情報システム障害の再発防止のための組織的マネジメントの調査WG報告書

平成 24 年 4 月 5 日

独立行政法人 情報処理推進機構
技術本部 ソフトウェア・エンジニアリング・センター

情報システム障害の再発防止のための組織的マネジメントの調査WG報告書

独立行政法人情報処理推進機構

Copyright© Information-Technology Promotion Agency, Japan All Rights Reserved 2012

はじめに

情報システムの障害が事業者の外に影響を与えた事故の発生数（但し、新聞等のメディアで報道されたもの）は、2010 年頃から沈静化傾向にあるものの、依然 月あたり 2～3 件程度で推移している。
【IPA/SEC 「SEC journal 26 号」(2011 年 10 月発行)、「同 27 号」(2012 年 1 月発行) 「情報システムの障害状況」】
大きな情報システムの障害が起きると、その原因が取り沙汰される。曰く、情報システムのなかのバグが見逃された、情報システムの管理活動に弱点があった、といった具合である。
しかし、情報システムやその管理における欠陥をすべて取り除くのは非常に困難である。

その理由は、まず第1に、情報システムを欠陥なく作ることが難しいということである。これにはソフトウェアの「形がない、見えない」という性質が関係する。
第2には、情報システムへの要求が変化するということである。事業者を取り巻く外部環境、それを受けての事業者の事業・業務、それらを遂行する上での情報システムへの要求は日々変化する。事業者は、要求の変化に対応できるよう、情報システムをたびたび作り変えたり、改修したりする。その過程で情報システムに欠陥が入り込むことがある。[1] また、作り変えや改修の結果、情報システムが複雑になれば、その管理活動も複雑になる。
第3には、情報システムへの要求、特に信頼性に関わる要求につき、情報システムの関係者の合意を形作ったり、維持したりすることが難しいということである。情報システム自体の信頼性についてはSLA[2]等、記述や合意の方法があるものの、利用者視点での信頼性、すなわちSLAで合意されたサービスレベル内外での情報システムの変化がその利用者に与える影響までを予想して表現したり、合意を得たりすることは難しい。これには先述の事業者を取り巻く外部環境の変化（情報システムの利用者層の変化を含む。）も関係する。[3]

IPA/SEC は、これまで、上記のうち主に第1の理由に関係して、「定量化」、「見える化」やプロセスにおける取組みなど、情報システム（特にその中に含まれるソフトウェア）を適切に構築する方法についての知見を収集・整理・提供してきた。
しかし、第2、第3の理由に関しては、外部環境の状況変化などに対応していく必要があり、そのために「定量化」のような“知覚神経系”の活動と、プロセスにおける取組みのような“運動神経系”の活動とを結びつける、組織的な“大脳”の活動が重要になる。すなわち、情報システムの稼働（と、それによるITサービスの利用者への提供）にて起きていることを総合的に観察し、その品質上の問題を識別して必要十分な打ち手を判断、実施し、それで十分なITサービスが提供できているか判断するために再び観察に戻る、というループを運営する主体と能力が必要ということである。

本調査では、情報システムの安定稼働、ITサービスの円滑かつ安定な供給を担う事業者の情報シ

[1] 大手銀行における ATM、インターネットバンキングの障害（2011 年 3 月発生）が、これにあたる。
[2] Service Level Agreement の略。
[3] 携帯通信会社における通信の不具合（2012 年 1 月発生）が、これにあたる。

ステム部門が、それを損なう「障害」や「インシデント」をどのように管理しているかという観点で、その取組みを調査し、整理した。

情報システムの関係者の稼働品質に関する活動の一助となれば、大変幸いである。

目　次

第1章　調査の概要

1.1 調査目的

今日、情報システムは事業者にとって事業運営に不可欠な基盤であり、情報システムの障害は事業・業務に悪影響をもたらす。この悪影響は、ときに事業者内におさまらず、事業者の顧客にまで及び、また、メディアに取り上げられて第三者の知るところになることもある。

どのような障害がどのように事業・業務に影響するか、障害を抑制するためにどのような活動が必要か、その活動をどのような役割分担で行うべきかといった事柄は、情報システムと事業・業務との関係、情報システムや情報システム部門の内容や生い立ちによって異なる。つまり、事業者によって異なる。したがって、情報システムの障害や障害の影響を極小にする手段を事業者共通に扱うのには限界がある。[4]

但し、運用中の情報システムにとって重要なのは「稼働品質」[5]であり、この「稼働品質」について目標を立て、その目標の達成のために管理活動をしているということは、ほぼ全ての事業者に共通しているであろう。
つまり、

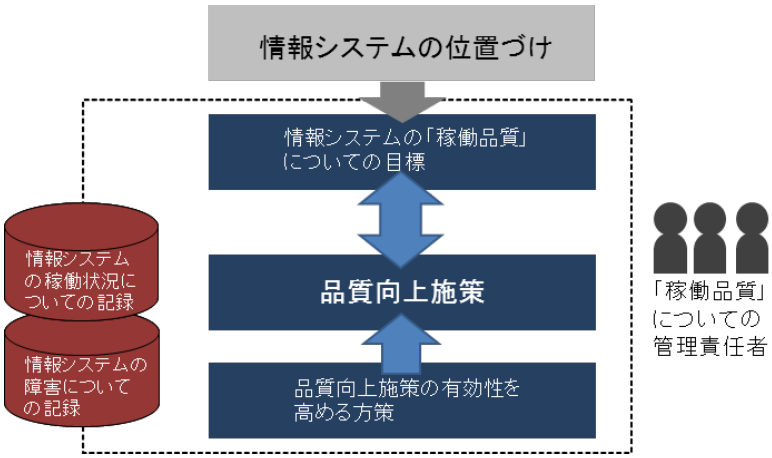
- ● 情報システムの「稼働品質」について、何らの目標を設定する。
- ● その目標に収斂するような、「稼働品質」を維持・向上するための施策（以下、「品質向上施策」）を立案、実施する。
- ・ 「稼働品質」の目標を立てるにあたり、情報システムの方針を参照する。
- ・ 品質向上施策を立案、実施するにあたり、その有効性を高める方策を併せてとる。
- ・ 上記のような活動を指揮する組織機能を持つ。
- ・ 上記のような活動に必要な情報システムについての記録を取り参照する。

という項目について、事業者は取組みを持っていると予想される。（図表１－１）

---

[4] 先述した「重要インフラ情報システム信頼性研究会」では、報道された障害事例の現象・原因を分析することにより、障害の再発防止に有効と思われる方策を表にまとめることを行った。その結果を付録Bに再掲する。本表は、事業者が現状の取組みに関して、他の視点がないか点検をするために有効である。次のステップとして事業者が障害の発生を防止するためにどのような方策をどの程度行うべきか、ということについては事業者が各々の事情に応じて独自に取り組む必要がある。

[5] この報告書では、「稼働品質」を以下と定義する：　情報システムが事業基盤としての役割を果たせない（例：情報システムが停止し業務が通常どおり実施できなくなる、または情報システムの利用者に迷惑をかける）ことにより、事業上の損出をどの程度発生させているかを表した指標。



図表１－１　予想される事業者の「障害管理」の取組み

さて、「はじめに」にも書いたように、情報システムを欠陥なく構築することは困難である。また情報システムへの要求、情報システムの利用環境も変化するため、障害を抑止して「稼働品質」についての目標を達成するには、目標に照らして情報システムに起きていることを観察、分析し、必要な打ち手を策定、実施し、再び情報システムを観察する、という改善ループを回すことが必要である。

事業者は、改善ループの管理者や回し方に、事業者ごとの事情に応じた工夫をこらしていることが予想される。その事業者ごとの取組みの「事例」を調査し示すことで、同じく「稼働品質」に関わっておられる情報システムの関係者に対し、現状の活動における気づきや見直しに資する情報を提供するのが本報告書の目的である。

1.2 調査方法

本調査では、成熟した「障害管理」の取組みを持っていると予想される事業者[6]を選び、情報システム部門のなかの「稼働品質」に責任を有している方にヒアリングすることで行った。
調査対象の事業者の業種別内訳は以下である。

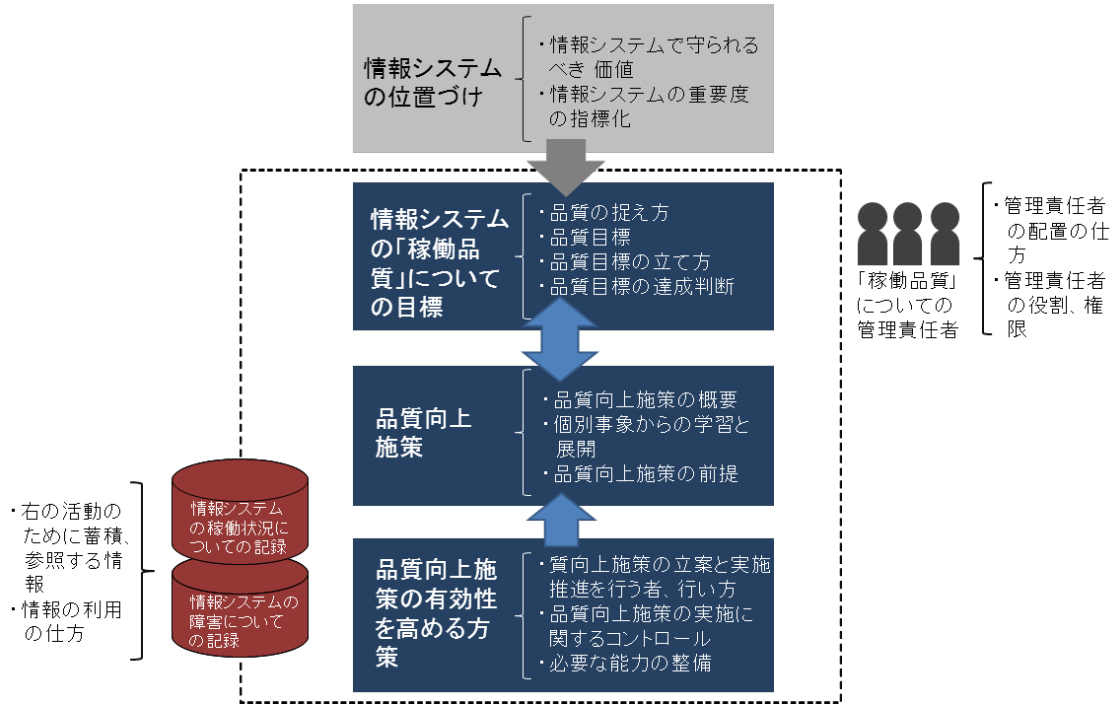
[6] 調査対象の事業者の選定にあたっては、事業者が過去に行った講演、またIT関係誌に取り上げられた記事を参考にし、自身の情報システムの品質が如何に獲得できているか説明を行ったことのある事業者を選んだ。

業種	調査対象の事業者数
金融	3
運輸	2
製造	2
合計	7

図表１－２　調査対象の事業者の業種別内訳

「稼働品質」に責任を有している方や部署が情報システム部門の内外に複数ある場合もあり、その場合は相互の関係や役割分担についても尋ねた。

まず、いくつかの事業者に図表１－１を示して取組みの要素につきヒアリングを行い、事業者の取組みの調査項目を図表１－３に詳細化した。さらに図表１－３と仮想の事業者の実施例を表にまとめ、図表１－２の事業者にそれぞれの取組みの詳細をヒアリング形式にて尋ねた。



図表１－３　事業者の「障害管理の取組み」の調査項目（概要）

1.3 調査および調査結果のまとめの監修

調査方法の策定（本報告書の「1.1 調査目的」、「1.2 調査方法」）、調査結果の整理、まとめ（第2章～第4章を中心に全体）について、その妥当性につきご意見を頂くため、IPA/SEC にて、2011 年 12 月～2012 年 3 月の間 「障害管理の事例評価WG」を持ち、計4回のWG会合をお願いした。
WG委員の各位は以下のとおりである。

主査	国民健康保険中央会	島谷 二郎
委員	コミューチュア情報システム	岩佐 洋司
委員	全日本空輸	蔵本 直樹
委員	東京証券取引所	藤田 邦彦
委員	デロイト トーマツ コンサルティング	岡本 晋

（敬称略 ・ 順不同）

事務局 IPA/SEC 金沢 成恭

第2章　調査結果

2.1 調査結果の概要

調査結果のうちの抜粋を、図表２－１および図表２－２に示す。また、調査結果の全体については別紙Aに示す。

調査対象の各事業者についての、主要な特徴は、以下のとおりである。

■A社（金融）

・運用部門内に、全ての情報システム（と、それによって提供されるITサービス）の「稼働品質」の管理責任者が置かれ、開発・運用・調達など、「稼働品質」に関わる全てを管理していた。

・「稼働品質」の目標設定、品質向上施策の立案と実施推進は、その管理責任者の指揮によりトップダウン式に実施されていた。

■B 社（金融）

・情報システムの企画部門内に、**情報システムごとに管理の「チーム」が置かれ、「稼働品質」を管理していた。**

・さらに、情報システム全体を含む事業リスク全体について、リスク管理部が取りまとめを行なっていた。

■C社（金融）

・稼働品質を含む、情報システムの品質は、情報システムの企画部門が管理していた。

・日々の「稼働品質」の状況に触れる**運用部門は、情報システムの品質のうち運用に関わるものを構造化して管理するとともに、運用の標準化、異常（予兆を含む）の検知、通報、運用から見た問題の原因の分析を担っていた。**

■D社（運輸）

・情報システムの運用を統括している情報システム子会社が「稼働品質」に責任を持っていた。

・ITサービスごとに「稼働品質」の管理責任者が、情報システム子会社内に置かれていた。
また情報システム全体の「稼働品質については情報システム子会社の運用統括部門が管理していた。

■E社（運輸）

・情報システムは現場で様々な形で使用されている、とのことであった。

・「稼働品質」についての要求も様々であるため、事業部門と開発・保守・運用を担う情報システム

子会社が協議しながら、個別の情報システムの品質向上のための活動を行なっていた。

・本社の情報システム部門は、個別の情報システムの品質向上に関する活動に横串を通し、全体の品質向上施策に反映していた。

■F社（製造）

・アプリケーション、アプリケーション基盤（アプリケーション部品）、IT基盤に層化して管理されていた。アプリケーション基盤、IT基盤は原則1種類に標準化されていた。

・情報システム部門のアプリケーションの担当者は、標準化されたアプリケーション基盤、IT基盤の使用を前提に、事業部門と合意した品質を実現するようにアプリケーションを開発していた。上記において、アプリケーション基盤、IT基盤が「稼働品質」を損なわないことは、これまでの実績で確認されている。

■G社（製造）

・製造を支えるため情報システムは現場で様々な形で使用されている、とのことであった。

・本社の情報システム部門（開発・企画部門）は、様々な「稼働品質」に関する活動に横串を通していた。

いずれの事業者でも、情報システム（と、それによって提供されるITサービス）の品質について、管理責任を負う組織、要員をおいていた。但し、その組織、要員の置き方や役割、その組織、要員が関与する品質についての目標の立て方、品質向上施策の内容については、事業者ごとに多少の違いが見られた。

事業者に共通する取組みを2章 2.2～2.3 で、ある事業者に見られた特徴的な取組みを3章で扱う。

		A社 （金融）	B社 （金融）	C社 （金融）
情報システムの役割・位置づけ	情報システムで守られるべき価値	**「情報資産の保全」**	**事業に必要なITサービスの品質（機密性、完全性、可用性）を維持すること**	**金融取引において、顧客間の公平性が損なわれないこと**
	情報システムの重要度の指標化	・個別の情報システム（正確にはITサービス）について、可用性（4段階）、機密性（2段階）、完全性（2段階）に区分し、ITサービスカタログに整理している。	必要な機密性、完全性、可用性で区分している。	・個別の情報システムについて、業務重要度、事業者外の利用者に提供しているか事業者内に閉じているか、によって区分している。
情報システムの「稼働品質」についての目標	「稼働品質」に関する目標	・障害がないこと（**障害とは、情報システムを用いた業務に対する悪影響、情報システムの利用者**（事業者内利用者、主要顧客）**への迷惑**）	・障害がないこと（**障害とは、情報システムを用いた業務に対する悪影響、情報システムの利用者**（事業者内利用者、主要顧客）**への迷惑**）	・障害がないこと（**障害とは、情報システムを用いた業務に対する悪影響、情報システムの利用者**（事業者内利用者、主要顧客）**への迷惑**）
	「稼働品質」の目標の立て方	・運用部門の管理責任者が、情報システム全体について、目標を定める。 ・目標として**年あたりの障害発生数の上限を、**（定められた開発プロセス、運用プロセスによる）**前年までの実績と品質向上施策の期待効果から定める。** ・障害が及ぼす影響度によって、障害の重軽を区分し、その重軽ごとに目標となる上限を設定する。	・個別の情報システムを担当する「チーム」が目標を定める。 ※「チーム」は外国為替、融資・・・というビジネスフローごとにある。 ・目標として**年あたりの障害発生数の上限を、前年までの実績と相対的な改善目標、特別要因（情報システムのリリース計画や業務量変化など）、品質向上施策から定める。**	・運用部門の管理責任者が、情報システム全体について、目標を定める。 **・全情報システムについて、KPI-KGIの構造で目標を設定する。** ・上位の目標については、中期経営計画の目標をもとに年度目標を定め、さらに情報システム群ごとのチーム目標に落とす。 ・事業部門との間でITサービスごとに摺りあわせ、稼働率などサービスカタログの中に目標を置く。
	「稼働品質」の目標の達成の判断	・発生した障害をカウントする。	・発生した障害をカウントする。	・サービスカタログの中の数値を満たすことが基本 ・但し、利用者ごとの異なる要求の充足の状況も見る。
品質向上施策	品質向上施策の概要	・運用部門による要件（特に非機能要件）をレビューする体制とチェック項目を定めている。 ・運用部門による、要件の情報システムへの実装をレビューする体制とチェック項目を定めている。 ・運用関連の成果物（例：オペレーターガイド）をレビューする体制とチェック項目を定めている。 ・運用業務でのスキル依存の排除を徹底している。	・運用部門による要件（特に非機能要件）をレビューする体制とチェック項目を定めている。 ・年間スケジュールの下、最低年1回以上実施する情報システム異常時への対応訓練を行なっている。	・キャパシティ管理にて、事業者外（顧客）の利用の変化の予兆を捉える。委員会（月1回）で状況を報告し、エスカレーションの必要有無の判断をする。 ・運用部門に引き渡されたドキュメントを書き換えることによって、運用オペレータが参照するドキュメントは利用しやすく属人性がでないものを用意している。 ・作業員が見るドキュメント、体制はほぼ標準化している。
	個別の事象（障害など）からの学習と展開	・個別の障害と再発防止策を「トラブル分析シート」へ記録する。 ・運用部門の管理責任者が、個別の障害の再発防止策を展開する必要性と展開範囲についての判断する。	・トラブル報告書を作成する。 ・情報システム部門全体として教訓集を整備している。 ・詳細にはチェックリストに整備し、汎用化できるものは開発手順などに反映する。	・障害記録を作成する。 ※障害記録を事後的もに活用する。一例として、情報システムの置き換え時に、運用からの要件を開発側に示す際に活用する。
	上記の品質向上施策の前提	・ITサービスの品質管理責任は運用部門にあるという原則がある。 ・そのために、運用部門は、開発の重要局面においてレビューに参加し（計4回）、レビューに合格しなければ開発部門は運用部門に成果物を受け渡すことは出来ない、というルールがある。	・リスク管理部門の承認がなければ、開発や運用の方式の変更は認めない（つまり、標準の方式どおり必ず実施する）というルールがある。 ・各情報システム担当の「チーム」による、障害原因の分析、品質向上施策の立案と実施は、全てエビデンスを使って、リスク管理部門ほかに説明するという行動習慣がある。	・運用部署でITILベースで何をするかを決め、開発から受け取る際に充足されていない場合は、受け取らない。 ・アプリケーションやミドルウェアの設計時から、運用設計まで含めた冗長的な仕組みを定めておく。
品質向上施策の有効性を高める方法	品質向上施策の立案と実施推進を行う者や行い方	・運用部門の管理責任者が情報システムの状況を見ながら判断し決定する。 ・情報システム部門会議で上記の決定が承認される。	・各情報システム担当の「チーム」が判断し決定する。	・運用部門が、個々のシステム評価を月1回の稼動報告で確認し、品質向上のために横展開すべきものがあれば共有する。
	品質向上施策の実施に関するコントロール	・運用部門内において、個別の品質向上施策につき管理責任者から各情報システムの運用担当者に実施の徹底を指示する。（これは毎月の「稼働品質」の状況をみて判断し行う。） ・運用部門の管理責任者が、開発工程での運用部門レビューに各情報システムの運用担当者を割り当てること、及び運用担当者の判断を評価して、開発工程の問題有無を総合判断する。	・品質管理活動の全体はリスク管理部門が管理する。 ・汎用化できる障害の再発防止策は運用から開発部門に戻し、アクションを決め、期限までに実施させる。	・運用部門で、運用チーム毎の目標とチーム間の調整をする。ブレイクダウンしたKPI/KGIを用い、四半期単位でその達成を確認する。

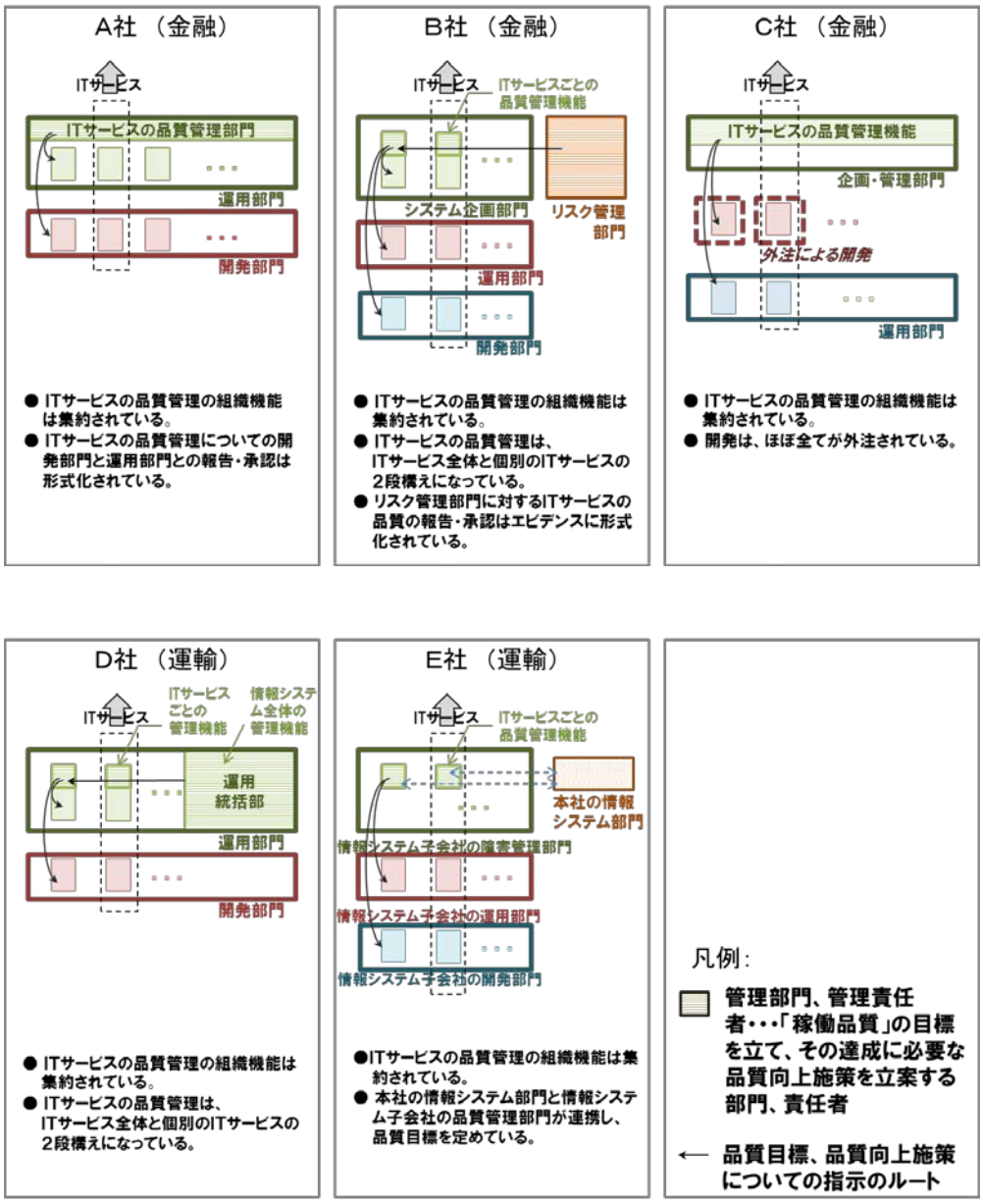
図表2－1　事業者の「障害管理の取組み」の調査結果の抜粋　（その1）

		D社 （運輸）	E社 （運輸）
情報システムの役割・位置づけ	情報システムで守られるべき価値	**運航への影響がないこと**	**サービスの継続**
	情報システムの重要度の指標化	・重要度に応じてシステムカテゴリ（AAA,AA、A）を定めている。AAAは運航管理、予約、貨物という運航に直接関係するもの ※システムカテゴリごとにSLA（停止可能時間を含む）が定められている。	・特に顧客サービスに関係するものを重要と定義している。
情報システムの「稼働品質」についての目標	「稼働品質」に関する目標	・重大障害がゼロであること（**障害とは、情報システムを用いた業務に対する悪影響、情報システムの利用者**（事業者内利用者、主要顧客）**への迷惑**）	サービスに必要な様々な目標 ・以下については、共通した定量目標が設定されている。 ー端末復旧時間（利用不可状態から利用可能状態に復旧するまでの時間） ー 「安全稼働指数」（ソフトウェア投資額あたりの障害発生件数）
	「稼働品質」の目標の立て方	・情報システム全体については運用統括部門が管理する。 ・各情報システム（ITサービス）についてはそれぞれの管理責任者が管理する。 ・障害を重大障害（運航、顧客への金銭的影響に関するもの）、重障害（復旧までの時間ほか）、その他の障害に分け、**重大障害はゼロ、重障害は前年度比減という目標を置く。** ・事業部門との協議によりSLAが決まり、そこから詳細な目標が導かれる。コスト勘案によりSLAが見直されることもある。	・本社の情報システム部門と、情報システムの開発・保守・運用を担う情報システム子会社で協議して定める。 **・障害の影響度をレベル分けし、影響度の高いものを対象に目標設定する。目標は前年度の実績を元に定める。**
	「稼働品質」の目標の達成の判断	・発生した重大障害、重障害をカウントする。	・発生した障害をカウントする。
品質向上施策	品質向上施策の概要	・運用統括部門の要件（特に非機能要件）をレビューする体制とチェック項目を定めている。 ・運用部門による、要件の情報システムへの実装をレビューする体制とチェック項目を定めている。 ・情報システム部門内および事業部門と共同での訓練を実施している。	・サービスに関して責任を負う事業部門と、情報システムの開発・保守・運用を担う情報システム子会社で協議し立案する。 ・事業で用いられている情報システムは多彩であり、品質向上施策も多方面に渡る。
	個別の事象（障害など）からの学習と展開	・障害データベースに記録する。 ・重い障害については、PMT（ヒューマンエラーの分析手法）を用いて、再発防止策を検討する。 ・原因分析の結果を含む障害分析シートを作成し、運用部門全体で共有する。	・本社の情報システム部と情報システム子会社で品質向上施策（障害の再発防止策等）について共有、検討し、必要により他の情報システムへの横展開を行う。
	上記の品質向上施策の前提	・ITサービスの品質管理責任は運用部門にあるという原則がある。	・情報システム子会社が、情報システムの開発・保守・運用を担っており、品質向上施策の策定や実行を行う。 ・その実施状況については定期的に本社の情報システム部門に報告する。
品質向上施策の有効性を高める方法	品質向上施策の立案と実施推進を行う者や行い方	・各ITサービスについては、それぞれの管理責任者（サービスマネージャ）が決定する。 ・情報システム全体については運用統括部門が管理する。	・サービスに関して責任を負う事業部門と、情報システムの開発・保守・運用を担う情報システム子会社で協議して、判断や決定を行う。
	品質向上施策の実施に関するコントロール	・各ITサービスの管理責任者は品質向上施策による目標の達成に責任を持つ。 ・運用統括部門では、運用に関わる情報を吸い上げ、必要に応じ指示を出す。	・情報システム子会社が、品質向上施策のコントロールも担っている。 ・本社にある情報システム部門で、個々の事案に関する品質向上施策をモニタすることはあるが、情報システム子会社が行う品質向上施策全体についてはモニタしていない。

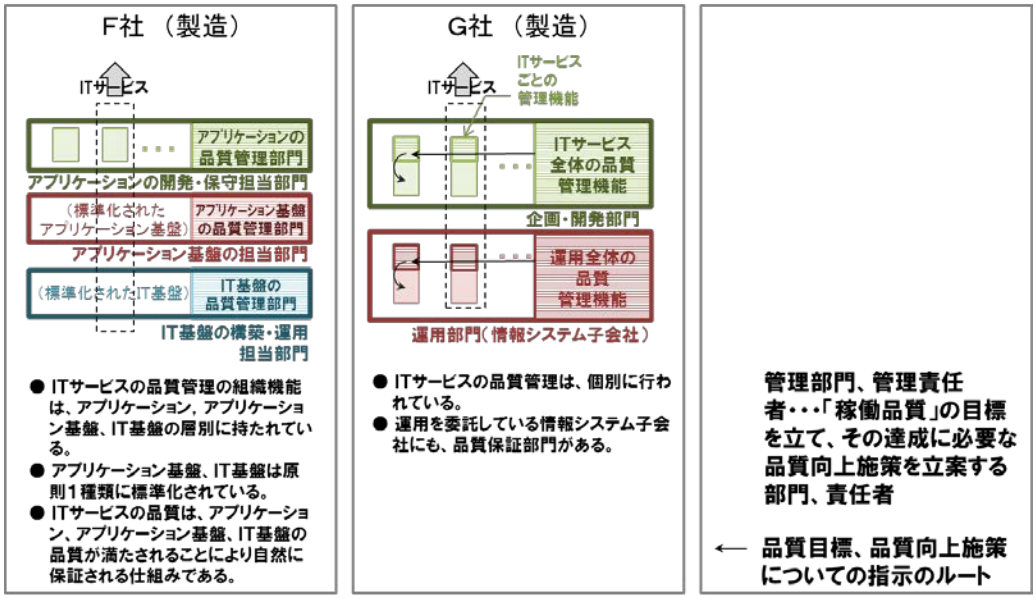
図表2－1　事業者の「障害管理の取組み」の調査結果の抜粋　（その2）

		F社 （製造）	G社 （製造）
情報システムの役割・位置づけ	情報システムで守られるべき価値	一番は**出荷に悪影響を与えないこと**、 他 事業に悪影響を与えないこと	**・お客様にご迷惑をおかけしないこと** （受発注や、一般顧客がアクセスするEC系が優先）
	情報システムの重要度の指標化	・事業の観点から、情報システムの重要度（4段階）は設定されているが、これは情報システムのIT基盤の構成の決定に関係し、障害管理には関係しない。	・重要度の順は、人命に関わるもの、全社員に関わるもの(コミュニケーション、広報)、受発注(生産管理、受発注、物流、調達)、支払い・決済（取引先に関わるもの）、内部向け、カタログサイトの順である。 ・システム毎に、品質ランク、回復優先区分、対策レベル、目標復旧時間が決まっている。
情報システムの「稼働品質」についての目標	「稼働品質」に関する目標	・定性的な目標は、情報システムの稼働品質は（定性的には）安定感があり、その安定感を維持すること **・定量的な目標は、障害発生件数の上限値** ・定性的な目標から定量的な目標に移行中である。	・これまでの実績、（実績がないものについては情報システムの規模など）、イベントを踏まえ設定する。
	「稼働品質」の目標の立て方	・アプリケーション、アプリケーション基盤、IT基盤の層ごとにいる管理責任者が、目標を定める。 ・目標として**年あたりの障害発生数の上限を、**（定められた開発プロセス、運用プロセスによる）**昨年までの実績と品質向上施策の期待効果から定める。** ・障害が及ぼす影響度によって、障害の重軽を区分し、その重軽ごとに目標となる上限を設定する。	事業部門と、情報システムの開発・保守・運用を担う情報システム部門で協議し定める。 ・テーマ種（開発、運用）別に、年あたりの障害発生数の上限を定める。 ・目標には、イベントを加味する。
	「稼働品質」の目標の達成の判断	・発生した障害をカウントする。	・発生した障害をカウントする。 但し個別事情もあるので、単純比較はしない。
品質向上施策	品質向上施策の概要	・IT基盤の構成の見直しとIT基盤の運用の改善（仮想化などのIT基盤の高度化への対応、セキュリティ対応の強化、IT基盤を構成する製品のVer管理の徹底など）	・マニュアルの整備、アプリケーション見直し、体制変更。 ・障害管理プロセスガイドラインの策定。
	個別の事象（障害など）からの学習と展開	・各情報システムの担当者により、インシデント・データベースに記録する。 ・インシデント・データベースの情報は、テーマ別WGによる標準化推進活動や要員が参加する失敗分析会、研修でも活用する。	・再発防止策の妥当性は、各情報システムの担当要員が最終的に判断する。 ・チームレベル、ビジネスユニットレベルで原因追求を実施し合意をする。 ・情報システム子会社では、**障害から学んだことを、お客様価値向上に活かす。**（お客様に影響を与えたことを、全責任者が出席する「障害事例から学ぶ会」に報告、気づきを与え合う。） ・共有の場として、**各事業部門の品質責任者や品質担当が参加する「品質交流会」にて良い事例等の紹介を実施する。**
	上記の品質向上施策の前提	**・アプリケーション基盤**（アプリケーション部品）、**IT基盤の標準化を図るとともに、データベースの正規化を実施**してアプリケーション層での運用をなくすなど、運用における問題が生じにくい構造にしている。	**・現場力強化が重要という考えである。**
品質向上施策の有効性を高める方法	品質向上施策の立案と実施推進を行う者や行い方	・アプリケーション、アプリケーション基盤、IT基盤の層ごとにいる管理責任者による判断と決定	・品質保証部門が年度の品質方針を立案し、各事業部門の品質責任者と品質担当を支援しながらモニタリング、評価、是正を実施する。 ・収集情報は品質保証部門がまとめ、毎月実施の事業部門の「品質会議」にて計画差異含む評価結果と対策検討を実施。 全社の評価結果は、経営会議にて報告する。
	品質向上施策の実施に関するコントロール	・アプリケーションの品質管理には、CMMIを活用している。 ・IT基盤の品質管理には、ISMSを活用している。	・各事業部門が実施している品質向上活動（各種テーマを設定した小集団）支援や課題のあるプロジェクトの支援等、現場に入込むことを行なっている。支援の1つとして、活動が進むための各種データ提供、事例紹介、アドバイス、品質会議での発表の場の確保がある。

図表2－1　事業者の「障害管理の取組み」の調査結果の抜粋　（その3）



図表２－２　事業者の「障害管理の取組み」の組織の模式図 （その１）



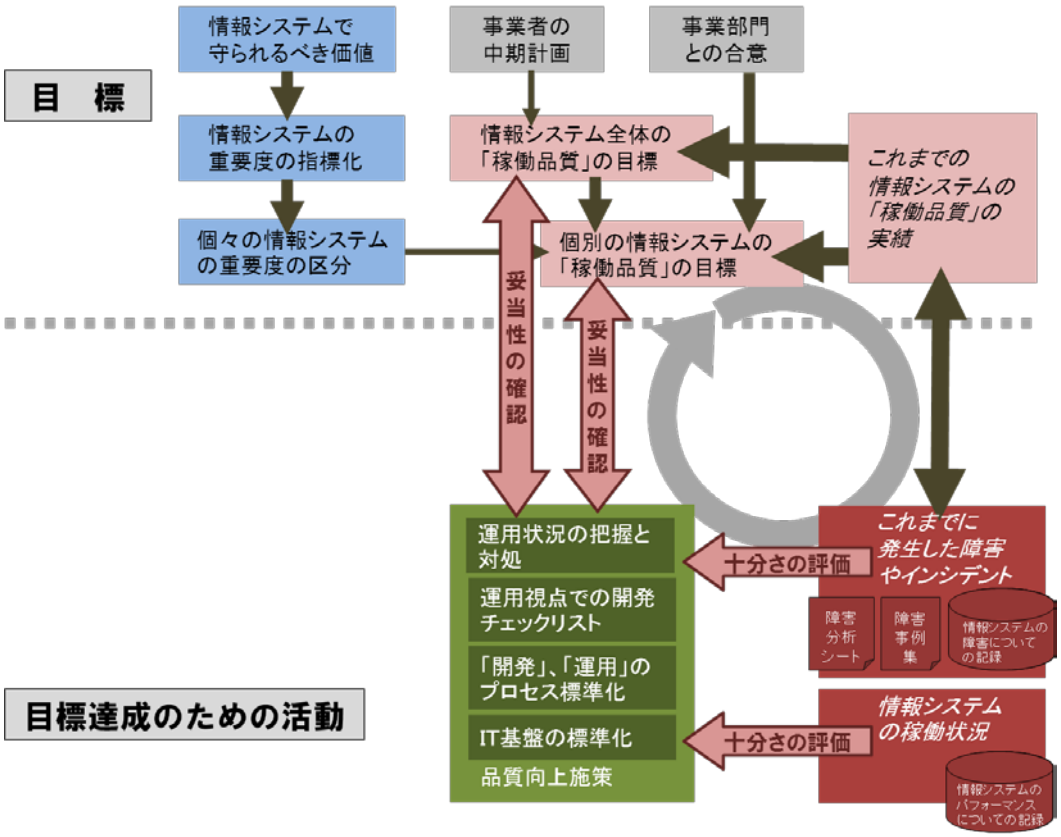
図表２－２ 事業者の「障害管理の取組み」の組織の模式図 （その２）

2.2 事業者の取組みの共通事項

ここでは、図表２－１、図表２－2などの調査結果にて、調査対象の事業者に共通的に見られたことを整理して示す。なお、以下にて、「全ての事業者にて」とは調査対象の全7事業者、「多くの事業者にて」とは調査対象のうち４～６事業者、「幾つかの事業者にて」とは２～３事業者で、それぞれ行われていたことを指す。まず、(1)で事業者に共通する取組みの構造を示し、(2)～(8)でその要素を取り扱う。

(1) 事業者共通の取組みの構造

調査対象の事業者には、図表２－３のような取組みの構造が共通して見られた。
但し、項目間の関連の強さ（図表２－３の図中では、矢線「→」の太さ）は、事業者により違いが見られた。



※　上図の中の矢線「→」の太さは、太いほど多数の調査対象事業者で、矢線の両端の要素を結びつけた取組みをしていたことを示している。

図表２－３　事業者共通の「障害管理」の取組みの構造

(2) 情報システムで守られるべき価値

この「情報システムで守られるべき価値」とは、情報システムに大きな問題が発生したとしても、最低限守られなければいけない事業上重要な価値とは何か、を表したものである。[7]
回答の内容は、事業者ごとに異なっていたが、以下の点では共通していた。

ア) 顧客、取引先など、事業者外の関係者への情報システムの障害の影響を最小に抑えるために何が必要か、という視点で語られていた。

但し、情報システムの障害が及ぼす影響をどう見ているかは、事業者により異なっていた。

イ) 情報システムの障害の影響には、①障害が継続すると、時間経過とともに影響が大きくなっていく性格のもの、②障害がひとたび起きれば、それだけで大きな影響が出てしまう性格のものがある。 ①を強く意識している事業者は金融(2.1 では「B社」、「C社」)、運輸(同じく「D社」、「E社」)であった。これらの事業者は、情報システムの障害が顧客の迷惑に直接関係し、その影響の大きさは時間経過ととも増す。②を強く意識している事業者は金融(同じく「A社」)であった。同事業者は金融商品についての顧客との契約情報を失うことが情報システムの障害に関する大きなリスクである。製造(同じく「F社」、「G社」)は前出の事業者に比べると情報システムの障害が、即座に事業者に対する影響を及ぼす度合いは大きくない模様であった。[8]

なお、上記ア)の考え方は、事業者の「障害」の捉え方にも通じており、全ての事業者で、「障害」とは"情報システムを用いた業務に対する悪影響、情報システムの利用者(事業者内外の利用者および顧客)への迷惑"という捉え方がなされていた。

(3) 情報システムの重要度の指標化

情報システム(と、それによって提供されるITサービス)は、多くの事業者において4段階程度の重要度に指標化されていた。情報システムの重要度は、上述の「(2) 情報システムで守られるべき価値」を受けて、事業・業務への直接的な影響、特に事業者の外(顧客、取引先など)に影響が及ぶか否かによって決められていた。
但し、この情報システムの重要度が、次にどのような項目と結びついているかは、事業者により以下のような違いがあった。

ア) 情報システムの重要度は、その情報システムの「稼働品質」の目標に反映されている。

イ) 情報システムの重要度は、その情報システムの「稼働品質」の目標を決める際に参考にされ

[7] 多くの事業者では、「情報システムに関する方針」の中で扱われている。
[8] この「IT=ビジネス」か否かの度合いは、後述する「3.6 事業者内品質についてのリスクの事業者内の共有」の取組みの程度に関係してくる。

ている。

ウ） 情報システムの重要度は、優先順位（リソースの割当てや、同時の障害が発生したときの復旧の順序）に関係し、「稼働品質」の目標には直接関連させていない。

ア）に当てはまるのは、金融（2.1 の「A社」）および運輸（同じく「D社」）であった。これらの事業者は、「契約の締結と履行」、「運航の継続」といったように「情報システムで守られるべき価値」が平易な言葉で言い表される。
一方、ウ）に当てはまるのは、製造（2.1 の「F社」および「G社」）であった。これら事業者は、性格が異なる情報システムを多数持ち、「情報システムで守られるべき価値」を一言で表現するのは難しい。
「情報システムで守られるべき価値」がシンプルに言い表される事業者ほど、情報システムの重要度と「稼働品質」の目標を直接結びつけていると言えそうである。

⑷ 情報システムの品質目標の立て方、達成の判断

情報システムの「稼働品質」、言いかえるとITサービスの品質の目標は、多くの事業者において年あたりの「重大な障害の発生件数」[9]のように簡単に測定や判断ができるものによって行われていた。発生した障害が「重大な障害」か否かは、障害が与えた影響の程度を

（影響、迷惑のあった時間） × （影響の及んだ業務の量、迷惑を受けた利用者の数）

といった考え方で、指標化することによって判断していた。

但し、「稼働品質」の目標の立て方は、以下の点で事業者ごとに異なっていた。

ア） 「稼働品質」の目標は、情報システム全体でのみ設定している。

イ） 「稼働品質」の目標を、個別の情報システムについて設定している。但し、それを個別の情報システムの重要度と関連づけてはいない。

ウ） 「稼働品質」の目標を、個別の情報システムについて設定している。そして、それを個別の情報システムの重要度と関連づけている。

[9] 幾つかの事業者では、障害の重大さを3段階程度の等級に区分し、その障害の等級ごとに「年あたりの障害発生数の上限」を目標として置いているものもあった。

また、その目標値は、全ての事業者において、前年度の実績からの相対値として設定されていた。[10] 目標値の設定において、多くの事業者は後述する品質向上施策の期待効果を織り込んでいた。

[10] 前年度の「稼働品質」の実績をベースに今年度の目標を考えるということは、前年度の実績は事業部門の要求を大きく下回らなかったということだと考えられるので、こういう目標の立て方でも事業部門の要求は織り込まれていると考えて良いであろう。
また、SLA レベルの詳細な品質に関する目標については、幾つもの事業者で、事業部門との協議結果を多く含んでいた。

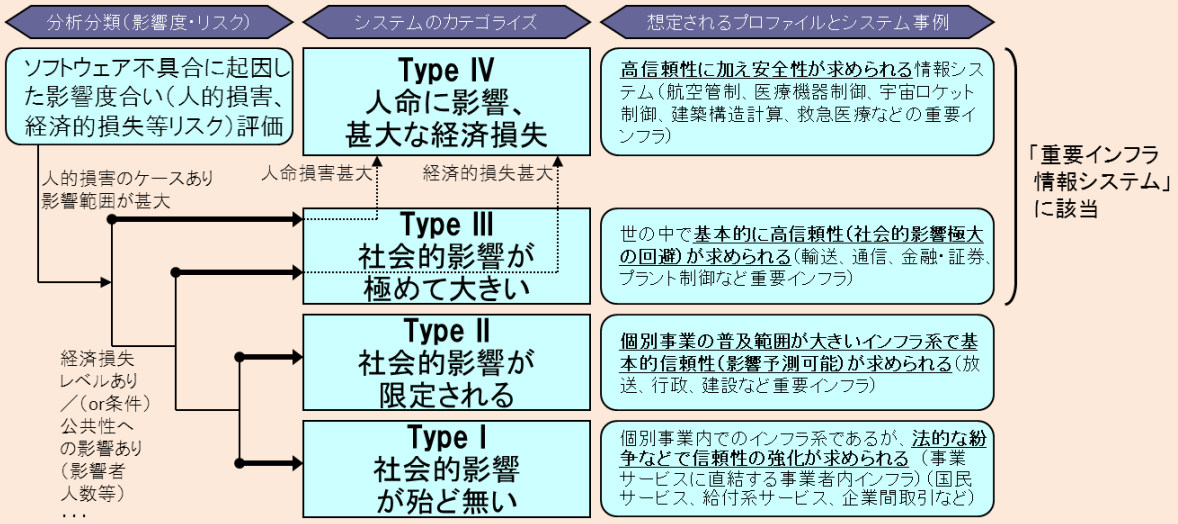
コラム　IPA/SEC の研究会の「システム・プロファイリング」との対比

IPA/SECは、2009～2011 年度に組織した「重要インフラ[11]情報システム信頼性研究会」を通じて下図のような『情報システムの重要度』に関するモデルを扱っている。
このモデルは、

ア）社会的に重要度の高い情報システムでは、情報システムの性格・内容に応じて適切な格付けがなされるべきではないか。

イ）そして、その情報システムの格付けに基づく品質が確保されるべきではないか。つまり、格付けに応じて、情報システムの品質目標や品質向上施策の強弱が決められるべきではないか。

という考えに基づいている。



図表Ａ　「重要インフラ情報システム信頼性研究会」で扱った「システム・プロファイリング」

今回の調査対象の事業者では、ア）はほぼ全ての事業者で似た考え方が取られていたが、イ）については取っていない事業者が殆どあった。
この理由は、「はじめに」および後述のように、以下の点にあると考えられる。

[11]「重要インフラの情報セキュリティ対策に係る第2次行動計画」（2009 年 2 月 3 日　内閣官房情報セキュリティセンターの情報セキュリティ政策会議）においては、「重要インフラ」とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるものと定義されている。同計画では、情報通信、金融、鉄道、航空、電気、ガス、水道、物流、医療、自治体サービスの10分野が防護すべき対象として掲げられている。

Ａ）事業者が抱える、性格の異なる情報システムの品質目標を、一次元的な品質の「ものさし」上にプロットすることは困難である。
（特に、利用者視点での信頼性、すなわち情報システム内の変化がその利用者に与える影響までを考慮しようとした場合）

Ｂ）情報システムの品質目標がある程度まで向上した状態では、⑴個別の情報システムに対して同じ品質向上施策を実施して結果を出すことは難しくなる。また、⑵個々の品質向上施策がどれだけ品質目標に寄与するかは見えにくくなる。

【注】 なお、本調査報告書の調査対象は、「重要インフラ情報システム」と一般的な事業者内で使われている情報システムの両方を含んでおり、「重要インフラ情報システム信頼性研究会」が対象とした情報システムの層とは異なっている。

(5) 品質向上施策の概要

多くの事業者で見られた品質向上施策には次のようなものがあった。

【障害の発生を抑制するために定常的に行う施策】

ア) 運用状況の把握と対処[12]

- 情報システムが提供するITサービスのサービスレベルの規定
- サービスレベルの変動、特に予め定められたしきい値からの逸脱(その予兆を含む)の監視
- サービスレベルの変動の原因分析と対処、対処がサービスレベルを安定させたことの確認
- 同じく、コンポーネント[13]の稼働状況の変動、特に予め定められたしきい値からの逸脱(その予兆を含む)の監視
- 同じく、コンポーネントの稼働状況の変動の原因分析と対処、対処がコンポーネントの稼働状況を安定させたことの確認
- 上記を推進する部署と役割の規定

↑ 後述の「オ) 障害の原因分析、再発防止策の立案と展開」などにより、必要都度、上記のサービスレベルの監視と対処の方法を改善していく。

イ) 開発プロセスおよび運用プロセスの標準化

- 情報システムの開発終了時に、運用のために充足できているべき成果が確実になるよう、開発プロセスを改善
- 通常の運用について、マニュアル化、自動化による運用業務の属人性の排除
  (幾つかの事業者では、運用オペレータの操作を自動採取し、マニュアルからの逸脱、誤操作がないかの監視も実施)
- 臨時の運用については、複数の運用要員による相互確認をしながらの実施
  (幾つかの事業者では、運用要員の適性を確認するための資格制度を検討中)
- 上記を推進する部署と役割の規定

↑ 後述の「オ) 障害の原因分析、再発防止策の立案と展開」により、必要都度、上記のプロセスを追加・修正していく。

ウ) 運用視点での開発のチェック

- 運用視点での開発チェックリスト
  (多くの事業者におけるチェックリストの運用は以下のようであった: 開発部門が、情報

[12] いわゆる ITIL (IT Infrastructure Library)のなかの「キャパシティ管理」のことである。
[13] 「コンポーネント」とは、ITサービスの提供に不可欠な、プロセッサ(の処理性能)、ネットワーク(の帯域幅)、補助記憶装置(の容量)などのことである。

システムの開発・保守のプロジェクト内でチェックし、運用部門がそのチェック結果の確からしさを点検する。チェック項目は、改善ループを回すなかで追加・修正していく。）

・運用部門による開発の主要フェーズ終了時点でのレビュー

・運用部門による開発終了時の終了判断妥当性確認

・上記において、開発された情報システムが運用要件を満たしていること（運用関係の成果物の完成を含む）を確認すること。確認できない場合は、開発の次工程あるいは運用への移行を差し止めるルール

・上記を推進する部署と役割の規定

↑　後述の「オ）　障害の原因分析、再発防止策の立案と展開」などにより、必要都度、上記のチェック項目を追加・修正していく。

エ）　IT基盤の標準化

・　ハードウェア、OS、ミドルウェアのスタックを製品レベルで具体的に指定し、それからの逸脱について制限をかけること
（標準化されたスタックを何種類までに絞り込むか、また例外をどの程度許すかについての判断は、事業者によって異なっていた。）

・　IT基盤の運用を標準化すること

・　上記を推進する部署と役割の規定

↑　後述の「オ）　障害の原因分析、再発防止策の立案と展開」により、またハードウェア、OS、ミドルウェアの製品サイクルに応じて必要都度、上記の内容を更新していく。

【障害が発生したときにその再発、類似障害の発生を抑制するために行う施策】

オ）　障害の原因分析、再発防止策の立案と展開

・　個別の情報システムの担当者または「稼働品質」の管理責任者による、障害の検出、原因の分析、暫定対策と再発防止策の立案、およびこれらについての障害データベースへの記録

・「稼働品質」の管理責任者による暫定対策の承認

・「稼働品質」の管理責任者または情報システム部門の会議による、障害の原因の分析結果、再発防止策の内容の妥当性の検討

・「稼働品質」の管理責任者または情報システム部門の会議による、再発防止策の展開の検討と個別の情報システムの担当者への指示

・　上記を推進する部署と役割の規定

コラム　「品質向上施策」についての参考資料

上記 2.2 「⑸ 品質向上施策の概要」は、調査対象の事業者から共通的に挙がった汎用的なものであるが、詳細な施策については、次の資料が参考になる。

ア）日本銀行金融機構局
「リスク管理と金融機関経営に関する調査論文
システム障害管理体制の実効性向上に向けた留意点」
（2012 年 2 月、Web 掲載文書；
http://www.boj.or.jp/research/brp/ron_2012/ron120216a.htm/）

イ）社団法人 日本情報システム・ユーザー協会（ＪＵＡＳ）
「情報システムの信頼性向上ガイド
障害を発生させない、被害を拡大させないための、システム対策」
（2010 年 7 月、図書）

ウ）本資料の付録Ｂ
～IPA/SEC「重要インフラ情報システム信頼性研究会」（2008～2010 年度）
で扱った、障害事例に学ぶ対策

なお、上記のうちア）については、障害や「品質向上施策」について、それを扱う上での事業者のなかに必要な体制、もつべき視点をも扱っている。

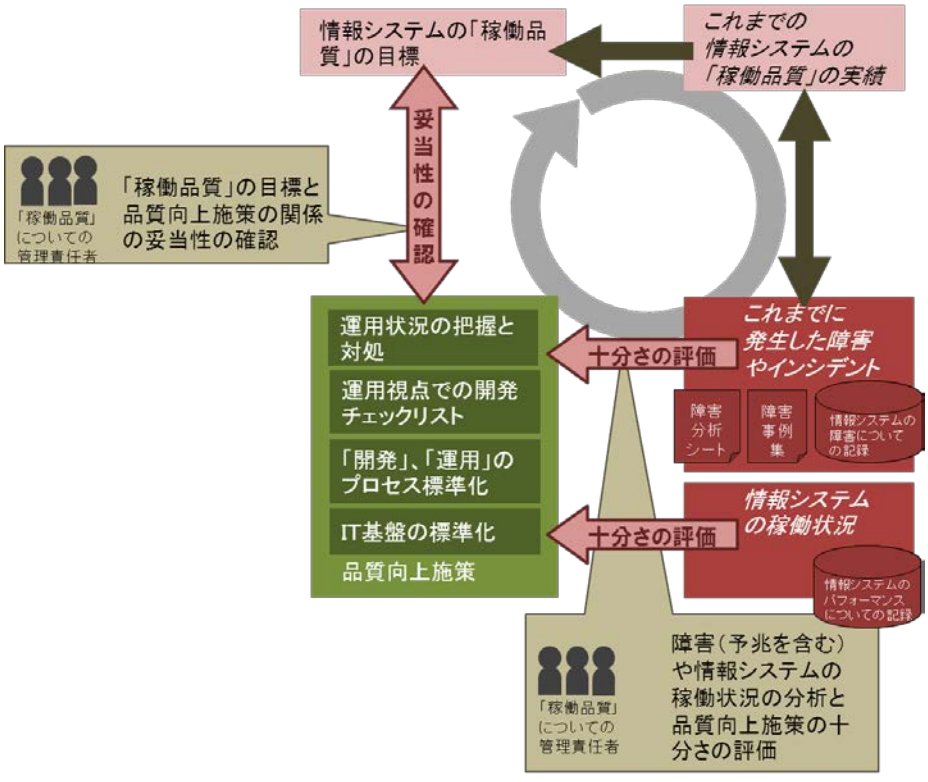
⑹ 品質向上施策の策定と実施の管理体制

「⑸ 品質向上施策の概要」のア）～エ）の策定は、全ての事業者で、情報システムの「稼働品質」の管理責任者の関与のもと行われていた。また、品質向上施策の実施については、「稼働品質」の管理責任者が指揮をしていた。これらの策定、指揮をしていたのは、基本的には「⑷ 情報システムの品質目標」を立てている者と同一であった。

つまり、この管理責任者が、「稼働品質」の目標に対する、品質向上施策の妥当性を吟味し、必要なら品質向上施策の増強を行い、そして品質向上施策の実施を推進している、ということである。

また、この管理責任者は発生した障害、インシデントの事象内容と原因、および情報システムの稼働の状況をモニタリングし、それらへの対処として品質向上施策の十分さを評価することも行なっていた。（図表２－４）

この管理責任者は、多くの事業者において、情報システム部門（情報システム子会社を含む）のなかの運用部門に置かれていた。



図表２－４ 情報システムの「稼働品質」の管理責任者の役割

なお、品質向上施策の策定と実施において、管理責任者が参照していた情報については、この節の「⑻ 情報システムの状況や障害の記録」および「3.2 品質目標と品質向上施策との関係」に後

述する。

(7) 品質向上施策についての人的な面での取組み

多くの事業者で行われているのは、次の2点であった。

ア)「稼働品質」の管理責任者の配置、および管理責任者の選抜と育成

- 情報システム(によって提供されるITサービス)全体、または個別の情報システム(によって提供されるITサービス)ごとに、「稼働品質」の目標の達成、そのための品質向上施策の立案と実行の指揮に関する管理責任者を置くこと。
- 適任と思われる管理責任者の候補者を選抜すること。またはジョブ・ローテーションのなかでの候補者を任命すること。
- 最初は、管理責任者の候補者を現役の管理責任者の補佐役に任命すること。実践を通じて、候補者の「稼働品質」や障害に関する指揮力の向上を図ること。

イ) 事業者内の事例による、情報システムが抱えた問題の例や情報システムに関する課題意識の情報システム部門の要員間での共有

- 障害やインシデントをデータベースに登録して、情報システム部門の要員に閲覧を許すこと。また、後述する事例研究会など、品質に関する研究に活用すること。
- 「稼働品質」の管理責任者が障害事例シート(事象、原因の構造、問題解決策の構造を含む)を作成し、回覧すること。
- 情報システム部門の要員による障害事例についての事例研究会を行うこと。
- 事業者内で、品質に関係するテーマ別WGを設置し、討論を行うこと。

(8) 情報システムの障害などの記録

「稼働品質」を損なう事象の内容や原因を理解、共有したり、現行の品質向上施策の妥当性をチェックし必要があれば追加対策を展開したりする上で、障害やインシデントの記録は非常に重要である。

全ての事業者が、情報システムの障害やインシデントについて記録をとっていた。また、多くの事業者では、「品質向上施策」の有効性を判断するためや、障害やインシデントの原因、影響範囲、類似性などを分析するために、情報システムの稼働状況に関する記録を、障害やインシデントの記録

を管理責任者の手元に置いていた。

幾つかの事業者が行なっている障害やインシデントの記録の様式を総合したものを図表２－４に示す。

障害やインシデント自体の情報	障害 ID 番号	
	障害の発生または検出の日時	
	障害の発見、検出の方法	{機器名、エラーメッセージ内容、発見者}
	障害の内容	{機器名、部署、場所、事象}
	障害の継続性	以下の分類 《継続、間欠、散発、単独》
	障害の既知・未知の別	
	障害の事業・業務および事業者外への影響	{影響範囲、影響金額、影響時間、左から導かれる影響指数}
障害やインシデントの原因についての情報	原因の分析者	
	原因の分析結果	{根本原因、作り込み原因、見逃し原因}
	上記の原因が、障害を引き起こすまでの経過	
	原因が障害以前から内在していた場合には、原因が障害を発生させた「きっかけ」に関する情報	
	原因分類1 （プロダクト）	以下の分類 《アプリケーションの欠陥、IT基盤の故障・欠陥、ネットワークの故障・欠陥、運用に関するドキュメントの欠陥、運用のオペレーションのミス、外部調達したITサービスの欠陥、付帯設備の異常・故障》
	原因分類2 （プロセス）	以下の分類 《開発で生じた欠陥、開発したものの移行・展開で生じた欠陥、利用者への普及・展開で生じた欠陥、運用で生じた欠陥 （実際には、これより細分化された工程に区分）》
	原因に関係する外注先（ベンダ）	
暫定対策に関する情報	暫定対策の実施内容	
	暫定対策の実施結果	
再発防止策の関する情報	再発防止策の策定者	
	再発防止策の内容	
	再発防止策の実施計画	
	再発防止策の内容および実施計画の報告と承認の状況	
	再発防止策の実施状況	
障害やインシデントへの対応のクローズ判断		

※ 上表は、障害やインシデント1件ごとにつき記録される情報の構造を示している。

図表2－5 障害やインシデントの記録内容（例）

2.3　調査結果についての考察

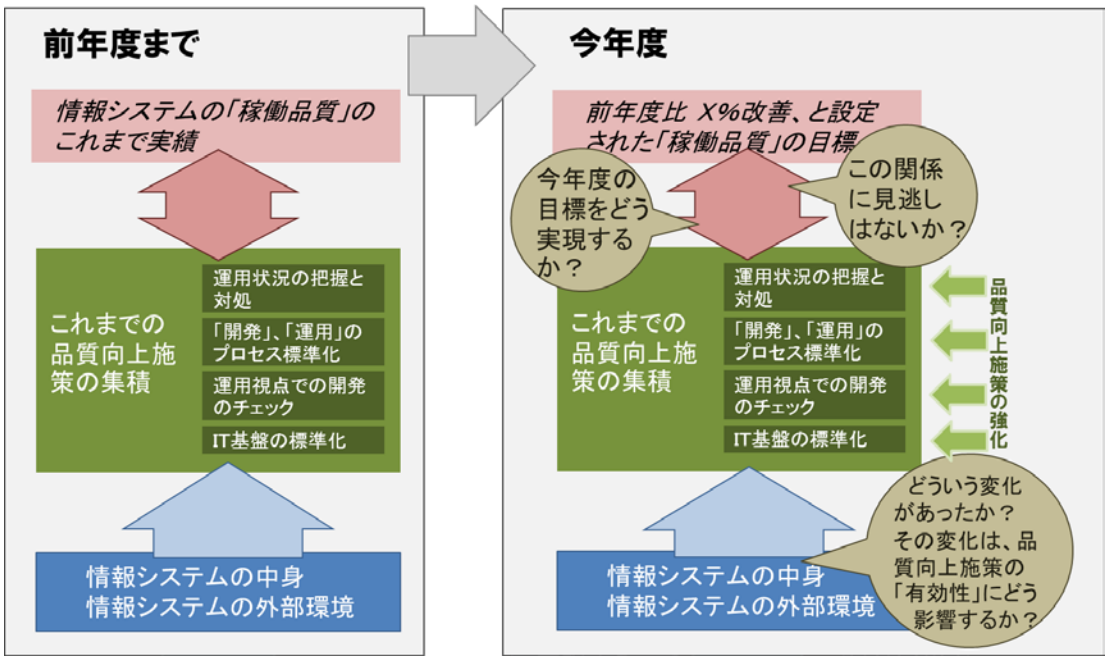
情報システムの「稼働品質」が安定している事業者では、品質向上施策の今日までの集積が、今日の「稼働品質」の達成に必要十分な状態になっている。
今回の調査対象の事業者は、この状態を前提としつつ、

ア）情報システムの中身はどのように変わったか？　外部環境（利用者の層や利用の仕方を含む）にどのような変化が生じているか？　それによって品質向上施策の手直しは必要になっていないか？

イ）今年度の「稼働品質」の目標を達成するためには、どのような品質向上施策の手直しが必要になるか？

ウ）これまでの「稼働品質」の実績と品質向上施策との関係で見逃されていることはないか？

といった点をチェックし、情報システムの「稼働品質」の維持・向上に必要な活動の展開を継続していた。（図表２－６）



図表２－６　情報システムの「稼働品質」を維持・向上する仕組み

このア）～ウ）のチェックとそこから必要となる施策の展開を担っているのが、情報システム部門（情報システム子会社を含む）に置かれた「稼働品質」の管理責任者である。

多くの事業者では、**「稼働品質」の管理責任者を運用部門に置いていた。**そして、事業者によって程度の違いはあるものの、その管理責任者は、「稼働品質」に対する結果責任を負っており、目標

の設定と、その目標の達成に必要な品質向上施策を「企画」、「開発」、「保守」、「運用」の枠を超えて指揮する権限を持っていた。（「開発」、「保守」の標準化されたプロセスへの関与も含む。）**その権限に基づき、管理責任者は、「稼働品質」の目標が達成できるよう、品質向上施策の内容を**（必要に応じて）**強化するとともに、その実施を指示およびモニタリングしていた。**（図表２－７）

多くの事業者が、こうした管理責任者を運用部門に置いているのは、「稼働品質」やそれを阻害する問題事象（典型的には障害）を観察しやすく、その問題事象の原因分析を適確に行いさえすれば、上記のア）～ウ）を捕捉しやすいからだと考えられる。

事業者の情報システムにおいて、運用を行いつつ「稼働品質」をモニタリングする役目は、今回の調査対象に限らず、どの事業者の情報システム部門にも置かれているであろう。
重要なのは、その役目に、どういうレベルでの観察をさせ、どこまでのことを統率させるかという、事業者による情報システム部門内の役割分担や体制にあると考えられる。[14]

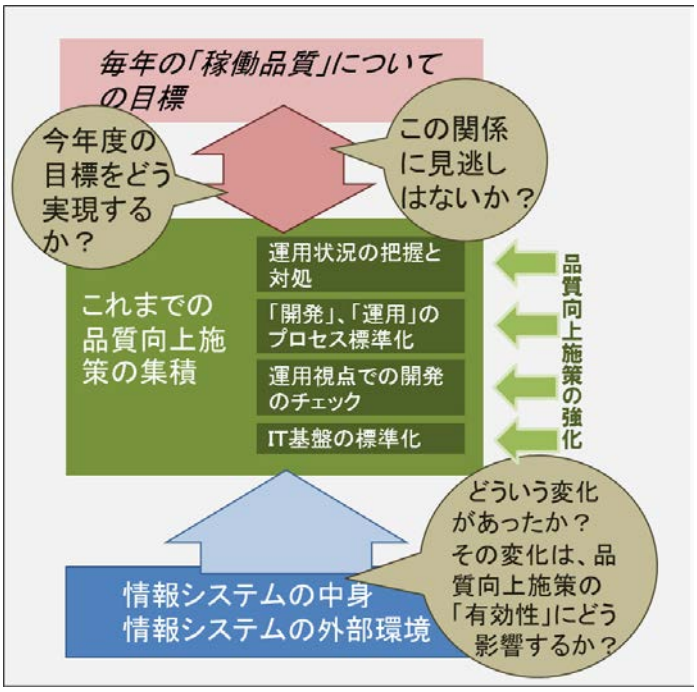
[14] この役割分担や体制を適確かつシンプルに実現しているのは、今回の調査対象のなかでは「A社」であった。「A社」の取組みのポイントについては、3章（3.1～3.2、3.5）でも紹介している。

第3章　事業者の取組みにおけるポイント

ここでは、調査対象の事業者の取組みの中で、事業者ごとの違いが目立った点、各個の事業者において特徴的であった点を取り上げる。

3.1　品質目標と品質向上施策との関係

「稼働品質」の管理責任者は、先述したように情報システムの「稼働品質」の目標と品質向上施策との関係が適確であるよう管理する必要がある。（図表３－１）



図表３－１ 「稼働品質」の目標と 品質向上施策の関係の管理

図表３－１の管理には、情報システムの状況について観測すべき事柄が決められ、観測結果が情報システムの「稼働品質」の管理責任者に集約されていることが必要である

金融（「A社」）では、図表３－２のような情報が収集されていた。　収集情報は、3.2 で触れた同事業者の管理責任チームが収集範囲を決定し、収集方式を定め、収集した情報の分析を行なっていた。

情報システムのパフォーマンスに関する記録	各情報システムの｛サービスレベル、トラブル管理状況、変更の状況、稼働率、性能、セキュリティの状況、サプライヤの状況、付帯設備の状況｝の情報

図表３－２ 「A社」で観測、記録している、情報システムの稼働状況についての情報

なお、品質向上施策に関しては、幾つかの事業者から、次のコメントもあった。

ア） 「稼働品質」の管理活動を強化した後、数年間（つまり、数サイクル）は、効果が期待される新しい種類の施策が次々と出てくるが、それらを開発や運用の標準（プロセスの規定、チェックリストの項目、レビューの方式や参加部門、それらの会議での承認ルールを含む）のなかに組み込んでいくと、段々と品質向上施策は成熟していく。

イ） 次の段階では、全ての情報システムに共通して効果が上がると見込まれる品質向上施策はひと通り策定、実施しているという状態になる。この段階では、個別の情報システムの個別の事情に応じて、若干のハズレ施策が出ようとも、品質目標を達するのに必要な施策は立てて実施するという考え方が必要になる。

ウ） また、個別の品質向上施策は、他の品質向上施策と関係を深めていく。その結果、どの品質向上施策でどの程度の効果が上がっているかを識別することがあまり意味をなさなくなる。

イ）やウ）の感覚を持てるようになれば、品質向上施策がかなり行き着いていたということであろう。

3.2 品質管理における担当部署、責任者の置き方

先述したように、今回の調査対象の多くの事業者では、情報システムの「稼働品質」を担う体制、責任者が集約されていた。

最も厚い体制を敷いていたのが、金融（2章の「B社」）および運輸（同じく「D社」）であり、以下の特徴を持っていた。

ア） 情報システム全体と、個別の情報システムの「稼働品質」につき、それぞれの管理責任者を置いていた。

イ） 個別の情報システムの「稼働品質」の管理責任者は、目標の設定と品質向上施策による目標の達成に責任を持っていた。[15]

ウ） 情報システム全体の「稼働品質」の管理責任者は、全体統括とともに、「稼働品質」についての適確な目標設定、品質向上施策の立案と推進についての助言、情報システム部門内の情報の流通などにより、個別の情報システムの「稼働品質」の管理責任者を支援していた。

比較的シンプルな体制を敷いていたのが、金融（同じく「A社」）であり、以下の特徴を持っていた。

ア） 運用部門は、「運用」を名乗らずITサービス提供の管理部門を名乗っていた。

イ） その部門内に、情報システム全体の「稼働品質」に責任をもつ少人数の管理責任チームが置かれていた。

ウ） 2章に先述したように、この管理責任チームは、「運用視点での開発のチェック」、「開発プロセスおよび運用プロセスの標準化」、「IT基盤の標準化」について、これらを統制する権限を持っていた。

エ） 個別の開発プロジェクトでの運用視点でのチェック、レビューへは、運用部門（正確には、ITサービス提供の管理部門）の個別の運用担当者が参加していた。管理責任チームは、個別の運用担当者にチェックシートなどの道具を提供するとともに、チェック、レビューの機会への運用担当者のアサイン、運用担当者のチェック、レビュー結果のモニタリングと評価、必要都度の個別の指示を行なっていた。

[15]事業者によっては、管理責任者の職務遂行を助けるため、情報システムに生じていることを分析する（障害発生時の原因分析を含む）補佐要員が管理責任者につけられているケースもあった。

コラム　「稼働品質」の管理責任者の人選

「2.2 ⑹ 品質向上施策の策定と実施の管理体制」、「2.3 調査結果についての考察」でも触れたように、「稼働品質」の管理責任者は情報システムの「稼働品質」について重い責務を負っている。
管理責任者の能力は、「3.2　品質管理における担当部署、責任者の置き方」にも書いたように、業務への従事を通じて伸ばされていく面もあるが、その候補者の人選も重要である。
情報システム部門の統括経験のある方に、管理責任者の候補者の人選についてヒアリングした結果は以下であった。

- 情報システム部門で、開発と運用の両方の経験（または相当する知見）があること
  そのなかで、自身が担当する情報システム部門だけではなく、他の情報システムとの調整や全体のスケジュールの検討・調整を行った経験があること
  （例：決算作業の計画や年末年始の特殊運用の検討などでは、個々の情報システムの担当者が関係する事業部門と調整した結果を持ち寄って、全体の運用作業のスケジュールを決めていくといったことが必要になる。そのような情報システム部門全体が関係する作業に、個別の情報システムの代表として参加し、主体的な役割を果たしたことがあること）
- 個別の情報システムを代表するには、担当する情報システムの運用を良くわかっていることが必須　（他の情報システムとのデータ連携や、運用の順番、事業部門の作業内容とスケジュールの理解および事業部門との調整を含む。）
- 事業部門の経験は必須でない。
- 運用の実務知識として、ＩＴＩＬやＩＳＯ２００００シリーズなどの国際標準を理解しており、なおかつ実務への適用を考える気持ちを持っていること
- “全体最適”の考え方と判断ができ、その中で“個別最適”の要素も無視することなく、妥当な線でまとめていくことができること
- 部門間調整のために、コミュニケーション力、リーダーシップ（ソフトに理屈で牽引するというタイプも良い）、フェアさ、柔軟性、粘り強さといった基礎能力や資質を有していること

3.3 具体的な幾つかの品質向上施策

ここでは、「運用視点での開発のチェック」、「開発プロセス、運用プロセスの標準化」という汎用的なもの以外で、1～2の事業者に特徴的に見られた品質向上施策（但し、情報システム全体について実施されているもの）を紹介する。

(1) IT基盤の標準化のさらなる推進

製造（2章での「F社」）は、HW（製品仕様レベル）、OS（製品レベル）、ミドルウェア（製品レベル）からなるIT基盤の製品スタックを1種類に標準化していた。[16]

OS、ミドルウェアは、かつては商業製品を使用していた。それらを段階的にオープンソース・ソフトウェアに置き換えていった。置換えにあたっては、情報システム部門内のIT基盤技術グループが、製品の成熟度や世間における利用実績、製品サポートの提供状況、事業者内のこれまで情報システムの要求を支えることが可能か、という点で評価した。

これらは、主として情報システムの調達コストの削減のために行われた。

しかし、IT基盤の運用におけるミスの大幅減、IT基盤に障害が発生したときの原因の切り分けの迅速化にも大きく貢献している、ということであった。

この事業者は、標準化されたIT基盤に仮想化技術などを追加したプライベート・クラウドを構築しており、コスト削減、情報システムのリリースの迅速化をさらに推進しながら、IT基盤の「稼働品質」を向上しようとしている。

(2) 冗長化に伴う新たなリスクへの対応

稼働時間について厳しい要求がある情報システムについては、サーバ構成を多重化することにより、HWなどIT基盤製品の異常に備えているものが多い。

但し、情報システムの冗長化は、予備系への切替え失敗など、別の種類のリスクを伴う。

金融（2章での「A社」）は、処理容量は異なるものの同じ機能を持たせた2セットの情報システムを別々のデータセンターに保有しており、一般業務向けのITサービスを平日は第一データセンターから、週末は第二データセンターからという様に、毎週、情報システムの現用系／予備系を切替えていた。

運用部門からすれば、切替えは日常業務の1つであり、データセンター・レベルでの障害発生に関して通常時から備えをしていることになる。

---

[16] 「IT基盤の製品スタックを1種類に標準化している。」といっても、この「標準」はハードウェア、OS、ミドルウェアの製品の世代交代に応じて変化していく。「1種類」とは、新しく構築される情報システムに用いられるIT基盤は、“それぞれの時点では”1種類しかない、という意味である。実際には、個別の情報システムが構築された時期により、世代の異なるIT基盤が混在してしまっている。但し、この事業者は10年程度を目処に情報システムを『再構築』するということをくり返し、個別の情報システムのIT基盤が大きく異ならないようにもしている。なお、この情報システムの『再構築』は、情報システムの要員がその情報システムの内部構造、つまりアプリケーション・ソフトウェアが動く仕組みを理解する機会としても重要である、というコメントもあった。

(3) アプリケーション層の運用のオンライン化

情報システム内の主要なデータベースの正規化は、「データ品質の向上」、「データ活用の高度化」などの目的で行われることが多いが、これも情報システムの「稼働品質」を改善する上で大いに役立つ。

事業者が複数の形式の異なるデータベースを抱えている場合、データベース間の整合は夜間のバッチ処理で行われることは多い。バッチ処理の実行自動化はある程度可能だが、月末、期末、年度末などは、それぞれの末締め処理に合わせ、通常とは異なるバッチ処理が必要になることもある。

その通常とは異なるバッチ処理は、多くの場合人手で行われ、その時に操作ミスがあると大規模な障害につながり得る。

金融（2章での「B社」）は、情報システムの世代交代の際、データベースの正規化を併せて行った。製造（2章での「F社」）も、データベースの正規化を段階的に行い、バッチ処理というアプリケーション層での運用を基本的に全廃した。

その結果、運用ミスを原因とした障害発生を大きく減らすことができた、ということであった。

3.4 外部ITサービス（クラウド）の管理

本調査では、情報システム部門の管理が直接及びにくい、外部ITサービスの「稼働品質」の管理についても尋ねた。
クラウドを含む外部ITサービスについては、そのコスト・メリットには魅力があるものの、品質に関し不安材料がある。幾つかの調査対象の事業者がコメントした不安材料とは以下であった。

- 外部ITサービスは、SLA を含めた「稼働品質」の目標について、事業者が外部ITサービスの供給者との合意（契約）をすることは出来る。但し、その「稼働品質」の目標が、どのような品質向上施策で支えられているかを知ることは難しく、その結果「稼働品質」の目標が達成することの確からしさ、さらには「稼働品質」が年々改善されていく見通しについて、事業者が確証をもつのは困難である。

この不安材料に関連して、クラウドを含む外部ITサービスの採否や「稼働品質」の管理の仕方について尋ねたところ、調査対象の事業者の考え方は以下のものに分かれた。

ア）（大量調達するなど、外部ITサービスの供給者にメリットのある条件を提示する引換えに）、事業者内部の「稼働品質」の目標、品質向上施策の実施、情報システムの稼働状況の測定結果に関する情報と同等の情報提供を求める。また、提供された情報を分析しリクエストを出す。
イ）外部ITサービスの提供者が標準的に示す情報にて管理を行う。但し、外部ITサービスの提供が突然停止したとしても、事業・業務への影響が限定的なものに限って外部ITサービスの調達を行う。
ウ）外部ITサービスの調達は行わない。

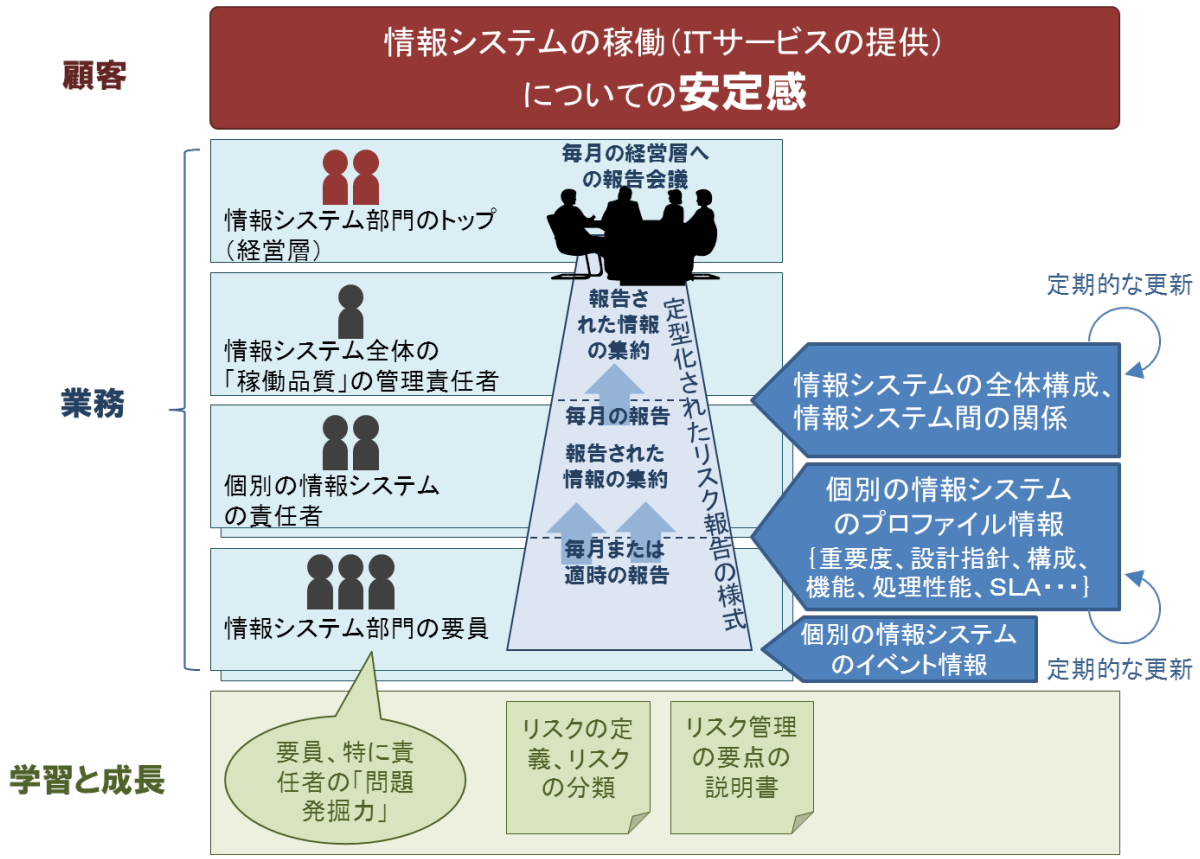
調査対象の事業者のなかには、ITサービスの種類ごとに、上記のア）～ウ）の考え方を使い分けている事業者もあった。

やや特殊な例としては、業種標準的な外部ITサービスが１つの供給者（ベンダ）から寡占的に供給されており、事業者の競合者の多くもこれを採用しているため、その外部ITサービスが止まったときには競合者も同じ影響を受けることで割り切ってその外部ITサービスを使用している、というものがあった。

3.5　品質についてのリスクの事業者内共有

さて、2 章から 3.4 までに書いてきたこととは、情報システムに「稼働品質」の目標を立てそれを達成するための様々な管理である。では、その管理がうまく行っているか、情報システムの「稼働品質」に危うい点があるとすればそれはどこか、ということについて事業者内で判断し、状況共有するにはどのようなことをしたら良いであろうか。

図表３－３に、金融（2章の「A社」）によるリスク管理の方式の概要を模式化した図を示す。



図表３－３　情報システムの「稼働品質」についてのリスク管理の構造（例）

「A社」で行われていることを列記すると、以下になる。

ア）　情報システムの「稼働品質」に関するリスクについて、「リスク管理の要点」の説明や、リスクの識別の仕方がドキュメント化され、情報システム部門の要員全員に提示されている。

イ）　個別の情報システム部門を管理する要員から、情報システム全体の「稼働品質」の管理責任者へのリスクの報告方式（タイミング、報告の書式、報告先）が定型化されている。

ウ） 情報システム部門の要員は、「稼働品質」についてリスクを識別する基準情報は、個別の情報システムのプロファイル情報としてまとめられている。このプロファイル情報は常に現状を反映したものになるよう更新されている。

エ） 「稼働品質」のリスク情報は、情報システム部門の上位層に向かって情報集約されていき、毎月１回の会議にて情報システム部門のトップ（経営層）に報告され、評価を受ける。

なお、「A社」では、外部から調達している情報システムやITサービスにおいても図表３－３の管理を実施していた。すなわち「業務」の下側の層から上側の層に対して行われる、所定のリスクの報告方式（タイミング、報告の書式、報告先）を情報システムや外部ITサービスの提供事業者に対しても求め、事業者内の情報システム、ITサービスと同等にそのリスクについての管理を行なっていた。

また、調査対象のうち金融（2章の「A社」、「B社」）では、情報システムの障害、それによる事業・業務への悪影響や顧客への迷惑を、事業・業務を停滞させるリスクのなかの一分野と捉え、統合したリスク管理をしていた。
具体的には、個別の情報システムの「稼働品質」（言いかえるとITサービスの品質）の管理責任者の後ろに控えているのは「リスク管理部」という全社組織であり、この組織は情報システムにまつわるリスクを、事業リスクの一分野と見て活動していた。[17] 情報システムについてのリスク管理の手法は、他のリスクと同じ方式に行われているということであった。

[17] このような組織の置き方は、「IT＝ビジネス」の金融事業者だからこそ、であろう。

コラム　障害が多発している状況からの脱出

「2.3 調査結果についての考察」では、「稼働品質」の管理責任者の役割について述べ、また「3.5 品質についてのリスクの事業者内共有」では、その役割による活動の結果として「稼働品質」にまつわるリスクがどうなっているかを共有する方法について述べた。
これらは、情報システムの稼働状況が安定している、つまり障害発生があまり多くない状況になって初めて有効になるようにも思われる。
それでは、障害が今なお多く発生している事業者では、どのような考え方を取ったらよいであろうか。

現在では、「3.5 品質についてのリスクの事業者内共有」に述べたリスク管理の方式に似た仕組みを持っているが、過去には障害を多発させていた事業者の情報システム部門統括経験者にヒアリングした結果は以下である。

・障害を多発させていたときは、情報システムの運用部門は、「決まったことを間違いなく正確にやればよい」という文化であった。
・その運用の文化を改革することから着手した。
・改革に先立っては、これまでの反省点をまとめると共に、コンサルタントを活用する等、外からの視点において、やるべきことを整理した。
・改革の実施にあたっては、限られた数の出向社員と情報システム運用子会社のプロパーからなる運用部門に、新たに数名を出向させ、運用部門の体質・文化を変えると共に制度面の整備を進めた。この出向者には情報システム子会社の役員クラス１名も含む。
・改革の第一段階が終了したのちも、情報システム部門の開発部隊と運用部隊のなかの組織再編を行うとともに、人材交流をして、さらに運用部門の体質改善をした。

つまり、「2.3 調査結果についての考察」の「稼働品質」の管理責任者の役割や、「3.5 品質についてのリスクの事業者内共有」の「稼働品質」にまつわるリスクを共有する方法は、上記のような改革の結果として出来上がったということである。
「稼働品質」の管理責任者の設置や、「稼働品質」にまつわるリスクを共有する方法は、形から入ることもできる。ただし、上記のような情報システム部門が抱える構造的な課題の把握や解決の模索を伴わないものは、その実効性に限界がある可能性を意識すべきであろう。

3.6 障害が防ぎきれなかったときへの備え

本項は、情報システムの「稼働品質」の目標、そのための品質向上施策とは直接関係がないが、利用者視点での信頼性とは関係する項目なので、取り上げる。
金融（特に銀行）や運輸においては、情報システムの障害が、事業者内の事業・業務への悪影響を通じ、事業者の顧客へと及ぶタイムラグが、「分」、「秒」の単位である。[18] したがって、情報システムの障害が防ぎきれなかった非常時にも、情報システムの内外で障害の影響を最小限に抑える活動が重要である。
調査対象のうち、金融や運輸の事業者では、事業者の BCP/BCM とも連動させて、以下の項目について厚い取組みが行われていた。

ア） 非常時の情報システム関係者の招集体制の取り決め
- 発生した非常時の事象に応じた、招集する情報システム関係者の範囲、招集までの時間、招集場所の規定
- 非常時の指揮系統、権限についての規定 （例： 非常時が収まるまでの社長権限レベルの臨時委譲）
- 招集された情報システム関係者の行動ルール （例： 岡目八目でのコメントを良しとする。自分の担当外についても意見を言う。）
- 経営層への報告の規定

イ） 非常時の情報システムの利用者（事業部門、関係会社）の行動ルールの取り決め
- 事業・業務を保護する優先順序についての規定
- 非常時の事業・業務の実施についての規定 （顧客への対応を手作業で行う措置、顧客の受ける影響を最小にするための臨時措置を含む。）

ウ） ア）とイ）に関する訓練
- 訓練は、本番の事業・業務にも影響を与えるため、年間計画にてリソースを含む実施計画を立案する。
- 情報システムの障害 → 事業・業務への影響 → 事業者の顧客への影響、と影響が波及していく過程についての訓練のシナリオを策定する。
- 情報システムについては可能な限り本番環境の使用は避けるが、業務環境については本番に近いものを使用する。
- 本番の事業・業務に影響があるため、訓練は実施の予告は行う。（但し、シナリオ内容については予告しないケースもあり） 但し、情報システムに閉じた訓練の場合は予告なし

[18] 利用者への影響規模も大きい。過去の障害事例でも、利用者への影響が1万人以上、経済的影響が10億円以上に達したものが複数起きている。

に実施するケースもある。

- 実施の結果を分析し、ア）、イ）の関連規定を改善する。
- ア）、イ）にて指揮を執る者のスキル向上の場を兼ねる。

コラム　品質目標、品質向上施策と 情報システムの状況を結び付ける思考力

「3.1 品質目標と品質向上施策との関係」に書いたように、情報システムの「稼働品質」の目標とそのための品質向上施策の関係を管理するのは、調査対象の多くの事業者において、「稼働品質」の管理責任者である。
しかしながら、個々の品質向上施策の実施や、障害の検出や一次的な取扱いについては、情報システム部門の多数の要員が関わっているので、その要員の論理的な思考力の底上げは非常に重要である。[19]

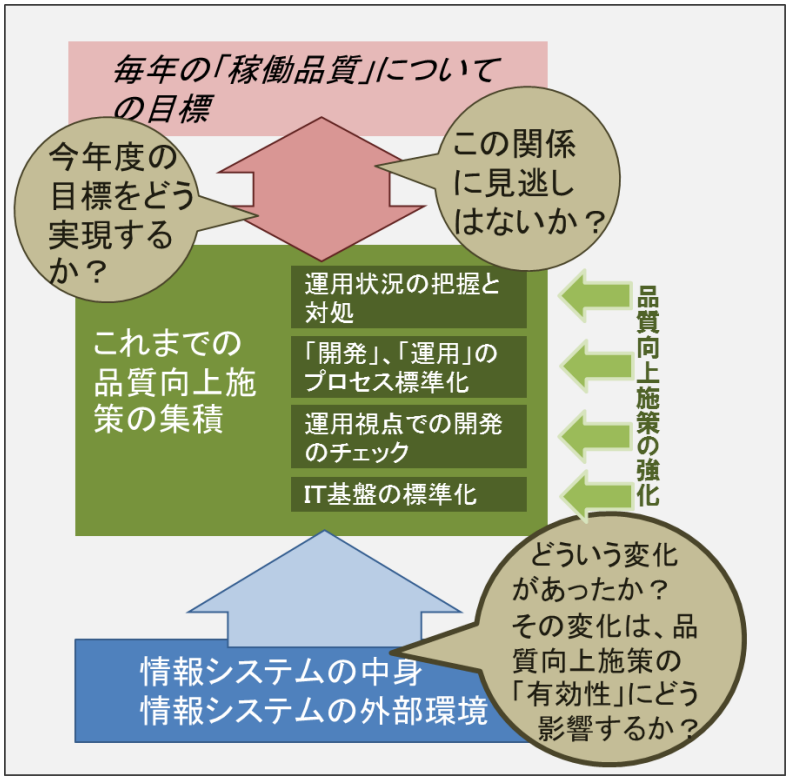
幾つかの事業者で、以下のような情報システム部門の要員を対象にした論理的な思考力の育成活動が行われていた。

ア）自事業者内の失敗事例（障害に至ったケース）を題材とした、「なぜなぜ」力育成研修会
イ）情報システム部門のグループごとの失敗分析会
ウ）イ）とは逆に、事業者の事業部門の品質管理部門との異種交流
エ）失敗事例のケーススタディに、必ずロジックツリーによる分析シートを付けるという行動習慣

[19] 余談であるが、調査対象の事業者のうち過半数から、情報システム部門の要員の論理的な思考力につき、その衰えが進んでいると感じるとのコメントがあった。

情報システム、特にソフトウェアに長く携わっておられる方には当たり前のことで恐縮であるが、情報システム、およびソフトウェアの品質を保つためには、それを開発・保守・運用するプロセスとその結果であるプロダクトの関係を管理することが重要である。
これは、本報告書の調査テーマである、情報システムの「稼働品質」の管理や、障害の管理についても同じである。

つまり、情報システムの「稼働品質」、言い換えるとITサービス（プロダクト）の品質についての目標を達成するために品質向上施策に含まれるプロセスが十分であるかが継続的にチェックされる必要がある。
2.3 や 3.1 でも述べたが、品質向上施策の有効性、十分さ程度は、毎年の「稼働品質」の目標や、情報システムの中身や外部環境の変化などによって変わる。特に、情報システムの外部環境の変化（利用者層や利用方法の変化）については、事業者が全てコントロールできるわけでないので、その状況変化を見極め、品質向上施策を調整する必要がある。



図表４－１ 「稼働品質」の目標と 品質向上施策の関係の管理（再掲）

今回の調査のなかで、調査対象の事業者から異口同音に語られた言葉は、以下の点であった。

- 情報システムの「稼働品質」について、目標を明確にすること
- その目標の管理責任者を明確にすること
- その管理責任者が、責任を果たす上で必要な権限、ルールを設定すること

そして、その「稼働品質」の管理責任者は「2.3 調査結果についての考察」でも触れたように、多くの事業者では情報システム部門内の運用部門に置かれていた。

一般的に情報システム部門は、その内部を「企画」、「開発・保守」、「運用」といった情報システムのライフサイクルに占める役割、あるいは「アプリケーション管理」、「ITインフラ構築」、「データセンター運営」といった技能別に分けられていることが多い。
こうした情報システム部門内の体制は、事業者毎のこれまでの事情を反映したものであるが、情報システムの内容や外部環境の変化のスピードが上がっている今日では、情報システムの「稼働品質」つまりITサービスの品質に関し、情報システム部門内の体制を横断して機能させる仕組みが必要になろう。

情報システム部門横断で機能させる仕組みについては、事業者それぞれに適した方式があると考えられる。図表２－１、図表２－2など本報告書のなかの情報を、各事業者の情報システム部門内の体制や情報システムの「稼働品質」の確保を点検するのに役立てて頂けると幸いである。

さらにもう一言加えると、上記のような取組みの必要十分さを事業者内の誰がどのように判断するかを明確にすることも非常に重要である。
「2.2 事業者の取組みの共通事項」の「(2) 情報システムで守られるべき価値」、および「3.4 品質についてのリスクの事業者内のリスク」でも触れたが、情報システムの「稼働品質」をどう位置づけ、それを損なう可能性をどのように評価するかは事業者によって異なっていた。
端的にいえば、「IT＝ビジネス」という色合いの強い事業者ほど、情報システムの「稼働品質」の状況のモニタリングや、それを損なうリスクを評価する仕組みが整備されていた。それらの事業者は情報システムの障害がすぐビジネスへの影響となって現れるのだから、事業者のトップが情報システムの「稼働品質」に関与するのは当然なことであろう。

ここで言う“事業者のトップの情報システムの「稼働品質」への関与”とは、情報システムが障害により機能しなくなったとき、どういう事業・業務上への悪影響が起きるか、それはどの程度まで許容できるか、許容できない場合どのような取組みでそれを防ぐか、これらを考えることである。

読者が関わっておられる情報システムが障害により機能不全になったとき、事業や業務はどうなるであろうか？
この問いへの感覚をもとに、「3.5 品質についてのリスクの事業者内共有」に示した情報システムの「稼働品質」のリスクを管理する方式につき、現状はどうか？ 本来どの程度のレベル感で実施するべきか？ について考えてみて頂きたい。

第5章　最後に

日本と米国では、品質への取組み方が大きく異なっているのではないか、という事がまま言われる。
たとえば、
米国では、
・ルールと責任はしっかり決められている。
・システムを構築したり、ツールを整備したりすることに長けている。
・一方で、品質を心配する意識は小さい。
反対に、日本では、
・ルールと責任は曖昧である。
・システム、ツールの構築や整備も米国ほどではない。
・一方で、品質を心配する意識はとても大きい。
であって、どちらもバランスに欠ける部分があるのでは、という指摘である。

本調査（ヒアリング）でも、まず抱いた印象は、各事業者において「品質を心配する意識」に支えられて、情報システムの「稼働品質」が守られている、ということであった。
続いて、ルールと責任であるが、情報システムの「稼働品質」に関しては、これは上で言われるほどではない。調査対象のうちの多くの事業者では、「稼働品質」についての管理組織が集約されており、また管理責任者の権限は明確に決まっていた。但し、「稼働品質」の管理責任者が情報システム部門内にどう置かれているか、管理責任者に障害の原因分析や品質向上施策の立案のためにどの程度のリソースが預けられているか、といった管理組織の置き方には事業者による違いが見られた。
最後に、システム、ツールについては、情報システムの管理責任者の置き方にも関係する部分があるが、情報システムにおける障害を事業者全体のリスクとどう結びつけているか、リスク管理のツールをどの程度活用しているか、という点について、事業者ごとに違いが大きく見られた。

情報システムに求められる「稼働品質」は、業種・業務の種類や事業者の方針によっても異なり、また品質を得るのはタダではないから、事業者は無闇に高い品質の目標を設定し、高度な取組みを考えるのは適切ではない。
しかし、日本の良い点である「品質を心配する意識はとても大きい。」という点だけに頼るのでは、時間とともに高度化、複雑化していく今日の情報システムを支えることは難しくなってきている。組織内外の「ルールと責任」、情報システムの問題を防護する「システム、ツール」の整備といった点から、各事業者が取組みの強化をしていくことは重要である。

事業者の情報システム部門（含　情報システム子会社）は、「企画」、「開発」、「運用」と、情報システ

ムに関わる立場によって、その内部が別れている場合が多い。しかし、情報システム部門の役割を事業・業務を牽引する情報システム、ITサービスの提供、と捉えるならば、その情報システムの「稼働品質」、ITサービスの品質に照らして、情報システムの「企画」、「開発」、「運用」を指揮していく組織内の仕組みが重要になろう。
今回の調査対象の事業者のうち幾つかは、それを「稼働品質」の管理組織、責任者として明確に置いていた。これが「ルールと責任」についての具体的な姿の例と考えられる。

今一つ、取り上げたいのは「情報システムの要件の複雑化」についてである。
「1.3　調査および調査結果のまとめの監修」に書いたWGの議論でも、社会サービスに「より良いもの」、「精緻なもの」を求める日本人の性向、それに応えようとする事業者の姿勢、その結果発生する業務の高度化、それに伴う情報システムの複雑化についての話題が出た。
当初から要件が複雑な情報システムを開発し運用するのは難しいが、そうでなくても事業・業務の高度化により、情報システムの要件は時間がたつとともに「複雑化」していくことはよくある。それに関し何らかのコントロールがないと、品質向上施策をいくら積み上げても「稼働品質」の目標を達成することは次第に難しくなっていく。
そこで、事業者は、事業全体の効率化や品質確保、顧客から見たわかりやすさ、ひいてはコストの適正化を考えて、制度や業務プロセスをできるだけシンプルにすることを常に考慮しつつ施策を考えるべきと思われる。

情報システム部門とすると、「情報システムの要件の複雑化」は、事業・業務上の必要によって部門外から対応を求められた結果生じるものであり、これを直接制御することは難しい。ただ、叶わないことがあるとしても、情報システム部門が中心になって『情報システムの「稼働品質」のリスクの状況』と『事業・業務の必要から見た情報システムの要件の管理』を連携させて考えていくことは必要であろう。

最後に、情報システムの「稼働品質」が安定的に確保できる仕組みを読者が作ることに、何らかのお役にたつことを願い、この報告書を終える。

参考文献

（本文中に挙げた文献は除く。）

- 『ITIL V3 ファンデーション』（Van Haren Publishing 刊、2010 年 7 月（日本版））
- 『システム障害はなぜ二度起きたか』（日経コンピュータ編集、日経BP社刊、2011 年 8 月）
- 『システム統合の「正攻法」』（大和田 尚孝 著、日経BP社刊、2009 年 11 月）
- 2010 年度版 企業IT動向調査2011（経済産業省 情報処理振興課、社団法人システム・ユーザー協会刊、2011 年 7 月）

【付録A】　事業者の「障害管理の取組み」の調査結果

		A社 （金融）	B社 （金融）	C社 （金融）	D社 （運輸）	E社 （運輸）	F社 （製造）	G社 （製造）
事業者の取組みの全体的な特徴		**・運用部門内に、全ての情報システム（ITサービス）の「稼働品質」の管理責任者が置かれ、**開発・運用・調達など、「稼働品質」に関わる全てを管理している。 ・「稼働品質」の目標設定、品質向上施策の立案と実施推進は、その管理責任者の指揮によりトップダウン式に実施されている。	・情報システムの企画部門内に、**情報システムごとに管理の「チーム」が置かれ、「稼働品質」を管理している。** ・さらに、情報システム全体を含む事業リスク全体について、リスク管理部が取りまとめを行なっている。	・稼働品質を含む、情報システムの品質は、情報システムの企画部門が管理している。 ・日々の「稼働品質」の状況に触れる**運用部門は、情報システムの品質のうち運用に関わるものを構造化して管理するとともに、運用の標準化、異常（予兆を含む）の検知、通報、運用から見た問題の原因の分析を担っている。**	・情報システムの運用を統括している情報システム子会社が「稼働品質」に責任を持っている。 **・ITサービスごとに「稼働品質」の管理責任者が、情報システム子会社内に置かれている。** **また情報システム全体の「稼働品質については情報システム子会社の運用統括部門が管理している。**	・情報システムは現場で様々な形で使用されている。 **・「稼働品質」の要求も様々であるため、事業部門と開発・保守・運用を担う情報システム子会社が協議しながら個別の情報システムの品質向上行なっている。** **・本社の情報システム部門は、個別の情報システムの品質向上の活動に横串を通し、全体の品質向上施策に反映している。**	・アプリケーション、**アプリケーション基盤（アプリケーション部品）、IT基盤に層化して管理されている。**アプリケーション基盤、IT基盤は原則1種類に標準化されている。 ・情報システム部門のアプリケーションの担当者は、標準化されたアプリケーション基盤、IT基盤の使用を前提に、事業部門と合意した品質を実現するようにアプリケーションを開発する。 上記において、アプリケーション基盤、IT基盤が「稼働品質」を損なわないことは、これまでの実績で確認されている。	・製造を支えるため情報システムは現場で様々な形で使用されている。 **・本社の情報システム部門（開発・企画部門）は、様々な「稼働品質」に関する活動に横串を通している。**
情報システムの役割・位置づけ	情報システムで守られるべき価値	**「情報資産の保全」**	**事業に必要なITサービスの品質（機密性、完全性、可用性）を維持すること**	**金融取引において、顧客間の公平性が損なわれないこと**	**運航への影響がないこと**	**サービスの継続**	一番は**出荷に悪影響を与えないこと、** 他 事業に悪影響を与えないこと	**・お客様にご迷惑をおかけしないこと** （受発注や、一般顧客がアクセスするEC系が優先）
	情報システムの重要度の指標化	・個別の情報システム（正確にはITサービス）について、可用性（4段階）、機密性（2段階）、完全性（2段階）に区分し、ITサービスカタログに整理している。	必要な機密性、完全性、可用性で区分している。	・個別の情報システムについて、業務重要度、事業者外の利用者に提供しているか事業者内に閉じているか、によって区分している。	・重要度に応じてシステムカテゴリ（AAA,AA、A）を定めている。AAAは運航管理、予約、貨物という運航に直接関係するもの ※システムカテゴリごとにSLA（停止可能時間を含む）が定められている。	・特に顧客サービスに関係するものを重要と定義している。	・事業の観点から、情報システムの重要度（4段階）は設定されているが、これは情報システムのIT基盤の構成の決定に関係し、障害管理には関係しない。	・重要度の順は、人命に関わるもの、全社員に関わるもの(コミュニケーション、広報)、受発注(生産管理、受発注、物流、調達)、支払い・決済（取引先に関わるもの）、内部向け、カタログサイトの順である。 ・システム毎に、品質ランク、回復優先区分、対策レベル、目標復旧時間が決まっている。
情報システムの「稼働品質」についての目標	「稼働品質」に関する目標	・障害がないこと （**障害とは、情報システムを用いた業務に対する悪影響、情報システムの利用者**（事業者内利用者、主要顧客）**への迷惑**）	・障害がないこと （**障害とは、情報システムを用いた業務に対する悪影響、情報システムの利用者**（事業者内利用者、主要顧客）**への迷惑**）	・障害がないこと （**障害とは、情報システムを用いた業務に対する悪影響、情報システムの利用者**（事業者内利用者、主要顧客）**への迷惑**）	・重大障害がゼロであること（**障害とは、情報システムを用いた業務に対する悪影響、情報システムの利用者**（事業者内利用者、主要顧客）**への迷惑**）	サービスに必要な様々な目標 ・以下については、共通した定量目標が設定されている。 　ー端末復旧時間（利用不可状態から利用可能状態に復旧するまでの時間） 　ー「安全稼働指数」（ソフトウェア投資額あたりの障害発生件数）	・定性的な目標は、情報システムの稼働品質は（定性的には）安定感があり、その安定感を維持すること **・定量的な目標は、障害発生件数の上限値** ・定性的な目標から定量的な目標に移行中である。	・これまでの実績、（実績がないものについては情報システムの規模など）、イベントを踏まえ設定する。
	「稼働品質」の目標の立て方	・運用部門の管理責任者が、情報システム全体について、目標を定める。	・個別の情報システムを担当する「チーム」が目標を定める。 ※「チーム」は外国為替、融資・・・というビジネスフローごとにある。	・運用部門の管理責任者が、情報システム全体について、目標を定める。	・情報システム全体については運用統括部門が管理する。 ・各情報システム（ITサービス）についてはそれぞれの管理責任者が管理する。	・本社の情報システム部門と、情報システムの開発・保守・運用を担う情報システム子会社で協議して定める。	・アプリケーション、アプリケーション基盤、IT基盤の層ごとにいる管理責任者が、目標を定める。	事業部門と、情報システムの開発・保守・運用を担う情報システム部門で協議し定める。
		・目標として**年あたりの障害発生数の上限を、**（定められた開発プロセス、運用プロセスによる）**前年までの実績と品質向上施策の期待効果から定める。** ・障害が及ぼす影響度によって、障害の重軽を区分し、その重軽ごとに目標となる上限を設定する。	・目標として**年あたりの障害発生数の上限を、前年までの実績と相対的な改善目標、特別要因（情報システムのリリース計画や業務量変化など）、品質向上施策から定める。**	**・全情報システムについて、KPI-KGIの構造で目標を設定する。** ・上位の目標については、中期経営計画の目標をもとに年度目標を定め、さらに情報システム群ごとのチーム目標に落とす。 ・事業部門との間でITサービスごとに摺りあわせ、稼働率などサービスカタログの中に目標を置く。	・障害を重大障害（運航、顧客への金銭的影響に関するもの）、重障害（復旧までの時間ほか）、その他の障害に分け、**重大障害はゼロ、重障害は前年度比減という目標を置く。** ・事業部門との協議によりSLAが決まり、そこから詳細な目標が導かれる。コスト勘案によりSLAが見直されることもある。	**・障害の影響度をレベル分けし、影響度の高いものを対象に目標設定する。目標は前年度の実績を元に定める。**	・目標として**年あたりの障害発生数の上限を、**（定められた開発プロセス、運用プロセスによる）**昨年までの実績と品質向上施策の期待効果から定める。** ・障害が及ぼす影響度によって、障害の重軽を区分し、その重軽ごとに目標となる上限を設定する。	・テーマ種（開発、運用）別に、年あたりの障害発生数の上限を定める。 ・目標には、イベントを加味する。
	事象の大きさの指標化	障害の重大さ（4段階） ＝ ｛自責・他責の別（3段階）｝ × ｛オンラインの影響度（3段階）｝ オンラインの影響度 ＝ 可用性 × 機密性 × 完全性	障害の重大さ（2段階）＝ Aランク：顧客に影響したもの、Bランク：顧客に影響しないもの 量的には、 顧客の利用人数×顧客が通常利用している金額	・大きな障害（インフラ系の障害）と、個々のシステム障害の二段階で定義。「事業継続に重大な影響を及ぼすリスクの発現」「有価証券等の売買を継続することができない、または継続することが適当でないと思われる状況」に関して、影響度A、B、C等、個々のシステムの特性に応じて定義。	運航への影響、お客様への影響（金銭面）	影響（お客様への影響）、停止時間	障害の重大さ（3段階） ＝ 障害の範囲　×　障害の継続時間　×　影響金額	・SS＝重大障害(データセンター倒壊・停電、EDI障害、ネットワーク切断、メール送受信不可)、中規模障害、小規模障害として定義。 ・品質情報管理システム＝日時、障害管理NO、ランク、処理状況、システム名、件名、BU名、障害ランク、起因区分、お客様への影響、暫定対応、抜本対策
	「稼働品質」の目標の達成の判断	・発生した障害をカウントする。	・発生した障害をカウントする。	・サービスカタログの中の数値を満たすことが基本 ・但し、利用者ごとの異なる要求の充足の状況も見る。	・発生した重大障害、重障害をカウントする。	・発生した障害をカウントする。	・発生した障害をカウントする。	・発生した障害をカウントする。 　但し個別事情もあるので、単純比較はしない。

（次頁に続く）

		A社 （金融）	B社 （金融）	C社 （金融）	D社 （運輸）	E社 （運輸）	F社 （製造）	G社 （製造）
品質向上施策	品質向上施策の概要	・運用部門による要件（特に非機能要件）をレビューする体制とチェック項目を定めている。 ・運用部門による、要件の情報システムへの実装をレビューする体制とチェック項目を定めている。 ・運用関連の成果物（例：オペレーターガイド）をレビューする体制とチェック項目を定めている。 ・運用業務でのスキル依存の排除を徹底している。	・運用部門による要件（特に非機能要件）をレビューする体制とチェック項目を定めている。 ・年間スケジュールの下、最低年1回以上実施する情報システム異常時への対応訓練を行なっている。	・キャパシティ管理にて、事業者外（顧客）の利用の変化の予兆を捉える。委員会（月1回）で状況を報告し、エスカレーションの必要有無の判断をする。 ・運用部門に引き渡されたドキュメントを書き換えることによって、運用オペレータが参照するドキュメントは利用しやすく属人性がでないものを用意している。 ・作業員が見るドキュメント、体制はほぼ標準化している。	・運用統括部門の要件（特に非機能要件）をレビューする体制とチェック項目を定めている。 ・運用部門による、要件の情報システムへの実装をレビューする体制とチェック項目を定めている。 ・情報システム部門内および事業部門と共同での訓練を実施している。	・サービスに関して責任を負う事業部門と、情報システムの開発・保守・運用を担う情報システム子会社で協議し立案する。 ・事業で用いられている情報システムは多彩であり、品質向上施策も多方面に渡る。	・IT基盤の構成の見直しとIT基盤の運用の改善（仮想化などのIT基盤の高度化への対応、セキュリティ対応の強化、IT基盤を構成する製品のVer管理の徹底など）	・マニュアルの整備、アプリケーション見直し、体制変更。 ・障害管理プロセスガイドラインの策定。
	個別の事象（障害など）からの学習と展開	・個別の障害と再発防止策を「トラブル分析シート」へ記録する。 ・運用部門の管理責任者が、個別の障害の再発防止策を展開する必要性と展開範囲についての判断する。	・トラブル報告書を作成する。 ・情報システム部門全体として教訓集を整備している。 ・詳細にはチェックリストに整備し、汎用化できるものは開発手順などに反映する。	・障害記録を作成する。 ※障害記録を事後的もに活用する。一例として、情報システムの置き換え時に、運用からの要件を開発側に示す際に活用する。	・障害データベースに記録する。 ・重い障害については、PMT（ヒューマンエラーの分析手法）を用いて、再発防止策を検討する。 ・原因分析の結果を含む障害分析シートを作成し、運用部門全体で共有する。	・本社の情報システム部と情報システム子会社で品質向上施策（障害の再発防止策等）について共有、検討し、必要により他の情報システムへの横展開を行う。	・各情報システムの担当者により、インシデント・データベースに記録する。 ・インシデント・データベースの情報は、テーマ別WGによる標準化推進活動や要員が参加する失敗分析会、研修でも活用する。	・再発防止策の妥当性は、各情報システムの担当要員が最終的に判断する。 ・チームレベル、ビジネスユニットレベルで原因追求を実施し合意をする。 ・情報システム子会社では、**障害から学んだことを、お客様価値向上に活かす。**（お客様に影響を与えたことを、全責任者が出席する「障害事例から学ぶ会」に報告、気づきを与え合う。） ・共有の場として、**各事業部門の品質責任者や品質担当が参加する「品質交流会」にて良い事例等の紹介を実施する。**
	上記の品質向上施策の前提	・ITサービスの品質管理責任は運用部門にあるという原則がある。 ・そのために、運用部門は、開発の重要局面においてレビューに参加し（計4回）、レビューに合格しなければ開発部門は運用部門に成果物を受け渡すことは出来ない、というルールがある。	・リスク管理部門の承認がなければ、開発や運用の方式の変更は認めない（つまり、標準の方式どおり必ず実施する）というルールがある。 ・各情報システム担当の「チーム」による、障害原因の分析、品質向上施策の立案と実施は、全てエビデンスを使って、リスク管理部門ほかに説明するという行動習慣がある。	・運用部署でITILベースで何をするかを決め、開発から受け取る際に充足されていない場合は、受け取らない。 ・アプリケーションやミドルウェアの設計時から、運用設計まで含めた冗長的な仕組みを定めておく。	・ITサービスの品質管理責任は運用部門にあるという原則がある。	・情報システム子会社が、情報システムの開発・保守・運用を担っており、品質向上施策の策定や実行を行う。 ・その実施状況については定期的に本社の情報システム部門に報告する。	・**アプリケーション基盤**（アプリケーション部品）、**IT基盤の標準化を図るとともに、データベースの正規化を実施**してアプリケーション層での運用をなくすなど、運用における問題が生じにくい構造にしている。	・**現場力強化が重要という考えである。**
品質向上施策の有効性を高める方法	品質向上施策の立案と実施推進を行う者や行い方	・運用部門の管理責任者が情報システムの状況を見ながら判断し決定する。 ・情報システム部門会議で上記の決定が承認される。	・各情報システム担当の「チーム」が判断し決定する。	・運用部門が、個々のシステム評価を月1回の稼動報告で確認し、品質向上のために横展開すべきものがあれば共有する。	・各ITサービスについては、それぞれの管理責任者（サービスマネージャ）が決定する。 ・情報システム全体については運用統括部門が管理する。	・サービスに関して責任を負う事業部門と、情報システムの開発・保守・運用を担う情報システム子会社で協議して、判断や決定を行う。	・アプリケーション、アプリケーション基盤、IT基盤の層ごとにいる管理責任者による判断と決定	・品質保証部門が年度の品質方針を立案し、各事業部門の品質責任者と品質担当を支援しながらモニタリング、評価、是正を実施する。 ・収集情報は品質保証部門がまとめ、毎月実施の事業部門の「品質会議」にて計画差異含む評価結果と対策検討を実施。 全社の評価結果は、経営会議にて報告する。
	品質向上施策の実施に関するコントロール	・運用部門内において、個別の品質向上施策につき管理責任者から各情報システムの運用担当者に実施の徹底を指示する。（これは毎月の「稼働品質」の状況をみて判断し行う。） ・運用部門の管理責任者が、開発工程での運用部門レビューに各情報システムの運用担当者を割り当てること、及び運用担当者の判断を評価して、開発工程の問題有無を総合判断する。	・品質管理活動の全体はリスク管理部門が管理する。 ・汎用化できる障害の再発防止策は運用から開発部門に戻し、アクションを決め、期限までに実施させる。	・運用部門で、運用チーム毎の目標とチーム間の調整をする。ブレイクダウンしたKPI/KGIを用い、四半期単位でその達成を確認する。	・各ITサービスの管理責任者は品質向上施策による目標の達成に責任を持つ。 ・運用統括部門では、運用に関わる情報を吸い上げ、必要に応じ指示を出す。	・情報システム子会社が、品質向上施策のコントロールも担っている。 ・本社にある情報システム部門で、個々の事案に関する品質向上施策をモニタすることはあるが、情報システム子会社が行う品質向上施策全体についてはモニタしていない。	・アプリケーションの品質管理には、CMMIを活用している。 ・IT基盤の品質管理には、ISMSを活用している。	・各事業部門が実施している品質向上活動（各種テーマを設定した小集団）支援や課題のあるプロジェクトの支援等、現場に入込むことを行なっている。支援の1つとして、活動が進むための各種データ提供、事例紹介、アドバイス、品質会議での発表の場の確保がある。
クラウド等 外部ITサービスの品質管理	上記の品質目標や、品質向上施策の適用を、外部ITサービスに対してはどのように考えるか	採用する外部のクラウドサービスについては、自社基準に照らし品質に関する契約をしている。	まだ、外部のクラウドサービスは利用していない。 利用するときには、自社基準の品質を求めることになる見込み	・クラウドは、情報系システムでのバックアップとして機能を限定して使い出したところである。	・SLAが高いものについて、プライベート・クラウドとして仮想化を進めることを検討中。 ・業界としては外部サービスが主流なので、全く使わないことはない。人を送り込む、復旧を早くする方策を練る等で対応する。	現時点でクラウドは使っていない。（但し、プライベート・クラウドは別）	外部のクラウドサービスは採用しておらず、自社内でプライドサービスを運用している。自社内のサービス品質はIT基盤を標準化し運用してきた実績に基づいている。	・クラウド等の外部ITサービス関連については取組中であり、契約（サービスレベル定義、各種仕様等）での合意を基本とする。 ・クラウドはブラックボックスなので、自社基準に取り込むためには品質管理面で苦労している。自社ではあくなき品質の追求をするが、それと同じことを外部クラウド・ベンダには要求できない。
品質目標とそのための施策を策定し、品質目標を達成する上でのキーポイント（意見）		・品質目標を明確にすること ・品質目標の責任者を明確にすること ・品質目標の責任者が、その責任を果たす上で必要な権限、ルールを設定すること ・経営層の覚悟、コミットメント	・品質確保に必要な活動の策定と実施を、個別の情報システムを担当するチームとリスク管理部門との間で、エビデンスを使って確認する行動習慣	・監視体制の強化、運用マニュアルの改善 ・人材育成が重要と認識し、教育に力を入れる方向で検討中。	・品質管理活動を継続するポイントは、運用の重要性をトップが理解し、継続的な取り組みを進めることが必要。	・開始時点のコンセプト固め、変化点への対応、意識を高くもつこと ・情報子会社に依存せず、利用者側の意識を明確化すること	・改善の必要性について、当事者（＝各情報システムの担当者）の危機意識があること ・その危機意識により、改善活動（WG活動など）を実施すること（P=課題設定、D=施策案・・・） ・改善活動には当事者の主体性が不可欠 ・改善活動の主な成果物は教育資料	・現場力の強化が重要。 ・スキル等の問題もあり、期待通りに支援することが難しい部分もある。
品質確保・向上の活動全般について（意見）		・開発の品質は、運用の品質に比べればまだ予測しやすい。 ・運用の品質確保においては、数割のムダを覚悟で十分な品質向上施策を選択・展開必ることが必要。 ・品質向上施策の実施に関するコントロールは、運用部門の品質管理者が各情報システムの担当者を説得し、施策の実施を強めさせるという地道な作業。 ・こうした活動全体の結果として、運用期の品質がある。	・金融機関（特に日本）の顧客の情報システムに対する許容度合い（安定性、稼動予定日）が厳しいため、金融機関としてコストをかけざるをえない。 ・障害発生時に開発・運用・ユーザ部門の間に立つPD（Problem Determinator）の能力や、障害発生時にできるだけ多くの人間を巻き込むという文化等人系に関わる部分は、これまでの障害の経験が生きている。（今後、PD育成等を強化予定）	・現在のBCPの考え方は、西暦2000年問題や過去の障害事例を踏まえて成り立っている。 ・現在、3ヵ年計画で、運用手法を固めているところ。将来的にはコストの観点から積極的に外部活用していきたい。	・新しい法則、技術に基づいた障害は防げないという考えから、再発防止に注力。タイムリーな情報共有、人に対するするリこみが重要として、周知指標を作った。 ・日本では、ビジネスプロセス自体がシステムに組み込まれ、見えなくなっていることが問題。ビジネスサイド要求定義が必要。 ・障害に関するデータ分析が出来きれておらず、分析結果を施策に落とせていない。今後、アプリケーション部毎に分析担当官を置き、教育し、改善を進める仕組みに変えていく。	・上流工程で合意をとった上で開発を行うことで、運用期の障害を可能な限り発生させないようにする考え方をとっている。	・管理をアプリケーション、アプリケーション基盤、IT基盤に層化し、それぞれ標準化を図って、稼働品質を安定させるという方式の定着には、情報システム部門に優れたリーダシップと良いAP基盤、IT基盤を実現する技術力の両方が必要であった。 ・2006年頃まで、生産性向上（C, Dの切り詰め）の施策を相当行った。 ・現在、品質（Q）のために割けるリソースや時間（C, D）はそれほど多くない。 ・障害=0は理想かもしれないが、情報システム部門には、情報システムの付加価値、事業への直接貢献という、より高い優先順位のテーマが与えられている。 ・無条件に高品質ということよりも、利用者（業務部門）と合意すること、その期待にミートすることの方が重要である。	・製造業としての品質管理ノウハウ（ソフトウェア製造プロセスにあわせた品質チェック）にも取り組みたい。

【付録B】 障害事例分析と障害再発防止策

※ この【付録B】は、2011 年 3 月に IPA/SEC から発行した「重要インフラ情報システム信頼性研究会　平成21年度報告書」の付録の再録である。

以下は、「重要インフラ情報システム信頼性報告書（2009年度）」で報告した障害事例および障害再発防止策についての報告を再録するものである。なお、2008 年度、2009 年度の調査において、以下の調査は日本情報システム・ユーザー協会（以下、「JUAS」）に委託して実施した。

1. 障害再発防止策に関する調査の意義と、2009年度調査の主な成果

「重要インフラ情報システム信頼性研究会」の 2008 年度報告書では、他分野での障害対策への取組みとして、航空機の例をひきながら、様々な分野で障害再発防止の視点から事後安全計画としての障害分析やそこからの知見のフィードバックが重要視されていることを指摘している。

勿論、情報システムでも同様な考えがあり得るが、情報システムの場合はそれを構成するソフトウェアが障害に関係したときに、障害事象の可視化や原因分析が難しく、結果として現場で発生している様々な障害に対して再発防止策の立案というフィードバックも発展途上の段階にある。

2008 年度報告書では、総合的な情報システムの障害再発防止策立案の第一段階として、次の事項に関する議論結果を述べた。

- 重要インフラ情報システムで、2005 年 7 月以降 2008 年 10 月までの 3 年 4 ヶ月に Web 報道された個々の障害事例についての情報収集、障害事象の分析と推定原因の整理
- 障害再発防止に広く有効な方策の案
- ソフトウェアの開発／運用に関わるチェックリストの案

2009 年度の調査では、さらに 2008 年 11 月以降 2010 年 1 月までの1年 2 ヶ月に Web 報道された個々の障害事例の追加情報収集を行うとともに、重要インフラを含む情報システムの企画・開発・保守・運用に携わる有識者（一部障害事例の当事者企業の担当を含む）により、各障害事例の事象と推定原因の整理と再発防止策の策定を行った。

2009 年度の調査の主な成果は、次のとおりである。

- 2005 年 7 月～2010 年 1 月に Web 報道された障害事例として113件を収集した。
- このうち、重大かつ一般性があると考えられる障害の43件について、各障害事例の事象と推定原因の整理と再発防止策の精査を行った。
- 上記の再発防止策につき、情報システム部門がチェックすることが有意義な単位に編集して、上記期間に生じた障害に関係するチェック項目38区分55個を得た。

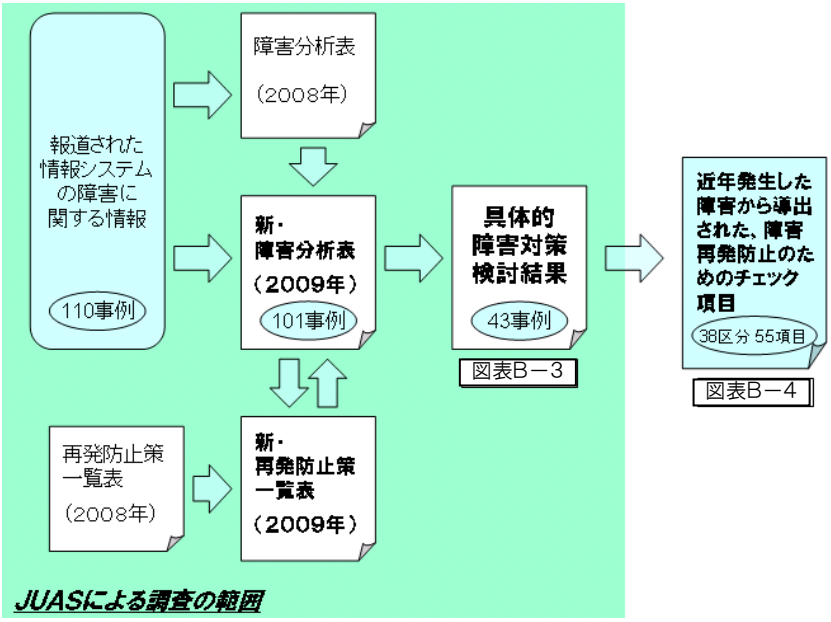
以降では、調査内容及び調査結果の分析に基づく議論の詳細について述べる。

2. 障害再発防止策の精査結果と分析

2.1 障害の推定原因の整理と再発防止策の検討

JUASでは、業界誌のWeb報道[20]で2005年7月～2010年1月に報道された障害事例を収集し、その各事象を分析した。

分析では、収集した事例のうち、重要でありかつ一般性があると考えられる障害事例を対象に、重要インフラを含む情報システムの企画・開発・保守・運用に携わる有識者延べ16名参加による検討WGにて討議し、各障害事例の事象と推定原因の整理と再発防止策の策定を行った。参加者には、一部障害事例の当事者企業の担当を含む。さらに、その各個の再発防止策から重要な部分を抽出し、情報システム部門がチェックできる単位に編集して、38区分55個のチェック項目を得た。調査の流れは、図表B－1のとおりである。



図表B－1　障害事例の調査と障害再発防止策導出の流れ

2.2 再発防止策の精査結果とチェック項目リスト

Web報道[5]から事例収集できた、重要インフラに関する障害事例は113件であった。そのうち101件が障害事象の分析が可能な情報を含んでいた。

さらにこの障害事例のうち、「経済的な影響」「社会的な影響」の観点からみて重大であって、かつ事業者固有のものではないと考えられる障害事例43件について、先述したJUASの検討WGにおいて、各障害事例の事象と推定原因の整理と再発防止策の検討を行った。検討には、10回の検討会、延べ約30時間を費やしている。（障害事例についての報道内容の時系列的な整理など、検討の準備作業の時間は含

20 Nikkei ITpro の Web にて公開されている情報を用いた。

まず。）

なお、検討対象の43件の障害事例の選択にあたっては、統一的基準は設定せず、障害の重大さ、一般性、分析のために入手できた情報の量等を検討WG参加者が主観的に判断することによって行った。但し、検討対象が類似の障害事例に偏らないための工夫として、10 回の検討会においては、図表B－2のように取り扱う障害事例の種類についての検討テーマを設定した。

開催回	検討テーマ
特別回	主要な「開発」「運用」「保守」における障害の対策
第１回	ユーザのプログラムミスの対策
第２回	ハードウェア／ネットワーク／電源の障害対策
第３回	ベンダなどのプログラム障害の対策
第４回	多量のデータ対策
第５回	プロセスコントロールシステム上の対策
第６回	運用上の各種設定ミスの対策
第７回	ユーザのプログラムミスの対策（２）
第８回	本番環境とテスト環境の区分不徹底の対策
第９回	オペレーションミス対策

図表 B－2　検討WGでの、障害事例の検討テーマ

上記検討の結果、それぞれの障害事例について各1項目以上の障害再発防止策の案を得た。その内容を、図表B－3に示す。

なお、この検討では障害再発防止策だけでなく、「問題早期発見」「緊急対策」「ダウン時間短縮対策」という、障害発生時の影響を極力少なくする方法についても考察している。これらの方法については空欄となっているものもあるが、これは検討の時間的制約から方法が案出できなかったものであり、方法が無い、ということではない。

さらに、この図表B－3に示された障害再発防止策について、重複を整理し、また情報システム部門が実施有無をチェックすることが出来る単位に編集して、38区分、54個のチェック項目を得た。導出されたチェック項目リストは、図表B－4のとおりである。

図表B－3　2005年7月～2010年1月に発生した障害事例における対策の検討結果

事例内容 （Web報道の要約）	障害概要 （Web報道の要約）	検討メンバーが 想定した主な原因	問題早期発見 ※問題発生時の原因特定	緊急対策	障害再発防止策 抜本対策 予防保全	障害再発防止策 抜本対策重要部分	ダウン時間 短縮対策
1．開発に関わる障害							
JR東日本が空席を販売できず、指定席販売システムに不備	新幹線と成田エクスプレスの一部で、本来は空席だった指定席を発売済みとして、販売していなかった。 原因は、4月1日に切り替えた指定席販売システムの移行時の不備。 東北、上越、長野、山形、秋田の新幹線57本と成田エクスプレス11本の計68本。座席数では合計5725席で、対象となる指定席4万3169席のうち13.6%。	システム切り替え時のテストで利用したデータの一部を元に戻し忘れたことなどが考えられる。			単に、テスト時に入力したデータを本番時にクリアせずに間違って引き継いでしまったように見える。そうであるとすれば手順漏れで、チェックリストの不整備が原因か。 しかしSEの立場からすると、チェックリスト通りに作業することは当然のこと。それ以外の事態が考えられる。例えば、更新がないと思っていたDBがテストで更新されていた、など。 原則として、本番環境でテストを行うべきではない。仮にそれをせざるを得ないことがあって本番環境でテストをするとすれば、本番環境に責任を持つ部署がこのテストでも責任を持って、本番稼働可能の状況への復帰まで行うべき。	・本番環境と同様のテスト環境を持ち、テストを実施する。 ・仮に本番環境でテストをする場合には、テストの環境について運用部門が責任を持つ。	
青森市役所、517件・1700万円の口座振替データを作成せず	5月1日引き落とし分の固定資産税の引き落としデータ作成の誤り。 517件約1700万円分のデータを金融機関に送付しなかった。	本稼働に先立ち1月から2月に実施したテストでの一時的に修正したプログラムを元に戻さずに本番稼働したため。	プログラマーと運用部門のチェッカーの関係密度の強化。	テスト済みのプログラムを活用。	①保守性 【変更性の課題】 構成管理（ライブラリ管理）が徹底されていない（バージョン管理の徹底）。 運用開始に向け正しい手順をもとにシュミレーション、作業実施がなされていない。 （臨時作業のために本来変更すべきでないプログラムを改変している可能性がある。） マネジメントスキームが不十分で、狭間の作業に漏れがある。（担当ベンダーが階層化されてしまい、監視ができていない。）	・構成管理（ライブラリ管理）の実施によって、プログラムのバージョン管理を実施する。	利用責任者の目視検査。
神戸新聞のシステム障害	障害が発生したのは紙面をレイアウトする「組版システム」。 2007年9月22日朝に、同システムのデータベース（DB）・サーバーにアクセスできなくなった。 システム本体はメインとバックアップを用意していたものの、DBを冗長化していなかったため全体が利用できなくなった。	日本オラクルの「Oracle9i Database」。データの検索を高速化する統計情報の採取処理をした後、データベースのシステムを強制終了すると、まれに起動ができなくなる問題がある。		京都新聞に組版を依頼して新聞を制作した。	①信頼性 【障害許容性の課題】 システム品質の要求レベルに見合った障害対策（データのバックアップ、待機系システム構築等）を行う。利用製品選定も同様。 ②機能性 【合目的性の課題】 システム設計局面で運用部門による妥当性検証を行い、あるべき運用方針にしたがってシステム設計を行う。	・システム設計局面で運用部門による検証を行い、あるべき運用方針にしたがってシステム設計を行う。	

ゆうちょ銀行の顧客情報照会システムの処理遅延	ゆうちょ銀の顧客情報紹介システムで、レスポンスの遅延が発生。	アクセス集中はあらかじめ予想されていたが、ピーク時の想定が甘かった。		当日昼間は照会システムをできるだけ使わないようにした。夜間に、ハードウェアの緊急増強を行った。	効率性 【資源効率の課題】 運用設計にて閾値越えを想定した仕組みを検討できていない。 ※画面設計の複雑さもレスポンス遅延要因と想定できる。	・情報システムの企画時にトランザクションの上限を設定し、設計時にその上限を超えた場合の対応方法を定義しておく。	
JRなど自動改札の障害	10月12日朝、首都圏のJRなど662駅で、「日本信号」製の自動改札機が使えなくなった。4400台の改札機が動かず、約260万人に影響。 自動改札機の組み込みソフトのバグ。センタからクレジットカードの特定データ件数が送られてくると電源を切るバグがあった。	単純なプログラムミス。しかしこのミスを、レビューでもテストでも発見できなかった。			このソフトウェアの本質は改札機の制御で、クレジットのチェックは付加的な機能である。この付加的な機能に問題があって、本質の機能に障害が起きるようなことがあってはならない。 ソフトウェアは疎結合の、シンプルな構造で作らなければならない。付加機能に問題があれば、その時は本質の部分だけを稼働させて、付加的な部分のサービスを停止する形で作成するのがよい。 これはソフトウェアの設計のレベルの問題ではなく、システム・アーキテクチャや、あるいは要求仕様に関わる問題である。	・要求仕様確定時に、情報システムの本質の機能と付加機能を区分する。 ・アーキテクチャの設計時に、付加機能に問題があってもそれを本質の機能の障害にしない仕組みを組み込む。	
日本郵政、民営化後の初給料に支払いミス	民営化後に初めてとなる同月分の給料支払において、一部の社員で、通勤や扶養などの手当てが実際より少なかったり、保険料などが控除されなかったりするトラブルが発生。社員約500人に影響。	本番用のコンバージョンミス、プログラムミスの可能性が高い。	本番データで新旧システムの実行を行い結果を比較しておくこと。	新旧の給与明細を全員、全項目の比較をプログラムを使って確認すること。	システム計画時より左記テストを総合テスト時に実施する方針を立てること。	・新旧の出力の全項目を比較するプログラムを使って、新しい出力の内容が妥当かを確認する。	
日本郵便の「後納郵便」で料金請求ミス	法人向け郵便サービス「後納郵便」の10月分料金請求の一部にミスが発生。総件数は約1万6000件。	顧客データの登録ミス。			データ入力も、やはりダブルチェックが原則。リスクを考慮して敢えてダブルチェックを行わないこともあり得るが、この場合そこまで考えてダブルチェックを割愛したとは思えない。	・データの入力でも、2名の担当者によるチェックを実施する。	
かんぽ生命でデータ処理ミス	年末調整に必要な保険料の払い込み証明書約890万件の発送が遅延。	原因はデータ処理のミス。実際の引き落とし日とマスタデータからのデータ抽出日がずれて、未納扱いに。具体的には、9月30日がデータ抽出日になっていたが、この日が週末に当たったため実際の引き落としが翌週の週初に、データ抽出がこの月末日の前の週末に行われて、不整合が発生した。	顧客に送るものは、あらかじめその部門の責任者が目でチェックし、確認してから送るということを実施する必要がある。		9月30日というリスクの大きい日の処理は、避けるべきだった。	・期末日、月末日、あるいは大きな作業が予想される日などには、急を要しない臨時作業をスケジューリングしない。	

JR西日本、特急列車が誤進入	京都発新宮行き特急列車が新今宮駅を通過する際、本来大和路線(関西線)ルートに進入すべきところ、誤って大阪環状線ルートに進入。 運休計31本、遅れ計26本、影響人員約3万人。	メーカーにおいて自動進路制御装置を製作した際、プログラムが正しく製作されず、機能検査が不十分であった。 列車ごとの進路は、ダイヤに基づく列車の順序にしたがって制御するよう製造する仕様のはずが、そのようになっておらず、新今宮駅手前に設置した制御点に早く到着した列車の進行方向にあわせて、出発側の分岐器が切り替わるプログラム仕様になっていたため。			①機能性 【合目的性の課題】 暗黙知の扱い: (1)要件に記載が漏れやすい下記内容について、要件定義工程および設計工程の早い段階で明文化している。 (業界常識、顧客常識および顧客ビジネス標準となっている業務手順・規約など) 暗黙知を形式知として明示(ドキュメント化)していく。 (※「何が暗黙知なのか」を明らかにする方法について、課題あり。) (2)要件網羅、要件要素間矛盾および妥当性の観点から。暗黙知による要求欠如、要求項目同士の矛盾および背景・スコープの不明確さなどを第三者要件定義診断を実施する体制を組織化する。 (3)要件定義書からの要件一覧化、各要件ごとにIDの付与および以降の設計書ならびに試験仕様書においてこのIDをベースに詳細化(IDの枝番付与等)しながらトレーサビリティを確保し、矛盾の発見を行う。	・業界の常識、顧客の常識および顧客ビジネスの標準となっている業務手順・規約などについて、要件定義工程および設計工程で明文化する。 ・前記事項が充分に記述されているかについて、第三者要件定義診断を実施する。 ・要件定義書から設計書、プログラム、及び試験仕様書まで、及びその逆方向について、トレーサビリティを確保する。	
東証先物システム障害	東証では同日午前10時59分にシステム障害が発生。3月まで取引できる株価指数先物の「東証株価指数(TOPIX)先物3月限月」の午後の取引を中止。	メモリ上のワークエリア初期化処理が漏れていたため、ワークエリアに残存したデータの影響でDBに不整合が発生し、約定処理が停止。			テストの一層の強化。プログラムロジックの机上検証。プロジェクト管理態勢の見直し。障害発生時の体制の見直し。障害時訓練の実施。	・プログラムロジックの机上検証を実施する。 ・障害発生時の体制の見直しを行う。 ・障害発生時の訓練を実施する。	
信金システム障害	全国信用金庫データ通信システムが信金から他金融機関向けの為替電文の送信ができない不具合が発生。74万件の為替取引が未処理。	電文を送信する際のソフトのバグ(OSの機能の一部)。 一度送った電文を再度送らないために、OSの機能の一部に日付のチェック機能を持ち込んだ。その日付が、それを管理している領域の桁数の問題で、あるタイミングでスタート時点に戻っていまい、その影響でシステムの日付が元に戻ってしまって、送られない電文が発生した。	情報システムの性格から、常時電文の滞留が発生している。しかしこの滞留の状態を時期や時間毎に把握し、併せてその監視をして、把握している状況との比較をする仕組みを持っておけば、発見はもっと早かったと考えられる。		ユーザ・プログラムの一部であろうが、OSの一部であろうが、このような機能をユーザとしてブラックボックスにしない、というスタンスを取りたい。	・情報システムの中に、一切ブラックボックスを持たない。	

2. 保守に関わる障害

JR東日本のSuicaで初の大規模トラブル	12月1日に日付が変わった時点で利用者が改札を通過できなくなり、ゲートを開放することで対処。	①プログラムミス 修正してはいけないものを修正 ②フラグの設定ミス ③テストケース不足 レアケースの未確認 ④リグレッションテスト不足 ⑤影響分析の不足 ⑥複数メーカーでの仕様統一の徹底不足	段階的切り替えを行うようにする。 部分的に試行切り替えを行う。	前のバージョンに戻す	①最初は適用範囲を限定し(エリアを分ける、駅構内でも特定の端末に限定する等)部分的に試行切り替えを行う。 ②バージョン管理情報照合の仕組みの用意。	・障害発生前の状態に早急に戻すための仕組みを作っておき、必要時にそれを使用する。 ・情報システムを修正した場合、もし可能なら全領域でその修正分を一斉に適用するのではなく、最初は適用範囲を限定し、部分的な試行切り替えを行う。	前日状態に早急に戻すための仕組み作り。 ↓ 送信側サーバおよび端末内で最低2世代のバージョンを持てるようにし、戻し作業をすぐに行えるようにする。
都営地下鉄のPASMO定期が無償発行のミス	都営地下鉄・光が丘駅の発売機で磁気の定期券をPASMOへと切り替えようとした利用者に対して、料金を請求せずにPASMO定期券を発行。	排他制御の問題。	トレース技術の向上 ミドルウエアを使用しての、トレース技術の活用。 アプリケーション開発時の、トレース用データの準備。		排他制御のテストケースの充実 保守開発・運用の標準化を作る。	・要件定義書から設計書、プログラム、及び試験仕様書まで、及びその逆方向について、トレーサビリティを確保する。	
東京都の納税通知書の送付ミス	住民に送付した自動車納税通知書が約3000通返送されたトラブルが発生。	テスト結果確認漏れ			アウトプットの改修前後チェックを行う。	・新旧の出力の全項目を比較するプログラムを使って、新しい出力の内容が妥当かを確認する。	
JR東海・西日本の新幹線ネット予約サービスに障害	インターネットから東海道・山陽新幹線の指定券や乗車券が予約できる会員制サービス「エクスプレス予約」において、早朝6時10分ころに障害が発生。	①性能対策の上限値テストの未実施。		前のバージョンに戻す。	①上限値を超えた場合の設計を組み込む。 ②本番環境に近い環境での負荷テストの実施。	・情報システムの企画時にトランザクションの上限を設定し、設計時にその上限を超えた場合の対応方法を定義しておく。 ・本番環境に近い環境で、負荷テストを実施する。	
「ケーブルプラス電話」の障害	KDDIがケーブルテレビ会社と提携して提供中の固定電話サービス「ケーブルプラス電話」が一部のユーザで利用不可能に。	①移行作業の失敗 →移行完了時の確認チェックポイントの未設定。 ②失敗時のリカバリの失敗。			①移行手順書の作成と確認の徹底	・移行手順書の作成と確認を徹底し、関係者間でその内容について情報共有しておく。	
厚生労働省、自治体への交付金支払いが100億円不足	国民健康保険の財政調整交付金を算出するシステムの欠陥により、全国の自治体(市町村)に交付する金額を誤って算定。	①省令のチェック不足 ②ユーザーのテスト不足 ③省令を理解している人の不足	確認チームを、自治体とベンダー一緒の組織として設ける。		①有識者による省令と要件定義のチェックを行う。 ＝発注者としての仕様確認を徹底する。	・有識者による要件定義のチェックを徹底する。	

ゆうちょ銀行の年金振込障害	午前9時から同9時30分までの間、ゆうちょ銀行の受取口座に振り込まれないトラブルが発生した。 仮定：個々の明細は正しかったが、総額部分でのチェックの桁数に誤りがあった。	①レビューの不徹底 ②テスト未実施			①有識者による仕様の確認 ②上限下限値のテストの確実な実施 ③本番前の稼働確認会議の実施	・有識者による要件定義のチェックを徹底する。 ・本番稼働開始前に稼働確認会議を実施し、変更点の確認、移行の手順、移行を取りやめて元に戻す時の判断基準とその実施方法などについて、関係者間で情報共有しておく。	
ゆうちょ銀が国債の取引残高報告書の作成ミス	国債を購入した顧客に送った取引残高報告書に記述ミス。	書面に利子を印字する計算プログラムに誤り。 このExcelファイルに埋め込まれた利子の計算式のうち、課税区分の扱いに間違いがあり、「課税」を「非課税」に、「非課税」を「課税」として計算。 事前にテストは実施していたが、障害対応などに関するプログラムの変更管理に問題があり、修正前のバージョンのファイルを使用。			①保守性 【変更性の課題】 システム資源全体（プログラム、ドキュメント、ツール、データ）を構成管理対象とする。 ②信頼性 【障害許容性の課題】 お客さま向け帳票などは本番移行直後での確認を行う。	・プログラム、ドキュメント、ツール、データなどシステム資源全体を構成管理の対象とする。 ・お客さま向け帳票などは本番移行直後での目での確認を行う。	
NHKが受信料を過剰徴収	請求額を計算するプログラムの不具合が原因で、一部の契約者から受信料を余分に徴収。	単身赴任者や親元を離れて暮らす学生を対象に受信料を割り引く「家族割引制度」を2006年12月に導入した際の対象プログラム改修に不具合。 56件の世帯から計23万8505円を余分に徴収。	改修部分が的確に対応できているかは、その変更を要求した人が自分で、目と手でしっかりと確認する必要がある。 さらに今回改修の対象にならなかった箇所にデグレが発生していないかの確認は、回帰テストで行うしか方法がない。 この両者を適切に組み合わせて、事前に充分にチェックすることが重要である。		料金計算の本質は、「単価×使用料」というたいへんシンプルなものである。しかし営業政策などの関連の対処がこの料金計算の中に持ち込まれ、料金計算はすでに例外処理の固まりになっている。さらに顧客の住所や氏名の変更などの対応もこのソフトウェアに持ち込まれていて、料金計算のシステムは限りなく複雑になってしまっている。ここに、この種類の問題が起きる要因がある。 経営者やシステムオーナーはこの事実を充分に認識し、リスクと効果を計った上で、料金計算に新しい仕組みを追加するかどうかを判断する必要がある。	・保守で改修部分が的確に対応できているかを、その変更を要求した人が自分の目と手でしっかりと確認する。 ・ソースプログラムに手を入れた場合、回帰テストを実施する。 ・適切に機会を設けて、複雑化した仕様の単純化を図る。	
ドコモのポータル入札システムに不具合	6月12日に発生したiMenu入札システムの不具合が発生。 本来は非公開の入札金額を公開。	最終設定のミス 急なルール変更 （6/11→6/12の短期間）	変更後、リアルタイムで監視する。	可変の値に対しての修正の戻しを、すぐに行えるプロセスの準備	①修正変更プロセスの確立 ②テスト計画の充実	・保守開発プロセスを確立する。	可変の値に対しての修正の戻しを、すぐに行えるプロセスの準備

東証でシステム障害発生、TOPIX先物など売買停止	システム障害が発生したため、東証株価指数（TOPIX）先物や同オプション、国債先物取引などの派生商品の午前の売買を停止。	直接の原因は、板のデータを蓄積する容量の上限値のパラメータ設定ミス。 東証の要件では、1銘柄1,280バイトの領域で、28,000銘柄分のデータ領域を上限値として確保することになっていたが、実際は、1銘柄4バイトの領域で、28,000銘柄と、誤ってパラメータが設定されていた。		モジュールを、前のバージョンに戻した。	テスト工程の見直し。システム外部監査の実施。開発ベンダーのプログラム改修時のチェック体制の強化。ベンダー管理の強化。システム障害の早期復旧を可能とする方策の検討。	・システムの外部監査を実施する。 ・開発ベンダーのプログラム改修時のチェック体制を強化する。 ・システム障害の早期復旧を可能とする方策の検討を実施する。。	
PASMOがバス運賃で二重課金，原因は運転手の誤操作	バス共通ICカード協会は2008年9月11日，非接触ICカードによる電子マネー「PASMO」と「Suica」でバスの運賃を二重課金する不具合があったと発表した。 今回の不具合はバス運転手によるICカード読み取り装置の誤操作が原因。 約6万件の誤課金が生じ，総額約1100万円を過大に徴収していた。	①バス運転手によるICカード読み取り装置の誤操作が原因。 ②ICカード装置と上位の読み取り装置の不整合。 ③教育・訓練・テストに対する中身の検証ができていない。 ④システム全体を鑑みた運用設計ができていない。 ⑤箱モノや上位のシステムのメーカーが複数に分かれており、総合的な仕様が把握できていない。 ⑥ICカードは独占的な仕様なので色々なシステムの組み合わせ事例がない。 ⑦オンライン端末として繋がっている電車のシステムと無線もしくはバッチ処理で行っているバスのシステムなどの仕様相違を理解できていない。	①総合的な運用確認テストの実施。 ②実務運用（利用者をイメージした運用）を考慮したテストを実施。 ③複数のユーザが集まって、多角的な視点もしくはユーザの立場に立って実運用を議論して、テストケースを確立する。 ④実運用（お客様視点）をイメージしたシュミレーションを実施する。 ⑤収入管理システムの検証機能（実収入）の確認。		①バス事業者への誤動作防止の指示徹底を通達。加えて、バスに搭載した読み取り装置のソフトウエアを改修し、運転手が読み取り装置をリセットしても二重課金しないようにする。 ②関係各社の役割分担／責任範囲を明確にする（役割分担が曖昧なことにより、本来すべきチェックが漏れている）。 ③提供するサービスの観点からトータル的な業務の矛盾がないように、運用設計を実施していく。 ④複数企業にまたがる社会インフラサービスは、小規模環境を構築し、常に実証環境を図る。	・複数企業にまたがる社会インフラサービスについて、関係各社の役割分担／責任範囲を明確にする。	
大和証券、取引所との接続に不具合で注文通らず	大和証券では午前9時5分から9時41分まで、大和証券SMBCでは午前9時から午後10時まで、株式注文システムに障害が発生。障害が発生している間は証券取引所への注文取り次ぎができなった。	制御システムの修正ミス	①ログトレース技術の向上⇒汎用データで不足する場合はアプリケーションで力バーする。②変更処理が完全であったかどうかを本番でウオッチすること。	前のバージョンに戻す	①サービス開始前の確認 ②影響分析の徹底 ③定番リグレッションテストケースを作成し、常に実施する。 ④疑似本番環境を準備し、事前に当環境でテストを実施する。⑤数時間様々なデータをテストできる回帰テストの実施。⑤修正確認会議の組織的実施。	・多くのテストデータを積み上げて、回帰テストを実施する。 ・本番稼働開始前に稼働確認会議を実施し、変更点の確認、移行の手順、移行を取りやめて元に戻す時の判断基準とその実施方法などについて、関係者間で情報共有しておく。	①分散リリースをする。→システム構成を本番、待機系等に分けて、順次リリースを行い、障害時には反映させていない方のみの縮退運転を行う。 ②コンテンジェンシープランを用意する。

	かんぽ生命の支払いミス	かんぽ生命、支払いミス4万8000件が判明。8月から顧客へ通知 。	日本郵政公社時代に判明した簡易生命保険のプログラムの誤り。 ①約種類の変更や年金額の減額などの契約変更を行った場合。一部の契約で配当金計算が誤っていた。 ②毎年一回顧客に送付する「支払年金額等のお知らせ」において、必要経費金額を端数処理プログラムの誤りにより1％分少なく算出した。			機能性 【合目的性の課題】 テスト実施不足、テスト結果検証不備が想定できる。 保守性 【安定性の課題】 大量でバリエーションの多いデータを取り扱うため、一度に障害を摘出することは困難。平常時の母体システムの品質向上活動(潜在バグ摘出)が不足していると想定できる。		

3．運用に関わる障害

totoシステムがダウン	スポーツ振興くじ(toto)の販売システムが5月12日午前、アクセス集中によって利用しにくい状態になった。	各販売チャネルとシステムをつなぐ接続ゲートウエイの処理がボトルネックとなりトラブル。			非機能要求の1つとして、入力されたトランザクションが情報システムの処理能力を超えた時にどう対応するのかを定義しておく必要がある。ユーザがこれに気付かなかった場合にはベンダーが問題提起を行い、ユーザに処理能力の限界とそれを超えた時の対処の方法を的確に理解してもらった上で、両者でこの情報を共有しておくことが必要である。 この要求に基づいてアーキテクチャを設計することになるが、ここで、全体を見たアーキテクチャの設計が必要である。今は中間サーバがブラックボックスになり、その処理能力が分からないため処理可能なデータ量が把握できない、という事態が起きることが多い。	・情報システムの企画時にトランザクションの上限を設定し、設計時にその上限を超えた場合の対応方法を定義しておく。	
「ひかり電話」がNTT東西間で不通	NTT東日本とNTT西日本の「ひかり電話」を接続する装置に障害が発生し、NTT東西間でひかり電話などが不通。 合計約318万チャネル。	NTT東西間のひかり電話中継網における接続装置(中継系呼制御サーバ)のハードディスクを交換した際のデータ設定により、ハードディスク内の一部データが破壊され(*)、このデータにアクセスがあり、異常処理が発生し、通話制御処理が停止。 〈1〉ハードディスクの交換に際し、作業者がコマンドパラメータを誤って投入したが、フェールセーフ機能が不十分でコマンドが正常に受け付けられたため、正しく処理が完了したと判断した。 〈2〉パラメータ誤りにより、ハードディスク内のデータの一部が破壊される問題がソフトウェア内に存在していた。			操作は、2人がペアになって行うのが鉄則。1人が入力し、もう1名がチェックする方式。 この障害の場合は保守作業の中での操作だが、本番作業では手順書に則って運用することが大原則。 仮に手順書があっても、それに基づいて的確に操作ができるように訓練しておくことが必要。仕組みはあるが訓練不足でその仕組みを生かすことができず、結果として障害が発生してしまった、というケースが散見される。 すべての面で標準化を推進し、例外を一切作らないというスタンスも、一方で重要。	・運用上の操作は、必ずオペレータがペアで実施する。 ・作業には全て手順書を用意し、その手順書に則って操作する。 ・手順書通りの操作を的確にできるよう、訓練を実施する。	

ANAチェックシン・システム障害	5月27日未明から、全日本空輸の国内線において、予約搭乗手続きや手荷物管理を担当するチェックイン・システムに障害が発生。 130便が欠航、306便が1時間以上遅れるなど、約7万人に影響。	接続系のネットワークスイッチのメモリ故障から中継系サーバがダウン。			この場合は全機能が停止したわけではなく、一部の機能は稼働していたと推察する。 この一部停止の場合にはその状態からリカバーしようとするのではなく、一旦全機能を停止して、健全なバック機に全業務を移管する方が、被害の拡大が少なく、回復も早い。このような判断と行動を即座にできるようになるためには、周到な準備と定期的な訓練が必要である。	・一部の機能が停止した時に、全部の機能を停止させて、バックアップ機に全業務を移管する方がスムースに回復することがある。このようなケースの判断とその判断に基づく作業手順をルール化し、訓練しておく。	
新生銀行が顧客267人に二重の出金処理	3月10日のある時間帯にキャッシュカードやデビットカードで出金した取引情報を、6月10日に再度、出金処理を実施。 対象顧客は267人。	バックアップ機を「訓練」のため一時的に本番稼働させた際、滞留した出動データを再度処理したため。			システム要求の確定からアーキテクチャの設計段階で、本番機とバックアップ機の関係を非機能要件として作り込んでおく必要がある。この中で、バックアップ機にデータが渡った時の振る舞いも明確にしておき、テスト段階でその確認を取っておく。 運用部門、及びユーザ部門が開発段階で、運用に必要な事項をソフトウェアに埋め込んでおくことも重要である。一例として、バックアップ機の稼働に関するノウハウと責任をバックアップセンター部門に持たせ、そこで得たこのノウハウを開発部門にフィードバックするという方法がある。 バックアップ機の稼働を途中段階で終わらさず、一日の締め時間まで稼働させる方が、後の対応がシンプルになる。	・アーキテクチャの設計までの段階で、本番機とバックアップ機の関係を明確に定義しておく。	
IP電話のスカイプで大規模障害	インターネット経由のIP電話を提供する「スカイプ」においてユーザーがログインができなくなり、IP電話の発信や受信、状態を示すプレゼンスの確認などができなくなった 。	Windows Updateがきっかけで，多数のスーパーノードのシステムが再起動。この結果，各Skype端末から認証要求が大量に発生し，残ったスーパノードがさらに倒れた。			Windowsアップデートやウィルス定義ファイルの更新など、一般にコンピュータを使用する環境の中で一斉に多量のダウンロードと再起動、及びその結果として特定のアドレスにアクセスの集中が生じることがある。これを予測して、瞬間最大アクセスに対する情報システムの設計を行っておくことが不可欠である。	・多量のダウンロードと再起動、及びその結果として特定のアドレスにアクセスの集中が生じることがあることを予想して、可能な瞬間最大アクセスに耐えられるよう情報システムの設計を行っておく。	

NTT西の通信障害	フレッツ・光プレミアム、フレッツ・V6アプリ、フレッツ・V6キャスト、フレッツ・グループ、フレッツ・オフィスをご利用の一部のお客様の通信ができない状況。 サービス向上にむけた工事の実施中、一部のお客様収容装置が高負荷状態となったため。NTT西日本管内4府県（大阪、兵庫、京都、福岡）。 故障ユーザ数：約2万9千ユーザ（フレッツ・光プレミアム）。	①NTT局内工事にて新機種に変更されたにも関わらず、従来どおりの手順でループをかけた。（ループは旧機種での対応手順となる）。 ②工事業者に新機種対応の作業手順が周知できていない。 ③ユーザー申告により、障害を検知した。当初はNTTは障害の発生すら把握していなかった。原因把握まで6時間も費やしている。 ④NTT内部での工事の情報共有が行われていなかった。 ⑤旧機種、新機種に対する資産管理（構成管理）ができていない。	①工事情報の共有化（どこで、どんな工事が行われているか一元管理しておく）。 ②ユーザー申告に対して、早期に対応する（自分を疑う）。	①ループしたケーブルの撤廃。	①装置のループを自動検知する（機種ごとに合わせたチェック機能を設ける）。 ②新規設備導入時の手順書を関係各所に周知徹底する。あわせて、教育訓練を実施する。 ③工事完了時に確認（発注者と受注者および工事者で）。 ④品質保証のために基準（発注者・受注者・工事者）の設定。 ⑤基準違反した時の罰則設定。 ⑥資産管理システムを構築する。運営方法を各自に順守させる。 ⑦ハードチェック。1時間に1回のルート確認。	・新規設備を導入する時の手順書を関係部門間で情報共有しておく。	
47NEWSのサイトでシステム障害	共同通信社と全国47都道府県52の新聞社がコンテンツを提供しているニュース・サイト「47NEWS」の配信システムで障害が発生し、ニュース内容の更新ができないなどのトラブルが発生。	メインのDBサーバで障害が発生。サブの待機系に切り替えたところネットワーク障害でダウン。 更に、復旧作業のバックアップデータのリストアで文字コードの誤りで文字化けが発生。		障害装置の修復。	常時2機稼動体制の採用。 待機系への切り替えテストの定期的実施。	待機系への切り替えの訓練を、定期的に実施する。	常時2機稼動体制の採用。
東京RDP障害	東京航空交通管制部にある航空路レーダー情報処理システム（RDP）において通信障害が発生し、航空機の運航に遅延が発生。 航空機の運航に遅延が発生した。	基盤（H／W）が故障し、バックアップ機能も正常に機能せず。	バックアップ系の本番系を監視している部分に障害が発生したものと見られる。そのため、本番系は順調に稼働していたにも関わらずバックアップ系は本番系が障害を起こしたものと誤認し、正常な本番系から障害を持っているバックアップ系に業務を引き継ごうとして、本当の障害を引き起こしてしまったケースと推察する。		個々の信頼性を高めて行くと、部分障害の場合に全体の信頼性を下げてしまうことがある。この場合には確認と対応を全て自動化するのではなく、人の手を介在させる必要がある。	・本番機からバックアップ機への切替を完全に自動化するのではなく、人間の判断と操作が入る余地を残しておく。	
住友信託銀行のシステム障害（66も併せて）	住友信託銀行の本支店窓口と現金自動預払機（ATM）とインターネット取引での入出金や振込み、及びゆうちょ銀行など他行やコンビニATMでも同行のカードを使った取引が全面的に停止。さらにその翌日、再度のシステム障害により、本支店のATM、インターネット・バンキング・システム、コンビニATMの「E-net」、ゆうちょ銀行、他行ATM、デビットカードでの取引が停止。 ATMなどの接続台数にかかわるパラメータの設定ミスと、前日に実施した取引ログ・ファイルのサイズ拡張に伴うパラメータ設定のミス。	①ログ・ファイルのサイズ拡張に伴うパラメータの設定ミス（2種類の異なるパラメータを誤って設定、プログラムにはファイル・サイズの設定個所が3つあり、そのうちの1つに誤った値を設定）。 ②ダブルチェックの不徹底。	①3カ月に1度程度行っている定期的なシステム変更作業を実施。定常作業による作業の簡略化、慣れによるヒューマンエラー。 ②ファイルサイズはモニタリングしているはず。しかし、ログファイルのエリアの拡張はテストできないので、ダブルチェックが必要。		①定例作業の完全自動化を指向し、プロセス等のワークフロー化を推進していく。 ②画面のハードコピーを残す。第三者がエビデンスを確認する（ヒューマンエラーの抑止）。 ③オープン化技術を施行し、運用管理の自動化を目指す。	・作業実施の結果や画面のハードコピーなど、操作の全てを記録に残し、第三者による確認のためのエビデンスにする。	

オンデマンドTVの視聴に不具合	映像配信サービス「オンデマンドTV」の視聴に不具合が発生し、約34時間視聴ができなかった。 西日本地域30府県の最大約4万7000世帯が、正常に番組を視聴できない状態が続いた。	コンテンツ視聴要求を管理するサーバーの不具合が引き金となり、対象エリアの視聴制御システムの輻輳が生じたため。			人気番組には、アクセスが集中することになる。人間の行動心理を読んだキャパシティ設定が必要である。	・情報システムの企画時にトランザクションの上限を設定し、設計時にその上限を超えた場合の対応方法を定義しておく。	
福井県美浜町のミサイル発射の誤警報	福井県美浜町で6月30日午後4時37分ごろ、「ミサイル発射情報、当地域にミサイルが着弾する恐れがあります」と緊急放送が町内に流れるトラブルが発生。	テストで使った「ミサイル発射」の警報データを削除せず、また動作確認に使った警報データの選択ミス。 J-ALERTには訓練専用の警報を流す仕組みがあるが、今回の作業では「ミサイル発射」の警報を誤って使用。			現場の人がシステムの細部まで知っていて作業に当たることができるという前提は、この場合成り立たない。システムを作った側がそこまで考慮して、的確な手順書を用意しておくべきだった。 こういう情報システムでは、全自動化は当然のこと。この障害で、実際の被害は出ていない。	・現場でのオペレータによる操作は極力シンプルにし、かつ的確な手順書を用意しておく	
全日本空輸、国内旅客の搭乗手続きや手荷物管理を行うチェックインシステム「able-D」の障害	顧客の搭乗手続きや荷物の登録ができなくなり、「飛行機が出発できない」「機材が折り返せない」という事態が発生。 羽田空港と国内各地を結ぶ便を中心に計53便が欠航。276便に1時間以上の遅れが生じ、連休中の旅行者ら5万4千人以上に影響。 ANAとシステムを共有しているスカイネットアジア航空の6便、アイベックスエアラインズの2便、スターフライヤーの2便も欠航。北海道国際航空(エア・ドゥ)便にも遅れ。	チェックイン端末を管理するサーバー内の、暗号化機能の有効期限の設定ミスによるもの。			有効期限のあるようなものを、重要インフラシステムに入れること自体に問題がある。しかし、入れないわけにはいかないのが実情だろう。その場合には、少なくとも時限爆弾が爆発する日を事前に共有して、リマインドする仕組みを持つべきである。 基本ソフトの範疇であろうが、ユーザ・プログラムの領域であろうが、情報システムの中にブラックボックスを持つことは避けなければならない。	・情報システムの中に、一切ブラックボックスを持たない。	
市町村の「うっかり」ミスで1万8223人から医療保険料を誤徴収	厚生労働省は10月10日、後期高齢者医療制度および国民健康保険の保険料を年金から天引きしている対象者のうち1万8223人の保険料が、10月15日に誤って徴収されることになると発表した。該当するのは保険証の支払い方法を天引きから口座振替に変えた人など。 市町村の担当者がデータ変更を誤るといった「うっかり」ミスが原因。市町村が依頼データを作成する際に、対象者の氏名や基礎年金番号などの入力を間違えたケースが457人分あった。このほか、市町村や国民健康保険団体連合会によるデータ提出漏れが1万6906人分あった。	①市町村の担当者がデータ変更を誤るといった「うっかり」ミスが原因 ②入力ミス ③システム的な入力チェックが出来ていない。 ④組織としてチェックする機能がない。 ⑤法律・制度変更に伴う、システム改修の期間が短い。 ⑥法律・制度変更に伴う、システム改修要件が各自治体でバラバラ(不整合がある)。 ⑦文化(慣習)に縛られた中、法律・制度変更を柔軟に対応しなければならないので無理した理不尽な帳票を策定する。	①要件定義・開発方式を変更する分、十分なシステムテストの期間及び体制を確保する。 ②ダブルチェック体制や管理体制の充実 ③テストデータやテスト環境を限定した場所で実施し、可能限り実データでの検証を行う。		①環境変化に伴う柔軟なシステム化要件の策定及び開発を行うこと。 ②法改正に伴い仕様を自治体に早期に情報を通達する。 ③要件が決められず納期優先で対応するシステムは開発方式・品質管理等を変更して実施する。が、稼働後に変更した開発方式・品質管理の差分を必ず埋める。 ④稼働後の開発体制を維持して、“③”の対応を確実に行う。 ⑤自治体や厚生労働省の各システムを連携させ、可能な限り手作業を無くす。(自動化) ⑥妥当な開発期間の維持、それを受け入れられる世間の常識の醸成。 ⑦各自治体がバラバラに作成しているシステムを同一システム(同様機能)に統一していく。	・各地方自治体がバラバラに作成しているシステムを、極力同一システム(同様機能)に統一していく。	

JR東の新幹線がシステム障害で始発から全面停止	JR東の新幹線がシステム障害で始発から全面停止、復旧は午前8時に延期。 13万7700人に影響。	前日のダイヤ乱れの影響で、運行システムCOSMOS(COmputerized Safety Maintenance and Operation systems of Shinkansen)内のデータの日付が不正な値になったため。 直接の原因は、列車データの入力が終わらないうちに午前5時にCOSMOSを立ち上げてしまい、それに気付いてデータ入力が終わった後それをCOSMOSに取り込もうとしたが、翌日のデータと認識されたことによる。			列車データを入れる担当(現場業務担当者)とCOSMOSの管理者(システム担当者)の間で、デッドライン(5:00)の情報共有がなかったと推定される。あるいは長年の運用の中でこれが暗黙知になっており、両方の担当者に忘れられていた可能性がある。さらに列車本数の増加と前日のダイヤの乱れなどで入力するべきデータ量が増加し、午前5時までに入力が終わらないデータ量になっていた可能性もある。 運用ルールの不徹底がある。デッドラインを過ぎた場合の対応方法のマニュアルと、それによる訓練、およびその訓練の結果を生かす実践が不十分。 これに近い出来事は、これまでにもあったはず。インシデント管理を行い、そこからこの事態に対する対策も立てられた。	・ 運用スケジュールを含む運用ルールを関連部署間で共有しておき、例外事項が発生した場合の対応方法のマニュアルと、そのマニュアルに基づく訓練を充分に行っておく。	
気象情報の配信システムがダウン、テレビやWebサイトなどの天気予報に影響	気象庁が収集した気象データを報道機関などに配信する「電文形式データ配信システム」がダウン。気象庁から報道機関などに地震・津波、注意報・警報、予報、観測データなどが配信できなくなった。 報道機関や気象事業者60社に影響。	富士通製UNIXサーバー(OSはSolaris)のCPUボードが故障。予備系サーバーが、起動に必要な本番系からの引き継ぎ情報を正しく読み込めなかった。引き継ぎ情報は、本番系と予備系のどちらからもアクセス可能な共用ディスクに格納してあった。共用ディスクに関連するハードもしくはソフトの不具合が重なったとみられる。			バックアップ機を持つところまでは良かったが、本番機に障害が起きてそのバックアップ機を稼働させ、本番機からの情報を引き継ぐところにも障害が起きてその情報が引き継げない、というところへの配慮がなされていなかった。 単に冗長化していることだけで満足せず、冗長化がきちんと実行されているか、実行できるかのチェックも、併せて必要である。	・ バックアップ機を持った場合、そのバックアップ機への切替が実行できるかのチェックを充分に行う。	
東京工業品取引所がシステムトラブルで全商品の立会を停止 。	東京工業品取引所によれば，2009年5月12日10時30分ごろより，同取引所に設置している共同利用型ネットワークゲートウエイの一部で接続できない状態が発生。11時35分に全商品の立会を停止した。	取引注文を処理するシステムと取引参加者をつなぐネットワーク上のルーターのプロセサの利用率が99%に達し、動作が不安定な状態に陥った。			過負荷になったのは、待機系のルータだった。なぜ待機系のルータが過負荷になったのかの原因は不明。本番系・待機系の相互監視の設定が、かえってループを引き起こした可能性がある。 基本的には、監視プロセスの確認と設計、及びテストを充分に行い、システム全体にブラックボックスを作らない、ということを実施する必要がある。	・ システムの中に監視プロセスを持つ場合、その監視プロセスの機能と設計内容の確認、及びテストを充分に行っておく。 ・ 情報システムの中に、一切ブラックボックスを持たない。	

	大証でシステム障害、先物取引の注文処理に遅延	大阪証券取引所の先物取引システムに障害が発生し、先物取引の注文処理に遅延が発生。 午後1時30分から約20分に渡り、先物取引の注文処理が遅延した。	引き金は、特定端末からの大量の訂正・取り消し注文だった。具体的には、特定の銘柄の注文40件に対し、ある証券会社のシステムの不具合により、取消注文が誤って700回以上繰り返されデータが滞留した。データ量にはある程度余裕を持たせていた。また、業務データは正しかった。これは想定外の事例で、買い手側の証券会社のミスであり、大阪証券取引所のシステム障害ではない。			このような場合でも、運用でカバーする対策が必要である。例えば、特定の端末からのエラーがある程度連続した場合に処理を受け付けない処置をする、というのが1つの方法である。想定外のデータが来たときに、あまりにも常識はずれなものは排除する仕組みを構築することも考慮する必要がある。	・想定外のデータが来たときに、あまりにも常識はずれなものは排除する仕組みを構築しておく。	
	JALのシステム障害。国内線チェックインと予約発券のシステム間のデータ連携に問題か	国内線の搭乗手続きを行うチェックインシステムの「JALPAS/D3」の障害でチェックイン業務に支障。 予約発券システムのホストコンピュータのOSに不備があり、データが予約発券システムに滞留したためチェックインシステムのレスポンスが遅れた。2便が欠航した。このほか85便で15分以上出発が遅れ、1万5304人に影響。	①ホストコンピュータのOSの更新が正常にいかなかった。分散システムのチェックインシステムでデータ不整合が発生。 ②本番環境と同等の環境がなく、センター側と分散側の連携テスト不足。 ③ホスト側が端末側に影響がないと判断。 ④ホストから端末までシステム全体の理解しているメンバが少ない（要員不足？） ⑤特殊なシステムでSEやバージョンアップの事例が少ない。	①レスポンス監視の仕組みを入れる。 ②お客様に直接影響を及ぼす部分はテストを重視。 ③システムリリース後、本番環境での実業務確認を早期に行う。 ④一斉にアクセスされることを想定したテストを考慮する（負荷テスト）。パフォーマンステスト（ストレステスト）を充分に実施する。 ⑤本番環境とテスト環境の相違を考慮してテストを実施する。	①バージョンアップ作業の後にリリースされたので、元のバージョンに戻す（実際のトラブルを想定した実地訓練の必要性・・・）。 ②複数バージョンを本番環境で稼働させる（本番環境のバージョンアップ時期をずらす？待機系が存在する場合）。 ③想定される障害発生時のリカバリ手順を整備する。 ④想定外の障害に対応して、開発担当者（当該関連システムに関わる人）をリリース時に立ち会わせる。	①バージョンアップの影響調査を周辺システムまで含めて実施する。 ②本番環境と同等の環境を用意し、ストレステストを実施する（本番データに近いデータを流す）。 ③繁忙期にはリリースをしない（イベントスケジュールを考慮）。 ④リリース凍結期間で、リリースする場合は、充分（通常の２倍）な体制を確保する。 ⑤緊急体制発動要領書の作成。	・情報システムの中に、レスポンス監視の仕組みを入れる。 ・システムリリース後、早期に本番環境での実業務確認を行う。 ・パフォーマンステスト（ストレステスト）を充分に実施する。 ・本番環境とテスト環境の相違を考慮してテストを実施する。	

図表B－4　2005年7月～2010年1月に発生した障害事例の情報から導出されたチェック項目リスト

「情報システムの信頼性向上に関するガイドライン第2版」『Ⅲ. 企画・要件定義・開発及び保守・運用全体における事項』		Web報道された43事例の分析から考察した、障害再発防止に必要な取り組み		
		取り組みの観点	障害の再発防止に必要と考えた取り組み	チェック項目
1. 企画・要件定義段階における留意事項	(2) 発注仕様への機能要件及び非機能要件の取込と文書化	重要度に応じた、要件各項目の位置づけの明確化と、位置づけを適切に反映した設計	要求仕様確定時に、情報システムの本質の機能と付加機能を区分する。 アーキテクチャの設計時に付加機能に問題があってもそれを本質の機能の障害にしない仕組みを組み込む。	□要求の各項目に対して重要度を明確にしているか。 □設計にあたって、重要度の低い要求の実現方式が、重要度の高い要求の実現を阻害することがないか、という観点での検討がされているか。
		情報システムを構成する要素の選択についての方針	情報システムのなかに、一切ブラックボックスを持たない。	□情報システムを構成する要素、特に情報システム基盤の要素についての選択基準が設けられているか。 □そのなかに、ブラックボックスの扱いの考え方が含まれているか。
		情報システムの利用の想定と不適切な情報システムの取り扱いに対する対処	想定外のデータが来たときに、あまりにも常識はずれなものは排除する仕組みを構築しておく。	□要件定義にて、情報システムの利用者層のスキルを想定し、情報システムの利用の仕方を想定しているか。 □その想定とは大きく異なる使い方を利用者がすることを防ぐ仕組み（利用方法を制限する機能）や方策（教育、訓練などによる使用方法の徹底）を策定しているか。
	(5) 非機能要件の実現に向けた利用者・供給者間での合意	非機能要求に関する 適切な要件の定義とそれを満たす適切な設計	情報システムの企画時にトランザクションの上限を設定し、設計時にその上限を超えた場合の対処方法を定義しておく。	□要件定義にて、情報システムの処理能力についての要件を十分策定しているか。 □さらに、情報システムの処理能力を超えたときの振舞いについて、要件を十分策定しているか。
			多量のダウンロードと再起動、およびその結果として特定のアドレスにアクセスの集中が生じることがあることを予想して、可能な瞬間最大アクセスに耐えるように情報システムの設計を行っておく。	□情報システムの処理能力についての要件定義にて、情報システムの運用・保守において必要となる主要な作業（例：パッチの配布、適用）とその作業によって新たに必要となる処理能力を十分勘案しているか。
			アーキテクチャの設計までの段階で、本番機とバックアップ機の関係を明確に定義しておく。	□要件定義と設計にて、障害発生時などの使用方法の想定を含めて、冗長構成の持ち方を策定しているか。
	(6) 利用者によるシステム要件に関する見解の統一	要件への暗黙知の十分な取り込み	業界の常識、顧客の常識および顧客ビジネスの標準となっている業務手順・規約などについて、要件定義工程および設計工程で明文化する。	□要件定義にて、日常的に従事、所属するものには明らかな業務・組織・利用者に固有、かつ情報システムに関係する事柄（いわゆる暗黙知）について、これを文書化する手続きは明確になっているか。 □上記の文書化を支援するコミュニケーションは十分なされているか。
			前記事項が十分に記述されているかについて、第三者要件定義診断を実施する。 有識者による要件定義のチェックを徹底する。	□要件定義の評価にあたり、業務・組織・利用者に固有な事柄に照らした取得ニーズの一貫性を評価する方法と評価者が策定され実施されているか。
2. 開発段階における留意事項	(7) テスト及びレビューの徹底	利用者、利用現場への適合性を十分確認する手続きの策定と実施	本番環境と同様のテスト環境を持ち、テストを実施する。	□システムテストの計画において、システムの適合性の確認を十分に行うための、本番環境の模し方、本番環境との差異、差異がテスト結果に与える影響とテスト結果の読み方が策定、評価されているか。
			パフォーマンステスト（ストレステスト）を十分に実施する。	□システムテストの計画において、本番でのストレスを模した上での、情報システムのパフォーマンスの妥当性を確認する項目が含まれているか。
			新旧情報システムの出力の全項目を比較し、新しい情報システムでの出力の内容が妥当かを確認する。	□システムテストの計画において、新旧情報システム間での比較等の方法による、同じ入力、処理を模した上での、情報システムの出力について、出力の妥当性を確認する項目が含まれているか。
			仮に本番環境でテストする場合には、テストの環境について運用部門が責任を持つ。	□システムテストの計画において、本番環境そのものを使用を予定する場合には、テスト目的を達成するための本番環境の使い方や、該情報システムの従前からの利用に影響を与えない方策の策定、及び実施に対して、的確な役割分担が策定されているか。
		確実な情報システム移行の方式、手順の策定と実行	移行作業書の作成と確認を徹底し、関係者間でその内容について情報共有しておく。 本番稼動開始前に稼動確認会議を実施し、変更点の確認、意向の手順、移行をやめて元に戻す時の判断基準とその実施方法などについて、関係者間で情報共有しておく。	□新しい情報システムによる、従前との業務およびシステム化対象範囲の違いを十分文書化しているか。 □新しい情報システムへの移行の方法や移行支援の手段は十分整備されているか。 □上記が、関係者で合意されているか。 □上記の、業務や情報システムの従前との違いや、移行方法の実施の結果にて予想される事態やそれへの対処方法（移行の中止、移行前への復元を含む）が整理され、関係者間で合意されているか。
			可能なら全領域でその修正分を一斉に適用するのではなく、最初は適用時範囲を限定し、部分的な試行切り替えを行う。	□情報システムの移行に関し、従前との業務およびシステム化対象範囲の違いから、一回で移行をはかる業務および情報システムおよび対象利用者の範囲を適切に設定しているか。
			新規設備を導入する時の手順書を関係部門間で情報共有しておく。	□情報システム基盤の変更または増強を図る際の手続きを明確にし、関係者間で合意しているか。
		情報システム稼動後の現場での主要な要件の充足可否の確認の手続きの策定と実施	システムリリース後、早期に本番環境での実業務確認を行う。	□情報システムの本番稼動後に、情報システムから期待した結果を得ているかを確認する方法を策定し、実施しているか。
			お客さま向け帳票などは本番移行直後での目での確認を行う。	□情報システムの本番稼動後の、情報システムから期待した結果を得ているかの確認のなかに、特に重要な出力（お客様向け帳票など）の妥当性を確認する項目が含まれているか。
3. 保守・運用段階における留意事項	*2. 開発段階における留意事項* (7) テスト及びレビューの徹底	保守した結果におけるソフトウェア要件充足の確認	保守開発のプロセス－修正変更のプロセス、テストの計画を確立する。	□保守における、問題報告・依頼修正の受理、分析、修正必要箇所の特定、修正の影響の評価、修正の実施、修正の結果の承認の手続きが策定され、実施されているか。
			保守で改修部分が的確に対応できているかを、その変更要求をした人が自分の目と手でしっかりと確認する。	□保守における手続きのうち、報告・連絡・承認に関するものについては、保守内容を承認する権限の設定され、保守作業ごとにその権限をもつ者による承認が実施されているか。
			多くのテストデータを積み上げて回帰テストを実施する。	□保守のテストにおいて、過去の保守作業でのソフトウェア品質についてのデータの蓄積をしているか。 □上記のデータに基づくテスト結果の評価が行われているか。
	(4) 保守に伴う変更作業・リリース手順等の整備と訓	保守の作業品質の確保	マスタデータの入力でも、2名の担当者によるチェックを実施する。	□マスタデータの作成・保守において、データの正確性を維持・向上する手続きが策定されているか。
			開発ベンダのプログラム改修時のチェック体制を強化する。	□外部に委託している運用・保守の作業をチェックする手続きが策定され、実施されているか。
	(1) 保守・運用機能を果たす体制・業務フロー等の整備及び利用者・供給者間での合意	的確な運用を実施するための手順、役割分担の定義と実践	運用スケジュールを含む運用ルールを関連部署間で共有しておき、例外事項が発生した場合の対応方法のマニュアルと、そのマニュアルに基づく訓練を十分に行っておく。	□運用の的確さを維持・向上するために、運用ルールと運用計画が策定され、関係者で合意されているか。 □上記の運用計画のなかには、運用作業についてのスケジュールが含まれているか。 □上記の運用ルールのなかには、例外が発生したときの対応方法が含まれているか。 □その例外が発生したときの対応方法について、訓練が継続的に行われているか。
			期末日、月末日、あるいは大きな作業が予想される日などには、急を要しない臨時作業をスケジューリングしない。	□関係者の間で合意が図られる運用作業のスケジュールは、処理の集中日など情報システムの稼動予測を踏まえて策定されているか。
			現場でのオペレータによる操作は極力シンプルにし、かつ的確な手順書を用意しておく。 運用上の操作は必ずオペレータがペアで実施する。	□運用の的確さを維持・向上するための、作業手順の改善が継続的になされているか。 □同じく、運用の的確さを維持・向上するための、牽制関係が構築されているか。
			手順書通りの操作を的確にできるよう、訓練を実施する。	□運用作業の手順や指示に対する正確さを向上するための要員の訓練が継続的に実施されているか。
			作業実施の結果や画面のハードコピーなど、操作の全てを記録に残し、第三者による確認のためのエビデンスにする。	□運用作業の手順や指示に対する正確さを検証するための記録及びその評価が行われているか。

4. 障害対応に関する留意事項	(1) 障害発生事象の検知と対応の整備	障害発生時の運用について、適切な手順、役割分担の策定と実践	システム障害の早期復旧を可能とする方策の検討を実施する。	□障害発生時の対応を迅速に行うための、対応の仕組みの改善が継続的になされているか。
			障害発生時の体制の見直しを行う。	□障害発生時の対策を迅速に行うための対応の仕組みの改善に、障害対応の体制の見直しが含まれているか。
			本番機からバックアップ機への切り替えを完全に自動化するのではなく、人間の判断と操作が入る余地を残しておく。	□障害発生時の対策を迅速に行うための対応の仕組みの改善に要員が適切に冗長構成を活用することによる、障害局所化の方法が含まれているか。
			障害発生時の訓練を実施する。	□障害発生時の対応の迅速さ、正確さを維持・向上するための要員の訓練が継続的に実施されているか。
			待機系への切り替えの訓練を定期的に実施する。	□障害発生時の対応の迅速さ、正確さを維持・向上するための要員の訓練に、情報システムの待機系への切り替えが含まれているか。
			バックアップ機への切替が実行できるかのチェックを十分に行う。	□障害発生時の対応を迅速に行うための、対応の仕組みに含まれる冗長構成が使用方法の想定どおり機能することが定期的に確認されているか。
			監視プロセスの機能と設計内容の確認およびテストを十分に行っておく。	□障害の発生を検出する仕組み、プロセスが明確化されており、その仕組み、プロセスの有効性、網羅性が継続的に確認されているか。
			情報システムの中に、レスポンス監視の仕組みを取り入れる。	□障害の発生を検出する仕組み、プロセスのなかに、情報システムのレスポンスの監視が含まれているか。
5. システムライフサイクルプロセス全体における横断的な留意事項	*3. 保守・運用段階における留意事項* (5) 情報システムの構成情報の完全性確保	要件の実現の追跡性	要件定義書から設計書、プログラム、および試験仕様書まで、及びその逆方向について、トレーサビリティを確保する。	□要件とその実現について、情報システムのライフサイクルにまたがる追跡性が確保されているか。
		要件から導かれた成果物の構成の追跡性	プログラム、ドキュメント、ツール、データなどシステム資源全体を構成管理の対象とする。 構成管理(ライブラリ管理)の実施によって、プログラムのバージョン管理を実施する。	□プログラム、ドキュメント、ツール、データなどの成果物を対象とした構成管理が実施されているか。 □上記のなかに、成果物のバージョン管理が行われているか。
	3. 保守・運用段階における留意事項 (3) ニーズや環境の変化へのシステム仕様の適切な適応	ライフサイクルを通しての情報システムのリスク評価と再企画	適切な機会を設けて、複雑化した仕様の単純化を図る。	□情報システムの中長期的な見直しのなかで、情報システムの適合性の再評価と、評価結果による情報システムの見直しが行われているか。 □上記の再評価のなかには、保守などによっての情報システムの要件の複雑化、肥大化の程度の評価が含まれているか。 □また、上記の見直しのなかには、再評価の結果をふまえた要件、仕様の再定義の観点が含まれているか。