練を実施した．本章で説明する．

3.1　訓練の計画と実施

特別体制訓練は，本番稼働前に4回に亘って実施した．各回の目的と内容を表5に示す．

表 5　特別体制訓練概要

訓練回	実施目的	訓練内容
1 回目	特別体制，役割，インシデント対応の基本フローを理解する	・架空インシデントをもとに，特別体制通常時を想定して訓練する ・本番環境や検証環境などの実機は使用しない ・特に障害時の報告・連携などの基本動作に注目して実施する
2 回目	特別体制，役割，インシデント対応の障害対応フローを理解する	・架空インシデントをもとに，特別体制ピーク時を想定して訓練する ・本番環境や検証環境などの実機は使用しない ・特に障害時の報告・連携などの基本動作に注目して実施する ・作業者全員が日報を作成し，作業実績管理できることを確認する
3 回目	特別体制における要員配置やシフト間の引き継ぎ方法について理解する	・架空インシデントをもとに，特別体制通常時を想定して訓練する ・本番環境や検証環境などの実機は使用しない ・ロケーション，会議，報告の擬似訓練を行う ・シフト間の交代手順の訓練を行う ・作業者全員が日報を作成し，作業実績管理できることを確認する
4 回目	訓練総仕上げとして，特別体制全般について具体的に理解する	・本番稼働初日を想定した体制，ロケーション，シフトに従い勤務し，本番稼働日の昼番，夜番の間に必要となる作業を全てシミュレーションする

訓練では，特別体制における役割と行動要領，インシデント管理ツールを使用したインシデント対応フロー，実際の顧客ロケーションで各チームの座席配置，昼番・夜番のシフト間の引き継ぎ手順を確認した．

毎回の訓練で，役割の理解と行動要領の習熟のために特に重要なのは訓練シナリオである．訓練シナリオの作成で検討した事項は以下のとおりである．

・訓練の目的，開始・終了時刻，場所
・バッチ処理の実行有無
・アプリケーションリリース作業の有無
・全体インシデント件数の設定（解析が必要となる件数，障害対応が必要となる件数）
・複数サブシステムにまたがるインシデント件数の設定
・高優先度対応インシデントの割り込み件数の設定
・チェックポイント会議などの会議体
・訓練参加者

同様に，訓練中に投入するインシデントの内容も重要である．5 名程度からなる訓練事務局を設置し，単なるシステムの操作方法などに関する問い合わせ，パッチなどの暫定対応が必要となる障害，恒久対応が運用回避となる事象など，一回の訓練あたり 20 件程度の訓練用インシデントを準備した．各インシデントは，本プロジェクトにおけるテスト工程で頻発した障害などを中心に，現実的に発生することが予想される事象を多く採用した．

3. 2　訓練結果の検証

毎回の訓練終了後に開催した訓練総括会議で，各役割の課題を訓練参加者全員で共有し，次回訓練時までに解決できるようアクションリスト化した．課題では，インシデント対応フローの改訂に関するものが最も多く，他には役割間のコミュニケーション方法の見直し，座席配置の見直しに関するもの，訓練の運営自体に対する提言として訓練時のインシデント件数を多くすることなどが議論された．

このように訓練のPDCAサイクルを回すことにより，特別体制計画の内容をブラッシュアップすることができ，かつ本番稼働までに各自の役割に対する意識と理解が深まり，訓練の目的を達成することができた．

4.　結果と考察

本番稼働日から3ヶ月後に実施した特別体制解除クライテリアの本評価において，クライテリアを満たした（目標達成した）ため，その1ヶ月後に特別体制を解除した．クライテリアを単に事後評価するための指標ではなく，目標（ゴール）として捉え，プロジェクトメンバーで共有したことが，今回の成功要因であった．

特別体制期間中は，約4,900件のインシデントが発生したが，特別体制に向けた訓練と特別監視運用が奏功して迅速かつ確実に対応することができ，安定稼働に繋げられた．期間中の課題として，インシデント数が事前の予想を上回ったこと，対応作業の高負荷が想定以上に続いたことが挙げられる．その原因は次の2点と考える．

- 修正したアプリケーションを本番環境へリリースする恒久対応を実施するまでの間，パッチや運用監視などの暫定対応が必要となるインシデントが多く発生したこと
- 一つの障害を起因として，複数の異なる問い合わせが寄せられたため，同一インシデントであるかの判定と管理に作業負荷が掛かったこと

インシデント件数の予測においては，想定した障害件数のうち暫定対応が必要になるインシデント数も予測し，暫定対応に必要となるツール設計・開発・テストおよび暫定対応後に必要となる継続的な運用作業に掛かる工数も考慮した上で，インシデント解析要員の体制を構築するべきである．

また，同一インシデントの判断については，問い合わせ内容をできるだけ汎化してインシデント管理ツールに登録し，プロジェクトメンバー全員が同一インシデントであることを判別できるようにする仕組みが必要である．

5.　お　わ　り　に

取引管理システムは顧客の基幹システムであり，インシデント対応の迅速性だけでなく確実性も求められたが，本番稼働後の特別体制を事前に綿密に計画し，十分な訓練を実施してプロジェクトメンバーへ特別体制計画の内容を浸透させることで，安定稼働へ繋げることができた．

＊1　日本郵便株式会社の取引管理システムは，先行と後続の2段階に分けて開発を実施した．先行開発は2013年4月に，後続開発は2016年2月にそれぞれ本番稼働した．

参考文献　［1］　伊藤直樹，「国内線旅客システム稼働後の障害対応への備え」，ユニシス技報，日本ユニシス，Vol.33 No.3 通巻 118 号，2013 年 12 月，P141 ～ 154

執筆者紹介　中　尾　茂　文（Shigebumi Nakao）

1999 年日本ユニシス（株）入社．電力会社向け電子商取引システム，官公庁向け電子申請システムのアプリケーション開発に従事．2010 年より日本郵便株式会社向けシステムのアプリケーション開発に従事．2014 年～ 2016 年に本稿で紹介した取引管理システム（後続稼働）プロジェクトに参画．