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の信頼性向上の取組みガイドブック

～情報システムの信頼性管理に必要な組織内の役割分担と活動の枠組み～

平成 23 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

【巻頭言】

東京大学大学院工学系研究科 教授 中尾政之

筆者は今、2011 年 3 月 13 日、M9.0 の東北地方の大地震・大津波のニュースを見ながら、本文を執筆している。そして 15 時半頃、福島第一原発の 1 号機の建屋の天井が崩落する事故が起きた。毎時 1 ミリシーベルトの放射線が照射され、解説者である同僚の関村教授の顔が引きつっていた。そして、20 時頃には海水を原子炉に注入して、廃炉覚悟の最後の手段に出ている。

現在インフラシステムは、ハードウェアでもソフトウェアでも、電気が供給されないと何もできない。1 号機では非常用のディーゼル電源が動かず、原子炉を冷やせなかったらしい。今回の地震は余りにも大きすぎ、電気が根こそぎに抹殺され、すべての重要インフラが事故後に働かなかった。

一般に、現在の日本の信頼性設計、安全システムは偉大である。今回の地震でも、23 万人の犠牲者を出した同規模のスマトラ大地震・大津波と比べれば、日本の安全システムはそれを 10 分の 1 以下に抑えている。ソフトウェアのシステムも同様に信頼性は世界的に高いと言われている。しかし、社会はさらなる高信頼性を期待しているのが現状である。世界一の技術と威張っても、津波の猛威の前には塵のようなものだったではないか。技術者は謙虚に反省すべきである。

本書は、生きるか死ぬかを問うようなカタストロフィックな災害を扱うのではない。もっと小規模で定常的だが、たとえば数万人の利用者のために毎日、稼動し続けなければならない、というようなソフトウェアの基幹システムを扱っている。ここでは、コンピュータを動かす電気が供給される限り、設計者が考えるとおりに失敗は防止できる。問題は考え落としである。

情報処理推進機構では、重要インフラ情報システムの信頼性向上を目指し、2008 年から研究会を開き、地道に活動している。この研究会では、失敗事例を集めて共通のパターンを抽出するボトムアップ的な研究と、高信頼性を確保するために必要な設計方法を提案するトップダウン的な研究を、同時進行的に実施した。

その研究会のチェアマンだった筆者が思うに、2011 年になっても理想的というレベルには達していない。前者のボトムアップの研究は失敗の具体的情報が収集できないので、共通パターンは上司の説教のように抽象的だった。たとえば、要件定義のレビューをもっと詳しくやれ、システムテストをもっと長くやれ、と言われても余りに定性的で、具体的にやるべき対策がわからない。後者のトップダウンの研究も同様に抽象的だった。満足すべき作業目標がプロジェクトごとに具体的に設定できず、どこまでやればいいのかよくわからない。と言いながらも、本ガイドブックは年々、より具体的に定量的に進化しており、有用であるという評価を得ている。これまでこのよう

な公の活動がこの業界になかったから。

日本の設計は、ハードウェアでもソフトウェアでも、インテグレイテッド設計、つまり擦り合わせ嗜好、カスタマイズ重視という特徴を有する。その結果、オタク的だが過剰機能で複雑なガラパゴスを作りやすい。そして、個々の製品が多様になる。どおりで共通の設計指針が作りにくかったわけである。アメリカが好きなモジュラー設計、縦割り組織、パッケージ重視とは正反対である。しかし、システムが大規模になると、要求機能が数万個に増えて、どれとどれが干渉するのか、設計者が容易に見つけられなくなる。信頼性に対して、日本のインテグレイテッド設計は分が悪い。

筆者が集めた重要インフラのハードウェアの事故データを見ると、半分は疲労・摩耗・腐食のような「経年劣化」の失敗であり、残りの半分は「あちらを立てればこちらが立たず」という「干渉設計」の失敗であった。一方で、ソフトウェアには「経年劣化」が起きないから、ほぼ全部が「干渉設計」の事故になる。そして、モジュラーよりもインテグレイテッド設計のほうが干渉を起こし易いから、日本では「干渉設計」の失敗防止が信頼性のキーポイントになる。

また、筆者の共同研究先のデータであるが、事故の 3 分の 1 は要件定義が原因であった。これも干渉設計の失敗の一つである。「お客様は神様だから」と言って、暗黙の要求まで全部、請け負った結果、思わぬ干渉が起きる。しかし、この失敗も 2005 年ごろから激減してきた。各ベンダーが大口赤字プロジェクトを殲滅するために、本ガイドブックが推奨するように、要件定義を確実に行うようになったからである。

このようないくつかの施策の結果として、重要インフラ情報システムの信頼性は一段と高くなった。しかし、鉄道の遅延時間や電力の停電確率のような、国際的に比較できる信頼性の指標が見つけにくいから、高信頼性になったことさえ認識されていないのが業界の現状である。本ガイドブックでは、指標としてシステム稼働率に注目しているが、彼我で稼動条件が異なるので単純に比較できない。

パラパラ見るとわかるが、本ガイドブックは定性的に失敗防止の真実を語っている。しかしながら、ハードウェアの設計指針のように、これだけ気をつければ確実にこれだけ信頼性が高まる、とは言い切れなかった。とは言え、ここにソフトウェアの失敗防止の方向性が提示されているのは確かである。今後とも国家の仕事として続け、日本の設計文化を高めるべきである。

本ガイドブックは、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。

「重要インフラ情報システム信頼性研究会」　委員一覧

座長	中尾　政之	東京大学大学院工学系研究科産業機械工学専攻教授
委員	淺野　正一郎	国立情報学研究所アーキテクチャ科学研究系教授
委員	天野　稔	東京電力(株)システム企画部長
委員	一柳　幹男	信金中央金庫　理事 システム部長
委員	宇治　浩明	(株)東京証券取引所ＩＴ開発部株式売買システム部長
委員	太田　忠雄	(株)ジャステック常務取締役 兼 常務執行役員営業本部本部長
委員	雄川　一彦	東日本電信電話(株)ＩＴイノベーション部長
委員	木谷　強	(株)エヌ・ティ・ティ・データ技術開発本部長
委員	坂野　正晴	(株)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
委員	島谷　二郎	国民健康保険中央会　理事
委員	鈴田　信	(財)金融情報システムセンター監査安全部長
委員	中村　之一	小田急電鉄(株)経営政策本部ＩＴ推進部課長
委員	野中　誠	東洋大学経営学部経営学科准教授
委員	淵　昌彦	東京ガス(株)導管ネットワーク本部防災・供給部施設グループ・マネジャ
委員	細川　泰秀	(社)日本情報システム・ユーザー協会副会長
委員	幸重　孝典	全日本空輸(株)執行役員

（オブザーバ）
内閣官房情報セキュリティーセンター（ＮＩＳＣ）
経済産業省 商務情報政策局 情報処理振興課

（事務局）
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）

（平成 23 年 3 月 15 日現在）

前　文

このガイドブックでは、「重要インフラ」と称される、国民生活や社会経済活動にとって重要な“社会サービス”と、その“社会サービス”を提供する仕組みとしての情報システムを扱っています。

●●●●●●●●●

“社会サービス”の突然の停止や機能低下は、国民生活や社会経済活動に重大な影響を与えます。このため、“社会サービス”やそれを支える情報システムには高い信頼性が求められます。

一方で、社会サービス”は事業者間の競争の対象でもあります。利用者の期待に応えるべく、“社会サービス”の高度化が日々図られており、また、“社会サービス”を支える情報システムの複雑化が進んでいます。

“社会サービス”を提供する事業者は、既に“社会サービス”の管理に大きな労力をかけていますが、“社会サービス”の高度化、情報システムの複雑化により、それらの信頼性確保のために一層大きな労力をかけることが必要になっています。
しかしながら、事業者間の競争を考えると、“社会サービス”やそれを支える情報システムの管理コストを大きく増やすことは困難です。
“社会サービス”を提供する事業者には難しい舵取りが求められています。

●●●●●●●●●

さて、情報セキュリティの領域では、「事故前提」の考え方が広まりつつあります。
経済産業省が 2003 年に発表した情報セキュリティ総合戦略には、「事故前提のしなやかな社会システムの実現」という考え方が掲げられています。これは、事故を起こさないことを目指すよりも、事故は起こり得るものと捉えて事故の予防と事故発生時の適確な対応により被害を少なくし回復力を高めることの方が、現実的な責任の果たし方として適切ではないか、という考えです。

この「事故前提」の考え方の背景にあるのも、社会の変化と、それを支える情報システムの複雑化です。
企業間の競争の高まりにより、企業間の事業連携の深化、雇用の多様化が進展し、それに伴って情報システムの構造や相互連携も複雑化しました。その結果、企業の事業やそれを支える情報シ

ステムにおいて、事故を皆無にすることは大変難しくなっています。

●●●●●●●●●

“社会サービス”とそれを支える情報システムの信頼性に関して、どういう姿勢をとるかは、各々の事業者が主体的に考えるべきことです。

しかし、前節のような「事故前提」の考え方、すなわち、事故は起こり得るものとして事故発生とその影響の拡大を抑制する方策を考えるという、リスク対応的な考え方を採ることで、事業者は新しい展開を図れる可能性があります。

例えば、事業者は、妥当と思われる「“社会サービス”の確実さに関する目標」[1]を立て、その目標を達成する方策（事故の予防、事故発生時の対応）を計画し実施する、という組織的な活動を行うということです。
そして、“社会サービス”の利用者に対して、「“社会サービス”の確実さの目標」とそれを実現するための取組みを示すことで、利用者の納得を得る、ということです。

この考えをとったとき、事業者は“社会サービス”を支える情報システムに対して何をするべきでしょうか。

まず、「“社会サービス”の確実さの目標」を扱う必要があります。
社会サービス”の利用者である各国民は、様々なニーズを持っています。しかも、各国民のニーズはその置かれた状況により変動します。したがって、短時間のうちに利用者の合意を得ることのできる「“社会サービス”の確実さの目標」を立てることは困難です。
そこで以下が必要になります。

ａ）提供する「“社会サービス”の確実さの目標」を主体的に策定し、定期的、継続的に、“社会サービス”の性格に適した言葉で利用者に説明し、コンセンサスを得る。

続いて、その目標をクリアするために必要な情報システムへの方策を実施することです。
ここでは以下が必要になります。

---

[1] ここでいう「“社会サービス”の確実さに関する目標」とは、例えば以下のものです。
・旅客輸送、物流サービスの定時運行の目標（裏返せば、許容される遅延の発生程度）
・金融サービスの正常提供の目標（裏返せば、許容されるサービス機能低下の発生程度）

ｂ） ａ）を実現するのに必要な「情報システムへの要求」を策定し、それを実現する「情報システムの管理の取組み」を実施する。

さらに、目標と、情報システムへの方策の間で、その整合性を確認します。
ここでは以下が必要になります。

ｃ） ｂ）を、「“社会サービス”の確実さの目標」の達成有無の点から評価し、必要に応じ、「情報システムへの要求」や「情報システムの管理の取組み」を更新する。

●●●●●●●●●

このガイドブックは、上記のうちｂ）およびｃ）の活動を中心に、なおかつソフトウェアの開発・保守で必要な、組織的の取組みについて説明しています。

このガイドブックは、第一に“社会サービス”を支える情報システムの関係者各位にあてて書かれています。
但し、前述したように、“社会サービス”とそれを支える情報システムに関する状況は、それ以外の事業およびそれを支える情報システムと似ています。
本書を手にとられた方の関わられている事業、それを支える情報システムで事故が漸増傾向にあり、それが事業の高度化、情報システムの複雑化と関係しているとお考えなら、本書の中をご覧になってみて下さい。

－ 目 次 －

序章　はじめに

■背景　～重要インフラ、および重要インフラ情報システムにおける課題

近年、国民生活や社会経済活動は、コンピュータシステムを応用したさまざまな機器や情報システムによって制御・管理されるサービスに支えられて営まれている。
このサービスには、その提供の停止や機能低下が国民生活や社会経済活動に大きな影響を及ぼすものを含んでいる。
典型的には、「重要インフラ」[2] が提供するサービス（以下、「重要インフラ・サービス」と呼ぶ）がそれである。

こうした状況の中、情報システムの障害が引き金になって、重要インフラ・サービスに支障が発生し、国民生活や社会経済活動に大きな影響が及んだ事案はここ３年でも引き続き発生している。これら事案の直接的な原因は、重要インフラ・サービスの提供のために用いられている情報システム（以下、「重要インフラ情報システム」と呼ぶ。）が、その製造ミス（要件定義ミスや、ソフトウェアへのバグの混入を含む）、故障、劣化、操作ミス、人間の不当な介入あるいは災害などによって、その情報システムに求められた要件どおりに機能できなくなったことである。

この１０年、情報システムの障害が重要インフラ・サービスに与える影響が広範囲になってきた背景には、いわゆるネットワーク社会の中で、重要インフラ情報システムが他の情報システムや他の事業者が提供するサービスと連携しながら、より豊かなサービス機能を利用者に提供しようとすることに伴う重要インフラのサービスの提供基盤全体（以下、「サービス提供基盤」と記す。）の複雑化がある。
サービス提供基盤の複雑化を伴う、重要インフラ・サービスの高度化の例には、図表－１のようなものがある。

[2] 「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。

業 種	重要インフラ・サービスの高度化の実施例
鉄道	大都市圏を中心とした、路線をまたがって直通運転する列車の本数と経路の増加
航空	携帯電話による航空券予約、購入やチェックインの手続きの提供
金融	金融機関間の相互接続や、コンビニ、スーパー、駅に設置したATM接続の拡大
物流	３ＰＬ[3]の進展や、ネット通販との連携に伴う与信・決済業務の拡充

図表－１　重要インフラにおけるサービス高度化の例

一般の事業者と同様、重要インフラを担う事業者（以下、「重要インフラ事業者」と呼ぶ）にも事業者間競争の圧力がかかっている。図表－１のようなサービスの高度化、そのためのサービス提供基盤の高度化は今後も続くであろう。
このサービス提供基盤の高度化は、その中で用いられる情報システムにとっては、課せられる要件の複雑化につながる。
これらの流れを受け入れながら、一方でこれまで以上の重要インフラ・サービスの安定的な提供を実現するために、重要インフラ事業者は、重要インフラ情報システムをどのように管理したらよいのであろうか。

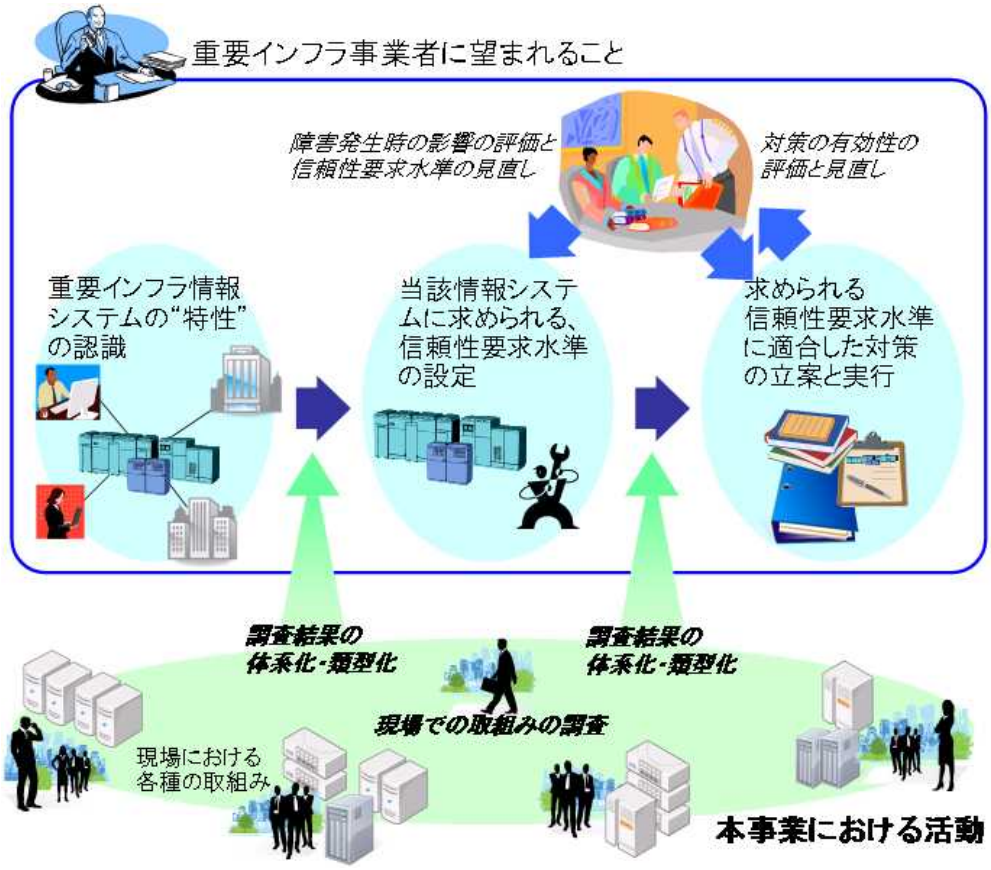
それが、本書が扱うテーマである。

本テーマを扱うにあたり、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（以下、「ＩＰＡ／ＳＥＣ」と記す。）では、２００８（Ｈ２０）年度からの３年間、「重要インフラ情報システム信頼性研究会」を組織し、以下のような活動を行ってきた。

・重要インフラ事業者等が実施している情報システムの信頼性確保の取組みの調査
・その調査結果を体系化・類型化し、重要インフラ情報システムの“特性”から求められる信頼性要求水準の設定やその水準に適合した対策の立案と実行をどのようにしたら良いかを明らかにすること

（活動全体のイメージを図表－２に示す。）

[3] サード・パーティ・ロジスティクスの略。ロジスティクスに関わる業務を一括受託するビジネスのこと



図表－２　「重要インフラ情報システム信頼性研究会」の活動イメージ

本書は、上記活動の集成として発行するものである。

■本書の構成

本書は、次のように構成されている。

序章　はじめに

第１章　重要インフラ情報システムの信頼性の状況

重要インフラ情報システムの信頼性が強く求められる背景や、重要インフラ事業者がとるべき考え方について説明する。

第2章　重要インフラ情報システムの開発・保守の管理フレーム

重要インフラ情報システムの信頼性確保に必要な取組みについて説明する。

これまでの重要インフラ情報システムに関する調査結果から、この情報システムに対する信頼性要求のまとめ方、それを満たすための活動についての考え方を「管理フレーム」として扱う。

第3章　信頼性確保の取組みに利用できる手法、ツール

ＩＰＡ／ＳＥＣあるいは他のＩＴ関連団体から提供されている、情報システムの信頼性向上のための手法やツールについて、それらが情報システムの信頼性要求やその実現にどのように活用できるかを説明する。

第4章　管理フレームの実施例

ある事業者における情報システム信頼性の確保の実施例を、第２章で取り上げた「管理フレーム」、第３章で取り上げた「手法、ツール」と対比しながら説明する。

終章　おわりに

今後の課題として、この本書で扱いきれなかったことを述べる。

■本書の想定読者

本書の想定読者は次とした。

●重要インフラ事業者（重要インフラ情報システムの管理責任者）

重要インフラ事業者に内にいて、重要インフラ情報システムの企画、要件定義、開発、運用、保守などのライフサイクルに関係する、情報システムの調達、情報システムが提供するＩＴサービスの供給に関する責任者

特に、その中で、重要インフラ情報システムとそのソフトウェアの信頼性の継続的な確保に責任を有している者

●重要インフラ事業者（重要インフラ情報システムのオーナー）

重要インフラ事業者において、重要インフラ情報システムの調達、運営に必要なリソースを提供する者

特に、その中で、重要インフラ情報システムが提供するＩＴサービスの事業上の利用、そこでの信頼性の継続的な確保に責任を有する者

●重要インフラ情報システムの供給者

ＩＴベンダー、重要インフラ事業者のＩＴ子会社などにいて、重要インフラ事業者に対する重要インフラ情報システムの提供に責任を有する者

特に、その中で、提供する重要インフラ情報システムとそのソフトウェアの信頼性の確保に重要インフラ事業者と連携した責任を有する者

●その他、将来上述のいずれかの立場になることが考えられる者

第１章　重要インフラ情報システムの信頼性の状況

１－１　重要インフラ情報システムが置かれた状況と課題

重要インフラの中の情報システムすなわち重要インフラ情報システムは、年々その重要性を増している。
その理由は以下である。

- 既に、多くの重要インフラにおいて、人間が手動で操作・制御していたのでは間に合わない、正確かつ大量のサービスが提供されている。そこでは多種かつ大量の情報システムが重要インフラにおけるサービス（以下、「重要インフラ・サービス」）を提供する基盤（以下、「サービス提供基盤」）の中に組み入れられ、人間に代わって、あるいは人間が及ばない操作、制御を行っている。
- これら重要インフラ・サービスを利用する国民生活及び社会経済活動は、上記の重要インフラ・サービスが継続的、安定的に提供されることを期待して営まれている。
- さらに、国民生活を豊かにするため、また社会経済活動を活発にするため、日々、追加的なサービスが考案され、提供されている。その結果、サービス提供基盤の中の情報システムは年々高度化される。
- 情報システムの高度化により、提供される重要インフラ・サービスは一回り大きくなる。そして、そのサービスの利便性が国民に実感され、かつ、そのサービスが安定して提供されるようになると、さらに国民生活は、その一回り大きいサービスが継続的に提供されることを期待して営まれるようになる。

こうして、提供される重要インフラ・サービスの質・量の拡大と、その国民生活や社会経済活動への定着のループが、サービス提供基盤に置かれた情報システム、すなわち重要インフラ情報システムの重要性を増していく。

しかし、こうした重要インフラ情報システムの重要性の増加に対して、それを十分に支える管理活動が確実に実施されているかといえば、そうは言い切れない。

具体的には、情報システムに何らかの不具合が生じた結果、重要インフラ・サービスの安定供給ができなくなり、その結果、国民生活又は社会経済活動に影響が及んだトラブル事例が、頻繁とはいえないものの近年でも発生している。（図表１－１）

業　種	時　期	トラブル事例　（概要）
鉄道	2007 年 10 月	自動改札機へのデータ授受の様式誤りがきっかけとなって、自動改札機が機能しなくなった。
金融	2008 年 5 月	情報システムの更新に伴って、他行に送付した電文の形式に誤りがあり、他行ＡＴＭとの間で入送金が不能になった。
航空	2009 年 6 月	ソフトウェアの更新に伴う、旅客チェックインシステムの障害で、航空便の欠航・遅延が多数発生した。
金融	2010 年 7 月	通信用システムの不具合により、他行との間で入送金が不能になった。

図表１－１　情報システムの不具合が重要インフラ・サービスの提供に影響を与えた事例

これらトラブル事例の直接的な原因は、重要インフラ情報システムが、その製造ミス（要件定義ミスや、ソフトウェアへのバグの混入を含む）等による故障、劣化、あるいは操作ミスなどによって、その情報システムに求められた要件どおりに機能できなくなったことである。この種のトラブルは、重要インフラ・サービスの利用者からみれば、「重要インフラ・サービスの提供の信頼性の不足」と捉えられる。

重要インフラ・サービス、あるいは重要インフラ情報システムの不具合について新聞等マスメディアで報道される件数は、2000 年台前半に比べれば減少している。また、重要インフラ情報システムの信頼性もここ数年は確実に確保されていることがうかがえる調査データもある。（調査結果の１つを、１－１の後のコラムに示す。）
しかし、人やモノの移動、契約や取引、あるいは生産や販売などの活動に目立った影響が及べば、マスメディアがこれを取り上げ、また国民が関心をもつことには変わりがない。

重要インフラ事業者には、重要インフラ・サービスに関して、その質・量の拡大と、安定供給とを同時に実現する取組みが求められている。

コラム　重要インフラ情報システムの信頼性の現状

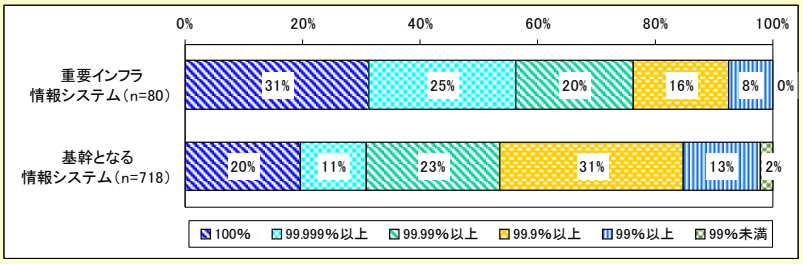
（社）日本情報システム・ユーザー協会（以下、「ＪＵＡＳ」）では、毎年、ＩＴ動向調査を実施している。ＪＵＡＳは、その 2009 年度の調査で情報システムの信頼性実績について調査を行った。内容は、情報システムの重要度と稼動率の関係などを調べたものである。結果は図Ａのとおりであり、重要インフラ情報システムについては、既に高い信頼性が確保されていることがうかがえる。

□調査結果:

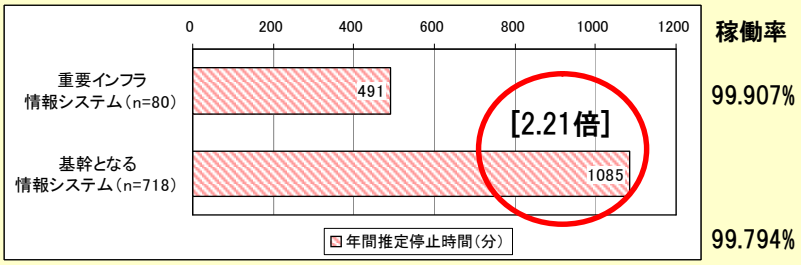
停止時間という観点だけから見れば、「重要インフラ情報システム」の信頼性は「基幹となる情報システム」より 2.21 倍高い。但し、「稼働率の目標値なしまたは不明」という企業が調査対象の 1/4 であった。

重要インフラ情報システムと基幹となるシステムの稼働率の比較

・稼働率99.999%から99.9%にかけて、年を追うごとに割合が高くなっていること、つまり情報システムの信頼性が年々高くなっていることがわかる。



重要インフラ情報システムと基幹となるシステムの稼動時間（推定）



図Ａ　企業等で使われている情報システムの稼動率の調査結果（２００９年度）

【 出典：ＪＵＡＳ　ＩＴ動向調査２００９】

１－２ 重要インフラ情報システムの特徴

重要インフラ情報システムの信頼性について考える前に、そもそも重要インフラや重要インフラ情報システムとはどのようなものであるか、その特徴を整理する。

重要インフラそのものと、そこで使用されている情報システムは次のような特徴を持つ。

（１）重要インフラの特徴

１．国民生活に欠かせない社会的なサービスを長期にわたって提供している。重要インフラの種類によっては１００年を超える歴史を有している。

２．重要インフラ・サービスへのニーズは、サービス利用者である国民や企業の所在や社会様式によって変化する。

３．したがって、重要インフラ・サービスへの信頼性に関する要求（以下、「信頼性要求」）の決定には、サービスの利用者である国民との合意が重要である。重要インフラ事業者は、国民の考え、価値観を把握して、提供するサービスについての目標を検討する必要がある。

（２）重要インフラのサービス提供基盤の特徴

１．重要インフラ事業者は、サービス提供基盤にその時代で使用可能な技術を適宜採用して、その信頼性や効率性を追求してきた。サービス提供基盤への情報システムの大規模な活用はここ３０～４０年に行われたことであり、情報システムの活用拡大は今後も続くと考えられる。

２．重要インフラのサービス提供基盤の構築のための投資額は非常に大きい。また、このサービス提供基盤の運営に関係する要員、また事業者内外での利用者は多数にのぼり、サービス提供基盤を世代交代させるには、教育、訓練も必要になる。こうしたことから、一度構築されたサービス提供基盤は、大きな欠陥が顕在化しない限り、改良がされながら使い続けられる。

３．サービス提供基盤では、サービスを提供するのに必要なさまざまな仕組みが、情報システムを含む多数の構成要素を使って作られている。これらの構成要素はサービスの円滑な提供において生じた問題への対応、または新たなサービスの提供の必要に応じて、改良、更新、追加される。

（３）重要インフラ情報システムの特徴

したがって、重要インフラ情報システムとは、重要インフラのサービス提供基盤の要素として、重要インフラ・サービスの質・量の拡大と安定提供のために、他の要素との連携を変化させつつ、改良、更新、追加されながら、長期にわたって使用されている情報システムである。（図表１－２）

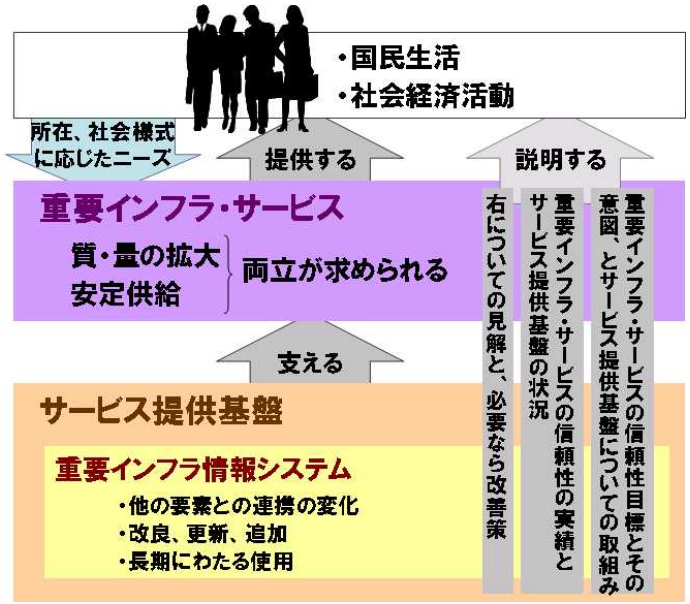
図表１－２　重要インフラ情報システムの特徴

１－３　その信頼性について求められること

ここまで、重要インフラ・サービスに求められていること、それを支える重要インフラ情報システムの性格、情報システムに求められる信頼性の内容について扱ってきた。
さて、重要インフラ事業者は、これらについて自らが満足できる結果を得られればそれでいいのであろうか。
重要インフラ・サービスの提供と国民生活、社会経済活動が密接な関係にあること、別の言葉でいえば重要インフラ・サービスの公共性、を考えると、単に結果だけを提示するのではなく、以下を説明できることが求められる。

① 重要インフラ・サービスの信頼性の目標、目標の意図、とサービス提供基盤（重要インフラ情報システムを含む）についての取組み
② 重要インフラ・サービスの信頼性の実績、サービス提供基盤（重要インフラ情報システムを含む）の状況
③ ①と②の差異についての見解、必要なら改善計画

サービス提供基盤の構成要素である重要インフラ情報システムの信頼性についても、上記の中で説明が求められる。（図表１－３）



図表１－３　重要インフラ事業者に求められる説明

コラム　重要インフラ･サービス、重要インフラ情報システムの信頼性と、それに掛けるコスト

重要インフラ・サービス、そのサービス提供基盤（重要インフラ情報システムを含む）の信頼性は重要ではあるが、それにどれだけのコストを掛けるのが妥当なのであろうか。

一般の事業であれば、商品やサービスについての信頼性を含む品質は、市場競争の中で、消費者や利用者にそれへの「期待」や「相場感」が形成されていく。各事業者は、その「期待」、「相場感」を如何に適切に読み取り、如何に効率的に達成するかが、腕の見せどころとなる。

一方、重要インフラにおいては、ある地域のあるサービスは、１事業者による寡占提供になっていることが少なくない。市場競争により品質への「期待」、「相場感」が形成される力は相対的に弱い。しかし、利用者はメディアが提供する情報あるいは個人間の情報交換によってそれなりの考えは持っている。重要インフラ事業者には、重要インフラ・サービスやサービス提供基盤の信頼性について、目標設定やその意図、また実績を説明し、また利用者の意見を吸い上げることで、利用者との合意を進め、信頼性の「相場感」を自ら形成することが求められる。

利用者との合意ができれば、そのあと重要インフラ事業者が考えるべきことは、それを如何にコスト最適で、かつ確実に達成するかである。

利用者の合意に基づき、求める信頼性を達成するための活動には、以下が考えられる。

① 重要インフラ情報システムなど、サービス提供基盤の構成要素の「誤謬」を皆無にすること

② サービス提供基盤の個々の構成要素に「誤謬」があっても、重要インフラ・サービスに影響しないように、構成要素の連携の仕方を設計し、また万一の対策を講じること

しかし、どのような重要インフラ・サービスにも適用可能な万能な答えは、今のところない。
上記においても①と②を択一の方策と捉えるより、例えば、

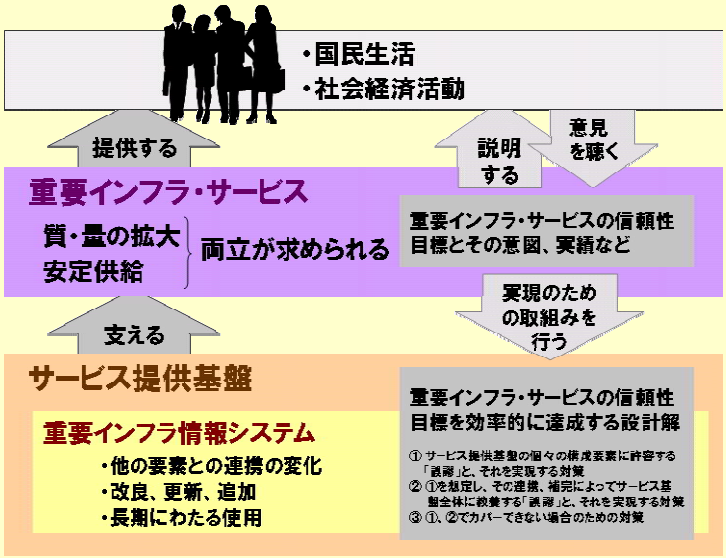
① サービス提供基盤の個々の構成要素に許容する「誤謬」の程度と、それを実現する対策

② ①を想定し、個々の構成要素間の連携、補完によってサービス基盤全体に許容する「誤謬」の程度と、それを実現する対策

③ さらに①、②ではカバーできないケースについての対策

とレイヤ化するのが、一つの考え方である。[4]
どのレイヤをどれだけ実施することで利用者との合意をコスト、時間の面から効率的に達成するのが適切か、について、重要インフラ事業者は、
(1) 事業者内の組織の特性や外部環境にあわせ、事業者が方針を立案し、
(2) その方針に基づいた活動を定義し、実施すべきである。

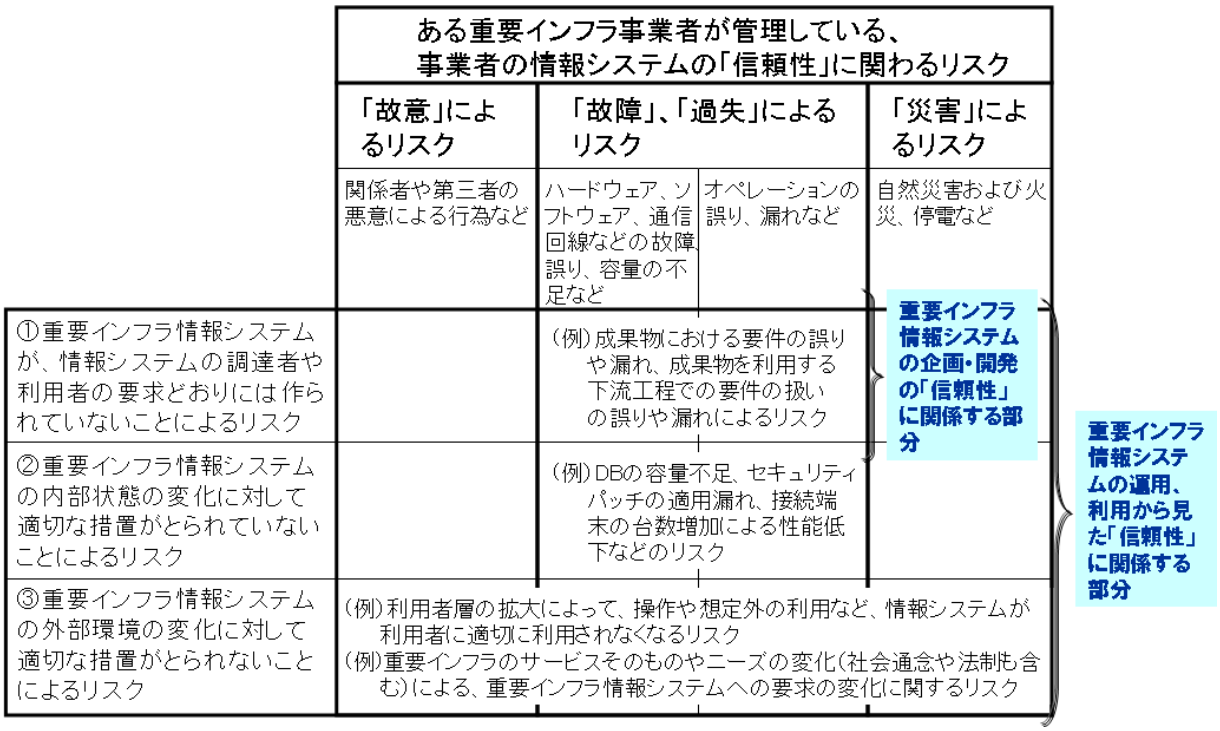
[4] 一言で言えば、リスク管理の考え方である。



図表Ｂ　重要インフラ事業者に求められる取組み

１－４　その信頼性とはどのような内容か。

次に、重要インフラ情報システムに求められる「信頼性」の中身について考えたい。
図表１－４は、ある重要インフラ事業者が、情報システムの信頼性を損ねるリスクをどのような範囲で認識しているかを図にしたものである。重要インフラ・サービスの安定提供を図るために必要な情報システムの信頼性について、「①要件の実現についての対応」、「②内部状態の変化への対応」、「③外部環境変化への対応」の３種類の対応を考えていることが分かる。



図表１－４　ある重要インフラ事業者が管理している、
情報システムの信頼性を損ねるリスク

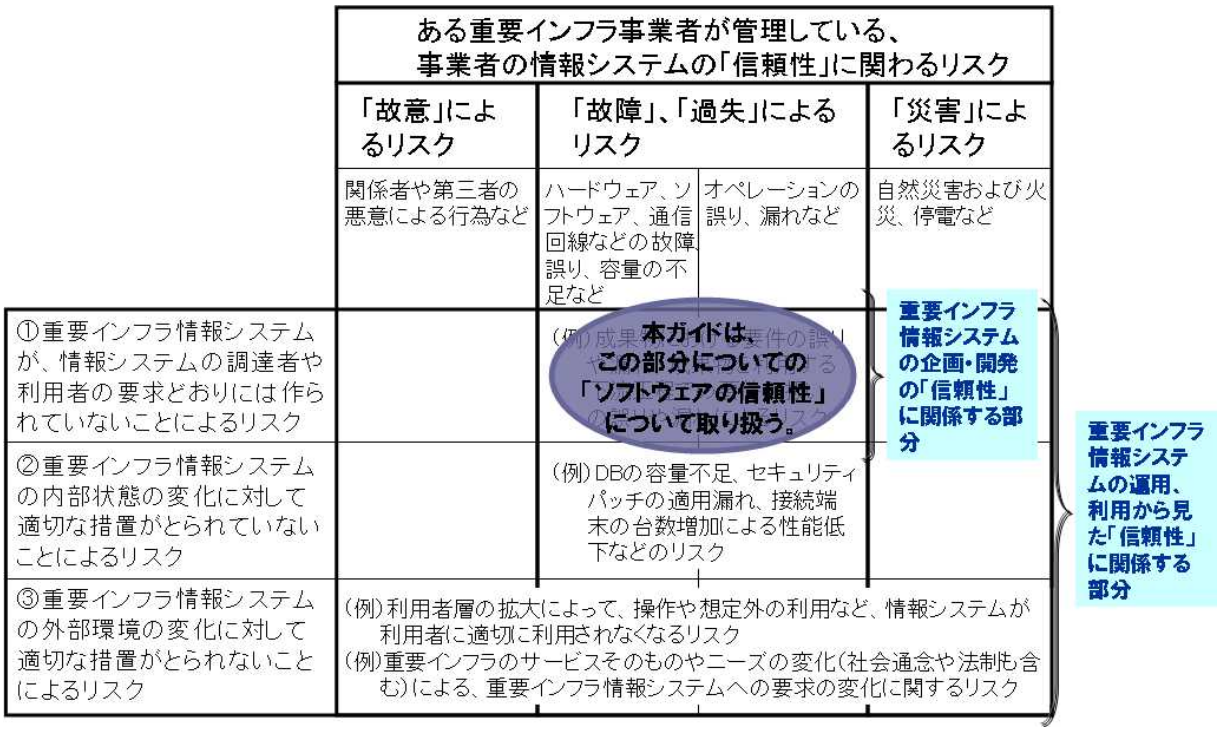
１－５　このガイドブックで扱う重要インフラ情報システムの信頼性

利用者である国民から見れば、重要インフラに求められるのはそのサービスの安定提供である。そのためのサービス提供基盤がどのように作られ、機能しているかは直接の関心事ではない。情報システムに障害が起きようとも、サービス提供基盤の他の構成要素により補完できていれば、おそらく利用者はそれに関心を寄せない。
すなわち、重要インフラ情報システムの信頼性は、重要インフラ・サービスの信頼性にとっての必要十分条件とはいえない。
しかしながら、１－１で取り上げたような事例が発生しているということは、重要インフラ情報システムの信頼性が重要インフラ・サービスの信頼性の鍵を握る構造になっている重要インフラが多数ある可能性がある。
そこで、本ガイドでは、重要インフラ情報システムの信頼性、特にその中に含まれるソフトウェアの信頼性について扱う。

ソフトウェアの信頼性は、
１．開発：要件が正しく記述され、それが正しく実装されているか。
２．保守：要件変更が正しく記述され、それが正しく実装し直されているか。
に大きく係わる。
つまり、本ガイドブックでは、重要インフラ情報システムそこに含まれるソフトウェアの信頼性について、図表１－５の範囲でこれを扱う。

注記

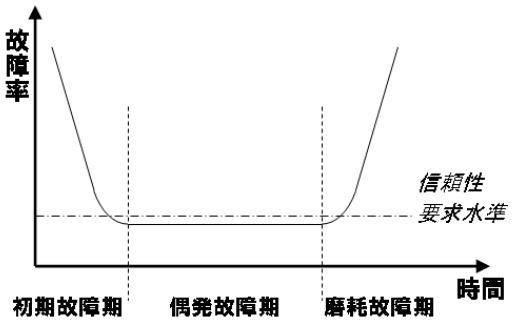
本ガイドブックでは、情報システムのうち特にソフトウェアにフォーカスすることから、その開発・保守に焦点をあて、**運用については一部を除き扱わない。**
情報システムの運用においては、ソフトウェア、及びその実行基盤を含む情報システム全体で信頼性を扱う必要がある。また、運用での信頼性の確保のためにソフトウェアに関して必要となる処置は、結局のところ保守（それによるソフトウェアの改良、追加）、および開発（それによるソフトウェアの追加または置換）ということになると考えられるからである。



図表１－５　本ガイドで扱う信頼性の範囲

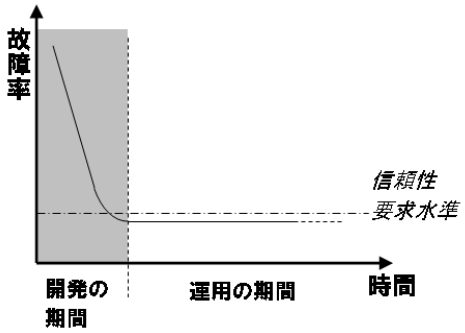
１－６ ソフトウェアの信頼性管理の要点

機械や装置などのハードウェアにおいて信頼性を扱うこととは、典型的には図表１－６の軸のような故障率曲線を考えることとされる。ハードウェアでは、故障率曲線はバスタブ曲線を描くものとして扱われることが多い。



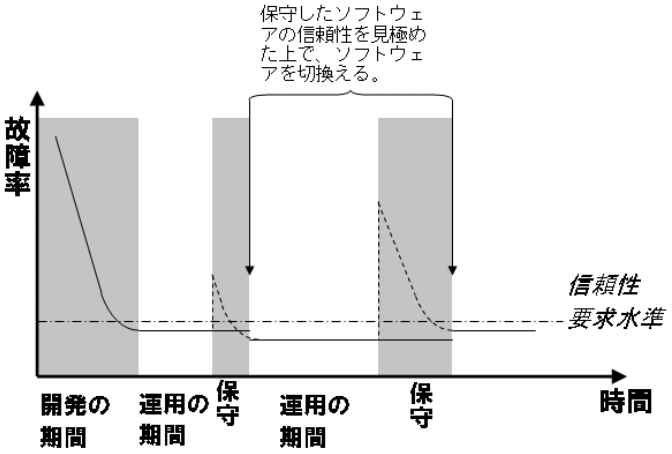
図表１－６　典型的なハードウェアの故障率曲線

一方で、ソフトウェアには、磨耗、劣化が原則存在しない。したがって、故障率曲線は図表１－７のようになる。



図表１－７　ソフトウェアの故障率曲線

つまり、ソフトウェアの開発・保守における信頼性管理の要点とは、初期故障が出つくし、ソフトウェアの信頼性が実用に耐える水準に達したことを如何に見極めるか、ということに尽きる。但し、重要インフラ情報システムのソフトウェアは、改良、更新されながら長期にわたり使われる。そこで、図表１－８のようにソフトウェアの信頼性を見極めるべき機会が何度も訪れることが特徴である。



図表１－８　重要インフラ情報システムのソフトウェアでの故障率曲線

第2章　重要インフラ情報システムの開発・保守の管理フレーム

１章で述べた、重要インフラ情報システムの特徴、そこで必要となる信頼性を確保する事業者の活動について、重要インフラ事業者の取組みについての調査結果をもとに説明する。

2－1　開発・保守の管理フレームの全体像

重要インフラ情報システムも、情報システムの一種であるので、その信頼性確保のために行える活動は基本的に同じである。たとえば、企画・要件定義あるいは開発の工程であれば、レビュー、テストといった信頼性向上のための方策を適確に実施することである。

しかし、重要インフラ情報システムでは、以下の点が、強く求められていると考えられる。

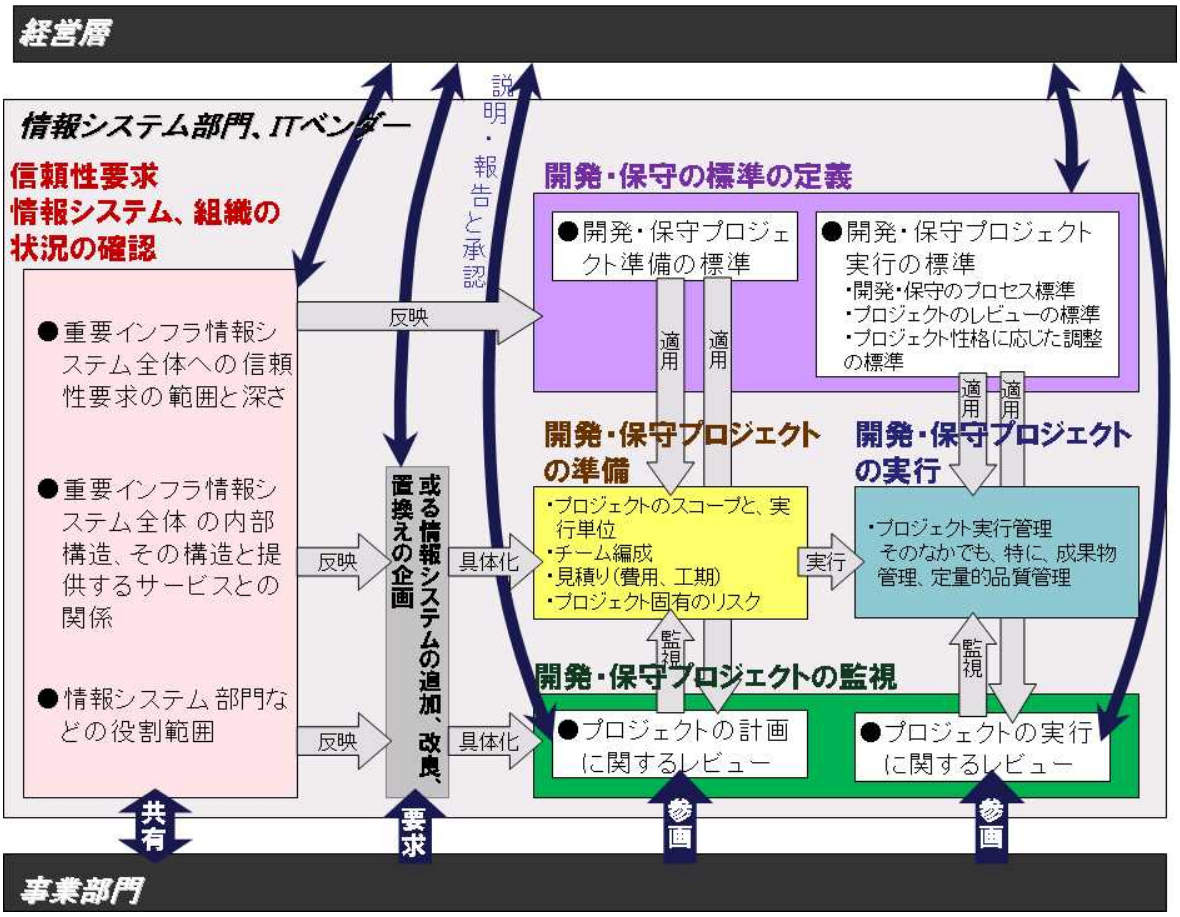
- *重要インフラ情報システムに必要な信頼性は、事業者と利用者である国民との間の重要インフラ・サービスの信頼性についての合意と結び付けて考える必要がある。*

上記を考えると、重要インフラ情報システムにおいては、一般の情報システムと同様に信頼性向上のための方策を適切に計画・実施することに留まらず、その信頼性向上の方策が事業者と利用者の合意を満たすのに有効であることの保証までされる必要がある。
保証までをするためには、以下のような目標となる「信頼性要求」を決め、その実現を確かめる活動が必要になる。

- 何についての信頼性をどの位必要とするのか、といった情報システムへの信頼性要求の明確化。さらに情報システムへの信頼性要求に影響する、情報システムの構造や、情報システム部門の役割範囲についての確認
- 情報システムへの信頼性要求を満たすための方法としての、開発・保守のプロセス標準、レビューの標準の定義
- 上項の標準を適用した、情報システムの開発・保守プロジェクトの準備
- 同じく、情報システムの開発・保守プロジェクトの実行
- 情報システムの開発・保守プロジェクトが確実に実施され、その結果、情報システムへの信頼性要求が確保されていることの監視
- 上記の活動を相互に適確に関連づけること

具体的には、図表２－１のような取組みである。
以降、この図表が示す範囲の活動を、重要インフラ情報システムの開発・運用の管理フレーム（以

下、単に「管理フレ―ム」と呼ぶ。）とし、以下の節でその内容を取り扱う。



図表２－１　重要インフラ情報システムの開発・運用の「管理フレーム」

２－２　管理フレームによって実現すべきこと

２－２では、重要インフラ情報システムの信頼性確保の取組みについて求められる基本的な事柄、および「管理フレーム」の意味について説明する。

２－２－１　信頼性確保の取組みの確立

２－１で、重要インフラ情報システムの強く求められている点として、次を述べた。

- *重要インフラ情報システムに必要な信頼性は、事業者と利用者である国民との間の重要インフラ・サービスの信頼性についての合意と結び付けて考える必要がある。*

ここで、各事業者は、以下のことに注意が必要である。

- 事業者と利用者である国民との間の重要インフラ・サービスの信頼性についての合意の内容は、重要インフラ・サービスによって異なっている。
- 重要インフラ・サービスの信頼性を、情報システムで支える方法には様々なものがあり、現行の方法は事業者や業種、過去の経緯により異なっている。
- 情報システムの信頼性に関わる事柄の、自社の情報システム部門、情報システム子会社、外部組織（ＩＴベンダーなど）による役割分担も、事業者によって異なる。

したがって、重要インフラ事業者は、情報システムの信頼性確保に関する他の事業者の取組みを参考にすることは出来ても、それをそのまま実施することが有効とは限らない。
各事業者は、事業内容やそこでの利用者との関係や、情報システムの位置づけや構造といった、事業者固有の状況に適した信頼性確保の取組みを確立することが必要である。
「管理フレーム」は、その信頼性確保の取組みを確立するための道具である。

２－２－２　信頼性を確保し続けること

重要インフラ情報システムは改良、更新、追加されながら数十年の長さにわたって使われる。したがって、重要インフラ情報システムの信頼性も数十年の長さで確保され続ける必要がある。
その間に、重要インフラを取り巻く環境は大きく変わっていくから、以下の３点については適宜見直しが必要である。

- 事業者と利用者（国民）との間の重要インフラ・サービスの信頼性についての合意の内容
- 重要インフラ・サービスの信頼性を、情報システムで支える方法
- 情報システムの信頼性に関わる事柄の、自社の情報システム部門、情報システム子会社、外部組織（ＩＴベンダー等）による役割分担

つまり、信頼性確保の取組みに改善サイクルを回し、「管理フレーム」の内容を描き換えていくことが必要となる。

この改善サイクルにおいて、事業者外の関係者とコミュニケーションをとることによって、その改善の有効性が更に高まることが期待される。そのコミュニケーションとは以下のようなものである。

- 利用者である国民に対する重要インフラ・サービスの信頼性についての実績値や、その改善策の概要説明、それに対する利用者の意見の収集
- 重要インフラ・サービスの信頼性を、情報システムで支える方法についての、同一業種内での知見の共有、異業種間での知見の交換
- 情報システムの信頼性確保の方法についての、外部組織（ＩＴベンダーなど）との協議

２－３　活動フレームとステークホルダー

２－３では、重要インフラ情報システムの信頼性確保の取組みのために、その情報システムのステークホルダーに求められる役割について説明する。
２－３の内容は、重要インフラ事業者で実際行われていることをヒアリングした結果（第４章にて説明）に基づいている。

２－３－１　重要インフラ事業者の情報システム部門、および外部組織

情報システム部門は、情報システムへの信頼性要求を把握、管理し、それを満たす開発・保守を準備、実行し、要求の実現性を確かめ、評価し、評価結果と必要なら対策を取りまとめる必要がある。具体的には、以下の役割が期待される。

期待される役割

(1) 情報システムへの信頼性要求のとりまとめ、管理
(2) 情報システム全体の構造、その提供サービスとの関係の整理
(3) 情報システム部門など情報システムの関係者の役割範囲の整理
(4) 情報システムの信頼性提供の見込みの情報システム関係者への提示
(5) 個別の開発･保守プロジェクトが､情報システムの信頼性提供の見込みを満たすようにする､準備と実行
(6) 個別の開発・保守プロジェクトが、情報システムの信頼性提供の見込みを満たしていることの監視
(7) 情報システムの信頼性の評価
(8) 情報システムの信頼性の評価結果に基づく対策の立案
(9) 情報システムの信頼性の評価結果と対策の提示
(10) 承認された対策の実施

上記は、広範にわたる上、(5)と(6)のように、同じ要員が活動することが適当でないものも含まれるので、情報システム部門の内部での適切な分担が欠かせない。

また、外部組織（ＩＴベンダーなど）には、重要インフラ事業者の情報システム部門との協議の上、以下の役割を代行することが期待される。

期待される役割

※ 以下の項番は、情報システム部門に期待される役割の項番と共通である。

(5) 個別の開発・保守プロジェクトが、情報システムの信頼性提供の見込みを満たすようにする、準備と実行

(6) 個別の開発・保守プロジェクトが、情報システムの信頼性提供の見込みを満たしていることの監視

(7) 情報システムの信頼性の評価

(8) 情報システムの信頼性の評価結果に基づく対策の立案

(9) 情報システムの信頼性の評価結果と対策の提示

(10) 承認された対策の実施

２－３－２ 重要インフラ事業者の事業部門

事業者のうち、情報システムの利用者である事業部門は、主に業務要件[5]レベルで、外部環境を把握して情報システムへの信頼性要求を作り、それが実現される過程をモニターし、実際の信頼性が十分かを評価する必要がある。具体的には、以下の役割が期待される。

期待される役割

(1) 重要インフラ・サービスの信頼性について、主に業務要件レベルでの外部関係者との合意

(2) 上記のうち、情報システムに関係する部分の識別

(3) 情報システムへの、主に業務要件レベルでの信頼性要求のとりまとめ

(4) 情報システムの信頼性提供の見込みの承認

(5) 個別の開発・保守プロジェクトの承認

(6) 個別の開発・保守プロジェクトへの監視への参画

(7) 情報システムの信頼性の評価結果と対策の承認

(8) 重要インフラ・サービスの信頼性について、主に業務要件レベルでの外部関係者への説明

[5] 「業務要件」については、２－３の後の囲み記事に示す。

２－３－３ 重要インフラ事業者の経営層

事業者の経営層は、事業要件[6]レベルで、外部環境を把握して情報システムへの信頼性要求を作り、それが実現される過程をモニターし、実際の信頼性が十分かを評価する必要がある。具体的には、以下の役割が期待される。

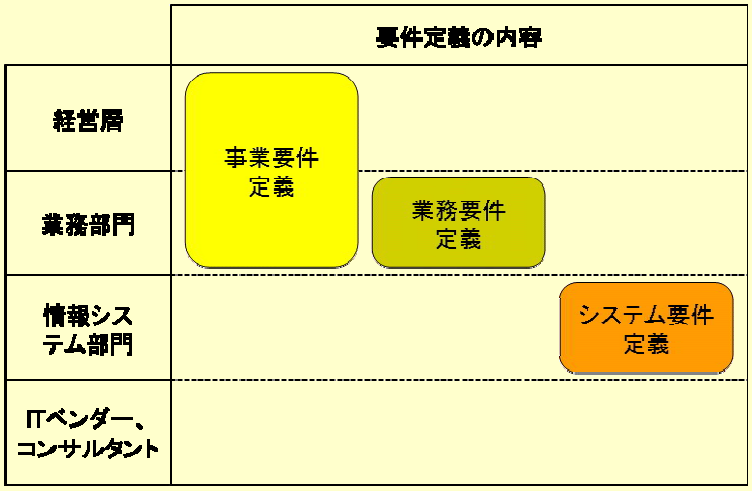
期待される役割

(1) 重要インフラ・サービスの信頼性について、事業要件レベルでの外部関係者との合意
(2) 上記のうち、情報システムに関係する部分の識別
(3) 情報システムへの、事業要件レベルでの信頼性要求のとりまとめ
(4) 情報システムの信頼性提供の見込みの承認
(5) 個別の開発・保守プロジェクトの承認
(6) 個別の開発・保守プロジェクトへの監視への参画
(7) 情報システムの信頼性の評価結果と対策の承認
(8) 重要インフラ・サービスの信頼性について、事業要件レベルでの外部関係者への説明

6 「事業要件」については２－３の後の囲み記事に示す。

コラム 「事業要件」と「業務要件」

事業要件、業務要件については、図表Ｃに示すような役割分担でその定義を行う必要がある。



名　称	項　目	内　容
事業要件定義	ビジネスモデルの検討　等	新規事業／社外連携／組織改編／部門間業務分掌変更／現行業務踏襲、セキュリティなど
業務要件定義	業務モデルの検討　等	業務内容（手順、責任・権限）、業務形態（ピークなど）、業務品質、性能目標、運用、移行要件、セキュリティなど
システム要件定義	システムモデルの検討　等	システム構成、業務アプリケーション（構造、ＤＢ・ファイル構造など）、運用、移行要件、セキュリティ、機密情報保護対策など

図表Ｃ　「事業要件」と「業務要件」

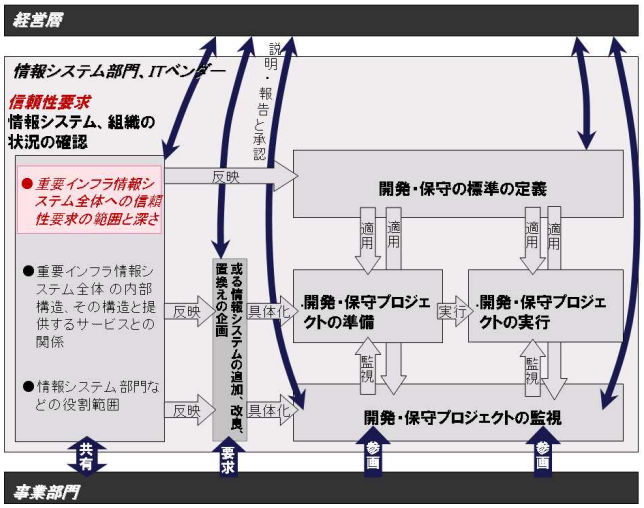
【「経営者が参画する要求品質の確保（第２版）」（IPA/SEC 2006 年 5 月）から抜粋】

２－４　活動フレームの構成要素

２－４では、２－１で示した「管理フレーム」について、その中に含まれる活動要素を１つずつ取り上げる。
２－４の内容は、重要インフラ事業者で実際行われていることをヒアリングした結果（第４章にて説明）に基づいている。

２－４－１　信頼性要求

重要インフラ情報システムが十分な信頼性を確保するためには、最初にその情報システムへの信頼性要求を決定することが必要である。



図表２－２　「管理フレーム」の中の「信頼性要求」

活動要素の目的

- 情報システムに求められる信頼性について、組織としての方針および基準をまとめ、ゴールを明確にする。

活動要素の概要

- 重要インフラ・サービスの信頼性を保つために、それを支える情報システムへの信頼性要求を決める。

実施する観点

- 情報システムへの信頼性要求は、重要インフラ・サービスへの信頼性要求と関連づける。
- 信頼性要求には、守るべきもの（価値）と、それを何からどの程度守るかを含める。

得るべきこと

- 情報システム全体への信頼性要求についての、基本的な考え方

得たことの活用

- 開発・保守の標準を整備する際に、その狙いの形で反映する。
- 個別の情報システムの信頼性に関する要求に反映する。

留 意 点

- 情報システムへの信頼性要求は、事業者内外へのサービスの円滑な提供という面だけでなく、情報システムが扱う情報の保全も含めて検討する。
- また、法制による要求や社会からの期待されることへの対応も含めて検討する。

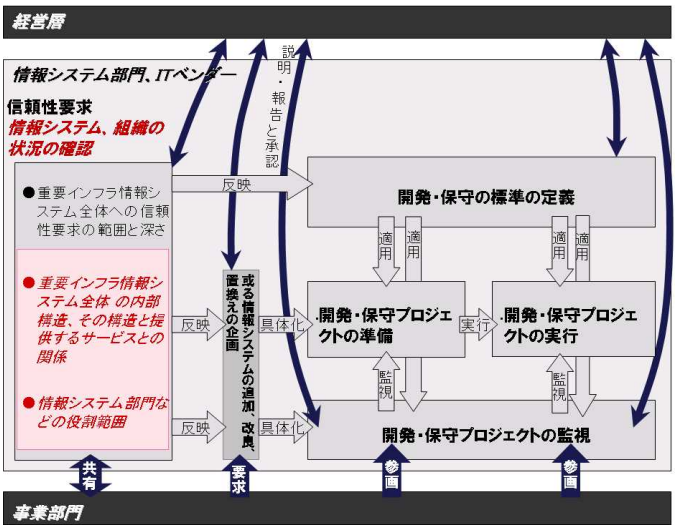
活動要素の実施例

■ Ａ社

情報システムで必要な価値を「情報資産の保護」に置き、これを低下させるリスクを識別した。その中には個人情報保護や金融商品取引法（企業会計報告の適正性の担保）という観点を含めた。

２－４－２ 情報システム、組織の状況の確認

次に、前節の「信頼性要求」をどのような情報システムの構造において実現するか、また、それをどのような組織の役割において実現しようとするか、ということに関する整理が要る。



図表２－３　「管理フレーム」の中の「情報システム、組織の状況の確認」

活動要素の目的

- 情報システムの信頼性についての組織の方針、基準を実現する方策を定める上で、意識すべき制約事項を整理する。

活動要素の概要

- 信頼性確保における制約事項を、以下について確認する。
  －情報システム、ソフトウェアの全体の内容および内部構造
  －情報システム部門などの能力および役割範囲

実施する観点

- 情報システム、ソフトウェアの構造と重要インフラ・サービスとの関係を明らかにする。
- 情報システム部門などの役割範囲から信頼性確保において取組み可能なこと、限界を認識する。

得るべきこと

- 情報システムやそれが提供するサービスを維持、変更する上での制約事項
- 情報システムの開発・保守について、事業者内で実施すること、外部組織（ＩＴベンダーなど）に委託することに関する基本的な考え方

得たことの活用

- 開発・保守の標準を整備する際に、その狙いや前提条件として反映する。
- ＩＴベンダーなどとの交渉、契約にあたっての基本的な考えに反映する。
- 個別の情報システムの信頼性に関する要求に反映する。

活動要素の実施例

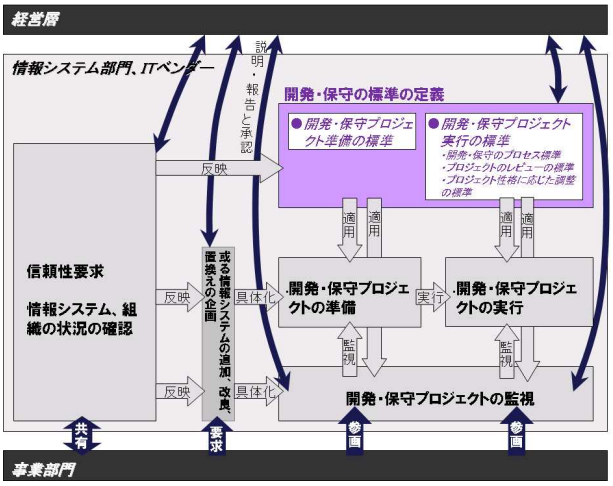
■ Ｂ社

情報システム部門が担っている役割は要件定義までで、以降の開発はＩＴベンダーに委託している。

そこで、情報システムの信頼性向上活動において、まず「上流完璧主義」という考え方を採り、要件定義書の品質を徹底改善した。また、要件定義より先のソフトウェアの開発工程においてＩＴベンダーの責任を明確にした。結合テスト以降の共同レビューにて要件が実現されたかを厳重に確認した。

２－４－３　情報システムの開発･保守の標準の定義

次に、情報システム、ソフトウェアの開発、保守を行うプロジェクトについて実施すべきことを定める。



図表２－４　「管理フレーム」の中の「開発・保守の標準の定義」

活動要素の目的

- 情報システムの信頼性についての組織の方針、基準を実現する方策を、制約事項を踏まえて、情報システムの開発・保守プロジェクトにおいて守るべきルールとして具体化する。

２－４－３－１　開発･保守プロジェクトの準備の標準

活動要素の概要

個別の情報システムの信頼性確保に必要なプロジェクトの準備の方法を定める。

実施する観点

- 個別の情報システムのどのような性格、位置づけを重視するかを明確にする。
- 上記に応じて、プロジェクトと準備する方法を示す。
- また、個別のプロジェクトに固有なリスクを認識し、それに対処する方法を示す。
- 標準の適用の例外を取り扱う方法を示す。
- プロジェクトの準備をする者の役割と権限を明確にする。（情報システムを利用する事業部門や経営層の役割を含む。）

得るべきこと

- 開発・保守プロジェクトの準備の方式

得たことの活用

- 開発・保守プロジェクトの準備、実行において適用する。

留 意 点

- 情報システムの信頼性確保を行い易くする１つの方法は、過去の似たプロジェクトを探して、それを再現することである。

活動要素の実施例

■ ＩＰＡ／ＳＥＣ

情報システムの重要度、性格に応じた「タイプ」の定義の仕方について１つの案を提示している。この「タイプ」を用いて開発・保守を行う情報システムを分類することで、類似の開発・保守プロジェクトの実施例を参照しながら、プロジェクトの準備が実施できるようになる。（その詳細を２－４－３－１の後の囲み記事に示す。）

■ Ａ社

ＩＰＡ／ＳＥＣが定義したものに近い「タイプ」を用い、社内の情報システムを区分している。（但し、情報システムの重要度に加え、情報システムの利用が社内に閉じているか否かで「タイプ」を区分しているところが、ＩＰＡ／ＳＥＣの案とは異なる。）

個別の開発・保守プロジェクトでリスクが大きいものについては１つ上の重要度をもつ情報システムと同等に扱うと決めている。

■ Ｂ社

ＩＰＡ／ＳＥＣが定義したものに近い「タイプ」を用い、社内の情報システムを区分している。（但し、情報システムの重要度に加え、情報システムの利用が社内に閉じているか否かで「タイプ」を区分しているところが、ＩＰＡ／ＳＥＣの案とは異なる。）

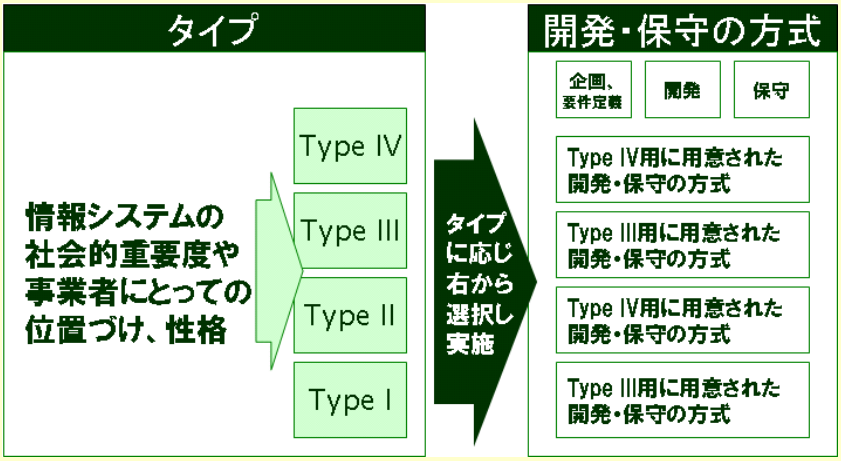
過去に実施した大規模の情報システムでは、プロジェクトを複数のサブ・プロジェクトに分割し、１つのサブ・プロジェクトで「タイプ」に対する開発・保守プロジェクトの準備、実行の内容妥当性を検証したのち、他のサブ・プロジェクトにそれを適用した。

コラム　情報システムの重要度、性格に応じた「タイプ」

２－４に述べたように、重要インフラ情報システムが十分な信頼性を確保するためには、最初にその情報システムへの信頼性要求を決定することが必要である。
そのなかでは、その信頼性要求に応じた方策を講じることが必要になる。

このとき、以下の進め方ができると、個別の情報システムの扱いがやり易くなる。（図表Ｄ）

１．情報システムに求められる信頼性要求を類型化して「タイプ」に区分する方法を予め決めておく。
２．各「タイプ」に対して、開発・保守プロジェクトにて実施する方式（プロセス、手法など）も予め決めておく。
３．個別の情報システムを１．の方法で「タイプ」に区分し、２．に応じて開発・保守の方式を選択する。



図表Ｄ　情報システムの「タイプ」に応じた開発・保守の実施方式の選択のイメージ

上記の１．については、信頼性要求に関して同じ扱いをしてよい情報システムを区分する方法を考えることが必要である。

重要インフラ事業者の取組みをヒアリングした結果（４－１にて説明）では、「タイプ」を以下のような要素を加味して決定していた。

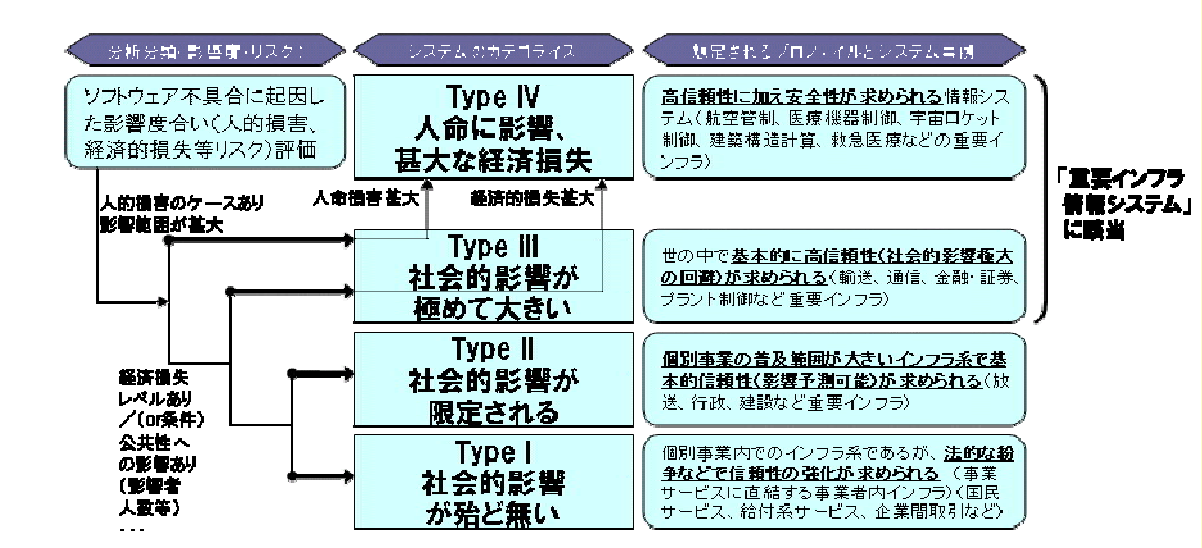
１）取り扱う情報システムの社会的な重要度
　その情報システムに障害が発生したときの、社会的影響（国民生活や社会経済活動への影響）、人命への影響といった観点

２）取り扱う情報システムの事業者にとっての位置づけ、性格
その情報システムが誰にどの様に使用されているか。その結果、その情報システムに障害が発生したときの、利用者の業務やステークホルダーの心証に与える影響などの観点
３）その情報システムの企画、要件定義、開発、保守におけるプロジェクトに固有のリスク

なお、上記のうち１）と２）に関しては、事業者と利用者である国民との間の重要インフラ・サービスの信頼性の合意に基づき、それを情報システム全体の構造でどのように実現するか、個別の情報システムにどのように負わせるか、を踏まえて考える必要がある。

「タイプ」は、個別の情報システムを適確に区分できるように定義した方が良いが、一方で多くの「タイプ」を定義すれば、２．の「タイプ」に応じて予め決めておく開発・保守プロジェクトのプロセスが煩雑になる。タイプの数は４つ前後が妥当であろう。

ＩＰＡ／ＳＥＣが、図表Ｄにおいて「１）取り扱う情報システムの社会的な重要度」に着目して、情報システムの「タイプ」を定義した例が図表Ｅである。この図表での「タイプ」の定義は、情報システムに障害が発生したときの社会への①の経済的な影響、②公共性の影響、③人命への影響を合わせて考えるようにしている。また、情報システムの「タイプ」はその「信頼性要求水準」をそのまま表すものとしている。



図表Ｅ　情報システムの「社会的な重要度」に着目した「タイプ」の定義例

２－４－３－２　開発･保守プロジェクトのプロセスの標準

活動要素の概要

- 個別の情報システムの信頼性確保に必要なプロジェクト内のプロセスを決める方法を定める。

実施する観点

- 個別の情報システムのどのような性格、位置づけを重視するかを明確にする。
- 上記に応じて、プロジェクト内のプロセス（特に、プロジェクト内で実施するテスト、レビューの実施方法や密度）を選択、調整する方法を示す。
- 過去の同様なプロジェクトにおける定量的な品質管理の結果を利用する方法を含める。
- プロジェクトを実施する者の役割と権限を明確にする。（情報システムを利用する事業部門や経営層の役割を含む。）

得るべきこと

- 開発・保守プロジェクトの準備におけるプロジェクト内プロセスを決める方式

得たことの活用

- 開発・保守プロジェクトの準備、実行において適用する。

留 意 点

- 定めたプロセスの有効性、十分さを確かめるには、品質指標を用いた管理が不可欠である。
- プロジェクト内のプロセスについて、標準を守ることの重要性をプロジェクトに働きかける。その方法の１つとしてはプロジェクトデータを事業者内で収集・共有し、標準の有効性を確認する方法がある。

活動要素の実施例

■　ＩＰＡ／ＳＥＣ

２－４－３－１で述べた「タイプ」に応じて、事業者が開発・運用プロセスで、どのような品質指標をどのような基準値とともに使用しているかを、調査した。その詳細を**付録【１】ソフトウェアの品質管理に用いる指標と基準値**に示す。

■　Ａ社

「タイプ」によらず、１種類の開発・保守プロセスを規定している。また、プロジェクト固有の性格に応じて開発・保守プロジェクトの内容を調整するルールを策定中である。

■　Ｂ社

「タイプ」に応じた、複数の開発・保守プロセスを規定している。また、プロジェクト固有の性格に応じて、開発・保守プロジェクトについての、レビュー会議の持ち方を変えるルールがある。

２－４－３－３　開発･保守プロジェクトの監視の標準

活動要素の概要

- 個別の情報システムの信頼性確保に必要なプロジェクト外からの監視の仕方を決める方法を定める。

実施する観点

- 個別の情報システムのどのような性格、位置づけを重視するかを明確にする。
- 上記に応じて、プロジェクト外からの監視（手法、タイミング、体制）を選択、調整する方法を示す。
- 監視をする者の役割と権限を明確にする。（情報システムの利用者である事業部門や経営層の役割を含む。）
- 品質保証の専任者を置き、プロジェクト外から監視する者に含めることを検討する。

得るべきこと

- 開発・保守プロジェクトの準備におけるプロジェクト外からの監視を決める方式

得たことの活用

- 開発・保守プロジェクトの準備、監視において適用する。

留 意 点

- 開発・保守プロジェクトの監視にかけられるリソースは、プロジェクトのリソース以上に制約がある場合が多い。したがって、複数プロジェクトに対する適切な配分を意識する。
- その上で、更に監視の実効性を挙げるために、プロジェクトと監視する者との間で牽制関係の構築、維持に注目する。
- 監視の専任者に必要な資質をどのように選抜または育成し、どのように役割・権限を与えるかについて検討する。
- 情報システムのオーナー、利用部門による監視が安定的に行えるようにするため、教育などのプログラムを整備する。

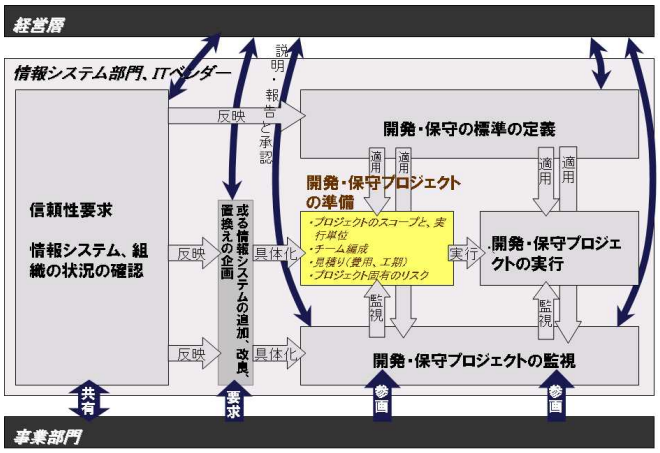
活動要素の実施例

■　Ａ社

情報システムの「タイプ」に応じた、監視の仕方（監視に参画する職位、レビューなどの監視の形式、タイミングと会議体、使用するツールを含む）を定義している。また、品質保証の責任部門を定義し、責任者を配置している。監視に参加する情報システムの利用部門向けの教育、テストの内容を策定し実行している。

２－４－４ 開発･保守プロジェクトの準備

情報システム、ソフトウェアの開発、保守に際し、個別のプロジェクトでのやり方を定める。



図表２－５　「管理フレーム」の中の「開発・保守プロジェクトの準備」

活動要素の概要

● 個別の開発・保守プロジェクトにおいて、「情報システムの開発・保守の標準」を用いて、プロジェクト内のプロセスや方策を決定する。

実施する観点

● 適切にプロジェクトを準備する。

（＊本項は、ＩＰＡ／ＳＥＣの既存図書[7]に詳しいので、本書では省略する。）

得るべきこと

● そのプロジェクトによって以下がどう維持または改善されるのかを目論見の作成と関係者との共有

－情報システム、ソフトウェアの全体の構造、その複雑さ

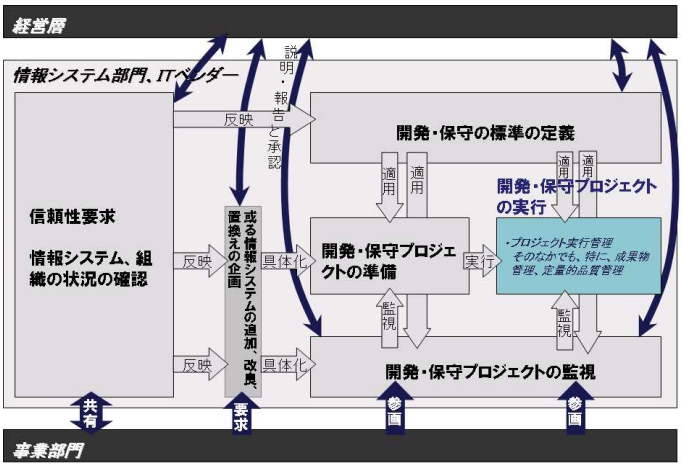
－情報システム、ソフトウェアの構造と提供サービスとの関係

－情報システム、ソフトウェア、提供サービスの信頼性

[7] 既存図書は、３－２に挙げている。

２－４－５ 開発･保守プロジェクトの実行

２－４－４のプロジェクトの準備に基づき、これを実行する。



図表２－６　「管理フレーム」の中の「開発・保守プロジェクトの実行」

活動要素の概要

- 準備に基づいて、適切に開発・保守プロジェクトを実行する。

実施する観点

- 適切にプロジェクトを実行する。

（＊本項は、ＩＰＡ／ＳＥＣの既存図書[8]に詳しいので、本書では省略する。）

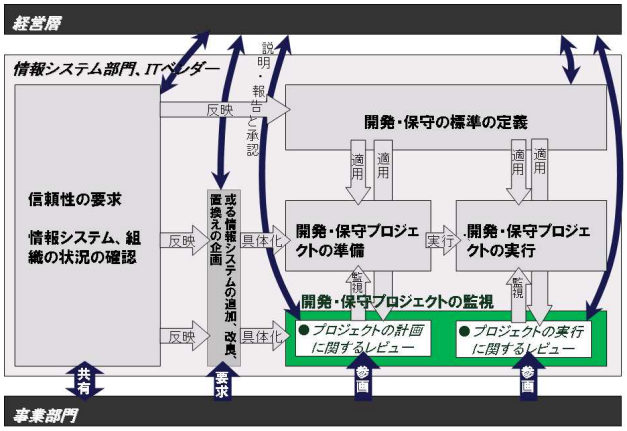
得るべきこと

- 上記によって、開発・保守プロジェクトの準備の際の目論見が達成できる見込みであることの確からしさ

２－４－６ 開発･保守プロジェクトの監視

２－４－５のプロジェクトの実行に際して、プロジェクト外からこの監視を行う。

[8] 既存図書は、３－２に挙げている。



図表２－７　「管理フレーム」の中の「開発・保守プロジェクトの監視」

活動要素の目的

- 個別の情報システムの開発・保守プロジェクトにおいて、情報システムの開発・保守の標準が守られ、情報システムの信頼性についての基準が満たされていることを確認する。

活動要素の概要

- 準備に基づいて、適切に開発・保守プロジェクトをプロジェクト外から監視する。

実施する観点

- プロジェクトの監視を適切に実行する。
- テスト、レビューを確実に実施することだけでなく、それらの実施の有効性を確認する仕掛けを作る。
- そのために、事業者内の関係者に加え、必要なら事業者外の組織に監視への参加を要請することを検討する。

得るべきこと

- 開発・保守プロジェクトの実行における、プロジェクトと監視する者の間の牽制関係を機能させること
- それによって開発・保守プロジェクト内のプロセスの有効性を高めること
- 上記によって、左の目論見が達成できる見込みであることの確からしさを確認すること

留 意 点

- 牽制関係は、開発・保守プロジェクトを実施する上の関係であり、そこに個人や組織の利害が混じらないように配慮する。
- 監視する者の意見や分析結果が、プロジェクト実行の確実さにつながる仕掛け作りや雰囲気の醸成に注意を払う。

活動要素の実施例

■ Ｂ社

大規模システムの開発において、事業者内、ＩＴベンダーの実務者、責任者、社外の有識者を含んだ共同レビュー体制を整備し、機能させた。

その共同レビューで承認が得られなければ次工程に進めない決まりとした。

２－４－７ 開発･保守の継続的な改善

２－４－１から２－４－６の活動をしたことによる、情報システムの信頼性確保の有効性を評価し、必要な改善を施す。

活動要素の目的

- 情報システム全体において、情報システムの開発・保守の標準により、情報システムの信頼性についての組織の方針、基準が実現されていることを検証する。

活動要素の概要

- 開発・保守プロジェクトの実行の結果、情報システムが２－４－１の信頼性要求を満たしているか確認する。
- 必要があれば、２－４－２から２－４－６で、開発保守の標準やその個別プロジェクトへの適用方法に関する対策を講じる。

実施する観点

- 情報システムの信頼性を評価する視点、方法を明確にする。
- その信頼性の評価結果により、必要な対策を優先順位とともに計画し、実施する。
- 即座に解決が図れない問題については継続的に追跡する。
- 情報システムの信頼性が悪化したという結果だけでなく、悪化する可能性も管理する。
- 事業者の外部環境の変化にも目を向ける。

得るべきこと

- 信頼性の評価結果
- 評価結果に基づく対策

得たことの活用

- 信頼性要求の見直し
- 情報システムの構造や情報システム部門の役割の見直し
- 情報システムの開発・保守の標準の改善（定量的な品質管理の実施方法を含む。）

留 意 点

- 信頼性の評価方法、評価結果、その対策は、事業者内で適切に共有する。
- そのうち、適切な内容を事業者外の関係者に公開する方法を検討し、実施する。

活動要素の実施例

■ ＩＰＡ／ＳＥＣ

2005 年～2008 年に発生し、メディアで報道された情報システムの障害事例（119 件）の情報を収集し、情報システム有識者により、その障害原因の推定、再発防止策をたて、信頼性向上対策として取りまとめた。その詳細を**付録【２】障害事例分析と障害再発防止策**に示す。

■ Ａ社

情報システムの障害が、事業部門、社外利用者に与えた影響を測る「トラブル影響度」という評価指標を定義し、その測定結果を評価し、必要ごとに対策を立案している。また、半期ごとにこの「トラブル影響度」を含む信頼性の状況と対策に関しての、経営層、事業部門を含む事業者内での共有を行う場を持っている。

第3章　信頼性確保の取組みに利用できる手法、ツール

第２章で述べた、重要インフラ事業者に必要な取組みを再整理すると次のようになる。

１．情報システムへの信頼性要求を定める。
　重要インフラ情報システムにとって、どのような信頼性がどれだけ必要なのかということを検討し、定めること
２．信頼性の確保に必要な活動（プロセスや方策）を定める。
　情報システム部門の役割範囲や、重要インフラ情報システムと重要インフラ・サービスとの関係に合わせて、その信頼性を確保するプロセス、方策を定義し、実施すること
３．信頼性の確保を監視、検証する。
　２．を実施した結果、１．の信頼性要求が満たされたか確認すること

本章では上記を行うにあたり、重要インフラ事業者を含む重要インフラ情報システムの関係者にとって有用と思われる手法、ツールを紹介する。

3－1　信頼性要求を定める際に利用できる手法、ツール

ここで必要になるのは、信頼性を確保するにはどんな活動が必要なのか、どのような信頼性を損なうリスクを想定するべきなのか、という情報である。
既に事業者は、情報システムの信頼性確保のために、さまざまな活動を行っている。信頼性確保に関するベストプラクティスなどの情報は、その十分さを確認するに大きな手がかりとなる。
また、事業者は過去に情報システムに発生した障害等信頼性低下が発生した際の情報を蓄積しているであろう。そのような情報も、情報システムに必要な信頼性を考える上で重要である。
但し、過去発生した信頼性低下の原因に関する情報から、将来の信頼性低下を引き起こす原因全てを予想することはできないので、上述のような事業者内に蓄積された情報と、情報システムの信頼性を損なうリスクを取り扱った情報を併せて活用することにより、どのような事態に対する備えが必要なのかを更に幅広く考えられるようになる。
以下に、信頼性確保に必要な活動、および信頼性を損なうリスクを取り扱った既存の手法、ツールを挙げる。

名称	COBIT Ver4
発行者	情報システムコントロール協会（米国 ISACA） 日本語版は、日本ＩＴガバナンス協会（以下、「ITGI Japan」）
発行形態	PDF 文書
入手先（日本語）	ITGI Japan の Web サイト
概要	情報システムの管理についてのベストプラクティスである。 管理に必要な、「計画と組織」、「調達と開発」、「運用と支援」、「モニタリング」の４分類、３４のプロセスを示している。 また、各プロセスについて、成熟度の向上、業務や結果の測定に役立つ情報を提供している。

名称	システム管理基準
発行者	経済産業省
発行形態	PDF 文書(2004 年 10 月)
入手先（日本語）	経済産業省　商務情報政策局　情報セキュリティ政策室の Web サイト
概要	情報システムの管理において、事業者が整備・運用すべき管理項目（コントロール）を「情報戦略」、「企画業務」、「開発業務」、「運用業務」、「保守業務」、「共通業務」の６分類、２８７項目示している。 姉妹編である「システム監査基準」を用いて、監査を行う場合には、監査人がその判断の尺度として用いる基準となる。

名称	情報セキュリティ管理基準
発行者	経済産業省　商務情報政策局　情報セキュリティ政策室
発行形態	PDF 文書（2009 年 2 月）
入手先	経済産業省　商務情報政策局　情報セキュリティ政策室の Web サイト
概要	情報セキュリティマネジメントの計画、実行、点検、処置に必要な実施事項を定めた「マネジメント基準」と、組織における情報セキュリティマネジメントの確立段階において、リスク対応方針に従って管理策を選択する際の選択肢となる「管理策基準」を示している。

上記の他に、事業者の情報システムの信頼性要求のスコープによっては、個人情報保護に関する

法令[9]、企業の会計報告の適正性に関する法令[10]、業界における情報システムの安全基準[11]なども参照すべき情報になる。

[9]「個人情報保護法」がこれにあたる。
[10] 「金融商品取引法」の中の企業会計の扱いに関する部分である。同法は「日本版ＳＯＸ法」と称されることがある。この法令に関してＩＴ統制（ＩＴ業務処理統制、ＩＴ全般統制）に関する情報も参照する必要がある。
[11] 金融事業者における例としては、(財)金融情報システムセンター（ＦＩＳＣ）が発行する、「金融機関等コンピュータシステムの安全対策基準・解説書」が挙げられる。

３－２　プロセス、方策を定める際に利用できる手法、ツール

情報システムへの信頼性要求を明らかにしたら、次はそれを十分満たすプロセスや方策を定め、実施する必要がある。
ソフトウェアの構築、運用という面から見れば、①誤りや漏れのない要件定義、②誤りや漏れを作り込まない、下流に持ち込まない開発、③誤りや漏れをおかさない運用や保守、という言い方になる。
そのためにどのようなことを行い、そこでどのよう表現形式を用い、どのような問題有無の観察をするべきかについては多数の情報が提供されている。

以降に各種の手法、ツールを挙げ、そのうち、特に重要なものについては詳細に説明する。

主に企画・要件定義の工程向け

名称	**「経営者が参画する要求品質の確保　～超上流から攻めるIT化の勘どころ～　第2版」**
発行者	ＩＰＡ／ＳＥＣ
発行形態	PDF 文書および図書（2006 年 5 月）
入手先	ＩＰＡ／ＳＥＣの Web サイト（PDF 文書）、図書購入サイトへのリンク有
概要	情報システムの要求品質の確保のために、経営者や利用部門などの事業者内の各位が、どのような観点、考え方をもって情報システムの企画・要件定義に関与すべきかを説明している。
重要インフラにおけるポイント	重要インフラ情報システムでは、役割分担とそれに基づく作業分担の取り決めが一層重要である。役割分担の考え方について基本的なことを理解するのに役立つ。

■「経営者が参画する要求品質の確保　～超上流から攻めるＩＴ化の勘どころ～　第２版」
３－２の前文で、情報システムの信頼性を確保するためには、各工程での漏れや誤りを防ぐことが重要であることに触れた。
しかし、この漏れや誤りの原因を遡っていくと、構築、運営される情報システムについての関係者の役割分担についての取り決めの不足や認識の齟齬がその根底にあることが多い。
この図書および次の図書では、昨今の情報システムに関する動向がどのようにその品質に影を落としているか、またそのような環境で事業者の経営層、情報システム部門、利用部門及び外部組織（ＩＴベンダー等）はどのような役割、責任を負うべきか、その役割、責任に応じ企画や要件定義の工程では何を行うべきか、を１７ヶ条の原理原則として説明している。

名称	**「実務に活かすIT化の原理原則17ヶ条 ～プロジェクトを成功に導く超上流の勘どころ～」**
発行者	ＩＰＡ／ＳＥＣ
発行形態	PDF 文書および図書（2010 年 10 月）
入手先	ＩＰＡ／ＳＥＣの Web サイト（PDF 文書）、図書購入サイトへのリンク有
概要	情報システムの要求品質の確保のために、要件定義などの超上流の工程に焦点を当て、発注者と受注者が守るべき考え方と行動規範を示すとともに、原理原則に関する失敗事例、成功事例を紹介している。
重要インフラにおけるポイント	「経営者が参画する要求品質の確保　～超上流から攻めるＩＴ化の勘どころ～第２版」と同様に、重要インフラ情報システムの関係者の役割の考え方について基本的なことを理解するのに役立つ。

■「実務に活かすＩＴ化の原理原則１７ヶ条
～プロジェクトを成功に導く超上流の勘どころ～」

前項で取り上げた“１７ヶ条の原理原則”について、プロジェクトのどのようなシーン、状況において重要となるのか、失敗事例や成功事例をひきながら、具体的な説明をしている。

名称	**「機能要件の合意形成ガイド」**
発行者	ＩＰＡ／ＳＥＣ
発行形態	PDF 文書
入手先	ＩＰＡ／ＳＥＣの Web サイト
概要	機能要件に着目して、情報システムの発注者と開発者の間に生じる認識の違いを克服するコツを扱っている。 システム振舞い、画面、データモデルなどの技術領域ごとのコツに加えて、合意形成を深める作業やコミュニケーションの方法についても説明している。

名称	「非機能要求グレード」[12]
発行者	ＩＰＡ／ＳＥＣ
発行形態	PDF 文書およびスプレッドシート
入手先	ＩＰＡ／ＳＥＣの Web サイト
概要	情報システムの非機能要件[13]を、漏れなく定義し、また要件の項目間でバランスをとるのに有用な方法を示している。 情報システムの企画及び要件定義の工程にて、この手法を用いることによって、非機能要件の的確な取扱いが期待できる。
重要インフラにおけるポイント	重要インフラ情報システムでは、期待される高い「信頼性要求水準」に照らして、適切な非機能要求グレードを選択すること、また、要求、要件の定義漏れによる問題を発生させることを防ぐ手段として、本情報を活用することが重要である。

■「非機能要求グレード」

情報システムに対する要求・要件には２種類ある。一つは、「機能要求」（ないし、「機能要件」。以下同じ。）と呼ばれ、情報システムによって業務を実施する上で必要な機能に関するもの、もう一つは、「非機能要求」（ないし、「非機能要件」。以下同じ。）と呼ばれ、例えば「障害発生、復旧にかけることを許す最大時間」など、「機能要求」以外の性能や拡張性、信頼性、セキュリティなどに関わる要求である。

「非機能要求」は、情報システム基盤、およびアプリケーション・ソフトウェアと情報システム基盤との関係に大きく影響する。

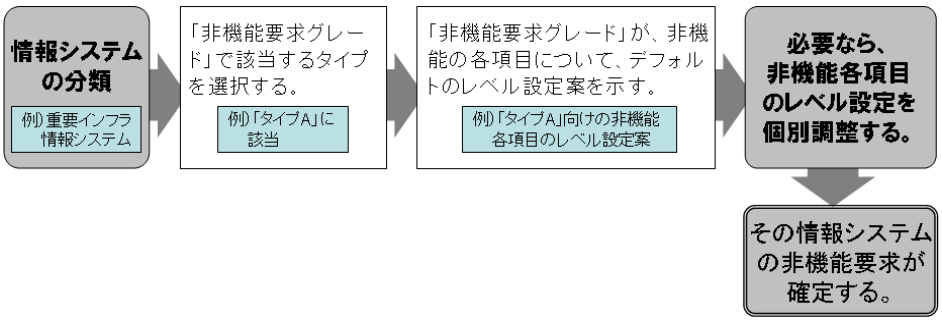
要求・要件のうち、「機能要求」は情報システムが提供するサービスに強く関係するため、利用者を含む情報システムの関係者の関心も高いが、「非機能要求」には情報システムが正常の時には意識しなくて済むもの、また利用者がイメージしにくいものも含まれるため、その要求・要件の決定やチェックで漏れや誤りが発生しやすい。

非機能要求グレードは、最重要の「非機能要求」の範囲を示すとともに、「グレード」という考え方で「非機能要求」項目間でバランスのとれた要求のセットを提供し、それを選択することで要求・要件を決める方法をも示している。（図表３－１）

この「非機能要求グレード」を要件定義、及び情報システムの調達者・供給者の間の情報共有の手段として使用することが、適切な信頼性を有する情報システムを構築し、その安定的な運用を実施することの大きな助けとなると考えられる。

[12] 非機能要求グレードは、NTT データ、富士通、日本電気、日立製作所、三菱電機インフォメーションシステムズ、沖電気工業（順不同）の６社により共同策定された後、2010 年に IPA/SEC に移管された。

[13] 非機能要求ないし非機能要件とは、情報システムの性能、拡張性、セキュリティなどの機能要求ないし機能要件以外の要求、要件の全般を指す。



図表３－１　「非機能要求グレード」を用いた、情報システムの非機能要求の決定への流れ

名称	**「ITプロジェクトの「見える化」 上流工程編」**
発行者	ＩＰＡ／ＳＥＣ
発行形態	PDF 文書および図書（2007 年 5 月）
入手先	ＩＰＡ／ＳＥＣの Web サイト（PDF 文書）、図書購入サイトへのリンク有
概要	プロジェクト運営の経験から、主に要件定義の工程における、プロジェクトの「危機」の兆候を「見える化」する方法を説明している。

主に開発、保守の工程向け

名称	**「高信頼化ソフトウェアのための開発手法ガイドブック　　－予防と検証の事例を中心にー」**
発行者	ＩＰＡ／ＳＥＣ
発行形態	図書（2011 年 4 月予定）
入手先	ＩＰＡ／ＳＥＣの Web サイトに図書購入サイトへのリンク有
概要	ソフトウェアの高信頼化のために、その品質保証活動（予防活動と検知活動）に関わる手法、技法の一般的事項および心得について説明している。

■「高信頼化ソフトウェアのための開発手法ガイドブック
－予防と検証の事例を中心にー」

ソフトウェアの高信頼化のために必要な品質保証活動（予防活動と検知活動）について、ソフトウェアの開発・保守プロジェクトで用いることができる手法、組織的改善の中で実施できる方策について説明している。

説明している事項は、以下である。

- 開発・保守プロジェクトにて、品質管理の実効性、効率性を向上するための各種のツールや技法（テストやレビューの実施方式など）
- 組織において、障害事例を予防活動に反映する方法（障害分析と対策立案の方法、品質特性を追求する方法）
- 開発方式を高度化する方法（要件やソフトウェア部品を追跡する方法、テストを高度化し網羅性をあげる方法など）

あわせて、ソフトウェア開発を自ら行っているユーザー企業、ベンダー企業の組織的取組み事例を７例取り上げ、各事業者がそれぞれの背景や課題意識の下、それぞれの組織的活動、体制整備を実施し、どのような結果を得たかについて紹介している。

これらは、第２章の「管理フレーム」の「開発・保守プロジェクトのプロセスの標準」において、その内容を規定したり見直したりする際に非常に有用であるが、もっと重要なのは、「開発・保守プロジェクトの継続的な改善」で活用することである。
すなわち、情報システムの信頼性確保について、その目標と実績に差異が発生したとき（典型的には障害の発生、またはその可能性があったとき）に、その事案を分析し、それを再発させない方法、再発の可能性を検知する方法として対策にまとめ、標準などの規定事項やその個別プロジェクトへの適用方法の修正を図る、ということである。（図表３－２）

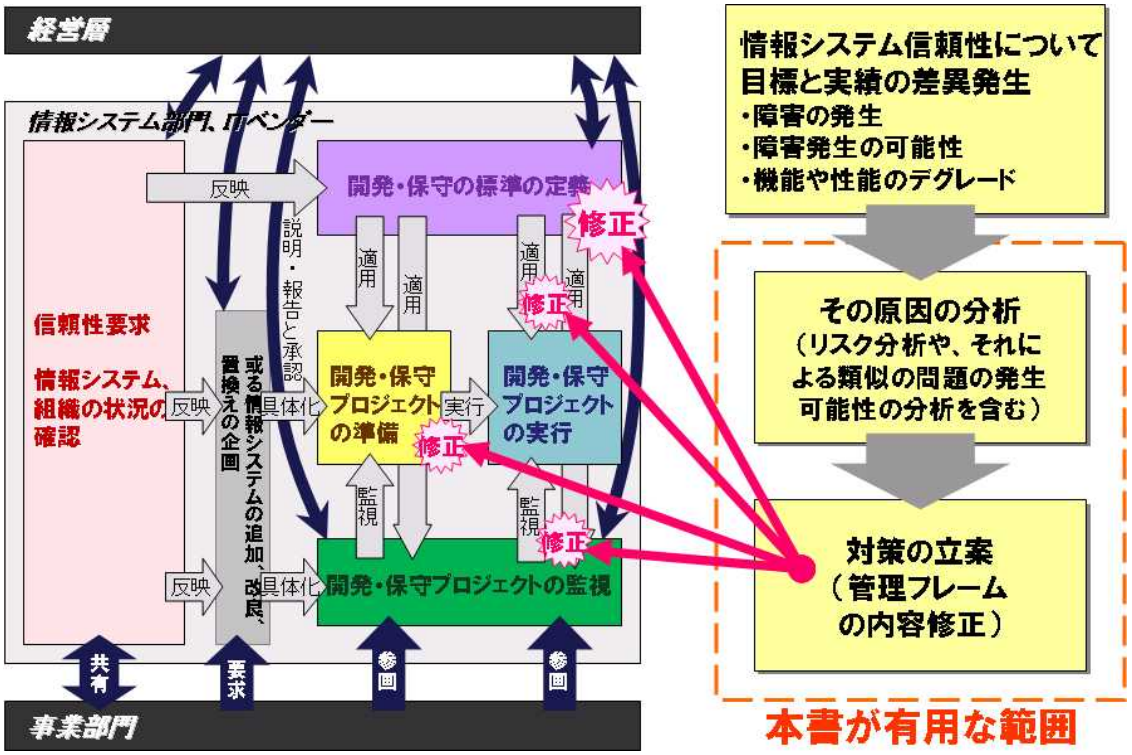


図３－２　「高信頼化ソフトウェアのための開発手法ガイドブック」を用いた、「管理フレーム」の内容修正のイメージ

名称	「ソフトウェア開発見積りガイドブック　～ITユーザとベンダにおける定量的見積りの実現」
発行者	ＩＰＡ／ＳＥＣ
発行形態	PDF 文書および図書（2006 年 4 月）
入手先	ＩＰＡ／ＳＥＣの Web サイト（PDF 文書）、図書購入サイトへのリンク有
概要	情報システム、ソフトウェアの開発の見積りについて、具体的な方法、ノウハウを紹介している。 その中で、調達者（ベンダー企業など）と供給者（ユーザー企業など）が見積りについて互いに納得できるようにするための方法、また、プロジェクト・組織が見積り能力を向上させる方法を説明している。

名称	「ソフトウェア改良開発見積りガイドブック　～既存システムがある場合の開発～」
発行者	ＩＰＡ／ＳＥＣ
発行形態	PDF 文書および図書（2007 年 10 月）
入手先	ＩＰＡ／ＳＥＣの Web サイト（PDF 文書）、図書購入サイトへのリンク有
概要	上記の図書による開発の見積りの続編として、改良開発の見積りについて、具体的な実施方法を紹介している。

名称	「ソフトウェアテスト見積りガイドブック　～品質要件に応じた見積とは～」
発行者	ＩＰＡ／ＳＥＣ
発行形態	PDF 文書および図書（2008 年 9 月）
入手先	ＩＰＡ／ＳＥＣの Web サイト（PDF 文書）、図書購入サイトへのリンク有
概要	上記の２つの図書を補完するものとして、ソフトウェアの品質検証と妥当性確認に関わるテストの見積り（テスト量、テスト生産性）について、具体的な実施方法を紹介している。

名称	「定量的品質予測のススメ　－ITシステム開発における品質予測の実践的アプローチ」
発行者	ＩＰＡ／ＳＥＣ
発行形態	PDF 文書および図書（2008 年 10 月）
入手先	ＩＰＡ／ＳＥＣの Web サイト（PDF 文書）、図書購入サイトへのリンク有
概要	情報システムの開発工程における、ソフトウェアの品質予測についてのアプローチや事例を収めている。プロダクトの品質とプロジェクトの品質の２つの面から品質予測の方法を示している。

名称	「ソフトウェア開発データ白書2010－2011」
発行者	ＩＰＡ／ＳＥＣ
発行形態	図書（2010 年 12 月）
入手先	ＩＰＡ／ＳＥＣの Web サイトに図書購入サイトへのリンク有
概要	ソフトウェアの開発プロジェクトのデータ（規模、工期、工数など）を収録したものである。第６冊となる「2010-2011 年版」では、24 社の供給者（ベンダー企業など）から提供があった 2,584 件のプロジェクトデータを収めている。 特に、自社内に過去情報の蓄積がない種類（規模、工期）のソフトウェアの開発を実施することになったときに、定量的管理を実施する上で参考となる情報を得るのに有用である。

名称	「共通フレーム2007　第2版　～経営者、業務部門が参画するシステム開発および取引のために～」
発行者	ＩＰＡ／ＳＥＣ
発行形態	図書（2009 年 10 月）
入手先	ＩＰＡ／ＳＥＣの Web サイトに図書購入サイトへのリンク有
概要	ソフトウェアのライフサイクルプロセスにおける作業項目を定義したものである。 事業者が開発や保守のプロセスを規定する際に参考になるとともに、開発を外部委託した場合の供給者（ベンダー企業など）の開発プロセスを評価する際にも用いることができる。

名称	「ITプロジェクトの「見える化」 中流工程編」
発行者	ＩＰＡ／ＳＥＣ
発行形態	PDF 文書および図書（2008 年 10 月）
入手先	ＩＰＡ／ＳＥＣの Web サイト（PDF 文書）、図書購入サイトへのリンク有
概要	ソフトウェア設計→プログラミング→単体テストまでの開発の工程において、下流工程に品質問題を持ち越さないために必要な管理に関する「見える化」の方法を、実際のプロジェクト運営の経験をもとに説明している。

名称	「ITプロジェクトの「見える化」 下流工程編」
発行者	ＩＰＡ／ＳＥＣ
発行形態	PDF 文書および図書（2006 年 6 月）
入手先	ＩＰＡ／ＳＥＣの Web サイト（PDF 文書）、図書購入サイトへのリンク有
概要	ソフトウェア結合テスト以降の開発の工程で、プロジェクト状況を評価し、発生した問題に適切に対処するための「見える化」の方法を、実際のプロジェクト運営の経験をもとに説明している。

名称	「ITプロジェクトの「見える化」 総集編」
発行者	ＩＰＡ／ＳＥＣ
発行形態	PDF 文書および図書（2008 年 10 月）
入手先	ＩＰＡ／ＳＥＣの Web サイト（PDF 文書）、図書購入サイトへのリンク有
概要	同シリーズの上流工程編、中流工程編、下流工程編を俯瞰し、「見える化」の実施の仕方を説明している。

名称	「高信頼性システム開発技術の動向」
発行者	ＩＰＡ／ＳＥＣ
発行形態	PDF 文書（2010 年 3 月）
入手先	ＩＰＡ／ＳＥＣの Web サイト
概要	ＩＰＡ／ＳＥＣが 2007 年に設置した高信頼性システム技術調査検討会において、「形式手法」について調査、整理した結果をまとめたもので、「形式手法」に関する様々な技法と、「形式手法」を用いた高信頼性システムの構築事例（航空宇宙・原子力・鉄道など）を紹介している。

名称	「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」
発行者	情報システムサービス産業協会（以下、「ＪＩＳＡ」）
発行形態	図書（2008 年 4 月発行）
問い合せ先	ＪＩＳＡ
概要	管理指標を用いた定量的なソフトウェア管理において、主に供給者（ベンダー企業）が管理に用いている情報についての調査結果をまとめたものである。事例情報には開発、保守だけでなく、運用の工程に関するものも含んでおり、それら工程で用いられている管理指標とその背景にある情報システム管理の考え方が収められている。

名称	「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」
発行者	ＪＩＳＡ
発行形態	図書（2009 年 3 月発行)
問い合せ先	ＪＩＳＡ
概要	管理指標を用いた定量的管理において、発注者（ユーザー企業など）と供給者（ベンダー企業など）の間で共有すべき情報や共有方法についての調査結果をまとめたものである。 情報システムの開発や保守の工程の大分部をベンダー企業に依存するユーザー企業に、特に有用である。

名称	「情報システム信頼性向上のための管理指標活用事例集」
発行者	ＪＩＳＡ
発行形態	図書（2011 年 3 月発行)
問い合せ先	ＪＩＳＡ
概要	様々な前提条件の下で実際に管理指標を活用しているマネジメント事例を収集し、管理指標活用上の留意点とともに取りまとめたものである。 事業者が、自らが置かれた状況での管理指標の活用を検討する際に役に立つ。

ライフサイクル全般向け

名称	**「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」**
発行者	情報システム・ユーザー協会（以下、「ＪＵＡＳ」）
発行形態	図書（2010 年 7 月発行）
問い合せ先	ＪＵＡＳ
概要	情報システムの信頼性を維持・向上するために重要な２０カ条を紹介している。 重要インフラ情報システムに発生した過去の障害を分析し、その再発を防止する観点から信頼性の確保のために重要な観点を説明している。 ソフトウェアでなく情報システム全体（ＩＴサービスを含む）の信頼性を確保するための方法について記述しており、２０カ条には「ＣＩＯの役割」「利用部門との関係」といったＩＴガバナンス色の強いものから、「要件定義書の作成」「品質評価」「移行」「情報システムの運用」と、情報システムのライフサイクル全体にわたって重要な点までが含まれている。
重要インフラにおけるポイント	巻末に紹介されているチェックリストを使用すると、情報システムの重要度に応じて２０カ条をどの程度まで実施するべきかについてのＪＵＡＳの推奨を得ることが出来る。

３－３　信頼性を監視、検証するのに有用な手法、ツール

この分野には、重要インフラ事業者が参考にできる情報で、かつ、簡単に閲覧できるもの（図書の形やＷｅｂで提供されているもの）はあまりない。

第２章の重要インフラ事業者へのヒアリングで明らかになった重要なポイントは、以下である。

・信頼性を確保するためのプロセスを実施する組織・人と、そのプロセスを実施した結果十分な信頼性が確保されたかを確認する組織や人との間に牽制関係を作ること。また双方の役割、権限を明確にすること

・信頼性が確保されたか確認すること自体の品質を安定させるために、そのためのスキル定義、スキルを維持するための教育、トレーニング、テストの設定、チェックリストなどのツールの整備を行うこと

3－4 その他、信頼性に関係する手法、ツール

上記の他に、組織、人、プロジェクトが、情報システムの信頼性を確保するために十分な活動を行っているか、大きな漏れはないかを点検するための手法、ツールが提供されている。

名称	**「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」**
発行者	経済産業省　商務情報政策局　情報処理振興課
発行形態	PDF 文書（2009 年 3 月）
入手先	経済産業省の Web サイト
概要	システムライフサイクル全般にわたりユーザー企業とベンダー企業が遵守するべき事項を定めたものである。 信頼性・安全性向上に向けての全般的配慮事項から始まり、企画・要件定義・開発及び保守・運用について、また、技術、人・組織、商習慣･契約に関して守るべきことを説明している。
重要インフラにおけるポイント	末尾の信頼性・安全性の水準に応じた必須・推奨事項の一覧表において、重要インフラ情報システムで遵守すべきことが指定されている。

名称	**「信頼性自己診断ツール」**
発行者	ＩＰＡ／ＳＥＣ
発行形態	ＰＣで利用可能なアプリケーション
入手先	ＩＰＡ／ＳＥＣの Web サイト
概要	上項、「情報システムの信頼性向上に関するガイドライン」を受けて、情報システム利用者（ユーザー側）と情報システム供給者（ベンダー企業）が、該ガイドラインの遵守度合いをそれぞれ測ることを可能とする評価指標が整理された。これが「情報システムの信頼性向上に関する評価指標（第 1 版）」である。 この評価指標に基づき作成されたのが本ツールで、事業者が組織、プロジェクトにおける信頼性確保の取組み状況を入力すると、信頼性・安全性の水準に応じた必須・推奨事項の一覧表との比較により、取組みの強み、弱みが評価、図示される。
重要インフラにおけるポイント	上記の「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」と同様、重要インフラ情報システムなど、情報システムのレベルを加味した取組みの評価を行うことが可能である。

第4章　管理フレームの実施例

ここまで、第２章では事業者が情報システムの信頼性を確保するために必要な取組みを「管理フレーム」という形で説明し、第３章ではその活動要素の詳細を決めるために参考になる情報を紹介した。
次に、本章では、「管理フレーム」の実施の仕方について説明する。
事業者により、情報システムの位置づけなどが大きく異なるため、「管理フレーム」の実施の仕方は唯一つに集約できない。
そこで、本章では、ある事業者の活動の調査結果をもとに、「管理フレーム」の実施例を紹介する。

4－1　管理フレームによる信頼性確保の事例

この節で取り上げるのは、金融事業を営む２事業者に、自らが保有する重要インフラ情報システムの信頼性の管理活動についてヒアリングした結果である。
この２事業者は、自らが保有、運営する重要インフラ情報システムの信頼性を確保し続けることに成功している。また、信頼性確保の取組みの全体像と成功している理由を講演会などで積極的に説明している。

以下の事例から分かるのは、以下のような点である。

1．情報システムへの信頼性要求は、Ａ社、Ｂ社でかなり異なっている。
2．また、情報システムとそれが提供するサービスとの関係、情報システム部門の役割も異なっている。
3．Ａ社、Ｂ社とも、開発・保守で、情報システムの「タイプ」に応じてプロジェクト実行の内容を変えている。但し、変える内容は、Ａ社では開発・保守プロジェクトの監視の仕方、Ｂ社では適用する開発・保守のプロセス標準と開発・保守プロジェクトの監視の仕方の両方である。
4．情報システムの開発・保守への事業部門や経営層の参画の仕方は、Ａ社、Ｂ社で似ている。

つまり、情報システム全体に共通する信頼性に関わる要求、要件はどこから出てくるか。またその要求、要件を個別の情報システムにどのように反映させるか。反映されたことをどのように確認するかが、事業者により異なり、その結果、「管理フレーム」の実施の仕方も異なる。

事例1　金融事業を営むA社

取組み強化のきっかけ

- 金融自由化政策や、同業他社との競争の激化により、取り扱う金融商品の種類が増加した。
- その結果、情報システムによる金融商品の取り扱いも複雑化した。
- それが事業遂行上の課題となり、経営層とも連携して、情報システムの信頼性確保にＡ社[14]全社を挙げて取り組むことになった。

取組みの主要な点

- 「情報資産の保全」を情報システムでの第一優先事項に置き、それを損なうリスクを識別することから、情報システムへの信頼性要求を明確にしている。
- 情報システムの開発・保守では、開発プロジェクトの監視に力を入れた。品質保証責任の部門、担当の役割を明確にするとともに、監視における経営層や事業部門の役割も明確にしている。
  なお、利用者である事業部門に関しては、情報システムのオーナー制度を設けて、情報システムのライフサイクル全般に関して、その責任、役割を明確にしている。

取組みでの特徴的な点

- Ａ社では、情報システムの開発・保守は自社で行っており、標準化の整備等については、取組み強化のきっかけが発生する前から継続的に実施していた。ＩＴが事業経営の重要なインフラであるという認識の下、情報システムの更なる信頼性確保が必要であるという認識から、外部組織（コンサルタント）の協力を得て取組みの強化を進めた。
- 情報システムの信頼性の目標は、情報システムのトラブルが利用者に与える悪い影響すなわち「トラブル影響度」をゼロにすることである。

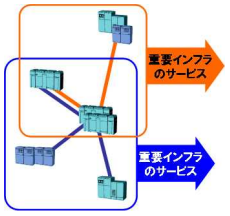
取組みの効果と、今後の展開

- 取組み強化の結果、情報システムの信頼性は大きく改善された。
  さらに、「トラブル影響度」を含む、信頼性の状況がＡ社内で共有されるようになった。
  信頼性における問題については、改善案が立てられ、それが難しいものは問題が継続的にトレースされるようになった。
- 但し、情報システムの信頼性を重視の結果、情報システムの管理のためのコスト増加につながる部分があるため、信頼性とコストの関係を引き続き検討している。
  これには、サービスベンダが提供するＩＴサービスをもＩＴ調達の候補に加えることにより、情報システムの信頼性確保の考え方を変える必要があることも関係している。

---

[14] この事例では、Ａ社とその情報システム子会社を区別することなく、全体をＡ社として扱っている。

取組みの全体を図表４－１に示す。

<table>
<tr><th colspan="3"></th><th>開発の工程</th><th>保守の工程</th></tr>
<tr><td rowspan="5">情報システムへの信頼性要求と情報システム、組織の状況の確定</td><td colspan="2">重要インフラ情報システム全体への信頼性要求</td><td colspan="2">「情報資産の保全」が最優先
契約者などの個人情報を保護する観点、金融商品の契約、売買を企業会計に適切に反映する観点での信頼性を含む。</td></tr>
<tr><td colspan="2">重要インフラ情報システムとそれが提供するサービスとの関係</td><td colspan="2"> 

提供する重要インフラのサービス間で、一部の情報システムが共用されている。情報システムとそれが提供するサービスの関係は比較的複雑。</td></tr>
<tr><td rowspan="3">自社情報システム部門の役割範囲</td><td>要件定義</td><td colspan="2">◎</td></tr>
<tr><td>開発、保守</td><td colspan="2">◎</td></tr>
<tr><td>運用</td><td colspan="2">◎</td></tr>
<tr><td rowspan="4">情報システムの開発･保守の標準の定義</td><td rowspan="4">開発・保守の標準の定義</td><td>情報システムの重要度、位置づけなどに応じた「タイプ」分け</td><td>情報システムの重要度と位置づけ（社外向けか社内業務向けか）により4段階に分類している。これに「リスク」を加味して情報システムの「タイプ」が決まる。</td><td>同左</td></tr>
<tr><td>「タイプ」と信頼性要求水準の関係</td><td>直接関係はしない。全ての情報システムは同一の信頼性要求水準である。</td><td>同左</td></tr>
<tr><td>「タイプ」や信頼性要求水準に応じたプロセス標準</td><td>全ての情報システムが同一の信頼性要求水準である。その水準を満たすための１種類のプロセス標準を定めている。</td><td>同左</td></tr>
<tr><td>「タイプ」や信頼性要求水準に応じたレビューの標準</td><td>「タイプ」に応じてレビュー（工程での境目での工程品質の確認と次工程への移行の可否の判断）に参加する職位を変更する。</td><td>同左</td></tr>
<tr><td rowspan="2">開発･保守プロジェクトの実行</td><td rowspan="2">開発・保守の標準（プロセス標準）の適用</td><td>プロジェクトの性格、状況に応じた、プロセスの調整</td><td>原則行わない。</td><td>同左</td></tr>
<tr><td>上記のプロセスの調整を行う方法の標準</td><td>現在はない。今後のテーラリングの方法の整備を予定。</td><td>同左</td></tr>
<tr><td rowspan="2">開発･保守プロジェクトの監視</td><td rowspan="2">開発・保守の標準（監視の標準）の適用</td><td>プロジェクトの性格、状況に応じた、レビューの調整</td><td>レビューの実施において、そのフォーマル度を変えることがある。（プロジェクト内に閉じたレビュー、公式なレビューなどを選択する。）</td><td>同左</td></tr>
<tr><td>上記のレビューの調整を行う方法の標準</td><td>レビューの調整を行う方法を標準として持っており、それを適用している。</td><td>同左</td></tr>
<tr><td colspan="3">事業部門の参画</td><td>「アプリケーションオーナー制」を敷いており、該当部門はレビューに参加する。利用部門にはレビュー参加に必要な教育、演習、テストが提供される。</td><td>同左</td></tr>
<tr><td rowspan="2">経営層の参画</td><td colspan="2">情報システム子会社の経営層</td><td>職位の１つとしてレビューに参加する。</td><td rowspan="2">同左</td></tr>
<tr><td colspan="2">本体の経営層</td><td>全体状況の説明を受け、承認する。</td></tr>
</table>

図表４－１　Ａ社における重要インフラ情報システムの管理

事例2　金融事業を営むB社

取組み強化のきっかけ

- 社外利用者向けのサービスで、期待される「サービスレベル」が損なわれる事案が発生した。
- また、外部環境の変化により、社外利用者に提供する「サービスレベル」の抜本的な改善が必要になった。
- Ｂ社は、該当サービスを提供する情報システム全体を更新することを決定した。新しい情報システムを構築するにあたり、その信頼性確保の取組みはＢ社[15]全社を挙げて実施することとした。

取組みの主要な点

- Ｂ社の情報システム部門は、企画、要件定義までを負う能力を有しているが、情報システムの開発における信頼性確保には、ＩＴベンダーの協力が必要である。そのため、ＩＴベンダーの選定には相当の検討期間をかけた。
- パートナーとなるＩＴベンダーを選定した後は、その役割分担を密に協議した。
- Ｂ社では、「上流完璧主義」を掲げ、誤り、漏れのない要件定義書を作成すること、及びその要件定義の内容がＩＴベンダー担当の設計書に漏れなく反映されていることを監視することに注力した。
- 監視は、Ｂ社とＩＴベンダーが共同で行うレビュー会議を中心とし、そこでＢ社、ＩＴベンダーの責任者がともに承認しなければ、次工程に進めない、といった決まりを作った。

取組みでの特徴的な点

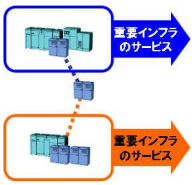
- 要件定義にて、その漏れ、誤りを防ぐ取組みとして、Ｂ社内の他の情報システムの設計書を参照すること、および要件定義書のチェックに外部の有識者を参加させることを行った。
- 情報システムの信頼性確保のため、開発の方式を一新した。そのため、過去のＢ社の開発プロジェクト実績のうち、参考にできるものは少なかった。
  そこで、新しい情報システムの構築において、その開発を複数のサブ・プロジェクトに分割し、１つ目のプロジェクトにおける出来を監視、検証したのち、他のサブ・プロジェクトも同様に実施することにした。

取組みの効果と、今後の展開

- 新しい情報システムは、稼動後１０ヶ月、大きな信頼性問題は生じていない。
- 今回の取組みは、今後の開発・保守プロジェクトへ基本的に適用していく考えである。

15　この事例では、Ｂ社とその情報システム子会社を区別することなく、全体をＢ社として扱っている。

取組みの全体を図表４－２に示す。

			開発の工程	保守の工程
情報システムへの信頼性要求と情報システム、組織の状況の確定	重要インフラ情報システム全体への信頼性要求		社外利用者に対する「サービスレベル」の維持が最優先	
	重要インフラ情報システムとそれが提供するサービスとの関係		 提供する重要インフラのサービスごとに、ほぼ独立した情報システムが用意されている。情報システムとそれが提供するサービスの関係は比較的簡単	
	自社情報システム部門の役割範囲	要件定義	◎	
		開発、保守	（外部に委託）	
		運用	◎	
情報システムの開発・保守の標準の定義	開発・保守の標準の定義	情報システムの重要度、位置づけなどに応じた「タイプ」分け	情報システムの重要度と位置づけ（社外向けか社内業務向けか）により4段階に分類している。	同左
		「タイプ」と信頼性要求水準の関係	各情報システムの信頼性要求水準は同一である。	同左
		「タイプ」や信頼性要求水準に応じたプロセス標準	規程の中で「タイプ」に応じた複数のプロセス標準を定義している。	同左
		「タイプ」や信頼性要求水準に応じたレビューの標準	「タイプ」に応じてレビュー（会議体で審議する、工程での境目での工程品質の確認と次工程への移行の可否の判断のこと、以下同じ。）に参加する職位を変更する。	同左
開発・保守プロジェクトの実行	開発・保守の標準（プロセス標準）の適用	プロジェクトの性格、状況に応じた、プロセスの調整	規程の中で、プロジェクト性格、状況に応じた調整を許している。	同左
		上記のプロセスの調整を行う方法の標準	レビューの調整を行う方法を標準として持っており、それを適用している。	同左
開発・保守プロジェクトの監視	開発・保守の標準（監視の標準）の適用	プロジェクトの性格、状況に応じた、レビューの調整	レビューの実施において、工程の境目の設定の粗密を変えることがある。	同左
		上記のレビューの調整を行う方法の標準	レビューの調整を行う方法を標準として持っており、それを適用している。	同左
事業部門の参画			該当部門はレビューに参加する。	同左
経営層の参画			職位の1つとしてレビューに参加する。	同左

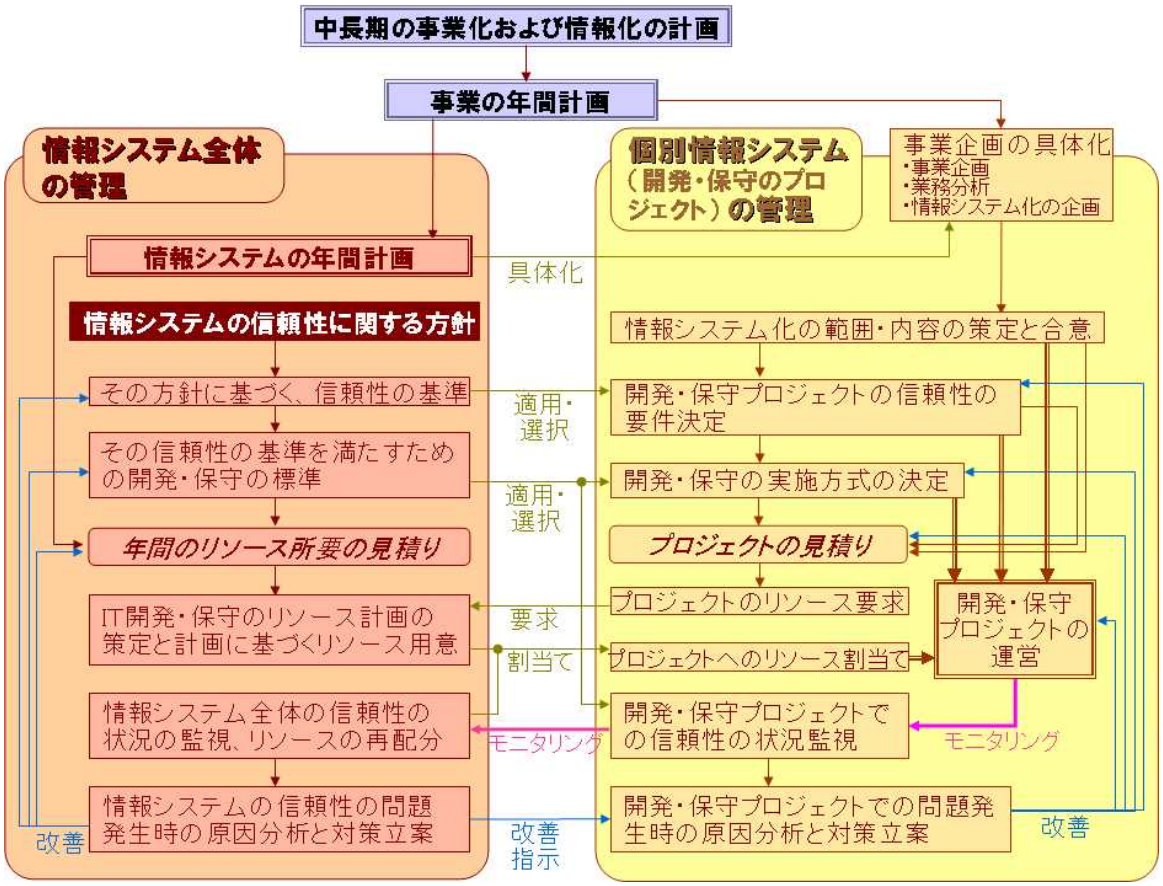
図表４－２　Ｂ社における重要インフラ情報システムの管理

４－２　管理フレームの実施例

以下では、４－１で“Ａ社”[16]として挙げた事業者における、「管理フレーム」の実施例を詳細に説明する。
Ａ社の「管理フレーム」全体の実施において特徴的なことは、以下の点である。

・情報システム全体に求められる信頼性を「情報資産の保全」と定めている。
・「情報資産の保全」を損なうリスクを、情報システム全体に共通で区分するとともに、リスクおよびリスク顕在化の程度を継続的に測ることにより、上記の「情報資産の保全」の遵守状況を管理している。
・個別の情報システムにおいて必要となる、開発・保守の実施の方式、またその方式の遵守と実施結果の妥当性確認を行うための監視の方式が“標準”として定められている。

Ａ社における、「管理フレーム」の実施の全体像は、図表４－３のようになっている。

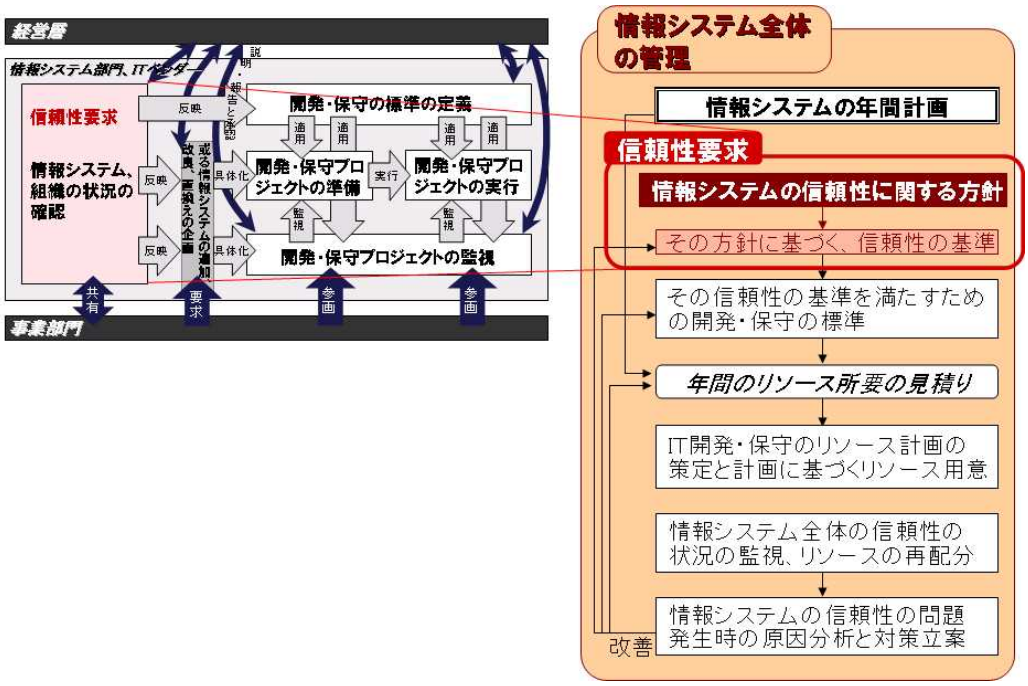


図表４－３　Ａ社における「管理フレーム」実施の全体像

[16] この事例では、Ａ社とその情報システム子会社を区別することなく、全体をＡ社として扱っている。

４－２－１　信頼性要求の実施例

４－２以下では、Ａ社における、「管理フレーム」の各活動要素の実施例を紹介する。
Ａ社の「２－４－１　信頼性要求」の実施は、図表４－４の部分である。



図表４－４　Ａ社における「信頼性要求」の実施

Ａ社の活動の主要な点

・Ａ社の**情報システムの信頼性に関する方針**は、「情報資産の保全」を第一目標とすること、である。
この方針は、経営層、事業部門、情報システム部門をまたいだ、情報システム全体についての方針検討の中で定められた。

・Ａ社は、この「情報資産の保全」を損なうリスクを区分している。
区分されたリスクには、以下が含まれている。
（１）管理不足等により、情報システムの能力不全に陥るリスク（情報システム要件の未達成）
（２）法制、業界規制、事業者外の関係者との契約など、ビジネス運営上必要な事項に対し、情報システムの能力不足が生じるリスク（ビジネス要件と情報システム要件の不整合）
これらのリスクをある水準以下に抑えることが、Ａ社にとっての信頼性確保の取組みでの重要事項になっている。

・これらのリスクは、(1)情報システムの障害により関係者に影響が及んだ案件についての原因分析、(2)事業環境やステークホルダーからの情報システムへの要求、期待の分析、の２種類から導かれている。

・Ａ社で、情報システムの信頼性を表現する指標のうち最も包括的なものは情報システムの不具

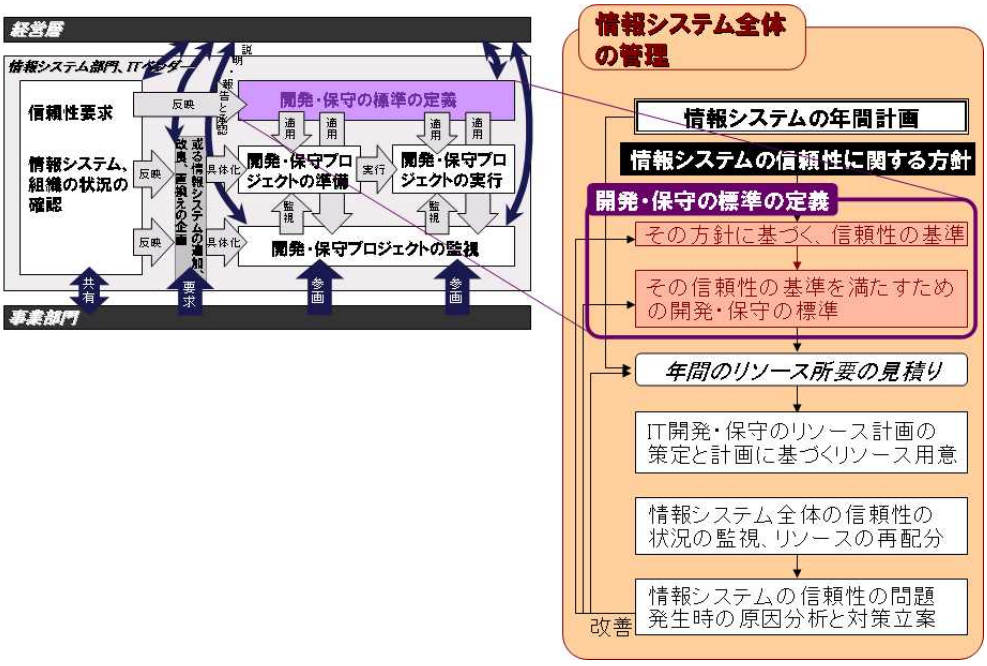
合が利用者（社内、代理店、契約者）に与えた影響を数値化した「トラブル影響度」である。

A社の活動でのインプット

- 法制および業界規制（金融商品取引法（実施に関する基準を含む、以下同じ）、米国ＳＯＸ法、個人情報保護法、セキュリティガイドライン、ＦＩＳＣ安全対策基準、監査に関する基準）
- ＩＴ管理におけるプラクティスおよび標準（ＣＯＢＩＴ、ＩＴＩＬ、ＩＳＯ１５４０８）

４－２－２　情報システムの開発・保守の標準の定義の実施例

Ａ社の「２－４－３　情報システムの開発・保守の標準の定義」の実施は、図表４－５の部分である。



図表４－５　Ａ社における「開発・保守の標準の定義」の実施

A社の活動の主要な点

- Ａ社の**開発・保守の標準**は、開発・保守プロジェクトの準備、実行、および監視に関して、必要なことの全てを定める、また具体的に指定する、という考え方で定められている。
  つまり、個々の開発・保守プロジェクトの準備、実行、およびに監視において、開発・保守の標準に記述されていないプロセス、また技法・ツールが追加的に採用されること、プロセスや技法の具体化が個別に図られることは、一部の例外を除き、基本的には無い。

・上記の考え方に基づき、次のような開発・保守の標準が整備されている。

ー開発・保守プロジェクトにおけるリスク評価の方式

開発・保守プロジェクトに関係するリスクの程度を評価する「リスクチェックシート」、稼動システムのリスク程度を評価する「システムリスク・アセスメントシート」というツールが提示されている。

これらで扱うリスクは何らかの形で「トラブル影響度」に関係するものである。

ー開発・保守プロジェクトの実施の方式

開発・保守プロジェクトの準備、実行で用いられるべき技法・ツールが含まれている。この中には、個々の開発・保守プロジェクトのリスク評価結果に応じて必要となる処置も含まれる。

また、標準の実施方式によらずに開発・保守プロジェクトを実施しようとするときの手続きも規定されている。[17]

ー開発・保守プロジェクトの監視の方式

開発･保守プロジェクトの規模やリスク評価結果に応じた監視のやり方が示されている。

ー開発・保守プロジェクトにおける事業部門の役割、守るべきことの規定

「アプリケーションオーナー制度」で以下を定めている。

（１）開発・保守プロジェクトに要員を供出するという、アプリケーションオーナーとしての事業部門の責務

（２）要員の役割（システム化計画の立案、要件の確定、要件が満たされていることの確認、開発工程終了の確認、利用促進・効果測定）と、工数についての考え方

・Ａ社では、事業者に求められることが具体的なもの、例えば法制や業界規制の一部からくる**信頼性要求**に関しては、そのために必要なことを事前に**開発･保守の標準**に盛り込んでいる。

一方、事業者に求められることが最初から全て明らかでないものについては、４－６に後述する**管理フレームの内容修正**を通じて、**開発･保守の標準**の継続的改善を図っている。

A社の活動でのインプット

・情報システムの信頼性要求、そのうち特に、「情報資産の保全」を損なうリスク

・ソフトウェア開発におけるプラクティス（ＣＭＭＩ）

・公開されている、または契約により入手可能な、他社、他団体のソフトウェア開発・保守の標準

[17] 新規性が高いプロジェクトなどでは標準の実施方式に依らないことがある。

A社の活動における留意点

・「アプリケーションオーナー制度」は事業者内における、発注者の役割と責任を明確にするための制度である。
「アプリケーションオーナー」は、事業推進上、個別の情報システムの開発・保守・運用を必要とする事業部門である。発注者の責任である、要件定義とその実現の確認を行う責務を負う。
・「アプリケーションオーナー」からの要員は必ずしもＩＴに詳しくないことがあるため、役割と実務についての教育を定期的に行い、適確な役割遂行を下支えしている。

コラム 「開発・保守の標準」の改善に利用できる技法・ツール

開発・保守の標準には、情報システムの信頼性の確保のために必要な事項が含まれている必要がある。
Ａ社が考える、情報システムの信頼性に関するリスクには、４－２に説明したとおり以下がある。
（１）管理不足等により、情報システムの能力不全に陥るリスク（情報システム要件の未達成）
（２）法制、業界規制、事業者外の関係者との契約など、ビジネス運営上必要な事項に対し、情報システムの能力不足が生じるリスク（ビジネス要件と情報システム要件の不整合）

このうち、（２）の法制や業界規制の一部には、情報システムの信頼性について具体的な要求をしているものがある。これらについては、開発・保守の標準の中に要求を満たすのに必要十分な方法やツールを具体的に盛り込むことは困難ではない。
一方で、（１）については、管理不足という原因と、情報システムの問題という結果のような因果関係を明確にしにくいものについては、最初から開発・保守の標準の中に必要十分に盛り込むことも難しい。

そこで、（１）については、以下の取組みが重要となる。
（Ａ）開発・保守の標準を、最初に定めるにあたって、標準についての基本的な考え方や範囲をよく検討すること
（Ｂ）適宜、情報システム自体に発生した問題を原因分析し、その対処を立案し、必要に応じて開発・保守の標準を修正するという継続的改善を行うこと

上記の（Ａ）（Ｂ）の実施には「高信頼性ソフトウェア開発技法ガイドブック」（ＩＰＡ／ＳＥＣ 2010 年 7 月）が有用である。
このガイドブックの第４章には、ソフトウェアの品質特性の分類（図表Ｆに、その部分を示す）および、障害分析における品質特性との関係づけや対策の実施例（図表Ｇに、その一例を示す）が提示されている。
このガイドブックは、（Ａ）開発・保守の標準をまとめるにあたり、トップマネジメントが組織全体の信頼性向上の方向性を定め、情報システム部門（品質管理）に指示するのに役立つ。
また、（Ｂ）問題への対処において開発・保守プロジェクトのリーダが、開発・保守の標準の継続的確認において情報システム部門（品質管理）が、それぞれ実効性のある方策を立案するのに役立つ。

代用特性		
品質特性	品質副特性	代用特性（2次）
機能性	合目的性	妥当性（利用者側の要件）の確認（レビュー、テスト）に対するユーザーとベンダーの役割分担
		暗黙要求（要件記述なし）の確認手段に関する取り決め
		仕様変更に対するユーザーとベンダーの合意
		ユーザー要件に対する設計書の必要十分性（トレーサビリティ）の検証
	正確性	計算精度やデータ精度要求の実装確認
		システム利用マニュアルの記述の正確性向上施策
		検証（工程整合）確認に対するユーザーとベンダーの合意
		上位設計書に対する下位設計書（またはプログラム、テスト仕様）の必要十分性（トレーサビリティ）の検証
	相互運用性	外部システムとの接続要求および仕様の確認（レビュー、テスト）に対するユーザーとベンダーの合意
		外部接続に対するデータ数、変換、編集（データ形式、コードなど）に関するコミュニケーション
		相互接続する他のソフトウェアのバージョンアップによる影響に対する考慮
		接続先外部システムとのコンテンジェンシープランの共有化
	セキュリティ	データ暗号化対策
		開発時でのデータ漏洩防止対策
		セキュリティ事故発生に備えた、追跡可能性および監査容易性などの向上施策
		セキュリティパッチなどの脆弱性の予防対策
		不正アクセス、不正ログインに備えたアクセス制御対策
		なりすましのモニタリング、警告機能に関する工夫
		データ損傷などのデータ保全対策
		セキュリティ要件（実装検証を含む）のユーザーとベンダーの合意
	機能性標準適合性	機能性に対応する規定（業務、内部統制、ISMS、国際会計など）および開発標準の適合監査対策

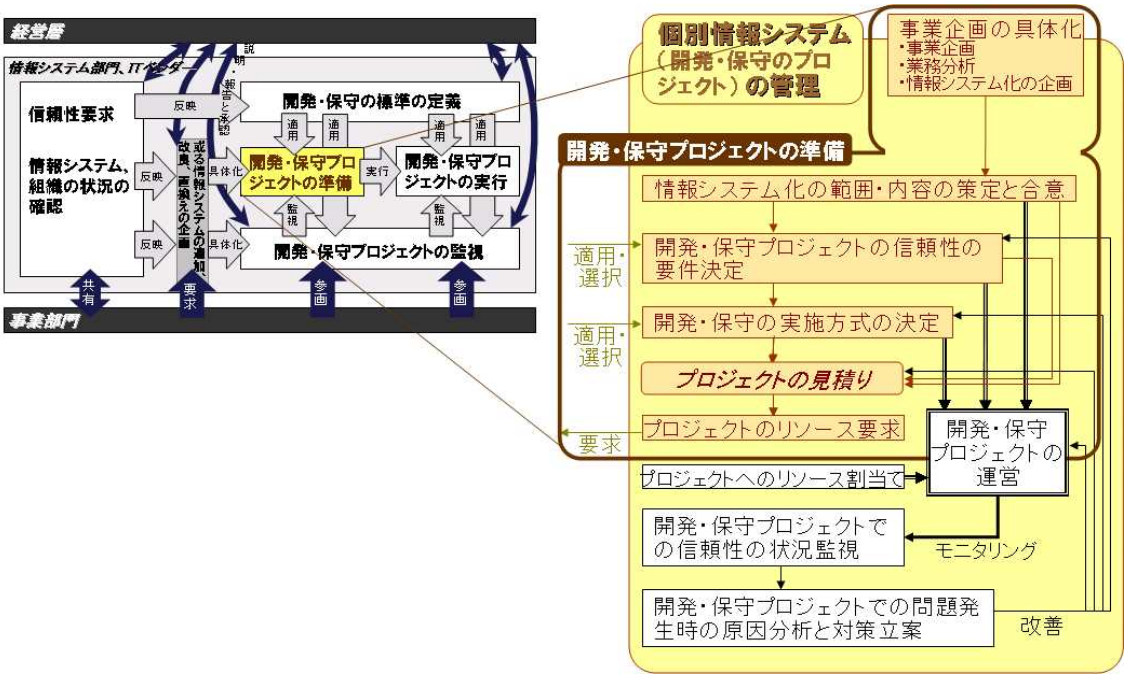
図表Ｆ　「高信頼性ソフトウェア開発技法ガイドブック」が提示する、ソフトウェアの品質特性（部分）

<table>
<tr><td rowspan="3">障害事例</td><td>業種</td><td colspan="5">通信</td></tr>
<tr><td rowspan="2">障害
発生元</td><td colspan="4">開発</td><td rowspan="2">保守</td><td rowspan="2">運用</td></tr>
<tr><td>要件定義</td><td>設計</td><td>実装</td><td>テスト</td></tr>
<tr><td></td><td>○</td><td>○</td><td></td><td>○</td><td></td><td></td></tr>
<tr><td colspan="7">携帯電話の利用料金請求にて、実際の請求額よりも1桁もしくは2桁多い金額を印字し請求書を発行してしまうといった障害が発生。料金管理を行うシステムと料金結果を受領するシステム（他社の請求書印刷システム）とのインタフェースで、特定の利用者にて考慮すべき小数点が無視された。</td></tr>
<tr><td>障害による影響度合い</td><td colspan="2">障害影響評価指標値</td><td>5</td><td colspan="3"></td></tr>
<tr><td colspan="7">発生件数は数万件にのぼり、全国各地の利用者へ影響を与える。利用者からのクレームに対する謝罪も必要となり、信用失墜となった。</td></tr>
<tr><td>根本原因</td><td colspan="6"></td></tr>
<tr><td colspan="7">インタフェース確認やテスト実施の必要性は認識していたが、相互での仕様確認やテスト実施負荷が重いこと、これまで接続実績があることを理由に、不十分な仕様確認やテスト密度で開発をすすめていた。</td></tr>
<tr><td>品質特性に準拠した
再発防止策</td><td colspan="6"></td></tr>
<tr><td rowspan="3">【再発防止策①】</td><td>特性</td><td>機能性</td><td>副特性</td><td colspan="3">正確性</td></tr>
<tr><td>代用特性
（2次）</td><td colspan="5">計算精度やデータ精度要求の実装確認</td></tr>
<tr><td colspan="6">計算途中の丸め誤差、集計時最終桁扱い誤りなどの微妙な誤差を防止するため、以下の手段を講じる。
a）起点日の考え方（片端計算、両端計算等）も含め、計算精度については、設計書に順序、計算途中での端数の取り扱いや桁落とし方法を明記して、ユーザと合意をとる。</td></tr>
<tr><td rowspan="3">【再発防止策②】</td><td>特性</td><td>機能性</td><td>副特性</td><td colspan="3">相互運用性</td></tr>
<tr><td>代用特性
（2次）</td><td colspan="5">外部システムとの接続要求および仕様の確認（レビュー、テスト）に対するユーザとベンダとの合意</td></tr>
<tr><td colspan="6">外部接続時は、開発の早い段階でプロトタイプを作成し、疎通確認を行う。
a）開発に先立ち疎通確認を行うことにより、開発の早期段階で、接続先とのインタフェースミス、環境設定ミスの洗い出しが可能となる。</td></tr>
<tr><td rowspan="3">【再発防止策③】</td><td>特性</td><td>保守性</td><td>副特性</td><td colspan="3">試験性</td></tr>
<tr><td>代用特性
（2次）</td><td colspan="5">試験性に配慮したソフトウェアおよびデータの構造化、ならびに他システム接続方式に関する施策</td></tr>
<tr><td colspan="6">アプリ基盤として、データベースマネジメントシステムなどに依存しないソフトウェアの構造化を行う。
a）PCなど簡易で軽量な環境にて下流テストが実施可能となり、試験負荷の軽減、テスト密度向上に寄与する。ただし本番環境とかけ離れている場合は、環境差異により障害が摘出できない可能性もあり、本番環境での確認が必要である。</td></tr>
</table>

図表Ｇ　「高信頼性ソフトウェア開発技法ガイドブック」が提示する、障害分析における品質特性との関係、対策の実施例（一例）

４－２－３ 情報システムの開発・保守プロジェクトの準備の実施例

Ａ社の「２－４－４　開発・保守プロジェクトの準備」の実施は、図表４－６の部分である。



図表４－６　Ａ社における「開発・保守プロジェクトの準備」の実施

Ａ社の活動の主要な点

・アプリケーションオーナーと情報システム部門（開発担当）とが共同で、開発・保守する情報システムの企画を行う。

－アプリケーションオーナーが主体となって、ビジネス企画とその中での情報システム活用の範囲と内容を決定する。

－情報システム部門（開発担当）が、ビジネス企画にも参加しながら、情報システム活用の範囲と内容の決定を、実現性や有効性につき、技術的な面から補佐する。

・Ａ社の情報システムの開発・保守の標準に基づき、対象の情報システムおよび開発・保守プロジェクトのリスクを評価し、開発・保守の方式を決定する。

－情報システム部門（開発担当）が主体となって、対象のプロジェクトのリスク状況を「リスクチェックシート」、「リスクアセスメントシート」を使ってまとめ、また、開発・保守の方式（基盤や調達方式の選択を含む）を決定する。

－アプリケーションオーナーは、ビジネスのリスクや特性を踏まえＢＣＰ[18]プログラムの適用程度などに広く関与する。

[18] Business Continuity Planning の略。災害など予期しない出来事の発生により、限られた経営資源で最低限の事業を継続する、また目標時間内に事業を再開するための計画

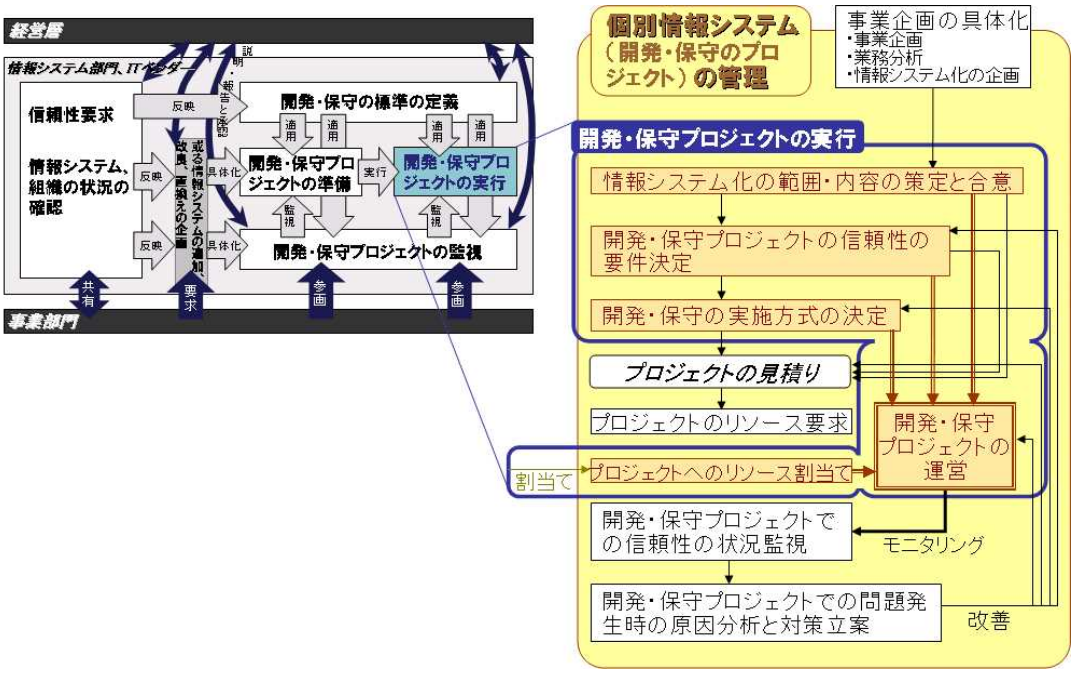
・情報システムの開発・保守プロジェクトに必要なリソースを見積り、プロジェクトとしての要求にまとめる。

A社の活動でのインプット

・前節の、Ａ社の開発・保守の標準

4―2―4　情報システムの開発・保守プロジェクトの実行の実施例

Ａ社の「２－４－５　開発・保守プロジェクトの実行」の実施は、図表４－７の部分である。



図表４－７　Ａ社における「開発・保守プロジェクトの実行」の実施

A社の活動の主要な点

・情報システム部門（計画）は、年間のリソース計画の中から開発・保守プロジェクトの要求に応じてリソースを割り付ける。

－割り付けるリソースには、情報システム部門および外部委託先の要員リソースの他、事業部門側が用意、確保するアプリケーションオーナーのリソースも含まれる。

－開発・保守プロジェクトに割り当てられたリソースは、該当プロジェクトおよび同時並行する他の開発・保守プロジェクトのリスク状況の変化をにらみながら、適宜割り付けをし直される。

・情報システム部門（開発担当）は、開発・保守プロジェクトの準備の結果と割り付けられたリソースを用い、開発・保守プロジェクトを実行する。

－開発・保守プロジェクトの実行では、品質指標を用いた管理を行う。この管理にはプロジェクトのリスク状況に関わる項目を含む。

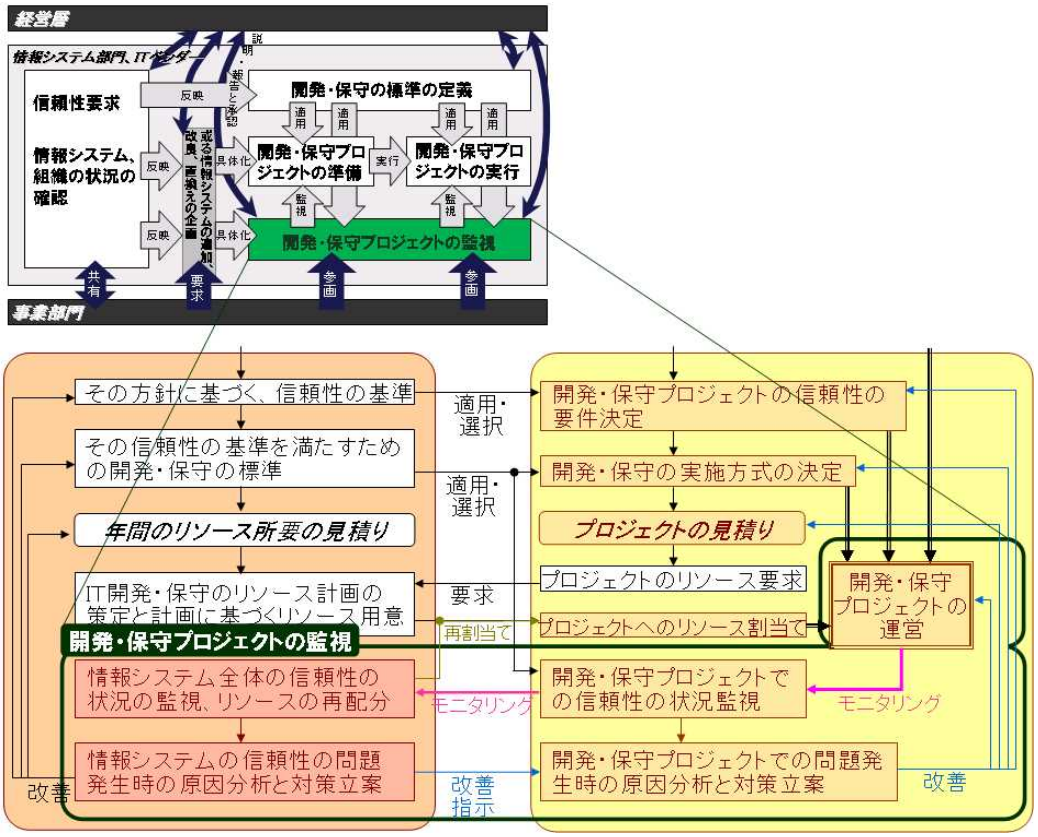
A社の活動でのインプット

・開発・保守プロジェクトの準備の実施結果

・開発・保守の標準

４－２－５ 情報システムの開発･保守プロジェクトの監視の実施例

Ａ社の「２－４－６　開発・保守プロジェクトの監視」の実施は、図表４－８の部分である。



図表４－８　Ａ社における「開発・保守プロジェクトの監視」の実施

A社の活動の主要な点

・開発・保守プロジェクトの監視について、タイミング、監視者、監視の実施程度、監視の視点は、開発・保守の標準に定められている。（開発・保守プロジェクトのリスク程度に応じた監視の仕方の調整を含む。）

・その標準にしたがい、情報システム部門（開発担当）は、毎週、個々の開発・保守プロジェクトでの信頼性の確保の状況をモニターする。

・情報システム部門（品質管理）は、毎月、個々の開発・保守プロジェクトの状況を評価し、全プロジェクトの状況を一覧にまとめる。一覧は経営層に報告される。

・また、アプリケーションオーナーは、情報システム部門（品質管理）とともに開発・保守プロジェクトのチェックポイントで、開発・保守の標準の遵守など開発・保守プロジェクトの適正性を確認し、主要な工程および開発・保守プロジェクトの終了を承認する。[19]

・開発・保守プロジェクトの監視の結果、必要に応じて、次の対処がとられる。

　－開発・保守プロジェクトのへ改善指示（テストや内部レビューの実施項目の追加や実施期間の延長など）

　－複数の開発・保守プロジェクト間でのリソースの割り付けの再配分

A社の活動でのインプット

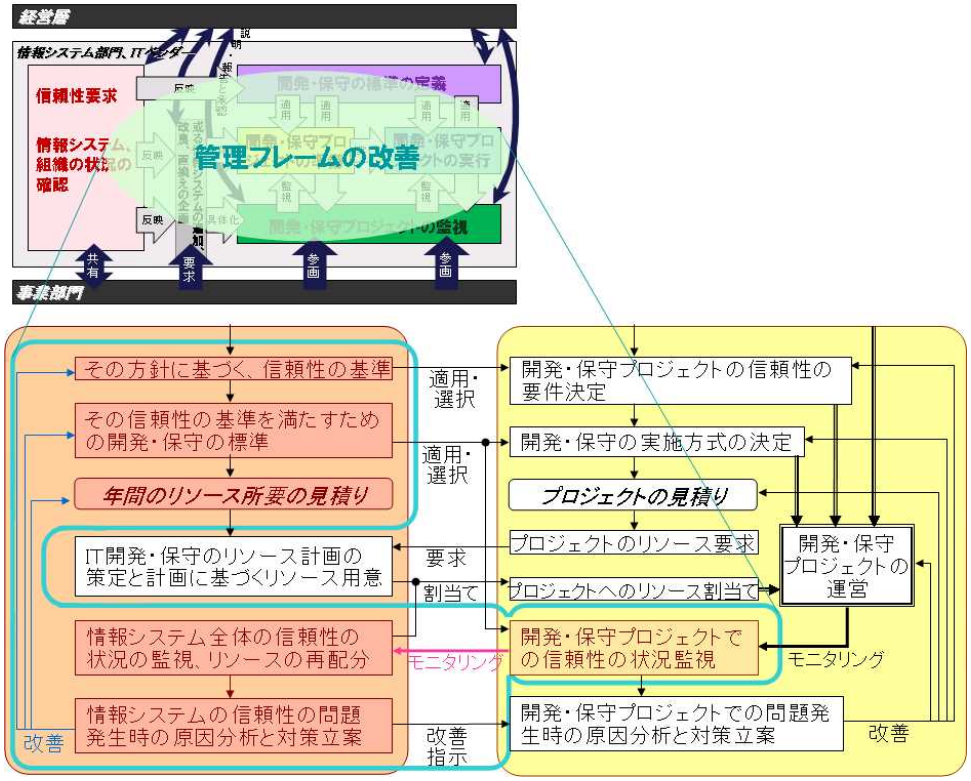
・品質指標を用いた管理による対象プロジェクトの状況、特にその中のリスク状況

・開発・保守の標準に定められた工程成果物についての、対象プロジェクトでの完成状況

[19] このガイドブックのスコープ外であるが、主要な工程の終了時点でのレビューには情報システム部門（運用担当）の責任者が参加し、運用に関する標準の遵守等の適正性を確認し、主要な工程および開発・保守プロジェクトの終了を承認していることを付け加える。

４－２－６　情報システムの開発･保守の継続的な改善の実施例

Ａ社の「２－４－７　開発・保守の継続的な改善」の実施は、図表４－９の部分である。



図表４－９　Ａ社における「開発・保守の継続的な改善」の実施

A社の活動の主要な点

・情報システム部門（品質管理）は、開発・保守プロジェクトの関係者の意見も聞きながら、開発･保守プロジェクトに共通する、情報システムの信頼性に関わる問題について原因を分析し、その対策案をとりまとめる。

－対策案には、開発・保守の標準やリソース配分の考え方の変更といった現行の標準の修正案と、その修正が有効であることを確認する場、方法（例：ある開発・保守プロジェクトでの試行採用）が含まれる。

・原因分析結果と対策案は、経営層、事業部門、情報システム部門が参加する会議に付され、承認される。

・信頼性要求、開発・保守の標準の見直しは、情報システムの信頼性の問題発生だけを契機とするのではなく、以下のような開発･保守における可能性の拡大をきっかけとしても実施される。

－新しい開発手法（例：アジャイル開発、クラウドサービス）の普及と、その採用が適していると考えられる情報システム化案件の発生

A社の活動でのインプット

・開発・保守プロジェクトで発生した問題
・その問題の原因分析に役立つ、開発・保守プロジェクト関係の見解や下記の情報
　　－品質指標を用いた管理によるプロジェクトの状況、特にその中のリスク状況の推移
　　－開発・保守の標準に定められた工程成果物についての、プロジェクトでの完成状況の推移

コラム　A社における情報システム信頼性に関する活動

４－２では、Ａ社における「管理フレーム」の実施例をみてきた。
これは一例であり、この方法が唯一つではない。
重要インフラ事業者など、情報システムの信頼性に全社を挙げて取り組む事業者は、その事業者の特質に合わせた実施の仕方を考えることが重要である。

さて、Ａ社における、情報システム信頼性に関する活動には、以下のような考えが一貫してあることが観察される。

●情報システム全体に対する信頼性要求を、「信頼性に関する第一目標」や「それを損なうリスク」という形で明らかにする。（情報システムの信頼性の「ものさし」を作る。）
●個別の情報システムでの信頼性要求を、次の活動要素で実現する。
　（情報システムの信頼性確保のための「ルール」とその「ルール」を守る仕組みを作る。）
　　①開発・保守の標準・・・・・開発・保守における必要を全てルールとして示すこと
　　②開発・保守プロジェクトの準備、実行・・①の遵守
　　③開発・保守プロジェクトの監視・・・・・②による①遵守の確認、①の有効性の検証
●情報システムの開発・保守に関わる者が「ルール」と役割に沿って業務を行えば、情報システムの信頼性が確保されるようになるまで、上記の仕組みを整備し、さらにその効果を確認し続ける。（「ルール」を適確に位置づけ、その位置づけを満たし続けるようにする。）

なぜ、このようなことが必要になったのだろうか。
次のような理由が考えられる。

[1] 情報システムの規模が大きくなり、その内部構造が複雑になると、情報システムの信頼性をプロセス（技法、ツールを含む）の規定だけでは実現するのは次第に困難になる。
何故なら、開発・保守に携わる要員の増加とともに、以下のようなプロセスの均質性に関する問題が大きくなるからである。
(1) 要員の自主性に任せただけでは、プロセスの規定が守られないことがある。（外部委託によりこの傾向が強くなることもある。）
(2) 要員のスキル差によるバラツキがでる。
■(1)に対しては、プロセスの規定が守られていることをプロジェクト外などから確認する必要がある。つまり「ルール」を守る仕組み、その仕組みの根拠としての「ルール」の位置づけが重要になる。
■(2)に関して、プロセス実施の結果、情報システムの信頼性が十分確保されているか確認し、必要ならスキル差を埋める補正（要員の配置を変える。プロセスをやり直すなど）をかける必要がある。ここで信頼性確保の確認のためには、情報システムの信頼性を判断する「ものさし」が必要になる。

[2] 国民生活や社会経済活動の変化が原因でビジネス環境が変化することにより、情報システムの信頼性要求を満たせなくなるリスクも変化する。また、技術の進展により、信頼性要求を満たす方法も変わり得る。
そこで、情報システムの信頼性を取り巻く環境の変化への対応の必要が生じる。
■これに対しては、数年ごとに、「ルール」とそれを守る仕組みの有効性を確認し、また新たな「ルール」とそれを守る仕組みの可能性を考えることが必要になる。

上記は、情報システム信頼性の捉え方に関する事柄である。答えは一通りではなく、事業者は自身が置かれている環境や、組織の能力、役割に応じた方策を考え、実践する必要がある。

終章　おわりに

■残された課題

このガイドブックでは、重要インフラ情報システムの信頼性について、事業者の取組みの調査結果から、その取組みで必要なことと、その取組みの要素を扱った。
但し、その取組みの内容については、方法論的に細かく述べず、その取組みで何ができることが必要なのか、取組みの要素間がどのような関係にあるのか、ということを俯瞰したにとどまっている。

重要インフラ情報システムの信頼性確保のために必要な取組み、活動を、それぞれの重要インフラ事業者が定義し、実施し易くするためには、以下のような点について更なる整理が必要である。

１．情報システムへの信頼性要求について

重要インフラ・サービスは、国民生活や社会経済活動に深く関係している。
したがって、そのサービス提供基盤の信頼性、その中に含まれる重要インフラ情報システムの信頼性は、利用者である国民とサービス提供者である重要インフラ事業者との間の、情報システムが支えている重要インフラ・サービスについての合意から出発すべきである。
信頼性を確実に高めるためには、第２章で説明したような信頼性確保の取組みを一層厚く実施する必要がある。情報システムに高い信頼性を持たせるには相応のコストがかかるということである。利用者の国民は信頼性を高めるコストを重要インフラ・サービスの利用料等の形で負担することになる。そこでこの合意が重要になる。
但し、国民と重要インフラ事業者とでは、サービス提供基盤、重要インフラ情報システムに関して持ち得る情報が異なる[20]から、その合意にあたってはサービス提供基盤、重要インフラ情報システムについての**「信頼性の表現形式」**や**「信頼性についての合意を得る方法、得る場」**が提供されることが好ましい。[21]

また、サービス提供基盤の中に位置する重要インフラ情報システムは、サービス提供基盤の一部分であるから、サービス提供基盤、重要インフラ情報システム全体の内部構造に応じて**「サービス提供基盤全体への信頼性要求をサービス提供基盤の要素への信頼性要求に分解する方法」**が提供されることが好ましい。

---

[20] 重要インフラの保安上の意味合いからも、重要インフラのサービス提供基盤、重要インフラ情報システムについて国民が知り得る範囲は限定されることになるであろう。
[21] 「信頼性の表現形式」や「信頼性について合意を得る方法、得る場の形成」については、今後の普及拡大が予想される「クラウドサービス」でも非常に重要になると考えられる。

２．情報システムの信頼性確保に必要な活動（プロセスや方策）を定めることについて

信頼性確保に必要な活動は、①情報システムへの信頼性要求、②情報システムの構造、③情報システム部門の役割範囲によって、適した取組みの持ち方が異なる。

今のところ、それぞれの事業者に適した取組みの持ち方は、事業者自らがその性格に応じて定めるしかないが、上記①～③により**事業者の情報システムの構造などを分類し、その分類に基づいて適した「管理フレーム」の実施の仕方（活動単位の内容、役割分担など）を整理**することによって、事業者に共通的なやり方を示せる可能性がある。

３．情報システムの信頼性の監視、検証について

ここはスキルに依存する部分が大きく、方法論になりにくい。信頼性の確認にその**職位、スキルを管理し安定的に割り当てる方法**、また信頼性を再現することを確認するにあたり、**信頼性を評価する視点、信頼性の確保に失敗した事例（その原因、失敗の再発を防止する対策を含む）**[22]について、**事業者間で情報共有する仕組みを整備すること**が有効と考えられる。

さて、ここまでは、現行の重要インフラ情報システムを対象に、その信頼性確保の取組みについて説明してきた。
もう１つ、現行の重要インフラ情報システムが抱え得る課題とそれを克服する必要に触れてこの節を終えたい。

第１章でも、重要インフラの中には 100 年を超える歴史を持ち、その長い歴史の中で、情報システムがサービス提供基盤の一部として最近になって導入されているものがあることについて触れた。
そういった重要インフラのサービス提供基盤では、それまで人間が行ってきた重要インフラの制御、管理の一部を情報システムに肩代わりさせることによって、重要インフラ全体の機能向上や運営の省力化を図っている。

しかし、サービス提供基盤の機能、性能の段階的拡大や老朽化に伴う更新、それに伴う情報システムのサービス提供基盤への段階的組込みによって、サービス提供基盤全体の内部構造が徐々に見えにくくなっているものがある。[23]

[22] 情報システムの信頼性の確保に失敗した事例の情報収集、傾向分析、国民および事業者への情報提供に関しては、現在のところ公的かつ業種横断的な取組みはない。マスメディアなど民間においては幾つかの取組みがなされているが、事例情報の入手に限界があるために十分な傾向分析が行えていない状況である。
[23] ＪＵＡＳにおける調査でも、段階的な機能拡張の結果、重要インフラ情報システムが有する機能のセットが非常に複雑になり、その管理が十分に行えず、情報システムに要求する機能要件を縮小させることによって、ようやくその信頼性が確保できた事例、およびそのような対応が必要になり得る障害事例があることが分かっている。

こうした重要インフラのサービス提供基盤については、その信頼性確保のためにある世代、ある時点を持って、大規模なサービス提供基盤の入替えを考えざるを得ない。
その新世代の重要インフラ情報システムを企画する際には、今後起こり得る外部環境の変化にどう対応しておくか、言ってみれば、重要インフラ情報システムの継続的な『進化』と『信頼性確保』をどう両立させるか、ということについて、その技法、手段を充実させることが必要と考えられる。

また、重要インフラ・サービスの信頼性確保という上位の目標のために、サービス提供基盤や重要インフラ情報システムは何をどこまで支えるのがコストや信頼性確保の確からしさからみて適当か、ということに関する議論も必要である。

■重要インフラ情報システムの関係者の各位へ

繰返しになるが、重要インフラの信頼性について最も重要なことは、①利用者である国民と信頼性について何らかの合意を行い、②その合意された信頼性を実現し続けることである。
①のためには、重要インフラ事業者が、自らの事業目的に照らしながらも利用者である国民に対し、自ら定め自らに課している重要インフラの信頼性について分かり易く説明すること、またその内容について対話をすることが必要である。
②のためには、重要インフラのサービス提供基盤の一部である重要インフラ情報システムにおいても、上述の合意に基づいた信頼性を保持し続けることが必要である。
そのために、重要インフラ情報システムの関係者の各位は「あるべき状態」を定義し、その「あるべき状態」を保っていることを説明できることが重要である。また、万一「あるべき状態」を外れた場合には、それがどういう取組みの不足によるものなのかを明らかにするとともに、その再発を防ぐ方策を説明できることが重要である。
上記を行うために必要な労力は決して小さくないが、まずは既存の取組みを整理することにより、上記の説明がどこまで出来るか、説明力が弱い部分にはどんな改善が可能か、を考えることから始めみてはいかがであろうか。

僭越なご提案をし、本書を終える。

参考資料

（順不同、本文中に具体的図書名を挙げたものを除く）

- 「ISO31000:2009 リスクマネジメント　解説と適用ガイド」　リスクマネジメント規格活用検討会編著　2010 年 2 月　日本規格協会

- 「IT保証の概念フレームワーク」 堀江著　2006 年 3 月　森山書店

- 「日経コンピュータ　2007年2月19日号 『実践！IT サービス・マネジメント』」 日経BP社

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

付　録

付録【１】ソフトウェアの品質管理に用いる指標と基準値

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、以下の一部の調査を日本情報システム・ユーザー協会（以下、「JUAS」）に委託して実施した。あわせて、情報サービス産業協会（以下、JISA）の協力を得た。

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、特にその中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

但し、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ー企業と、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ー企業に関し、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。ユーザー企業8社、ベンダー企業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

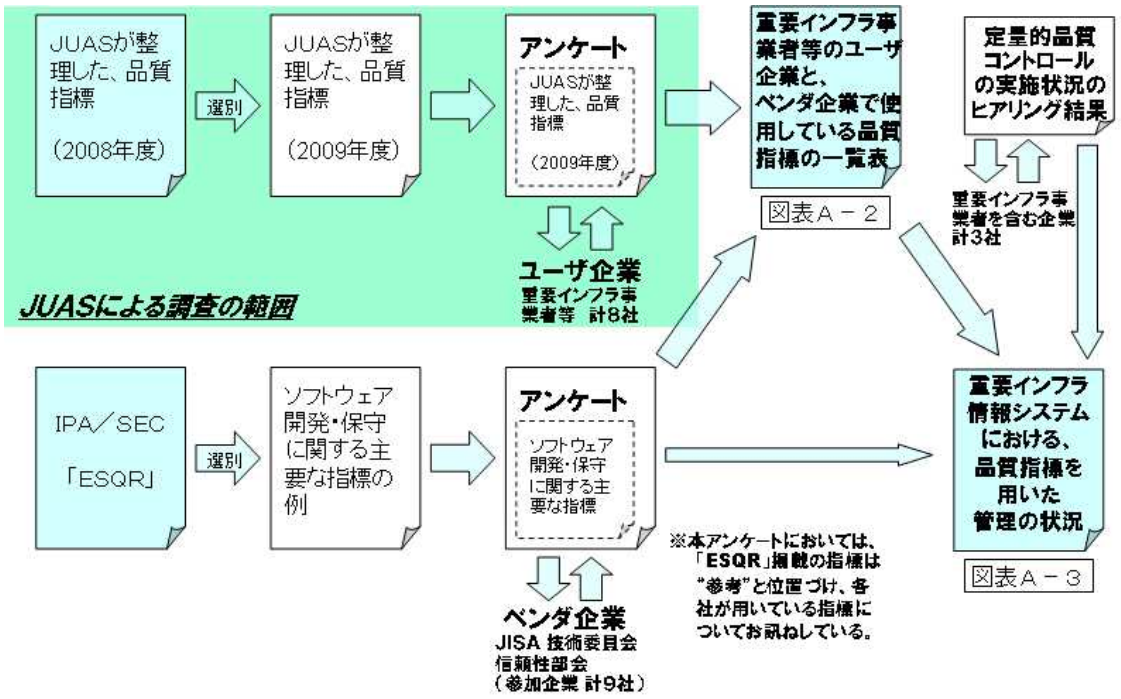
2.1 定量的品質コントロールの実施状況調査の進め方

JUASでは、ユーザー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、ベンダー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ー企業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A－1】のとおりである。



【図表A－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A－2】に示す[24]。このアンケート調査の方法は、次のとおりである。

1） ユーザー企業（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個の指標をユーザー企業に示し、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） ベンダー企業（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ー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A－2】をさらに加工し、ユーザー企業・ベンダー企業の合計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。[25] その結果を【図表A－3】に示す。

なお、同図表には、ユーザー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、ユーザー企業－ベンダー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ー企業1社のみから得られた情報も含まれている。

24 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。

25 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A－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	A社	B社	C社	D社	E社	F社	G社	H社	ベンダ企業									
			業種	製造	電力	航空	通信	金融	ガス	金融	金融	p社 システム1	システム1	q社 システム2	システム3	システム4	システム5	r社 システム1	s社 システム共通	t社 システム1	u社 システム1	v社 システム1	w社 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合		○	○				○		↓						↓	↓	○		
		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度		○	○				○												○
		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		○			○																
			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											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					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カバレッジ														○							
			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(ゴンペルツ曲線)			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(ゴンペルツ曲線)	○	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	サービスレベル	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A－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

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	
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	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	レビューで摘出された欠陥の密度	・UI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)	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			
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	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	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	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)		
	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

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
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 定期的報告・評価 事前合意の再調整
			バッチ処理の時間内の終了率	・バッチ処理正常終了率		
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		
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)

$$\frac{\text{(後続工程で明らかになったエラー件数)}}{\text{(成果物作成工程で明らかになったエラー件数)} + \text{(後続工程で明らかになったエラー件数)}}$$

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・評価	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
定期的状況共有	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
事前合意の再調整	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
工程終了の合意	工程の結果をチェックし、次の工程に移ることの合意

付録【２】 障害事例分析と障害再発防止策

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54個を得た。

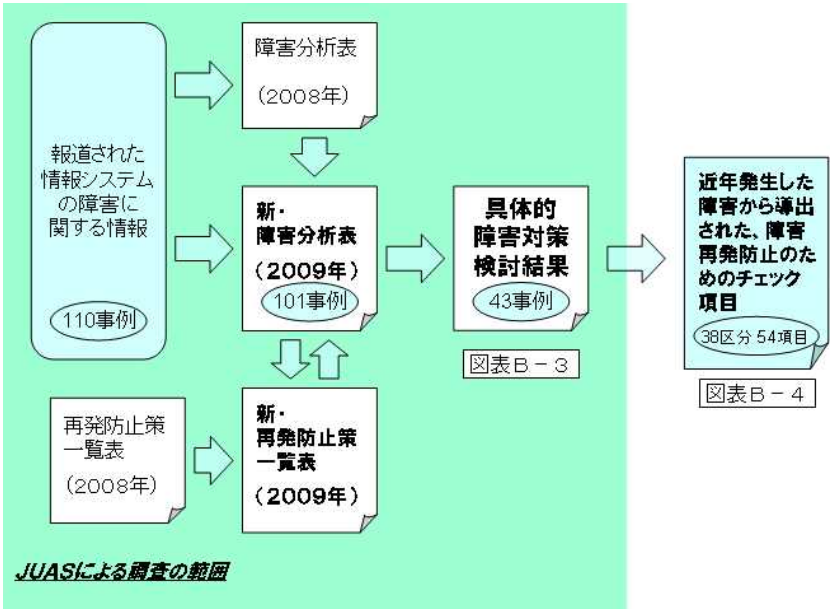
以降では、調査内容及び調査結果の分析に基づく議論の詳細について述べる。

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[26]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54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

[26] Nikkei ITpro（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。