独立行政法人 情報処理推進機構

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

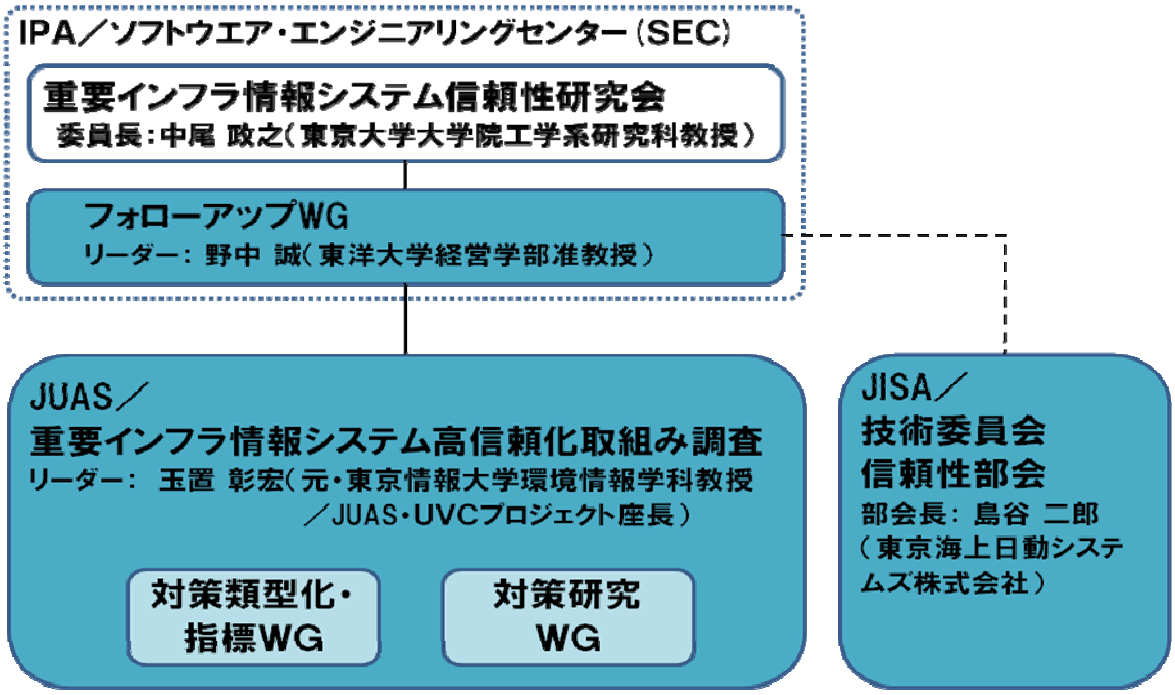
平成 22 年 3 月

独立行政法人 情報処理推進機構
ソフトウェア・エンジニアリング・センター

本報告書は、独立行政法人 情報処理推進機構（以下、「ＩＰＡ」と略記）が事務局として開催した「重要インフラ情報システム信頼性研究会」における審議結果を取りまとめ、公表するものである。

＜検討体制＞

「重要インフラ情報システム信頼性研究会」の下に「フォローアップWG」を設置し、実務的な議論を行った。また、社団法人 日本情報システム・ユーザー協会（以下、「ＪＵＡＳ」と略記）に調査を委託するとともに、社団法人 情報サービス産業協会（以下、「ＪＩＳＡ」と略記）から調査協力を得た。



＜検討メンバ＞

「重要インフラ情報システム信頼性研究会」委員一覧

（*） フォローアップWGのメンバを兼ねる

委員長	中尾　政之	東京大学大学院工学系研究科　教授
	淺野　正一郎	情報システム研究機構・国立情報学研究所　教授
	一柳　幹男＊	信金中央金庫　理事・システム部長
	太田　忠雄＊	株式会社ジャステック　常務取締役　常務執行役員・営業本部長
	雄川　一彦	東日本電信電話株式会社　取締役・IT イノベーション部長
	岸本　博之	財団法人金融情報システムセンター（FISC）　監査安全部長
	木谷　強	株式会社エヌ・ティ・ティ・データ 技術開発本部 副本部長

清田	辰巳＊	株式会社　東京証券取引所　　品質管理部長
後藤	真哉	小田急電鉄株式会社　経営政策本部 IT 推進部小田急 ICT センター長
坂野	正晴	株式会社みずほコーポレート銀行 IT・システム統括部 システムリスク管理室長
島谷	二郎＊	東京海上日動システムズ株式会社　専務取締役
野中	誠＊	東洋大学　准教授
淵	昌彦	東京ガス株式会社　導管ネットワーク本部　防災・供給部 制御設備グループ・マネジャー
細川	泰秀	社団法人日本情報システム・ユーザー協会　専務理事
宮本	史昭＊	東京電力株式会社　執行役員・システム企画部長
幸重	孝典	全日本空輸株式会社　執行役員・　ＩＴ推進室長

（オブザーバ）

経済産業省 商務情報政策局 情報処理振興課

（事務局・事務局補佐）

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

株式会社 三菱総合研究所

＜検討経緯＞

・重要インフラ情報システム信頼性研究会

2009 年 11 月 20 日(金) 第 1 回研究会

2010 年 3 月 17 日(水) 第 2 回研究会

・フォローアップ WG

2009 年 10 月 19 日(月) 第 1 回 WG

2009 年 12 月 8 日(火) 第 2 回 WG

2010 年 1 月 19 日(火) 第 3 回 WG

2010 年 2 月 12 日(金) 第 4 回 WG

2010 年 3 月 9 日(火) 第 5 回 WG

－ 目 次 －

序言 …….... 5

第 1 部 総論 ……..…….. 6
1. 本事業の目的 6
2. 本事業の 2009 年度の位置づけ 7
3. 本報告書が対象とする読者 10
4. 本報告書の構成 10
5. 2009 年度の調査の限界 10

第 2 部 重要インフラ情報システムのプロファイリング …… 12
1. 情報システムのプロファイリングに関する調査の意義と、2009 年度調査の主な成果 12
2. 情報システムのプロファイリングの調査結果と分析 13
3. 情報システムのプロファイリングについての今後の取組み 16

第 3 部 重要インフラ情報システムの定量的品質コントロール …… 18
1. 定量的品質コントロールに関する調査の意義と、2009 年度調査の主な成果 18
2.定量的品質コントロールの調査結果と分析 19
3. 定量的品質コントロールについての今後の取組み 26

第 4 部 障害再発防止策 …… 28
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 28
2. 障害再発防止策の精査結果と分析 29
3. 障害再発防止策についての今後の取組み 47

参考文献 49

付録

序言

本研究会の目的は、重要インフラ情報システムにおける社会的影響の大きいシステム障害の発生を抑止し、障害が発生した場合でもその影響範囲を局所化するための方策について、広く関係者の知見を伺い、重要インフラ事業者が重要インフラ情報システムの信頼性確保のために、インフラの種類によらず共通的に取り組めることを提示することである。

すでに、情報システムのライフサイクルでの信頼性確保の取組み、特に開発の工程でのそれについては、多くの調査、報告がなされている。そのほとんどは、情報システム一般を対象としているに対して、本報告書は重要インフラ情報システムを専ら扱っている。また、その社会的な位置づけ、また利用者の期待を受けて、情報システムの信頼性をどのように目標設定し、またその目標を達する手段をどのように計画・実施したらよいかについて、1つのアイディアを示した。

2009 年度の研究会活動では、2008 年度に実施した取組み[1]を引き継ぎ、次の 3 項目について調査・検討を行った。

(1)　重要インフラ情報システムのプロファイリング（第 2 部）
(2)　重要インフラ情報システムの定量的品質コントロール（第 3 部）
(3)　障害再発防止策（第 4 部）

2009 年度の調査においても、関係者の厚いご協力を頂き、実プロジェクトでの取組み内容や、実際に起きたシステム障害事例の分析を収めることができた。これにより、重要インフラ事業者が現在行っている情報システムの信頼性確保の活動を点検し見直す上での参考情報を得ることができるようになった。しかしながら、一層高い信頼性が期待される重要インフラ情報システムに必要な管理の全体像はいまだ明らかではない。また、生まれや位置づけが1つずつ異なる重要インフラ情報システムを俯瞰する視点の整備もこれからという状況である。

引き続き、IPAでは、重要インフラ情報システムの信頼性について、現場での取組み、考え方を構造化しながら、信頼性に係る課題や解決策の具体像を明らかにしていく考えである。

[1] 「重要インフラ情報システム信頼性研究会」の 2008 年度の度報告書は、ＩＰＡの以下のホームページに掲載している。
http://sec.ipa.go.jp/reports/20090409.html

第1部 総論

1. 本事業の目的

情報システムの利用拡大とともに、情報システムに起因する障害の社会的影響は広範になっている。特に重要インフラのサービス（情報通信、金融、航空、鉄道、電気、ガス、政府・行政、医療、水道、物流の10分野）を提供する各事業者の情報システムの障害が社会に与える影響は、大きな社会的関心事になっている。

これまで無事故前提社会であった日本では、報道にのぼるようなシステム障害事例であっても、海外の基準で考えれば、過剰反応といえる事象であることが往々である。システム障害に対する厚い対策には相応のコストを必要とすることを考えれば、システム障害が与える社会的影響や関係者が当該システムに期待する信頼性の程度に合わせて障害対策が講じられ、また過去の障害事例に照らした再発防止の取組みが実施されるべきである。

そこで、重要インフラの事業者には、その重要インフラを支える情報システムに対して、

①情報システムの特性を踏まえて、その障害による社会的影響から当該情報システムに求められる信頼性要求水準を設定し、

②その信頼性要求水準に基づいて、情報システムに各種の対策を講じる。

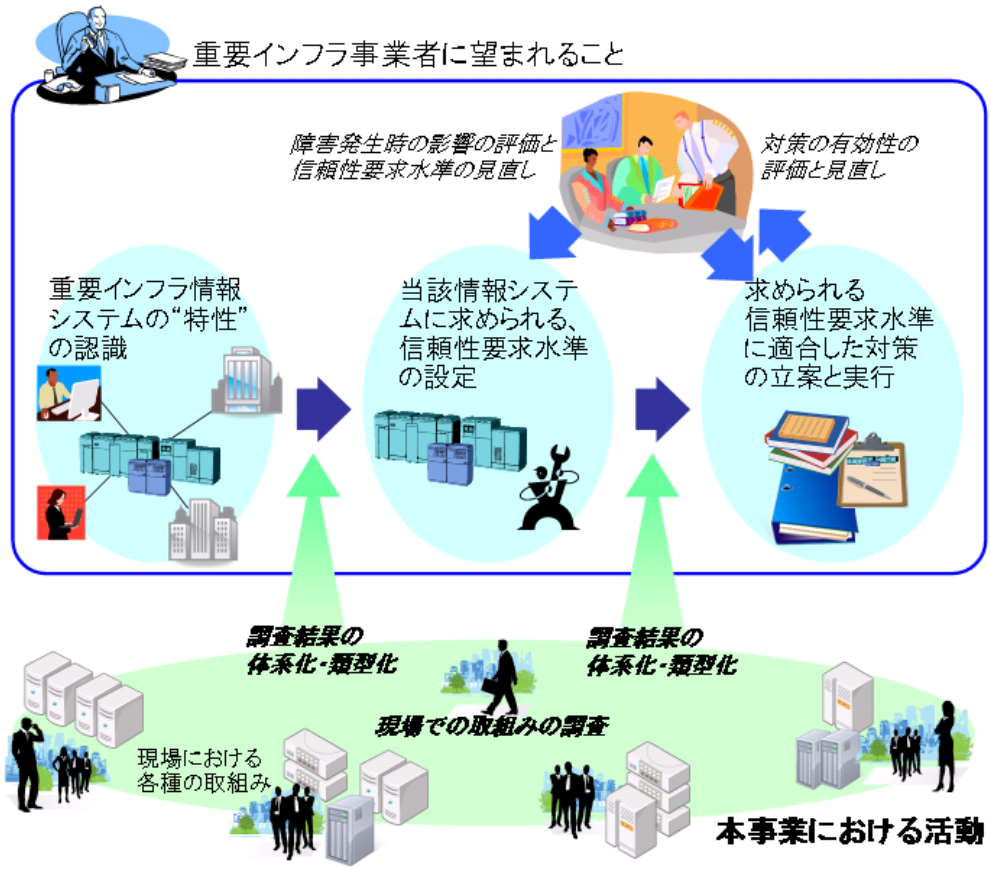
という一貫した行動をとることが望まれる。

また、重要インフラ情報システムは国民生活や社会・経済活動の重要な基盤であることから、情報システムに求められる信頼性要求水準とそれに基づく各種対策については、広く国民や社会に理解を得られることが必要である。そして、この理解のためには、その内容が合理的であること、たとえば、信頼性要求水準や各種対策のレベルが共通的な基準に従っていて、かつその内容について十分な情報が提供され、またそれが分かりやすく説明されることが重要である。

上記のためには、人、技術、プロセスの各面から情報システムの障害発生／被害拡大防止のための対策を体系化し類型的に整備することが必要である。

情報システムの障害は、複数の要因が複雑に関与するため、因果関係を明らかにしにくい。ただし、その対策は、経験則や記録を含めたさまざまな現場での現行の取組みを参考に、具体的な方策にして整理することは可能と考えられる。

IPA／SECでは、特に社会的に重要なインフラ部分を担う事業者の情報システムについて、その管理の考え方や障害事例の情報を継続的に収集・分類・分析し、その対応策を体系化し、重要インフラの各分野に応じた特性があるのかという観点も踏まえつつ、障害の再発防止に資する具体的な対策を示すことを目指している。



【図表１－１】　本事業における活動のイメージ

これらの成果を活用することにより、重要インフラ情報システムに求められる信頼性要求水準が適切に認識され、その信頼性要求水準に基づく対策が適切にとられて社会的に影響の大きい情報システム障害が抑制され、また障害による影響の規模が制御されることが本事業の主な目的である。

合わせて、重要インフラ情報システムにおける信頼性要求水準に基づく障害対策に関する社会的コンセンサス形成のために、本事業の成果が少しでも貢献できることを願っている。

2.　本事業の2009年度の位置づけ

本事業は、2008 年度からの継続事業である。以下に 2008 年度事業を振り返るとともに、2009 年度の事業概要を述べる。

2.1　2008年度の事業の概要

IPAが設置した、「重要インフラ情報システム信頼性研究会」では、2008 年度に、社会的に重要なインフラ部分を担う事業者の情報システム（以下、重要インフラ情報システム）の障害発生を減少させ、また障害による影響の規模を縮小する方策として以下のテーマ・内容について議論し、2008 年度報告書としてまとめた。

(1) システムプロファイリングの検討と提案

情報システムの運用時に発生するシステム障害はその利用者に様々な影響をもたらすと考えられる。中でも特に注視すべき影響として、情報システムの直接または間接の利用者に対する健康被害の有無や経済的損失の有無、あるいはその被害額などの被害程度を考えていくことが極めて重要になる。また社会インフラを構成する要素としての情報システムの場合、公共性なども重要な要素となる。

そこで、情報システムにシステム障害が発生した場合を想定し、その利用者に健康面、経済面に及ぼす影響の程度を数値として客観的に捉え、その程度によって情報システムに求められる信頼性要求水準を次の4タイプに区分するという考え方を採る情報システム「プロファイリング」について提案した。

Type Ⅰ: 社会的影響が殆どない。

Type Ⅱ: 社会的影響が限定される。

Type Ⅲ: 社会的影響が極めて大きい。

Type Ⅳ: 人命への影響、甚大な経済損失が予想される。

この情報システム「プロファイリング」は、IPA／SEC の組込みソフトウェアプロジェクトで策定された「組込みソフトウェア開発向け品質作り込みガイド(ESQR)」における情報システムプロファイリングの考え方を踏襲したものである。

これは、情報システム信頼性の議論のベースになる考え方であり、このプロファイリングスケールに基づき障害事例分析や障害を未然に防ぐ対策や品質指標の体系化を進めていくことが必要になると考えている。特にシステム開発時おいては、その信頼性や安全性・品質などの目標値を設定する際に、当該システムにどの程度の水準の信頼性が求められるかを、この情報システム「プロファイリング」を利用して客観的に評価し、目標設定を行うことを想定している。

(2) 高信頼システムの実装に向けた共通開発指針の検討

情報システムの信頼性を開発過程で逐次確認・評価し、その中で情報システムに求められる信頼性水準に近づけていくための定量的なコントロール手法の整備について、「共通リファレンス」として検討した。共通リファレンスの検討に際しては、IPA／SECの 組込みプロジェクトで策定した ESQR の考え方を踏襲した。ESQR ではシステムプロファイリングを明確に定義した上で、品質コントロールのための指標として、プロセス品質指標、プロダクト品質指標の大きく 2 カテゴリ約 30 種類の品質指標により、品質定量化を進め、その値による品質の開発段階でのコントロールを目指している。この考え方を参考に、重要インフラ情報システムの信頼性に関する品質指標を追加する方向で検討を加えた。また、オリジナルの ESQR ではこれらの品質指標に関する基準値を照会することにより、関係者間の定量化に関する意識向上と実用性を担保しているが、今回の検討でもこのコンセプトを是認し、重要インフラ情報システムに関する指標セットとその参考値掲載を基本的な方針とすることとした。

- プロセス品質指標

  システム構築の際に、信頼性や品質面に関する確認の作業として、レビューやテストなどをどの程度実施しているかについて作業ボリュームに対する作業工数比率などで評価する指標

- プロダクト品質指標

  システム構築の際に作成される(中間)成果物の出来栄え、特に信頼性や品質などの側面で問題ないかどうかを客観的に計測し、評価するための指標

(3) システム障害の類型化と障害対策指針の検討

障害事例の分析と対策検討に関しては、2005 年 7 月以降 2008 年 10 月までのマスコミで公表されたシステム障害事例(約 100 事例、12社)を精査し、次の検討を行った。

- 障害原因作り込みフェーズに関する類型化分析

  ライフサイクルでの各段階で、システム障害事例における障害原因の作り込みが行われたのかの分析

- 障害発生要因分析と対策分析

  12社において現実に発生したシステム障害およびその発生要因と対策、対策立案実行に関わる役割分担に関する個々の事例分析

- 障害対策に関するコスト分析

  「信頼性」に関わる対策コストの定量的な要因と尺度と、その結果としてのシステムプロファイルとの関係

- 障害再発防止に向けたチェック項目と診断方法

  上記を反映した情報システム・ソフトウェアのライフサイクル段階での利害関係者が信頼性確保のために共有すべきチェック項目とその個々の対策についての診断方法

- 障害対策に関するコスト分析

  上記を反映した情報システムレベルで不具合予兆の発見、検出、検証などをプロアクティブにコントロールするための障害事例から分析した評価指標の整備

(4) 情報セキュリティを重視した障害対策指針の検討

情報セキュリティインシデントの情報から、情報システムの開発の各段階で考えるべき対策を論じた。

2.2 2009年度の事業の概要

2009 年度は、2008 年度活動の継続として、上記(1)、(2)、(3)について、実際に重要インフラ情報システムに関わる組織、すなわち情報システムを用いて社会に提供している重要インフラを管理・運営している事業者(以下、重要インフラ事業者)とその他のユーザ企業、および重要インフラ事業者に情報システムを供給しているベンダ企業に対して調査を行い、それぞれの活用における実情をとりまとめた。また、その調査結果について議論した。

(1) システムプロファイリングの検討

2008 年度報告書で提案した、情報システムの特性からその信頼性の要求水準の決定の仕方を、重要インフラ事業者が有する情報システムに適用することが問題ないか、について調査した。

(2) 高信頼システムの実装に向けた共通開発指針の検討

重要インフラ事業者および重要インフラ事業者に情報システムを提供しているベンダを対象に企画・要件定義、開発、保守・運用の各段階における、品質指標を用いた定量的品質コントロールの実施状況を調査した。

(3)システム障害の類型化と障害対策指針の検討

障害事例情報のさらなる収集を行うとともに、重大かつ一般性の高い障害事例を深堀りし、システムの

企画・要件定義、開発、保守・運用の各段階で考えるべき対策の精緻化を行った。

なお、(4)情報セキュリティを重視した障害対策の検討は、情報システムの特性（例としては、利用者の範囲や利用者からの情報システムの見え方）が対策に及ぼす影響が非常に大きく、調査した結果を一般化することが困難と考えることから、2009 年度の活動からは除いた。

3. 本報告書が対象とする読者

本事業は、次の方々に資すことを目的としている。

- 重要インフラ事業者をはじめとした、その停止が社会に大きな影響をあたえる重要な情報システムを有する事業者
- 上の事業者に情報システムを供給するベンダ
- 上の事業者から委任されて、情報システムの管理にかかわるサービス提供者

4. 本報告書の構成

本報告書は、この第1部ののち、3部構成をとっている。

第2部は、「重要インフラ情報システムのプロファイリング」

すなわち、2.項でのべた、(1)システムプロファイリングの検討の調査結果について述べる。

第3部は、「重要インフラ情報システムの定量的品質コントロール」

すなわち、2.項の、(2)高信頼システムの実装に向けた共通開発指針の検討の調査結果について述べる。

第4部は、「障害再発防止策」

すなわち、2.項の、(3)システム障害の類型化と障害対策指針の検討における、対策の精緻化の結果について述べる。

5. 2009年度の調査の限界

本事業が対象とする重要インフラ情報システムは、「一品モノ」としての性格が強く、情報システムの位置づけ（想定する利用者や情報システムが利用者に提供するサービスはもとより、重要インフラの何を担うかという考え方や、重要インフラそのものの発展の経緯）が情報システムごとに大きく異なっている。

この違いを超えて、重要インフラ情報システムを議論するには、調査の方法や調査結果の解釈に相応の工夫が必要である。

2009 年度は、2008 年度の報告書の流れを汲んで、情報システムやソフトウェアについてのIPAがこれまで蓄えてきた知見を活用した活動を行った。重要インフラ事業者へのアンケート、インタビュー調査についても、IPA／SECからアクセス可能な範囲で行った。

ただし、本報告書に記述したことが、各種の重要インフラに対してどの程度普遍性を持っているのかは未検証である。

今後は、適切な共通テーマの設定や取り扱う課題や解決方法の抽象化を併せ考えながら、重要インフラ情報システムの管理、また利用により広くかつ共通的に活用できる知見を提供していきたいと考える。

第2部　重要インフラ情報システムのプロファイリング

昨年度に当研究会が提案した重要インフラに係る情報システムの特性から信頼性に関する要求水準を決定する「システムプロファイリング」のコンセプトについて、2009 年度は現実の情報システムへの適用を通じた有効性確認を行い、その適合性について調査した。

1. 情報システムのプロファイリングに関する調査の意義と、2009年度調査の主な成果

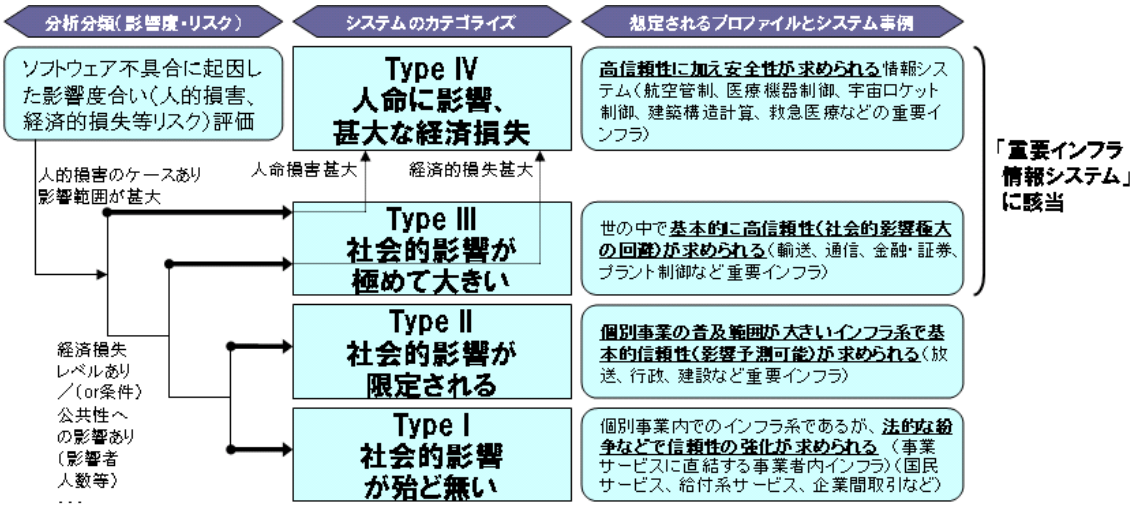
先述のように、IPAでは、2008 年度から「重要インフラ情報システム信頼性研究会」を設置し、システムの信頼性に対する要求水準（システムプロファイル）に関する議論を行っている。同研究会の 2008 年度報告書の「Part 2. システムプロファイリングの基本的な考え方」において、まず情報システムへの信頼性要求水準の評価を行い、それに基づいて重要インフラ情報システムを位置付けることの必要性とその方法について、以下のように述べている。

- 情報システムのプロファイリングに基づいて重要インフラ情報システムを位置付ける目的及びその効果

  “各システムに求められる信頼性要求水準に応じたリスク対応策をとることができるようになり、リスクを最小化するためのコストを適切な範囲に収めることができる。”

- 情報システムのプロファイリングの考え方についてのIPAの提案

  2008 年度報告書でIPAが提案した、情報システムのプロファイリングの構成案は、【図表2－1】のとおりである。すなわち、情報システムを、その障害によりもたらされる「人命・身体に与える影響」「経済的な影響」「社会的な影響」の3つの観点から評価することにより Type Ⅰ～Ⅳの4つのレベルに分類し、このうち Type Ⅲ／Ⅳを特に「重要インフラ情報システム」と位置づけることを提案している。



【図表2－1】 IPAが提案した情報システムのプロファイリング （2008 年度報告書より）

2009 年度の取組みでは、重要インフラ事業者にあたる企業・事業体に対して、その事業者（企業・事業体）が有する情報システムについてプロファイリングに沿って自身で分類してもらうことを通じて、IPAが提案した情報システムのプロファイリングを適用し、情報システムの信頼性要求水準を一次的に決定することができるかを調査し

た。

調査の主な目的は、IPAが提案したシステムプロファイリング方法を用いて、事業者がその信頼性要求水準が高く設定されるべき以下のような“特性を”もつ情報システムを識別し、「重要インフラ情報システム」として定義した Type Ⅲまたは Type Ⅳに分類することができるかという点について、確かめることにある。

- 当該情報システムの障害が、数分～数時間のうちに社会的に大きな影響を及ぼす、あるいは人命に影響を与える可能性がある。
- 当該情報システムの機能を、業務品質を維持しながら代替する手段（人間による手作業など）を用意することが技術的、または経済的な理由で困難である。

なお、調査に先立ち、重要インフラ事業者の保持するシステムであっても、全てが「重要インフラ情報システム」として分類される訳ではなく、中には社内的な経理業務システムのような、企業基幹システムもしくはその他のシステムとして分類されるものも含まれるはずである、という仮説をたてていた。

2009 年度の調査の主な成果は、次のとおりである。

(a) 2008 年度報告書のプロファイリング方法による実システムの信頼性要求水準の決定

重要インフラ事業者を含むユーザ企業 23の事業者が有する50の情報システムについて、事業者自身が分類した結果を調査したところ、27 システムが「重要インフラ情報システム」として分類されるとともに、分類の結果が、情報システムの“特性”に照らして誤っていると疑われるものは 5 システムにとどまった。このことから、事業者によるプロファイリングを用いた情報システムの信頼性要求水準の決定は、ほぼ適切に行えることが分かった。これはすなわち、当該システムプロファイリング方法の妥当性を表している。

(b) プロファイリングの適用において留意すべき点

プロファイリングにより、一度決定した信頼性要求水準が、その後の情報システムの位置づけの変化や、関係者の変化および関係者の期待の変化に対して、どの程度追従できるかについては調査していない。

また、時間経過に伴って、なんらかの要因が信頼性要求水準に影響していないかを評価して当該水準を見直す方法についても、提案と調査を行っていない。

以降では、調査内容の詳細について述べる。

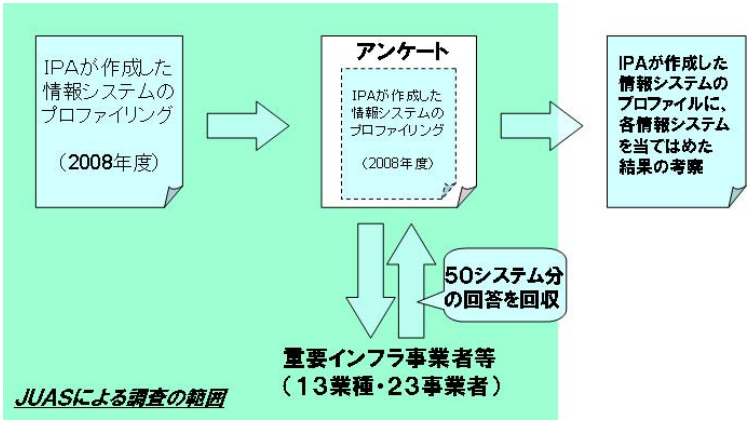
2. 情報システムのプロファイリングに関する調査結果と分析

2.1 プロファリングに関する調査の進め方

JUASでは、23の重要インフラ事業者等（企業・自治体）が有する50の情報システムを対象にアンケートを実施した。各情報システムについて、IPAが提案するプロファイリングの適用を事業者自ら行ってもらい、決定した Type とその判定理由を尋ねた。

また、このアンケートでは、情報システムの稼働率（目標、実績）、冗長構成の程度、バックアップの実施の程度といった、情報システムの信頼性に関わる構築・運用管理の事項についても併せて質問した。

調査の流れは、【図表2－2】のとおりである。



【図表2－2】 プロファイリングについての調査の流れ

調査対象の事業者は、内閣官房情報セキュリティセンター（NISC） 重要インフラ対策チームが指定している10の業種（情報通信、金融、航空、鉄道、電力、ガス、政府・行政、医療、水道、物流）および、重要度の高い企業内情報システムを有していると考えられる事業者から選んだ。

調査対象の事業者の業種は【図表2－3】のとおりであった。

業種	事業者数	業種	事業者数
情報通信	2	政府・行政	2
情報産業	1	医療	1
金融（銀行・保険・証券・信販）	4	水道	2
航空	2	化学・薬品	1
鉄道	2	鉄・非鉄金属・窯業	1
電力	2	サービス業	1
ガス	2		

【図表2－3】 調査対象事業者の業種

また、調査対象となった情報システムの内容は【図表2－4】のとおりであった。

情報通信	加入者情報交換機登録システム
	携帯電話パスワード認証システム
金融	株式･CB売買システム
	株式派生売買システム
	株式相場報道システム
	勘定系システム
	為替中継システム
	通常貯金システム
	保険金支払いシステム
航空	国内旅客システム
	運行管理システム
	予約･発券システム
鉄道	列車制御システム
	電子メールシステム
電気	原子力保全管理システム
	火力部門総合機械化システム
ガス	ガス高中圧導管遠隔監視制御システム
	ガス製造プラント制御システム
	お客様総合情報システム
政府行政	申請受付システム
	住民情報オンラインシステム
水道	水運用システム
	水道料金ネットワークシステム
	水源地管理システム
医療	電子カルテシステム

（注）上記では、名称がほぼ同じ情報システムを1行にまとめている。
また、調査対象全てを表記していない。

【図表2－4】 調査対象となった情報システムの内容

2.2 プロファイリングに関する調査結果

上述した調査対象の情報システムについて、情報システムを有する事業者から、全50システム分のアンケート回答結果が回収できた。

調査対象の50情報システムのうち、事業者が「重要インフラ情報システム」、すなわち Type Ⅲまたは Type Ⅳの区分に相当すると回答したのは27システムであった。アンケート回答結果には、プロファイリングが適用不能、すなわち、保有する情報システムについて、その信頼性要求水準を表す Type を自身では決定できない、というものは無かった。また、アンケート回答における、情報システムの名称から推定される情報システムの種類と信頼性要求水準を表す Type の関係は【図表2－5】のとおりであった。

Type Ⅰ／Ⅱと回答があった情報システム	
システム種類	回答数
生産／在庫／流通／販売管理	9
料金管理	4
契約管理	3
企業会計	2
情報伝達／共有	2
その他	3
合計	23

Type Ⅲと回答があった情報システム	
システム種類	回答数
金融取引／決済	7
用力(電気・ガス・水道)供給	5
運行管理(鉄道、航空)	3
通信管理	2
顧客管理	1
契約管理	1
料金管理	1
その他	1
合計	22

Type Ⅳと回答があった情報システム	
システム種類	回答数
用力(電気・ガス・水道)供給	3
運行管理(鉄道、航空)	1
その他	1
合計	5

【図表2－5】 アンケート回答の情報システムの名称から推定される種類と、プロファイリングの結果

上記のうち、網掛けをした情報システムが、その情報システムの“特性”から、Type Ⅲ、Ⅳに分類されることが妥当と考えられるものである。つまり、

- Type Ⅲ、Ⅳに分類されるのが適切と思われる情報システムが、Type Ⅰ、Ⅱに誤分類されたことが疑われるのは0システムである。
- 逆に Type Ⅰ、Ⅱに分類されるのが適切と思われる情報システムが、Type Ⅲ、Ⅳに誤分類されたことが疑われるのは5システムである。

つまり、誤分類が疑われるのは調査対象の情報システムの10%であった。

したがって、当該プロファイリングは、情報システムの“特性”から一次的な信頼性要求水準を求めるために使用できることが確認できたと考えられる。

また、各事業者が、それぞれの Type に区分した理由について目を転じると、理由が「経済的な影響」であったものは16、「社会的な影響」であったものは15であった。したがって、事業者が「経済的な影響」「社会的な影響」という観点で情報システムへの信頼性要求水準を決定することは支障ないと考えられる。

一方で、「人命・身体に重大に影響」に該当するとした情報システムは、重要インフラ情報システムにあたる27システムのうち3システムしかなく、この観点で情報システムへの信頼性要求水準を決定することの妥当性を判断することは、今回の調査結果からはできない。

3. 情報システムのプロファイリングについての今後の取組み

2008 年度にIPAが提案したプロファイリング方法は、重要インフラ事業者が情報システムの特性から一次的に信頼性要求水準を導くために使用できることは確認できた。

しかしながら、今回の調査は重要インフラ事業者など当時者による信頼性要求水準の導出を扱っており、導か

れた信頼性要求水準の妥当性をベンダや第三者に分かり易く示す方法、また、先述のように、この信頼性要求水準の決定が、情報システムの位置づけの変化や、関係者の変化および関係者の期待の変化に対して、どの程度普遍性を有しているか、さらに、時間経過に伴って、なんらかの要因が信頼性要求水準に与えているか否かを再評価し同水準を見直す方法については調査を行っていない。

事業者が情報システムの信頼性について説明するためにはこれらの方法を検証することが重要であると考えられ、検証を行うことは本事業にとっての引き続きの課題である。

第３部　重要インフラ情報システムの定量的品質コントロール

2008 年度に当研究会が提案した重要インフラに係る情報システムの信頼性向上に向けた定量的品質コントロールのコンセプトについて、現実のデータを通じた検証と有効性確認を行い、信頼性向上対策の実践に必要な参考情報をとりまとめることを目的に、重要インフラ分野ごとに実際のプロジェクトデータを収集するとともに指標管理の実態を把握するための調査を実施した。

1. 定量的品質コントロール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、システム開発における共通リファレンス（品質指標と参照目標値）を用いた定量的品質コントロールについて、「組込みソフトウェア開発向け　品質作り込みガイド （ESQR）」（2008年12月発行）で示された考え方を踏襲したメカニズムを提案するとともに、次の事項に関する議論結果を述べている。

- 重要インフラ情報システムを取り巻く課題、特にそのなかのソフトウェアの信頼性についての課題
  - ソフトウェアの信頼性の安定的な確保に関する課題
  - ソフトウェアの仕様変更などのダイナミクスへの適応に関する課題
- その課題の一部を解決するための「定量的品質コントロールメカニズム」の意義
- 「定量的品質コントロールメカニズム」で用いることが考えられる「プロセス品質指標」、「プロダクト品質指標」の例

ただし、2008 年度報告書では、定量品質コントロールの基本的な考え方と、重要インフラ情報システムでの活用を考え得る品質指標を中心に述べており、重要インフラ情報システムにとってどのような品質指標を用いた管理を行うことが効果的かつ効率的なのかを示すことまではできなかった。

そこで、2009 年度の調査では、重要インフラ事業者を含むユーザ企業と、重要インフラ事業者向けに情報システムを供給しているベンダ企業に関し、重要インフラ情報システムでの、品質指標を用いた情報システム、ソフトウェア企画・要件定義・開発・保守・運用の定量的品質コントロールの実施状況を調査し、品質指標とそれを用いた管理（プロセス品質の判断と対応）のあらましを明らかにすることとした。

2009 年度の調査の主な成果は、次のとおりである。ユーザ企業8社、ベンダ企業9社（延べ数）を対象とする調査により、開発・運用の各段階における定量的品質コントロールの実態について、次の事項が明らかとなった。

- 企画・要件定義の工程にて、品質指標を用いた定量的品質コントロールが行われていた情報システムが一部あった。
- 開発の各工程では、品質指標を用いた定量的品質コントロールは調査対象のほとんどの情報システムで行われていた。その中では、複数の企業間で類似の考え方による開発の工程の品質についての判断と対応が実施されていることが観察された。
- 運用・保守の工程でも、品質指標を用いた定量的品質コントロールが行われていた。

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. 定量的品質コントロールに関する調査結果と分析

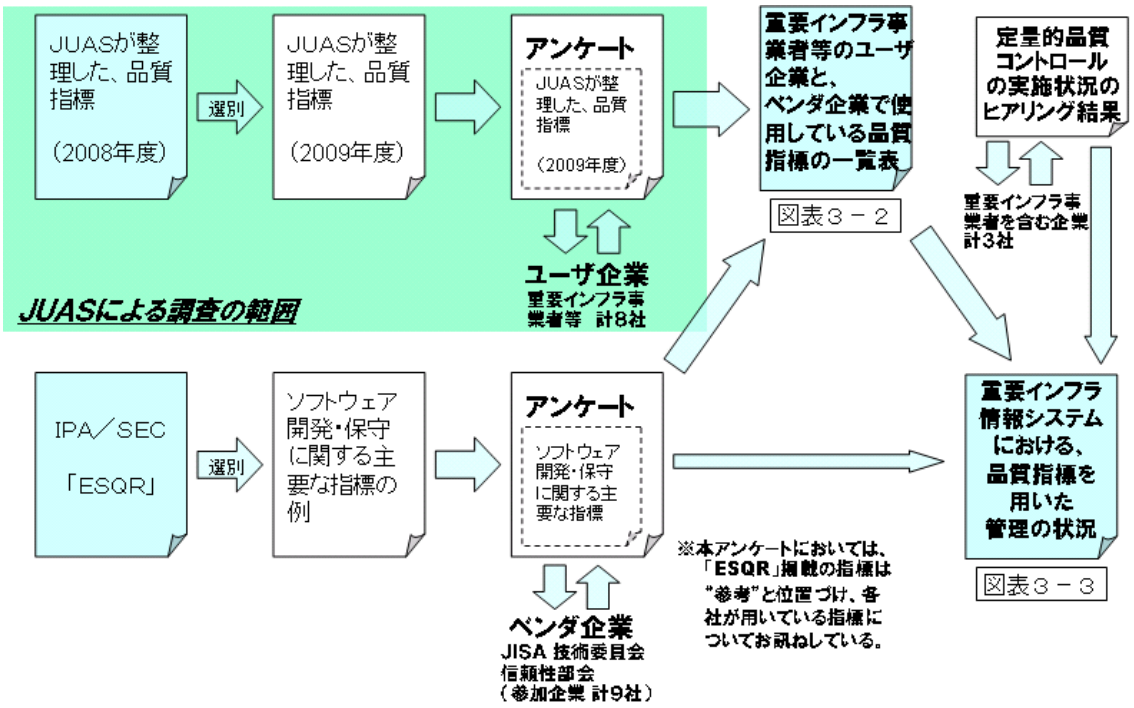
2.1 定量的品質コントロールの実施状況調査の進め方

JUASでは、ユーザ企業を対象に品質指標を活用した定量的品質コントロールの実施状況（使用している指標および目標値を含む）についてのアンケート調査を行い、8社から情報を取得した。

また、情報システムベンダの業界団体（JISA）の協力を得て、ベンダ企業を対象に重要インフラ情報システムを製造した際の品質指標を用いた定量的品質コントロールの実施状況についてアンケート調査を行い、9社から情報を得た。

さらに、品質指標を活用した定量的品質コントロールについて、先進的な取組みをしているユーザ企業3社への個別のインタビュー調査により詳細情報を取得した。このインタビュー調査では、使用している品質指標および基準値の他に、それらによって各工程での諸判断や発注者・供給者間のコミュニケーションがどのように行われているかについても聞き取りを行った。

調査の流れは、【図表3－1】のとおりである。



【図表3－1】 定量的品質コントロールの実施状況の調査

2.2 定量的品質コントロールに関する調査結果

重要インフラ情報システムにおける品質指標を用いた定量的品質コントロールの実施状況についてのアンケートの集計結果を【図表3－2】に示す[2]。このアンケート調査の方法は、次のとおりである。

[2] 但し、この集計結果には、情報システムやソフトウェアの信頼性に直接関係しないと考えられる品質指標、たとえば生産性や工程の進捗率に関するものは含めていない。

1） ユーザ企業（重要インフラ事業者等　計8社）向けアンケート

● JUASが 2008 年度の調査結果をもとにまとめた 53 個の指標をユーザ企業に示し、各企業における各品質指標の使用の有無と、開示可能な場合にはその基準値について尋ねた。

2） ベンダ企業（JISA　参加企業　計9社）向けアンケート

● 先述の「組込みソフトウェア開発向け　品質作り込みガイド　（ESQR）」から抽出した、主要な品質指標をベンダ企業に参考として例示し、重要インフラ情報システムの開発において各社が使用した主要な品質指標および開示可能な場合にはその基準値の提供を要請した。

両アンケート調査ともに、各企業が使用している品質指標の全ての回答を求めることはしていないことから、その回答内容から当該企業の定量的品質コントロールの全体像を論じることはできない。

個々の事業者の定量的品質コントロールの全体像を論じることが難しいことから、アンケート結果を集約し、複数の事業者が共通的に使用している品質指標から、定量的品質コントロールの最小公倍数的な状況を見ることとした。

具体的には、アンケートの集計結果【図表3－2】をさらに加工し、ユーザ企業・ベンダ企業の合計2社以上が使用している品質指標を抜き出して、一覧表化した。[3] その結果を【図表3－3】に示す。

なお、同図表には、ユーザ企業へのインタビューで得られた各品質指標の使い方（品質指標を用いた工程の判断や、ユーザ企業－ベンダ企業間のコミュニケーションでの利用）についても付記した。この付記部分についてはユーザ企業1社のみから得られた情報も含まれている。

[3] 但し、企画の工程の品質指標については、例外的に１社のみから得られた情報を含めた。

【図表3－2】品質指標についてアンケート調査の集計結果

区分		小区分	指標名	重要インフラ事業者を含むユーザ企業								ベンダ企業											
				A社	B社	C社	D社	E社	F社	G社	H社	p社	q社					r社	s社	t社	u社	v社	w社
			業種	製造	電力	航空	通信	金融	ガス	金融	金融	システム1	システム1	システム2	システム3	システム4	システム5	システム1	システム共通	システム1	システム1	システム1	システム1
企画	企画のドキュメントのレビュー密度と欠陥密度	レビュー	システム企画書単位量あたりのレビュー回数		○																		
		レビュー	システム企画書単位量あたりのレビュー時間		○																		
		レビュー	システム企画書単位量あたりのレビュー指摘数		○																		
		レビュー	企画に要する総時間に占めるシステム企画書レビュー時間の比率		○																		
		レビュー	システム企画書単位量あたりのレビューで発見するべき不整合を発見できなかった件数		○																		
要件定義	要件定義のドキュメントのレビュー密度と欠陥密度	レビュー	システム要求書単位量あたりのレビュー回数		○	○				○													
		レビュー	システム要求書単位量あたりのレビュー時間		○	○				○													
		レビュー	システム要求書単位量あたりのレビュー指摘数		○	○				○													
		レビュー	要件定義に要する総時間に占めるシステム要求書レビュー時間の比率		○	○				○													
		レビュー	システム要求書単位量あたりのレビューで発見するべき不整合を発見できなかった件数		○																		
開発	開発での要件、要件実現の管理	要件管理	要件変更密度																			○	
		仕様管理	仕様変更密度																				○
		仕様管理	仕様変更規模																				○
		機能管理	パッケージ機能数に対して、パッケージに変更を加える機能数																		○		
		機能管理	パッケージ機能数に対して、パッケージに追加する機能数																		○		
開発	開発のドキュメント量	成果物作成	プロジェクトの規模に対して、設計仕様書のボリューム																0.02頁／ソース1行				
		成果物作成	ソース規模に対してUI設計書のボリューム														2.7枚／Kstep						
		成果物作成	ソース規模に対してSS設計書のボリューム														3.0枚／Kstep						
		成果物作成	ソース規模に対してPS設計書のボリューム														3.0枚／Kstep						
開発	開発でのレビュー、テストの工数比	レビュー	開発に要する総時間に占めるレビュー時間の比率／開発全工数に対して、品質保証にかけた工数の割		○	○				○		↓							↓	↓	○		
		レビュー	プロジェクト規模に対して、仕様のレビューにかけた工数の割合									○								○			
		レビュー	プロジェクト規模に対して、設計のレビューにかけた工数の割合									○								○			○
		レビュー	プロジェクト規模に対して、ソースコードのレビューにかけた工数の割合									○											○
		レビュー	プロジェクト規模に対して、全てのレビューにかけた工数の割合									○								○	○		
		レビュー	システム設計書単位量あたりのレビュー回数		○	○				○										○			
		レビュー	システム設計書単位量あたりのレビュー時間／設計書ページあたりのレビュー工数		○	○				○						0.4～1.4h／頁 0.2～0.7h／頁 1.8～9.0h／頁	3.0h／頁 7.0h／頁 7.0h／頁				○		
		テスト	開発全工数に対して、テストにかけた工数の割合									↑							＞30%	○	○		
開発	開発のドキュメントとソースコードのレビュー密度と欠陥密度	レビュー	要件定義書エラー摘出密度																				○
		レビュー	システム設計書単位量あたりのレビュー指摘数／設計書エラー摘出密		○	○				○													○
		レビュー	要件定義に要する総時間に占めるシステム設計書レビュー時間の比率		○					○													
		レビュー	システム設計書単位量あたりのレビューで発見するべき不整合を発見できなかった件数		○																		
		レビュー	単位量あたりのレビュー回数		○					○													
		レビュー	単位量あたりのレビュー時間		○	○				○													
		レビュー	単位量あたりのレビュー指摘数		○	○				○													
		レビュー	工程毎レビュー欠陥摘出密度(基本設計)												20～90件／100頁	0.7～2.6件／Kstep	1.5件／Kstep		0.6件／Kc				
		レビュー	工程毎レビュー欠陥摘出密度(詳細設計)												40～233件／100頁	0.1～0.6件／Kstep	7.35件／Kstep		0.4件／Kc				
		レビュー	工程毎レビュー欠陥摘出密度(プログラム設計)												10～200件／100頁	3.5～8.0件／Kstep 0.2～0.5件／頁	7.35件／Kstep		0.2件／Kc				
		レビュー	工程毎レビュー欠陥摘出密度(プログラムソース)／机上デバッグ抽出バグ数															○	3.1件／Kc				
		レビュー	ソースコード規模に対して、インスペクションツールによる指摘数															○					
		レビュー	不具合検出率(レビュー)／仕様レビュー指摘率																	○	○		
		レビュー	単位量あたりのレビューで発見するべき欠陥を発見できなかった件数		○	○																	

開発		*開発したソースコードの内容*	プログラミング	ソースプログラムのコメント率		○			○											20%程度						
			プログラミング	コーディングルールの逸脱率									○														
開発	単体テスト	開発したソースコードのテスト密度と欠陥密度	テスト	プログラム1000stepに対して、実施すべき単体テスト項目										38～50項／Kstep	○	519.3～1557.8項／Kstep	75～150項／Kstep	35項目／Kstep		100項目／Kstep			○			
			テスト	単位量当たりの単体テストで発見された欠陥数		○				6.0～10.0件／KLOC				0.9～3.9／Kstep	○	4.25～12.75件／Kstep	6.8～11.6／Kstep	＜10件／Kstep	○	＜4.42件／Kstep			○			
			テスト	単体テストでのカバレッジ率							100%																
			テスト	C0/C1カバレージ															○							
			テスト	単位量当たりの単体機能テストで発見された欠陥数																							
開発	他社開発		テスト	パッケージベンダからの納入物件数に対して、検出した不具合件数																	○						
			テスト	投入したテストケース数に対して、検出した不具合件数																	○						
開発	結合テスト		テスト	プログラム1000stepに対して、実施すべき結合テスト項目										10～20項／Kstep	25～80項／Kstep	81.1～162.2項／Kstep	新規20～50項 改造50～150項／Kstep	4項目／Kstep		60項目／Kstep			○			
			テスト	単位量当たりの結合テストで発見された欠陥数		○			○	2.0～4.0件/KLOC	1.55件/KLOC			0.4～1.5／Kstep	1～4件／Kstep	0.6～1.79件／Kstep	1.4～3.2／Kstep	＜1件／Kstep	○	＜1.13件／Kstep			○			
開発	システムテスト		テスト	システムテストのテストケース密度(KLOC当たり)		○			○	15～34件／KLOC	103.66件/KLOC			5.38～9.96項／Kstep	5～15項／Kstep	3～32項／Kstep	10～20項／Kstep	2項目／Kstep		40項目／Kstep			○			
			テスト	システムテストのテストケース密度(FP当たり)		○	○	20～35件／KLOC		○																
			テスト	システムテストの障害密度		○	○	2～4／KLOC	80～120%	0.5～1.0件／KLOC	2.5件/KLOC	○		0.1～0.7件／Kstep	0.3～0.6件／Kstep	0.1～0.2件／Kstep	0.2～0.4件／Kstep	＜0.1件／Kstep	○	＜0.25件／Kstep			○			
			テスト	システムテストの障害率		○	○	±20%信頼度成長曲線(ゴンベルツ曲線)			2.30%	○															
			テスト	システムテストの収束率			○	0.5%未満信頼度成長曲線(ゴンベルツ曲線)	○	100%	100%	○													○		
開発	開発全体		テスト	テスト密度／テスト実行密度					↑	↑	↑		○	↑	↑	↑	↑	↑	○	0.18項／ソース1行		○	↑	○		
			テスト	バグ密度／不具合密度／不具合検出率(テスト)		↑	↑	↑	↑	↑	↑	↑		↑	↑	↑	↑	↑	↑	↑		○	↑	○		
			テスト	バグ検出割合／不具合検出割合＃実績値／予測値																		○					
開発			テスト	工程別の欠陥埋め込み密度		○	○	○																			
			テスト	開発期間中の総欠陥埋め込み密度		○	○																				
			テスト	システムテストでのデグレードの発生割合			○	0%																			
開発後		開発後の欠陥密度	全般	単位量あたりの残存欠陥件数			○	0件/年		○																
			全般	単位量あたりの納入から安定稼働までに検出された欠陥件数		○	○	0件/年							○					○					○	
			全般	納入後の欠陥密度			○	0%																			
			全般	ソフトウェアの品質と開発工数の関係			○			○																	
保守		*保守*	全般	保守作業の欠陥率				0%																			
運用		運用におけるサービスレベル	オンラインシステム	オンラインシステムの稼働率	99.9%		○	99.999%		99.70%	99.9%													○		
			オンラインシステム	サーバ／ホストの各種セットアップ作業の1回での成功率				100%																			
			オンラインシステム	お客様迷惑度指数	1～4		○				0		○											○			
			バッチシステム	オープン系バッチ処理異常終了率							0.18%													○			
			バッチシステム	ホスト系バッチ処理異常終了率						○	0.13%													○			
			ネットワーク	ネットワーク障害復旧時間遵守率				100%		○	100%													○			
			全般	年間の運用費用1億円当たりの、事業を中断した障害件数																							
			全般	稼働品質率				99.999%																			
			全般	組織の能力									○														

凡例：
- ○　当該企業で使用している品質指標（基準値の提示なし）
- 数値　当該企業で使用している品質指標（基準値の提示あり）
- ↓、↑　当該企業で類似の品質指標を使用（＝他欄に○または数値を表示）
- （ブランク）当該企業で、使用していない品質指標

【図表３－３】 重要インフラ情報システムにおいて、用いられている品質指標の範囲

フェーズ	カテゴリ	プロセスを測定する品質指標 (A)	(A) の品質指標の名称の例	プロダクトを測定する品質指標 (B)	(B) の品質指標の名称の例	指標によるプロセスの判断とプロセスへの措置（注４）	発注者と供給者の間で交わされるコミュニケーション（注４）
企画（注１）	企画のドキュメントの欠陥の作り込み工程と摘出工程との関係			現工程のレビューで摘出されず、後工程で明らかになった欠陥の割合	・見逃し率（注2）	パターン①	事前合意 定期的報告・評価 事前合意の再調整 工程終了の合意
	作成した企画のドキュメントのレビュー密度と欠陥密度	レビューを実施した密度（ドキュメント単位量あたりの、レビューの回数、時間）	－	レビューで摘出された欠陥の密度	－	パターン②	
要件定義	要件定義のドキュメントの欠陥の作り込み工程と摘出工程との関係			現工程のレビューで摘出されず、後工程で明らかになった欠陥の割合	・見逃し率（注2）	パターン①	事前合意 定期的報告・評価 事前合意の再調整 工程終了の合意
	作成した要件定義のドキュメントのレビュー密度と欠陥密度	レビューを実施した密度（ドキュメント単位量あたりの、レビューの回数、時間）	－	レビューで摘出された欠陥の密度	・要件定義書エラー摘出密度 ・仕様レビュー指摘率	パターン②	
開発	ソフトウェアコードの欠陥を摘出した工程の妥当性			しかるべきテストで摘出されず、後工程で明らかになった欠陥の割合	・すり抜け率 （注3）	パターン①	事前合意
	作成した設計のドキュメントのレビュー密度と欠陥密度 ／ 基本設計でのレビュー	レビューを実施した密度（ドキュメント単位量あたりの、レビューの回数、時間）	・UIレビュー工数率	レビューで摘出された欠陥の密度	・UIレビュー指摘件数	パターン②	定期的報告・評価 事前合意の再調整
	詳細設計でのレビュー	レビューを実施した密度（ドキュメント単位量あたりの、レビューの回数、時間）	・SSレビュー工数率	レビューで摘出された欠陥の密度	・SSレビュー指摘件数		
	プログラム設計でのレビュー	レビューを実施した密度（ドキュメント単位量あたりの、レビューの回数、時間）	・PSレビュー工数率	レビューで摘出された欠陥の密度	・PSレビュー指摘件数		
			左３工程に亘る指標の名称例： ・設計の見える化チェック ・設計書レビュー密度 ・レビュー密度		左３工程に亘る指標の名称例： ・設計の見える化チェック ・設計書エラー摘出密度 ・設計レビュー指摘率 ・不具合検出率（レビュー）		
	作成したソフトウェアコードのルールへの適合の程度			コーディングルールからの逸脱の割合	・コーディングルール逸脱率	パターン③	
				ソフトウェアコードに含まれるコメントの割合	・コメント率		
	作成したソフトウェアコードのテスト密度と欠陥密度 ／ ソフトウェアコードのレビュー	レビューを実施した密度（ドキュメント単位量あたりの、レビューの回数、時間）	・ソースコードレビュー密度	レビューで摘出された欠陥の密度	・机上デバッグ摘出バグ密度	パターン②	工程終了の合意
	単体テスト	テストを実施した密度（ソフトウェアコードの単位量あたりのテスト項目数）	・PTテスト項目数	テストで摘出された欠陥の密度	・単体テスト摘出バグ密度 ・PTテストエラー率		事前合意の再調整
	結合テスト	テストを実施した密度（ソフトウェアコードの単位量あたりのテスト項目数）	・ITテスト項目数	テストで摘出された欠陥の密度	・結合テスト摘出バグ密度 ・ITテストエラー率		
	システムテスト	テストを実施した密度（ソフトウェアコードの単位量あたりのテスト項目数）	・STテスト項目数	テストで摘出された欠陥の密度 ＃その収束率 ＃予測との差異	・総合テスト摘出バグ密度 ・STテストエラー率		工程終了の合意
			左３工程に亘る指標の名称例： ・テスト密度 ・テスト工程毎テスト密度 ・テスト実行密度		左３工程に亘る指標の名称例： ・バグ検出密度 ・障害密度 ・テスト欠陥摘出密度 ・不具合検出率（テスト） ・バグ密度（不具合密度）		

開発後	開発の終了後に残存している欠陥密度			開発の終了後に残存している欠陥密度	・システムテスト工程での残存欠陥密度 ・サービス開始後に発生した不具合の件数 ・本番稼動後3ヶ月間エラー率 ・本番稼動後1年間エラー率	パターン②	定期的状況共有
運用	情報システムの運転に関する目標の遵守の程度			オンラインの稼働率	・オンラインシステム稼働率	パターン③	事前合意
				バッチ処理の時間内の終了率	・バッチ処理正常終了率		定期的報告・評価
	情報システムの障害に対する復旧時間の目標の遵守の程度			ネットワーク障害の復旧時間の遵守率	・ネットワーク障害復旧時間遵守率		事前合意の再調整
	情報システムの運転において、利用者に与えてしまった悪影響の程度			利用者に与えた悪影響の大きさ（影響した人数×時間×深刻度）	・お客様迷惑度指数 ・お客様迷惑度	パターン③	定期的状況共有

注記

（注1）企画の工程の品質指標のみ、例外的にアンケートにて1社のみから回答のあったものを扱っている。

（注2）
$$\frac{\text{（後続工程で明らかになったエラー件数）}}{\text{（成果物作成工程で明らかになったエラー件数）＋（後続工程で明らかになったエラー件数）}}$$
で定義される。
※　この指標は、ある企業内で提案されている」もので、2010年3月時点ではまだ実用されていない。

（注3）（前のテスト工程で摘出すべきエラーの数）÷（当該テスト工程で摘出されたエラーの数）
で定義される。
※　この指標は、ある企業内で提案されているもので、2010年3月時点ではまだ実用されていない。

（注4）「指標によるプロセスの判断」「判断によるプロセスへの措置」に関して、判断および措置の間隔についての情報は、今回の調査では収集していない。

「指標によるプロセスの判断とプロセスへの措置」の実施のパターン：

パターン①	**これまでの工程の妥当性判断：** ・プロダクトを測定する指標(B)が想定範囲より大きい場合は該工程に、 ・逆に(B)が想定範囲に比べ小さい場合には後工程に問題がある可能性あり	・問題がある工程の作業の見直し
パターン②	**現工程見直し必要の有無、および次工程への移行可否の判断：** プロセスを測定する指標(A)に対して、 ・プロダクトを測定する指標(B)が想定範囲より大きい場合は前工程又は当該工程に ・逆に(B)が想定範囲に比べ小さい場合にはレビューに問題がある可能性あり	・前工程の見直し ・現工程での追加作業の実施（レビュー内容の点検、レビューの追加）
パターン③	**現工程見直し必要の有無：** ・プロダクトを測定する指標(B)が想定範囲に比べ小さい場合には該工程の作業を見直しする必要あり	・現工程での追加作業（開発） ・業務手順やインフラ見直し（運用） ・エスカレーションレベル（運用）

「発注者と供給者の間で交わされるコミュニケーション」の実施のパターン：

事前合意	**工程の進め方、分担、情報共有の形式および工程終了条件についての事前合意**
定期的報告・評	**工程のマイルストンないし一定間隔での成果物の評価 および、相手が行った成果物評価の検証**
定期的状況共	**工程にて挙がった課題とその解決についての一定間隔での状況の把握**
事前合意の再調	**工程の進め方、分担、情報共有の形式 および　工程終了条件についての再調整**
工程終了の合	**工程の結果をチェックし、次の工程に移ることの合意**

【企画・要件定義】

●上流の工程、すなわち、企画・要件定義でも、品質指標を用いた定量的品質コントロールは一部実施されていた。

●調査結果についての議論において、企画・要件定義の工程では、他の工程に比べて特に、単純に欠陥を個数で数えるだけでなく、それぞれの欠陥あるいは欠陥が含まれているソフトウェアモジュールの機能の重要度を合わせて考えることが重要、という指摘があった。

●今回の調査では、上記のような欠陥の「質と量」の両方をどのように管理しているかという視点、たとえば指標以外の手法との組合せについては調べていない。企画・要件定義の工程での品質の把握、判断の方法については一層の調査が必要である。

【開発】

●開発では、多くの情報システムにおいて、レビュー・テストの実施量と摘出された欠陥が工程ごとに測定されていた。

●各工程における摘出欠陥数の目標値を、複数の重要インフラ情報システムについて示したベンダ企業が2社あったが、いずれの企業でも開発終了時の摘出欠陥数の目標値、最終的な（つまりソフトウェア出荷時の）残存欠陥数の目標値は企業内で同一であった。

●開発の最終工程である、システムテストにおける摘出欠陥数の目標値は、ベンダ企業とユーザ企業の間で10倍以内の幅があった。（ベンダ企業、ユーザ企業各3社からの提示情報を比較した結果）

●ユーザ企業が明らかに使用している、開発段階での品質指標は、多くのユーザ企業において、システムテストにおける欠陥摘出のみである。このことから、ユーザ企業は、レビュー・テストという品質確保の活動の経過管理の多くの部分をベンダ企業に委ねている可能性がある。

●一方で、ある重要インフラ事業者では、ベンダ企業との間で開発の全工程にわたり、品質指標をどのような場でどのような立場の裁可のもと、どのような判断に用いるかを詳細に決め、それを実践していた。

●調査の過程および調査結果についての議論において、開発工程では品質指標について以下の考え方を持つことが必要との指摘が、重要インフラ情報システムにかかわるベンダ企業、重要インフラ事業者の双方からあった。

- 欠陥の作り込み工程と摘出工程の関係を分析することにより、各工程でのプロセスの妥当性をチェックすることが重要
- レビュー・テストという品質確保の活動全体にて、各段階で許容する残存欠陥数の上限をモデル化することにより、最終的な残存欠陥数を計画的に一定範囲内に抑えるような制御を反復的に行う考えを持つことが重要

【保守・運用】

●保守の工程での品質指標については、開発と共通する指標の活用を示唆する情報が1例あっただけで、今回の調査では詳細は不明である。

●運用においては、品質指標を用いた定量的品質コントロールは実施されていた。その中では、幾つかの共通的な品質指標がユーザ企業、ベンダ企業の双方で用いられていた。共通的な品質指標の中では、情報システ

ム障害発生の影響を、利用者の業務における影響から測定する品質指標が特徴的である。

●調査の過程において、運用工程では事業あるいは業務に係るリスクの大小の視点から品質指標の測定結果を評価し、各種対策を決めることが重要という指摘があった。

●なお、今回の調査では、情報システムに関する成果物（ソフトウェア、ドキュメント）の品質指標を中心に調査しており、情報システム自体の現象、振舞い、また運用のプロセスについての品質指標については、積極的には情報を収集していない。

このため、たとえば運用において、次のような情報システムが提供するサービスの品質について議論を行うためには、そこでの品質指標の活用した定量的品質コントロールの実情について、今後に調査することが必要である。[4]

- トランザクション量やレスポンス・タイムを定期的に測定して、利用者に重大な影響を与える可能性のある情報システムの信頼性に関わる予兆を把握し、システム障害の発生前に対処する。また、予兆を確実かつ容易に検知できるようにする仕掛けを情報システム内に具備させる。
- オペレータの誤操作の発生状況を定期的に測定して、誤りやすいオペレーションを特定し、誤操作による重大問題の発生前に、運用者への注意喚起やユーザ・インタフェースの改良を行う。

【システムライフサイクル全体】

●定量的品質コントロールの目標値については、統計的な処理に基づく基準値を示すには至らなかったが、参考値として公開可能な、数社の事例が得られた。

3. 定量的品質コントロールについての今後の取組み

今回の調査により、国内の重要インフラ事業者を含むユーザ企業と重要インフラ情報システムを供給するベンダ企業にまたがって、品質指標を用いた定量的品質コントロールの取組み状況が一部把握できた。

次年度以降、更に以下のよう点を考慮して、品質指標に関する調査検討を継続し、指標のリファレンス化に向けて活動していく予定である。

◆開発以外の工程での、品質指標を用いた定量的品質コントロールの実施状況

◆開発を含む工程での、品質指標を用いた「判断」や「コミュニケーション」の細かな粒度での実際 （インターバルやプロセスへの反映方法など）[5]

◆品質指標を用いた定量的品質コントロールを計画、実施する上での重要な考え方 （例:トレーサビリティ）

◆品質指標を用いた定量的品質コントロールの実施程度とコストとのバランスの考え方、あるいは定量的品質コントロールの実施程度の十分さを評価するための考え方

調査結果についての議論では、開発における管理が充実した結果、要件定義されたものの実装漏れというよう

[4] ただし、上記の例を含む保守・運用における品質指標の使用例は、以下の図書で既に明らかにされている。（IPAが次年度以降に「ガイド」を取りまとめる際に参考にすることを予定）
「信頼性向上のベストプラクティスを実現する管理指標調査報告書」（2008年4月） JISA

[5] ただし、開発工程における品質指標を用いた詳細な「判断」の考え方についての提案は、以下の図書で示されている。
「情報システム信頼性向上のための管理指標活用の普及拡大調査報告書」（2009年4月） JIISA

な問題が減った反面、上流の工程での要件定義の網羅性、運用における要件を上流の工程で十分に考慮することが不足していることへの対処が必要になっているのではないか、との指摘があった。この観点も今後の活動に反映する予定である。

第 4 部 障害再発防止策

2008 年度に「重要インフラ情報システム信頼性研究会」が提案した重要インフラに係る情報システムのソフトウェアの開発、運用に関わるチェックリストについて、実際のシステムへの適用を通じた検証と有効性確認を行い、信頼性向上対策の実践に必要な参考情報をとりまとめることを目的に、昨年度に引き続き具体的障害事例に基づくシステムライフサイクルの各プロセスでの対策の深堀り等を通じた調査・検討を行った。

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。

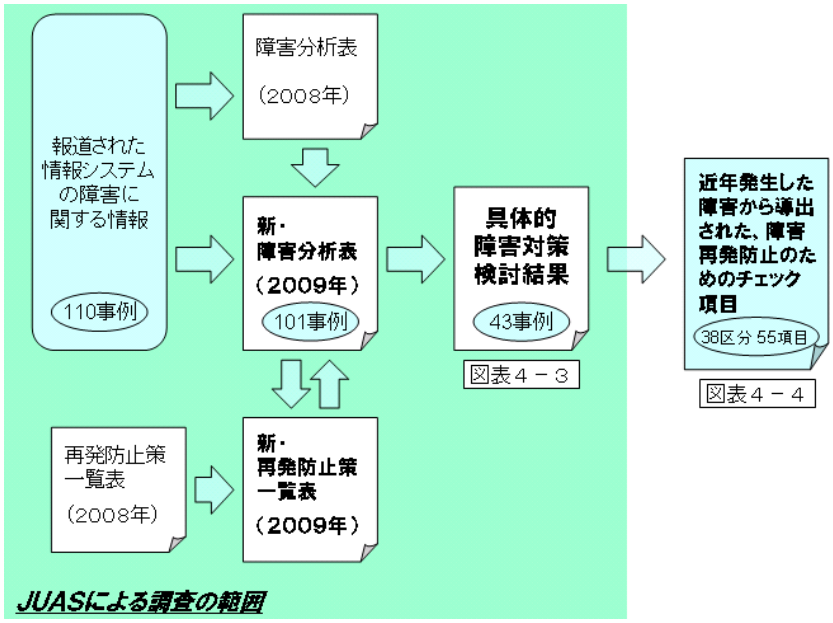
以降では、調査内容及び調査結果の分析に基づく議論の詳細について述べる。

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[6]で直近4年半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4－1】のとおりである。



【図表4－1】 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。ただし、検討対

[6] ITpro の Web にて公開されている情報を用いた。

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4－2】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4－2】 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4－3】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4－3】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、55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4－4】のとおりである。

【図表４－３】 直近4年半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	・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カバーする。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、滞留した出勤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	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４－４】 直近4年半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
			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練	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。

なお、【図表4－4】においては、得られたチェック項目（38区分、55個）を、経済産業省発行の「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）」の『Ⅲ．企画・要件定義・開発及び保守・運用全体における事項』に記載されている各項目に対応付けて整理している。得られたチェック項目の概要は次のとおりである。[7]

【企画・要件定義】

●要件ごとの重要度の取り決め、利用者の特性に合わせたシステム機能の企画、処理能力についての取り決め、暗黙知の扱い、といった、ともすると情報システムの仕様を定める段階で欠落することのある事柄についてのチェック項目が挙がった。

【開発】

●システムテストの計画内容および実行環境、システム移行方式、システム以降後の評価といった、完成したシステムの本番適用前後での妥当性判断に関するチェック項目が挙がった。

【保守・運用】

●手続き・手順の規定、体制・役割分担、指示や実行結果の記録といった、保守・運用のプロセスの確からしさを上げ、またその確からしさを確認する方法に関するチェック項目が挙がった。

【障害対応】

●障害への対応方法、体制の策定、予備リソースの確保、訓練といった、障害発生時の対応の迅速化のための備えに関するチェック項目が挙がった。

【システムライフサイクル全体】

●トレーサビリティの確保、保守によって変化していく情報システムの仕様の棚卸し、といったチェック項目が挙がった。

上記は、情報システムの信頼性を確保するために、情報システムの利用者、供給者がその責務において、実際の業務に反映することが必要な事柄であるが、同時に経営者の責務における、必要なリソースの投入、説明責任とも強く関係する事柄と考えられる。（「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」の『Ⅱ．信頼性・安全性向上に向けての全般的配慮事項』にある、経営者の責務 「(3) CIO(情報統括役員)の登用と活用」「(4) 説明責任の認識」に関係）

【図表4－4】のチェック項目は、実際に発生した障害事例に基づき、重要インフラを含む情報システムに関わる有識者によって分析された障害事象、再発防止策から導出したものであり、類似障害の再発防止には有効と考えられる。

[7] 以下の記述の区分は「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」の『Ⅲ．企画・要件定義・開発及び保守・運用全体における事項』による。

ただし、このチェック項目リストの使い方としては、以下の点に留意する必要がある。

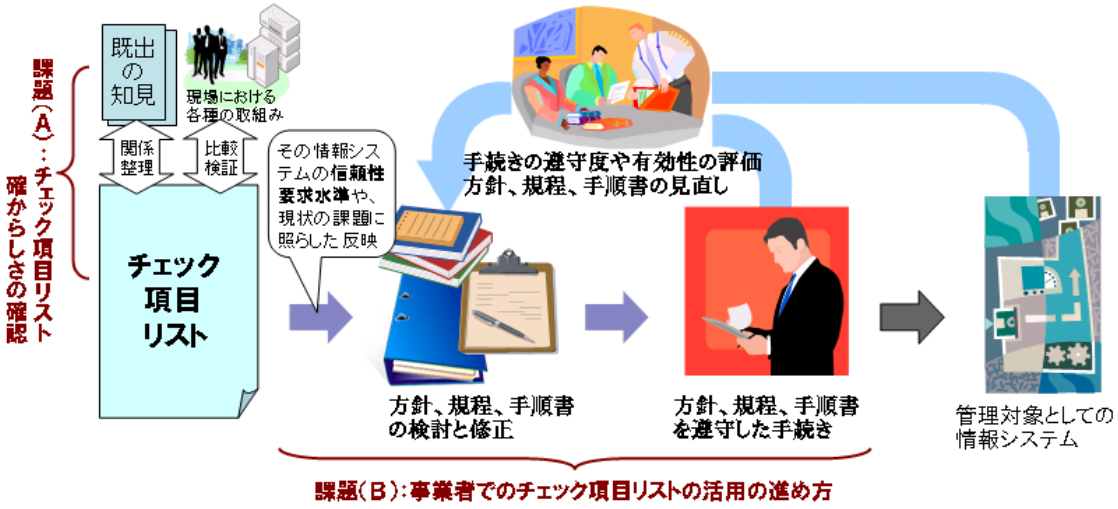
- このチェック項目リストは、例えば、①チェック項目に関係する、情報システムの管理の方針、規程、手順書を明らかにし、その内容がチェック項目リストの各項に対して十分か検討し、必要があれば修正、②併せて、その方針、規程、手順書が遵守されていることを確認する方法を定め、定期的にその確認作業を実施、③定期的に①②の活動の有効性を評価、というような活動の中で使用されるものである。関係者が日々の点検に使用するものではない。

上記を含め、チェック項目リストには、以下の項目が今後の課題として残されている。

(A) チェック項目リストの内容の障害再発防止についての網羅性の検証

(B) 上記①～③に例示したような、事業者の中でのチェック項目リストの活用方法の明確化

(イメージを【図表4－5】に示す。)



【図表4－5】 チェック項目リストについての課題

3. 障害再発防止策についての今後の取組み

2009 年度の調査では、過去4年半にWeb 報道された障害事例を元にした再発防止策、チェック項目リストを検討し、実際に発生した事案を材料とした検討ができた。2009 年度の成果をもとに、次の2点について更に検討を重ねることにしたい。

(a) チェック項目リストの精度の向上

2009 年度公開したチェック項目リストの網羅度を、他の知見との関係の整理や現場で実施されている障害対策の施策の比較など、いくつかの角度から検証するとともに、より網羅的なチェック項目リストや対策案を策定し、リファレンスとして公開することを目指す。

(b)事業者の組織的取組みにフォーカスした調査

以下の事項を念頭に、事業者の協力を得ながら、関係者に対する個別のヒアリング等によるフィールド調査を主体とした活動を実施する。

- ◆ 事業者の情報システムの管理の方針
- ◆ 事業者がこれまでに認識した主要な障害
- ◆ 事業者、または利用者が認識する障害発生の直接的原因とその背景
- ◆ 上記を踏まえた、事業者の現行の障害再発防止策の全体概要
  （類似障害の再発防止に向け、事業者が整備した障害分析および状況共有の仕組みを含む）
- ◆ 上の障害再発防止策の具体化、改善等のPDCAサイクル
- ◆ 以上にて観察される、障害再発防止策を各事業者が整備する上で重要な観点 （例：経営者とは、リスクベースでの現状や改善計画の共有を行う。）

上記の調査の中では、プロファイリングによって得られる情報システムの（確保されるべき）信頼性要求水準と、当該情報システムで採られている諸施策が実現している信頼性要求水準の対比も行う。

参 考 文 献 （順不同）

●「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」　（２００９年３月）　経済産業省

●「信頼性向上のベストプラクティスを実現する管理指標調査報告書」　（２００８年４月）　社団法人　情報サービス産業協会

●「情報システム信頼性向上のための管理指標活用の普及拡大調査報告書」　（２００９年４月）　社団法人　情報サービス産業協会

●「ユーザ企業　ソフトウェアメトリックス調査２００９　ソフトウェアの開発・保守・運用の評価指標」　（２００９年７月）　社団法人　日本情報システム・ユーザー協会

●「組込みソフトウェア開発向け　品質作り込みガイド」　（２００８年１２月）　独立行政法人　情報処理推進機構

付 録

付録１　プロファイリングによる 情報システムの信頼性要求水準の決定と、必要な信頼性向上の対策について

付録２　プロファイリングによる 情報システムの信頼性要求水準の決定の単位

付録３　詳細調査データ

３－１　プロファイル分析　（ユーザ企業の情報システムの特性の調査結果）

３－２　指標のまとめ　（ユーザ企業で用いられている品質指標の調査結果）

３－３　障害分析表　（2009 年度版）

３－４　再発防止策一覧表　（2009 年度版）

３－５　障害対策の取組み方法