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

平成２１年３月２４日

経　済　産　業　省

前文

近年、大規模な情報システムにおいて障害が相次ぎ、国民生活への影響が深刻化し、また、情報システムの大規模化、かつ他の情報システムとネットワークでつながり情報システム全体が複雑化することで、一度の情報システム障害で広範囲に影響を与える事例がますます増えてきています。この大規模化・複雑化した情報システムの障害では、障害原因の特定から完全復旧まで多大な労力と時間を必要とし、しばしば長時間にわたるサービス停止など我が国の経済活動に少なからぬ影響を及ぼすなど、情報システムの信頼性向上が喫緊の課題となっています。

このような状況を受け、経済産業省では平成18年6月15日にシステムライフサイクル全般にわたりユーザ企業とベンダ企業が遵守するべき事項を定めた「情報システムの信頼性向上に関するガイドライン」（以下、信頼性ガイドラインという。）を策定、平成19年4月13日に信頼性ガイドラインへの遵守度合いを測るための評価指標である「情報システムの信頼性向上に関する評価指標（試行版）」（以下、信頼性評価指標（試行版）という。）を策定し、情報システムの信頼性向上に向けた取組を進めてまいりました。

経済産業省では、より一層の信頼性向上の取組に向けて、信頼性評価指標（試行版）をさらに詳細化した評価指標を元に、平成19年11月に信頼性向上に関する取組状況のアンケート及びヒアリング調査を実施しました。その結果も含め、信頼性ガイドラインの利用者あるいは有識者等の意見を通じて、「記述事項全般に対して更に具体的で踏み込んだ内容の追加」、「他の指針や標準類との関係整理」、あるいは「運用フェーズ全般での不足事項の追記」など、幾つかの改善ポイントが判明いたしました。

本ガイドラインは、これら調査結果も鑑みて、ユーザ企業及びベンダ企業双方の有識者により信頼性ガイドラインの見直しを実施し、改訂版としてとりまとめたものです。

本ガイドラインが、情報システムに係る人々に積極的に活用され、情報システムの信頼性向上に寄与することを切に願っています。

信頼性ガイドライン及び評価指標の改訂検討会　名簿

岩佐洋司	住友電工情報システム株式会社
太田忠雄	株式会社ジャステック
奥沢　薫	日本電気株式会社
織田　巌	NEC システムテクノロジー株式会社
木谷　強	株式会社 NTT データ
清田辰巳	株式会社東京証券取引所
島谷二郎	東京海上日動システムズ株式会社
徳武康雄	富士通株式会社
中田雅弘	株式会社日立製作所
中村伸裕	住友電気工業株式会社
野瀬徹郎	株式会社日立製作所
古川正紀	特定非営利活動法人 埼玉ITコーディネータ
細川泰秀	社団法人 日本情報システム・ユーザー協会
柚木　勉	富士通株式会社
吉川浩史	東京ガス株式会社

目次

Ⅰ．総論 1
1. 目的 1
2. 定義 1
3. 対象 2
4. 情報システムの分類 3
(A) 重要インフラ等システム 3
(B) 企業基幹システム 3
(C) その他のシステム 3
5. 本ガイドラインの構成 3
6. 本ガイドラインで示される対策の実施 3
Ⅱ．信頼性・安全性向上に向けての全般的配慮事項 4
1. 関係者の責務 4
(1) 情報システム利用者の責務 4
(2) 情報システム供給者の責務 4
(3) 共同作業であることの認識 4
2. 経営層の責務 4
(1) 情報システム障害が経営リスクの問題であることの認識 4
(2) 経営資源の投入 5
(3) CIO (情報統括役員) の登用と活用 5
(4) 説明責任の認識 5
(5) 保守・運用の重要性の認識 5
(6) 事業継続計画の策定と訓練の実施 5
3. 未然防止と事後対策の両側面からの対策の実施 5
4. 信頼性・安全性向上に向けた多面的取組の必要性 6
5. 情報システム障害に対する動作の基本 6
Ⅲ．企画・要件定義・開発及び保守・運用全体における事項 6
1. 企画・要件定義段階における留意事項 6
(1) 信頼性・安全性水準の定義と利用者・供給者間での合意 7
(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 7
(3) 設計等上流工程における品質確保の重要性の認識 7
(4) 機能要件の実現に向けた利用者・供給者間での合意 7
(5) 非機能要件の実現に向けた利用者・供給者間での合意 8
(6) 利用者によるシステム要件に関する見解の統一 8
2. 開発段階における留意事項 8
(1) システムライフサイクルプロセスの確立と文書化 9

(2) 役割分担・責任権限の利用者・供給者間での合意 9
(3) 定量的見積りの実施 9
(4) 情報システムの複雑化の回避 9
(5) 情報システムの障害対応能力の向上 10
(6) 誤操作等防止への配慮 10
(7) テスト及びレビューの徹底 10
(8) 検収基準の明確化 11
3. 保守・運用段階における留意事項 11
(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 11
(2) 保守の取扱方針の利用者・供給者間での合意 11
(3) ニーズや環境の変化へのシステム仕様の適切な適応 11
(4) 保守に伴う変更作業・リリース手順等の整備と訓練 12
(5) 情報システムの構成情報の完全性確保 13
(6) 恒常的な運用状況の監視と管理 13
(7) 定量的見積りの実施 13
4. 障害対応に関する留意事項 14
(1) 障害発生事象の検知と対応の整備 14
(2) 問題の診断と根本原因の究明 14
(3) 再発防止に向けた障害に係る各種情報の保持と活用 14
(4) 重大な障害に対するリスクの把握と緊急対応の利用者・供給者間での合意 15
(5) 関連・類似システムの障害情報の活用と情報公開 15
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 16
(1) 経験則のみによらないプロジェクトマネジメントの導入 16
(2) 定量データを活用した管理 16
(3) 健全なプロジェクト運営に向けた活動の実施 16
(4) 第三者によるレビュー及び監査の実施 16
(5) 仕様変更の取扱に関する利用者・供給者間での合意 17
(6) 情報セキュリティ対策の実施 17
Ⅳ．技術に関する事項 17
1. 開発手法・ツールの活用及びテスト環境の整備 17
(1) 利用者・供給者間での情報共有 17
(2) 各種開発手法・ツール等の活用 18
(3) テスト環境の整備 18
2. 信頼性・安全性向上に向けた技術の活用及び留意事項 18
(1) アーキテクチャの確立 18
(2) インターネット経由のアクセスへの対処 19

(3) 信頼性･安全性に関する評価技術の活用 19
(4) 信頼性･安全性の向上に向けた先端技術の活用 19
Ⅴ．人・組織に関する事項 20
1. 人材育成･教育の実施 20
(1) 人材の育成･教育 20
2. 組織の整備 20
(1) 知識･スキルに応じた人材登用･配置 20
(2) 独立した品質保証部門の設置 21
(3) 契約の妥当性･遵守状況のチェック体制の構築 21
(4) 開発部門と運用部門の相互チェック体制の構築 21
Ⅵ．商慣行・契約・法的要素に関する事項 21
1. 契約における重要事項の明確化 22
(1) システムライフサイクルプロセス全体における重要事項の規定の明確化 22
(2) 仕様変更の取扱に関する規定の明確化 22
(3) 障害発生時の対応手順等の規定の明確化 22
(4) 障害発生時の責任関係に関する規定の明確化 22
(5) 事業継続計画における分担及び責任の明確化 22
2. 情報システム構築の分業時の役割分担及び責任関係の明確化 22
(1) 情報システム利用者を含めた複数のシステム供給者間での責任明確化 22
(2) 一部分を供給するシステム供給者の責任明確化 23
(3) 再委託先発注時のシステム供給者間の責任明確化 23
3. 着実な契約履行 23
Ⅶ．実効性に関する担保措置 23
1. モデル契約の見直し･活用 23
2. 政府調達における活用 24
3. 信頼性評価指標及び診断 (ベンチマーキング) 方法の整備 24
Ⅷ．その他の関連事項 24
1. 開発プロセスの共有化 24
2. 障害事例データベースの公開 24
3. 事例･定量データの蓄積･公開 24
4. 組込みシステムの信頼性確保 24
5. ガイドラインの定期的見直し 25
6. 安全基準等策定時における活用 25
参考：本ガイドラインに関係する法令、国際規格及び日本工業規格等 26
1. 法令 26
2. 国際規格及び日本工業規格 26
3. 基準･指針･資格類 26

添付資料

表１　情報システム障害に係る原因の種別
表２　信頼性・安全性の水準に応じた必須・推奨事項及び関連規格等

Ⅰ．総論

１．目的

現在、我が国の国民生活及び社会経済活動の IT 利用度は、コンピュータの処理性能の飛躍的向上やインターネットの普及等の結果、かつて無いほど高まっている。このため、情報システムの障害による業務・サービスの停止や機能低下の社会的影響は日々、深刻化してきており、システムの信頼性・安全性向上は喫緊の課題となっている。

本ガイドラインは、情報システムが本来保持すべき信頼性・安全性を確実に具備させることを目的とし、情報システムの企画・要件定義・開発から保守・運用にわたり関係者が遵守すべき又は遵守することが望ましい事項を定める。

情報システムに係る事業者及び関係省庁等が本ガイドラインを参照し、適切な措置を講じることが望まれる。

２．定義

本ガイドラインにおける定義を示す。

・「情報システム」

「コンピュータを用いて構成されるソフトウェア、装置・機器等のシステム及び処理・記録されるデータ・データベース」を総称したものをいう。具体的な構成要素として、個別に開発されるソフトウェア（組込みソフトウェアを含む）及びパッケージソフトウェア並びに当該ソフトウェアが動作するコンピュータ装置、周辺機器、通信装置、施設・設備及びデータ・データベース等が含まれる。複数の情報システムがネットワーク等を介して連携して一体のシステムとみなせる場合はその全体を指す。

・「情報システム関係者」

情報システムの企画・要件定義・開発及び保守・運用に携わる発注者、利用者、受注者、開発者及び運用者等を総称したものをいう。

また、**「情報システム利用者」**とは、情報システム関係者のうち、発注側の経営者、利用者、企画者、開発者、運用者及び保守者等をいい、「情報システム供給者」とは、情報システム関係者のうち、受注側の経営者、開発者、運用者及び保守者等をいう。

なお、**「情報システム利用者」**の中における、業務・運用部門等の利用部門と、情報システム部門等の供給部門との関係等を検討する際には、本ガイドラインにおける「情報システム利用者」と「情報システム供給者」を各々の役割に応じて適宜読み替えること。

・「情報システム障害」

各事業において発生する障害（サービス停止、機能低下等）のうち、IT の機能不全が引き起こす障害をいう。

情報システム障害は、通常、情報システムが内包する不具合やシステム動作に係る前提条件の運用環境下における変化等をきっかけとして引き起こさ

れ、原因としては以下のようなものが挙げられる（表１を参照)。

（１）要件の誤り
（２）ソフトウェアの誤り
（３）調達ソフトウェアの不具合
（４）ハードウェア故障・性能低下等
（５）製品間インターフェイスの誤り
（６）性能・容量等の不足
（７）移行時の誤り
（８）運用・保守方法・手順等の誤り
（９）情報システム障害発生時の対応の誤り・遅れ

・「システムライフサイクルプロセス」

情報システムの企画・要件定義・開発段階から保守・運用段階に至るプロセス全体をいう。

・「信頼性・安全性」

「信頼性」とは、与えられた状況下で定められた期間中に当該システムが提供する機能やサービスが期待通りに動作し、正しい結果を出す性質をいい、**「安全性」**とは、主として人命、経済活動及び国民生活を脅かすことを未然に防ぐ性質をいう。

・「要件」

情報システムが実現すべき事項をいい、機能要件と非機能要件から成る。**「機能要件」**とは、利用者の要求を満足するためにソフトウェアが実現しなければならない機能をいい、**「非機能要件」**とは、機能要件以外のすべての要素（性能、容量、情報セキュリティ、拡張性等）をいう。

３．対象

本ガイドラインの適用対象を示す。

・対象システム

情報システム全般を対象とする。具体的には、国民生活や社会経済活動の基盤である重要インフラ[1]及び企業等の業務システム、さらには自動車・情報家電・医療機器・携帯電話等に実装される組込みシステム等が含まれる。本ガイドラインではこれらの情報システム全般の共通指針、特にエンタープライズ系システムを想定した共通指針を定める。

・対象となる活動

システムライフサイクルプロセス全体にわたる活動全般を対象とする。

・対象者

[1] 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、我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。「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む)」、「医療」、「水道」、「物流」の 10 分野。(「重要インフラの情報セキュリティ対策に係る基本的考え方」、2005 年 9 月 15 日 情報セキュリティ政策会議決定、p.2～3)

情報システム関係者全般を対象とする。

・情報システム障害の種別

情報システムの仕様やソフトウェア・ハードウェアの欠陥、操作ミス、故障、性能・容量不足等によって引き起こされる障害、悪意のある第三者からの攻撃を対象とする。

４．情報システムの分類

本ガイドラインでは、求められる信頼性・安全性の水準に応じ、情報システムを以下のように段階的に分類する。

（A）重要インフラ等システム

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・社会経済活動の基盤であり、その機能が低下又は利用不可能な状態に陥った場合に、我が国の国民生活・社会経済活動に多大の影響を及ぼすおそれが生じるもの、人命に影響を及ぼすもの及びそれに準ずるもの。

（B）企業基幹システム

企業活動の基盤であり、その機能が低下又は利用不可能な状態に陥った場合に、当該企業活動に多大の影響を及ぼすおそれが生じるとともに、取引先や顧客等、相当程度の外部利用者にも影響を及ぼすもの。

（C）その他のシステム

重要インフラ等システム及び企業基幹システム未満の水準のもの。

５．本ガイドラインの構成

本ガイドラインでは、情報システムの信頼性・安全性水準の向上に向け、以下の各章において具体的な対策を示す。

Ⅱ．信頼性・安全性向上に向けての全般的配慮事項
Ⅲ．企画・要件定義・開発及び保守・運用全体における事項
Ⅳ．技術に関する事項
Ⅴ．人・組織に関する事項
Ⅵ．商慣行・契約・法的要素に関する事項

６．本ガイドラインで示される対策の実施

本ガイドラインで示される対策は、情報システムに求められる信頼性・安全性の水準に応じた推奨度が定められる（表２を参照）。実施に当たっては、情報システム利用者及び情報システム供給者は、対象となる情報システム及び業務等の特性を勘案の上、最適な対策を選択するとともに、具体的な適用方法を検討する。また、対策自体の見直しを行う PDCA サイクル[2]を定期的に回し継続的な改善を図るほか、障害発生時やプロジェクト完了時等に対策が計画通りに実施されているかの確認及び評価を行う。

[2] PLAN（計画）、DO（行動）、CHECK（評価）、ACTION（改善）のプロセスサイクルにより、品質の向上や業務改善を進めていくマネジメント手法。

Ⅱ．信頼性・安全性向上に向けての全般的配慮事項

１．関係者の責務

（１）情報システム利用者の責務

情報システム利用者は、業務・サービスの提供者としての責任を自覚し、業務・サービスの継続性確保の観点から、情報システムの重要度に係る要求事項を明確にし、内部における利用部門と企画及び要件定義・開発・保守・運用部門の役割分担及び責任の明確化を図らなければならない。

特に、複数の構成要素及び複数のシステム供給者の分業によるシステム構築を行う場合には、システムライフサイクル全体にわたり、利用者の視点からシステム統合状態での信頼性実現レベルを確認しなければならない。

同時に、情報システムに内在する不完全性も自覚して、業務・サービスと情報システムの機能を峻別し、仮に情報システム障害が発生した場合であっても業務・サービス本体機能の維持の為に必要な資源（人材及び予算等）及び技術等を動員して業務・サービス本体機能の維持に努める。また、ノウハウ蓄積、組織整備、人材育成を図り、事前に障害対策及び定期的な訓練とその評価を行わなければならない。

（２）情報システム供給者の責務

情報システム供給者は、情報システム利用者と合意した役割及び責任を果たすため、そのシステム供給に対し最大限努力するとともに、情報システム利用者に対する重要事項等の説明及び必要な情報の提供等、情報システム利用者の支援に努めなければならない。

また、自らが供給するシステムの信頼性・安全性水準の向上に向け、情報システムの企画・要件定義・開発及び保守・運用に係る技術の向上、組織整備、人材育成等、多面的な取組を恒常的に行わなければならない。

（３）共同作業であることの認識

情報システム利用者及び情報システム供給者は、上記（１）、（２）の責務を踏まえた上で、システムライフサイクルプロセスの円滑な実施及び管理のためには両者の協力が重要であるとの認識に立ち、それぞれが担うべき役割及び責任を果たさなければならない。

特に、昨今、情報システムはネットワークを介し他の情報システムと連携することが一般的であることに鑑み、ネットワークを含めた全体の信頼性向上を図るために、ネットワーク等インフラ提供者とも連携し、役割分担を定め関係者で合意し、情報システムの運用を行う必要がある。

２．経営層の責務

（１）情報システム障害が経営リスクの問題であることの認識

情報システム利用者及び情報システム供給者の経営層は、情報システム障害の発生は、内部統制の破綻及び両者の甚大なビジネス上の被害と、社会的信頼を失墜させる経営リスクの問題であり、経営層による直接関与が必要であることを認識しなければならない。

（2）経営資源の投入

情報システム利用者及び情報システム供給者の経営層は、上記「１．関係者の責務」におけるそれぞれの責務を踏まえた上で、業務・サービス及び情報システムの信頼性・安全性の向上に向け、自らの責任を契約の中で明確にし、その責任に基づいて人的資源や開発設備等へ必要な経営資源を投入しなければならない。

一方で、要件定義が完了しないままプロジェクトが開始され、途中で追加要求が発生して開発規模が増加し、残余スケジュールの遅延リスクや品質劣化リスクの増大を招くことや、現状の経営資源と比較して過大となる情報システム開発案件を抱えることによる組織コントロールの低下リスク等の様々なリスクを勘案し、適正な開発規模に制御できる経営マネジメントを行わなければならない。

（3）CIO（情報統括役員）の登用と活用

情報システム利用者の経営層は、経営戦略及び情報戦略双方に対する理解及び判断が可能な人材を CIO として登用した上で、全体に対する投資の管理強化及び効率化等に向けて積極的に活用し、また、関係部門間の調整を図り、業務・サービス及び情報システムの信頼性・安全性向上に努めなければならない。

（4）説明責任の認識

情報システム利用者及び情報システム供給者の経営層は、情報システム及びそれが提供する業務・サービスに対して、双方への説明責任とエンドユーザへの説明責任について十分認識し、責務を果たさなければならない。

（5）保守・運用の重要性の認識

情報システムが提供する業務・サービスに対するビジネスニーズ及び取り巻く環境は常に変化する。情報システムが変化に対応し、常に最適な状態を保つためには、変化の予測と恒常的な改善が不可欠である。

特に情報システム利用者側の経営層は、変化の予測と改善活動の必要性を十分に理解し、それらを情報システムに反映させるための保守・運用段階における継続的経営資源の投入の重要性を認識しなければならない。

（6）事業継続計画の策定と訓練の実施

情報システム利用者の経営層は、情報システムに内在する不完全性を前提として、提供する業務・サービスの事業継続計画（BCP：Business Continuity Plan）の策定及び継続的な訓練を実施し、情報システム障害等の緊急時において、計画どおりに業務を継続できるようにしなければならない。一方、情報システム供給者の経営層も、契約等に基づき、当該計画を理解し、情報システム利用者が実施する訓練等が効果的かつ継続的に実現可能なように、計画や推進に関する技術的・人的な支援に努めなければならない。

３．未然防止と事後対策の両側面からの対策の実施

現在の情報システムは、大規模化・複雑化が進み、その構成要素も多種多様であることから、障害が発生する可能性を出来る限り抑える「未然防止」と、

障害発生時に業務への影響を最小限に抑える「事後対策（被害拡大防止、迅速な復旧、再発防止等）」の両側面からの対策が必要である。

４．信頼性・安全性向上に向けた多面的取組の必要性

情報システムの信頼性・安全性向上に向けた対策を実施するに当たっては、当該システムの重要性に応じて求められる信頼性・安全性の水準（JIS X0134：1999 システムおよびソフトウェアに課せられたリスク抑制の完全性水準　参照）を認識及び決定した上で、起こりうる情報システム障害を分析し、原因の種別（表１を参照）それぞれについて多面的な対策を講じなければならない。

また、情報システム利用者及び情報システム供給者は、情報システム利用者の経営層と協議しつつ、情報システムで利用する情報資産[3]を洗い出し、情報セキュリティ上のリスクを特定した上で分析・評価し、情報セキュリティ対策を講じなければならない。

当該対策を講じるに当たっては、情報システム利用者及び情報システム供給者双方の役割分担及び責任権限等を検討の上、合意しなければならない。

５．情報システム障害に対する動作の基本

情報システム利用者及び情報システム供給者は、情報システム障害に対処し、情報システムの信頼性・安全性向上を実現するため、以下の 4 つの観点からの措置を講じなければならない。

・情報システム関係者への情報システム障害の状況に関する迅速な周知
・情報システム障害の原因・要因の究明と除去
・情報システム障害の再発及び類似障害発生の防止
・情報システム障害による影響拡大の防止

III．企画・要件定義・開発及び保守・運用全体における事項

情報システム利用者及び情報システム供給者は、情報システムの重要性に応じて求められる信頼性・安全性の水準を実現すべく、企画・要件定義・開発段階から保守・運用段階のシステムライフサイクルプロセス全般にわたり、以下の事項について明確化し、共有しなければならない。システム再構築の場合でも、現行システムを含むすべての再構築範囲に対して、求められる信頼性・安全性の水準に応じて、新規開発の場合と同等の取り組みを行わなければならない。また、これらの内容は情報システム関係者間に周知徹底の上、確実に実行されなければならない。

１．企画・要件定義段階における留意事項

企画・要件定義段階において、情報システム利用者及び情報システム供給者は、情報システムの重要性に応じて求められる信頼性・安全性の水準を正しく認識及び決定しなければならない。また、常に当該システムが既存システムの信頼性・安全性に与える影響について分析、把握しておかなければならない。

その上で、当該システムの信頼性・安全性を実現するため、システムの機能要件及び非機能要件を整理、確認及び決定しなければならない。以下に具体的な方策を示す。

[3] 組織にとって価値をもつ情報

（1）信頼性・安全性水準の定義と利用者・供給者間での合意

情報システム利用者及び情報システム供給者は、前提事項、制約事項を明らかにした上で、情報システム全体の重要度又はサブシステム等情報システムの一部の重要度を明確にし、それらに応じて求められる信頼性・安全性の水準について定め、両者で合意すること。

（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

情報システム利用者は、情報システムの企画・要件定義に当たり、情報システム供給者に対し、情報システムに求める機能要件及び非機能要件並びにそれぞれに対する重要度、前提事項及び運用環境等を明らかにした上で、発注仕様を明確化及び文書化すること。

また、複数の情報システム供給者の分業によるシステム構築を行う場合には、役割分担や責任関係の複雑化により、情報システム全体の信頼性確保に影響を及ぼす可能性を考慮した上で、分担範囲について予め発注仕様に明確に定めておくことが重要である。

非機能要件については見落としがちであることから、情報システム利用者は経営層を含めて十分に検討を行うこと。

この時、情報システム供給者は情報システム開発のプロフェッショナルとして情報システム利用者に対して情報提供等を行い、意思決定を積極的に支援すること。

＜実施例＞

機能要件の具体化に当たっては、要求内容の妥当性の判断と実現に関する客観的な判断を可能とする必要がある。このため具体的な要求内容とその背景・理由、要求に関する定量的指標項目とその具体的な数値などを要求仕様定義ガイドライン[JUAS1]を参考に文書化する。さらに、情報システムに対する要求、基本設計書、外部設計書、内部設計書、テスト仕様書など、フェーズ全般にわたる各文書の構成管理を確実に実施する。

（3）設計等上流工程における品質確保の重要性の認識

要件定義や設計等上流工程における不具合は、後工程になるほど対応が困難となり、情報システムの品質・納期・コストに多大な影響を及ぼすことから、情報システム利用者及び情報システム供給者は、上流工程における品質確保の重要性を認識し、レビューやプロトタイピング実施等を行い、開発に入る前の品質確保に努めること。

（4）機能要件の実現に向けた利用者・供給者間での合意

情報システム利用者及び情報システム供給者は、発注仕様に定める機能要件及びその実現性並びに実現・運用コスト等について明確化及び文書化し、経営層を含め、合意すること。

特に企画・要件定義段階における仕様の曖昧さは開発の遅れやトラブルを誘発する可能性が高いことから、両者で緊密な協力のもと、精度の向上に努めること。

＜実施例＞

要求仕様定義ガイドライン [JUAS1]を参照の上、機能要件を明確にし、情報システム利用者及び情報システム供給者間において、技術的・コスト的な実現可能性について合意する。さらに、情報システムに対する要求、基本設計書、外部設計書、内部設計書、テスト仕様書など、フェーズ全般にわたる各文書の構成管理を確実に実施する。

（5）非機能要件の実現に向けた利用者・供給者間での合意

情報システム供給者は、情報システムの重要性に応じて求められた信頼性・安全性水準の達成に向け、ソフトウェアの品質に関する特性[4]に基づいて具体的な非機能要件を検討し、情報システム利用者に対する十分な説明を行うこと。

また、その内容及び評価指標のみならず、その実現性、関連技術（負荷分散、二重化・多重化、バックアップ等）及び実現・運用コストについて明確化及び文書化し、事業継続計画を勘案の上、情報システム利用者との間で経営層を含め、合意すること。

その際、情報システム利用者の経営層は、信頼性・安全性と実現・運用コストはトレードオフの関係にあり、高い水準の達成には相応のコスト及び時間を必要とすることを認識しなければならない。

＜実施例＞

JIS X 0129 及び非機能要求仕様定義ガイドライン UVCⅡ [JUAS2]を参照し非機能要件を明確にする。その上で情報システム利用者及び情報システム供給者による合同レビューを実施し、技術的・コスト的な実現可能性について合意する。

（6）利用者によるシステム要件に関する見解の統一

仕様の策定に当たり、情報システム利用者は、運用部門、情報システム関連部門、また必要に応じて経営層等、すべての関係者が見解を統一した上で情報システム供給者に対して要件を伝えていくこと。

また、情報システム利用者は、情報システム供給者に対し、システム要件に関する説明責任及び最終的な確定の責任があることを自覚すること。

＜実施例＞

情報システム利用者側のすべての関係者による合意形成のための仕組、手順等を確立し、実施する。

２．開発段階における留意事項

開発段階において、情報システム利用者及び情報システム供給者は、情報システムの重要性に応じて求められる信頼性・安全性水準の達成に向け、信頼性・安全性の検証・確認作業を含めた適切なシステムライフサイクルプロセスを確立し、実行しなければならない。以下に具体的な方策を示す。

---

[4] ソフトウェアの品質の特性は、以下のように分類される。(1)信頼性：指定された達成水準を維持する特性、(2)保守性：修正のしやすさに関する特性、(3)移植性：ある環境から他の環境に移すための特性、(4)効率性：使用する資源の量に対比して適切な性能を提供する特性、(5)機能性：明示的及び暗示的必要性に合致する機能を提供する特性、(6)使用性：理解、習得、利用でき、利用者にとって魅力的である特性（JIS X 0129）。

（1）システムライフサイクルプロセスの確立と文書化

情報システム供給者及び情報システム利用者は、情報システムの重要性に応じて求められる信頼性・安全性水準の達成を確実なものにするシステムライフサイクルプロセスを確立し、文書化する。

また、この文書化されたプロセスの実際のプロジェクトにおける実行を確実なものとするため、評価及び是正措置等を実施すること。

＜実施例＞

共通フレーム 2007[IPA1]を参照し、ライフサイクルプロセスを確立し、合意して文書化する。また、国際標準、国内標準を踏まえつつ、各プロセスで利用する組織内標準（各種ドキュメント雛形等）を策定する。

（2）役割分担・責任権限の利用者・供給者間での合意

情報システム供給者及び情報システム利用者は、システムライフサイクルプロセスに関する情報の共有化を図り、企画・要件定義・開発から保守・運用に至る各プロセスにおける役割分担及び責任権限等を明確化し、合意すること。

特に、国際分業も含め複数企業による開発体制になる場合、関係者間での情報の共有化、意思疎通に留意し、上記内容の合意を確実に行うこと。

＜実施例＞

共通フレーム 2007[IPA1]及び情報システム・モデル取引・契約書[METI6]を参照し、個々のプロセスに関する双方の役割・責任を契約書の中で明確にするとともに、各種ドキュメント、達成基準等をシステム開発の開始に先立って、情報システム利用者及び情報システム供給者間で合意しておく。

（3）定量的見積りの実施

情報システム供給者は、求められる信頼性・安全性の水準を満たす情報システムの開発にかかる価格の見積値を、その算出根拠（機能及び非機能要件、必要なソフトウェア、ハードウェア及び諸設備費用、規模、工数、工期、リスク等）とともに情報システム利用者に説明し、以降のプロジェクトマネジメントへのインプットとして有効に活用すること。情報システム利用者も定量的見積りを行い、自らの見積りに基づいて情報システム供給者と合意すること。

＜実施例＞

ソフトウェア開発見積りガイドブック[IPA2]を参考に、機能規模についてファンクションポイント法[5]等を活用した工数見積りを実施し、価格の算出根拠の一つとする。

（4）情報システムの複雑化の回避

情報システム利用者はシステムの大規模化や複雑化を極力回避するためにシステム化の範囲を適切に設定すること。情報システム供給者は大規模化及び複雑化を極力抑える設計を心がけること。

---

[5] ソフトウェアの機能(ファンクション)に注目し、これを数値化することにより、ソフトウェアの規模を獲得する技術。

＜実施例＞

情報システム利用者は、システム要件の取りまとめにおいて、既存の業務フローを見直し、システム処理を前提とした業務フローの策定やカバーする範囲の優先順位付けを行い、大規模化や複雑化の回避を図る。設計段階以降における新たな機能追加や改修は相当の費用と開発期間を伴うことを理解し、その必要性や費用対効果の十分な評価なしにシステム化範囲を拡大しないように適切な統制を実施する。情報システム供給者は既存の高品質なフレームワークやライブラリ等の積極的・効率的な活用により、与えられた要件に対してより簡略な設計を行う。

（5）情報システムの障害対応能力の向上

情報システム利用者及び情報システム供給者は、情報システムの設計に当たり、フェイルセーフ[6]の観点から、各種障害に対して発生時の業務・サービスへの影響の防止及び最小化に努めること。

＜実施例＞

システム構成要素や機能の多重化、ファイルの自動バックアップ機能、自動停止（あるいは縮退）機能、迅速な障害根本原因追求のための診断機能等を設計に織り込む。

（6）誤操作等防止への配慮

情報システム利用者及び情報システム供給者は、各種ユーザインタフェイス等の設計に当たり、フールプルーフ[7]の観点から、誤操作等の防止に努めること。

＜実施例＞

画面設計において、選択式の入力方式や確認を求めるダイアログ表示等、誤操作の防止に配慮した部品配置及び画面遷移等を行う。

（7）テスト及びレビューの徹底

情報システム供給者は、情報システムに求められる信頼性・安全性の水準に対応した品質保証計画（テスト計画、レビュー計画等）を作成し、情報システム利用者と合意すること。また、両者は、当該品質保証計画を着実に実行し、情報システムの機能要件及び非機能要件に対する適合性の確認に努めること。

特に、情報システム利用者による仕様適合性の確認及び実環境における稼動の確認に向け、情報システム利用者の協力によるテスト及び試行等を実施すること。

＜実施例＞

基本機能及び情報システムのテストのレビューに当たっては、利用者、運用部門等情報システム運用に係る関係者が参加し、運用の観点からのレビューを実施する。また、他システムとの連携も含め、本番に近い環境でテストを実施する。テスト及びレビューに当たっては、定量的指標に基づき

[6] 構成要素に故障を生じても安全性が保持されるように配慮された設計。
[7] 人為的に不適切な行為又は過失等が起こっても、信頼性及び安全性を保持する性質。

実施状況を把握する。なお、個別技法についてはソフトウェア品質知識体系ガイド[SQuBOK]を参照し、レビュー技法、テスト技法を評価した上で、活用する。

（8）検収基準の明確化

情報システム利用者は情報システム供給者に対し、明確かつ定量的な検収（受入）基準を提示すること。当該基準の作成に際し、情報システム供給者は、情報システム利用者に対して技術的な情報提供等を行い、積極的に支援すること。

＜実施例＞

非機能要件に関して、非機能要求仕様定義ガイドライン UVCⅡ[JUAS2]を参照し、評価及び判断可能な目標値を設定する。テストにおける検収基準に関しては、ソフトウェアテスト見積りガイドブック[IPA5]を参照する。

３．保守・運用段階における留意事項

保守・運用段階において、情報システム利用者及び情報システム供給者は、情報システムの重要性に応じて求められる信頼性・安全性水準の達成に向け、協同して適切な保守・運用を実行しなければならない。以下に具体的な方策を示す。

（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

情報システム利用者及び情報システム供給者は、安定した運用を維持し続けられるよう、体制の不備に起因するリスクの軽減を念頭におき、運用・保守のプロセス活動全般を実行するための機能を果たす推進体制（サプライヤなどを含む関係者全体での指揮命令系統、役割分担、責任権限等）及び承認手順を含む業務フロー等を整備・文書化し、両者で合意すること。

＜実施例＞

情報システム利用者及び情報システム供給者は、運用保守体制図及び運用フロー図を作成し、合意する。ISO/IEC 20000 のマネジメントシステムに関する事項等を参照し、体制等を整える。

（2）保守の取扱方針の利用者・供給者間での合意

情報システム利用者及び情報システム供給者は、保守に関し、訂正に係る保守（是正保守、予防保守）と改良に係る保守（適用保守、完全化保守）を峻別し、それぞれの保守内容について両者で合意すること。

＜実施例＞

情報システムの障害内容や保守対象部位により、影響度や重要性の段階（ランク）を定義し、それぞれのランクに応じた対応内容を文書化しておく。

（3）ニーズや環境の変化へのシステム仕様の適切な適応

ビジネスニーズや様々な環境の変化に伴い、企画・要件定義・開発の段階で合意された情報システムに対する要求仕様が保守・運用段階において変化

する可能性がある。情報システム利用者及び情報システム供給者は、情報システムの機能、可用性のレベル、キャパシティ等、情報システムに求められる要求の変化に対し、適正なコストと時間で対応するための評価及び管理等の活動を恒常的に実施し、必要に応じて改善策をとること。

また、悪意ある第三者からの攻撃に対しては、攻撃手法が日々進化していることを十分に考慮した上で、調達ソフトウェアに関する脆弱性及びパッチについても、最新の状況につき恒常的に情報収集を行い、必要に応じて対応を実施すること。

＜実施例＞

ISO/IEC 20000 等を参照して、機能、可用性、キャパシティ等に関するチェックリストを作成し、レビュー会議等で定期的に適用・点検する等の管理施策を検討する。

脆弱性に関する情報については、IPA、JPCERT/CC が運営している脆弱性対策情報ポータルサイトである JVN（Japan Vulnerability Notes）などを活用して情報収集を行った上、対策を実施する。

重要インフラ等システムや企業基幹システムで中核的役割を担うデータベースに対しては、データ量やアクセス件数の増加等の変化を恒常的に監視し、対応できる体制を整備する。

（4）保守に伴う変更作業・リリース手順等の整備と訓練

情報システム利用者及び情報システム供給者は、保守に伴う変更による事業へのリスクや影響を最小化し、迅速な変更管理を実現するために、両者間の契約に基づき、協力して以下の施策を検討すること。

- 変更作業・リリースの正式な承認と関係者・部署への通知のプロセスを整備する。
- 情報システムの保守や変更の目的や前提事項を確認し、変更によるリスクや影響を評価する。
- 変更内容に応じた、変更作業の仕掛け（手法）や手順の標準化により、作業精度の向上や効率化を図る。
- 変更内容の妥当性の確認・テストを十分行った上でリリースし、現場への効果的な利用を定着させる。
- 開発部門と保守/運用部門を分離し、牽制効果を持たせる事により、標準ルールの逸脱によるトラブル発生の防止を図る。
- 変更作業・リリースによって障害が発生した場合の対応手順（変更前への切り戻し手順、等）を整備する。
- 変更作業に起因して発生したサービスへの影響、標準ルールからの逸脱、顕在化/潜在するリスクや課題を記録、分析し必要な是正処置をとる。
- 必要に応じて、データやプログラムを保護するための対策を講じる。

＜実施例＞

マニュアルに基づく情報システムの導入訓練や緊急対応訓練を情報システ

ム関係者間で実施する。変更作業に際しては、影響するモジュール（プログラム）を特定し、予め作成しておいたテストデータを基に回帰テスト[8]を行う。また、新システムへの移行の前に、他システムとの連携や、データ移行、システム切替に関する検証方法を準備し、リハーサルを行う。また移行完了までに、利用部門へ新システム導入に伴う新しい業務取扱内容を周知するとともに、新システムの内容・操作について研修を行う。併せて、ISO/IEC 20000 の変更管理及びリリース管理に関する事項等を参照し、管理を実施する。

（５）情報システムの構成情報の完全性確保

情報システム利用者及び情報システム供給者は、情報システムの不適切な構成に起因する品質低下の問題を最小限に抑えるため、両者間の契約に基づき、協力して以下の施策を検討すること。

- システムライフサイクルを通して提供するサービスと構成アイテム（情報システム資源）を定義し、管理対象を明確化すること。
- 情報システム資源の各世代（過去の状態、計画された状態、及び現在の状態）に関する、正確な構成情報の維持を可能とする設備やツールを具備し、必要に応じて適宜に当該情報を利用可能にすること。

＜実施例＞

構成管理ツールや不具合管理ツール等を活用し、問題追跡性を確保する。ISO/IEC 20000 の構成管理に関する事項等を参照し、管理を実施する。

（６）恒常的な運用状況の監視と管理

運用を担当する情報システム供給者は、情報システム利用者の合意のもと、情報システムの運用状況に関するデータ（処理件数、性能等)を確実に取得及び蓄積するなど恒常的な監視を行い、両者の間で共有すること。また、監視中に情報システムに何らかの不具合を認めた場合、情報システム利用者とあらかじめ定めたプロセスに従って適切な対処を行うこと。情報システム利用者は監視中にシステム能力不足や、ビジネスの実態と情報システムの提供する機能の乖離等の兆候を認めた場合、情報システム資源や機能の見直し等の然るべき対応を行うこと。

＜実施例＞

情報システムの稼動状況を日・週・月・年単位で取得し、分析を行い、情報システム利用者に対して報告する。ISO/IEC 20000 の監視、測定及びレビュー、継続的改善に関する事項等を参照し、管理を実施する。

（７）定量的見積りの実施

情報システム供給者及び情報システム利用者は、求められる信頼性・安全性の水準を満たす情報システムの保守・運用に必要となる価格の見積値を、その算出根拠（必要なソフトウェア、ハードウェア及び諸設備費用、規模、要員、工数、工期、リスク等）とともに明確にすること。

[8] プログラムに変更を加えた場合に別の部分に影響が出ていないかを確認するテスト。

＜実施例＞

システム・リファレンス・マニュアル[JUAS5]の保守・運用の指標及びソフトウェア改良開発見積りガイドブック[IPA3]を参照し、情報システム供給者、情報システム利用者双方にとって納得性の高い見積値で合意する。

４．障害対応に関する留意事項

情報システム利用者及び情報システム供給者は、情報システムの想定運用環境において発生が予測される情報システム障害時の影響評価及び対応等を予め検討し、手順を整備し、情報システム関係者に周知徹底しておかなければならない。

また、実際の障害発生時には手順に従い影響評価を実施し、情報システム関係者や間接的影響者に速やかに告知の上、対策を講じなければならない。以下に具体的な方策を示す。

（１）障害発生事象の検知と対応の整備

情報システム利用者及び情報システム供給者は、障害発生等による計画外のサービス中断や品質低下の検出、障害の現象から欠陥箇所の究明、サービスの回復を可能な限り迅速に行い、両者で合意したレベルのサービスを回復するための復旧処置を施す機能を果たす体制・手順と機能・設備を整備し、事業運営への影響を最小限に抑えること。なお、情報システムを構成する主要なコンポーネント全体について当該機能の実現内容を両者で共有・合意すること。調達ソフトウェアやハードウェア製品等の供給者の協力も不可欠な場合もあることから、情報システム利用者及び情報システム供給者はこれらの製品供給者も体制に組み入れることを検討し、実現可能な対応範囲を両者の間で合意すること。

＜実施例＞

ISO/IEC 20000 のインシデント管理に関する事項等を参照し、管理を実施する。

（２）問題の診断と根本原因の究明

情報システム利用者及び情報システム供給者は、障害、品質の低下等の問題を客観的な方法等を用いて診断し、根本原因及び見逃されてしまった原因やそれらの解決策について究明し、それらの情報を確実に記録し再発防止に努める機能を果たす手順及び体制を整備すること。

＜実施例＞

情報システム障害の原因を、情報システム障害に係る原因の種別（表 1 を参照）で特定したあと、「当該原因がなぜ作りこまれたのか」、「なぜ発見できなかったのか」等、さらに根本原因の究明を行い、情報システム利用者及び情報システム供給者間で共有し再発防止を図る。併せて、ISO/IEC 20000 の問題管理に関する事項等を参照し、管理を実施する。

（３）再発防止に向けた障害に係る各種情報の保持と活用

情報システム障害の内容、影響（大きさ、範囲、継続期間、二次三次の関連障害の可能性等)、その原因及び解決策・対策等の事柄を確実に記録し、情報システム利用者及び情報システム供給者の間で経営層も含めて共有すること。

＜実施例＞

情報システム障害管理データベースを整備し、情報システム関係者間で共有化する。また、ISO/IEC 20000 の問題管理に関する事項等を参照し、管理を実施する。

（4）重大な障害に対するリスクの把握と緊急対応の利用者・供給者間での合意

情報システム利用者及び情報システム供給者は、災害に相当する重大な事象による情報システム障害等の緊急時の影響度に応じた継続性と復旧を実現する適切な対応手順（緊急時対応計画)を確実に整備し、経営層まで含めた指揮命令系統を明記した文書化及びマニュアル化を行い、両者で合意・共有すること。

その際、情報システム利用者は、情報サービスの損失が事業に与える影響を明らかにし、また、継続性に対する潜在的な脅威とその脅威が現実になる可能性を識別し、識別された脅威の管理対策をとるリスク管理を行ったうえで、適切な手順を整備すること。また、必要に応じて定期的に訓練等を実施し、対応手順を確認しておくこと。

情報システム供給者は情報システム利用者の行うこれらの活動に、あらかじめ定められた範囲で参画し、重大な障害に対するリスク把握と緊急対策が適切に実施されるよう協力すること。

＜実施例＞

情報システム利用者は事業継続計画策定ガイドライン[METI7]等を参照して策定した事業継続計画に基づき、情報システム障害発生時の対応手順・マニュアルを整備し、定期的な訓練等をしておく。事業継続計画の一環として本項目は実施されるが、事業継続計画策定のうち、IT に係る部分に関して IT サービス継続ガイドライン[METI5]が公表されており、参考とする。併せて、ISO/IEC 20000 のサービス継続性及び可用性管理に関する事項等を参照する。

（5）関連・類似システムの障害情報の活用と情報公開

情報システム利用者及び情報システム供給者は、自らに直接関係のない情報システムの障害であっても、情報の収集に努め、教訓とすること。

また、障害を起こした情報システムが重要インフラ等システムに相当するもの、あるいは広く経済的、社会的影響を与える情報システムである場合、原因究明を体系的に行い、その結果について、秘密及び開示による二次被害リスク等を勘案の上、情報システム関係者を問わず広く情報共有することが望ましい。

＜実施例＞

利用者、顧客への代替措置の周知、2 次被害や再発の防止などを目的とした、障害の事実、経過、原因、措置を含めた広報体制を確立する。

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

情報システム利用者及び情報システム供給者は、情報システムの重要性に応じて求められる信頼性・安全性水準の達成に向け、システムライフサイクルプロセス全体を通して適切な実施体制、管理体制、仕組及びルール等を整備し、これらを活用しなければならない。以下に具体的な方策を示す。

（１）経験則のみによらないプロジェクトマネジメントの導入

情報システム利用者及び情報システム供給者は、網羅的かつ定量的手法を取り入れたプロジェクトマネジメント方法を確立し、品質、コスト、進捗及びリスク等の事柄に関し、経験則のみによらないマネジメントを行うこと。

＜実施例＞

測定データの収集、分析、フィードバックと制御の組織的な手順を確立し、プロジェクトのスコープのぶれをなくすためのマネジメントを確立するなど、定量的プロジェクトマネジメントのための環境を整え、PMBOK[PMBOK]や P2M 等を参照し、定量的なコスト及び進捗の管理手法（アーンドバリューマネジメント[9]等）を導入する。

（２）定量データを活用した管理

情報システム利用者及び情報システム供給者は、見積り、サービス品質、ソフトウェア品質及びテスト等に関する指標の定量的な測定法を定め、データを収集及び共有し、情報システム利用者と情報システム供給者双方による管理及び目標達成に向けた活動に活用すること。

＜実施例＞

定量的品質予測のススメ[IPA4]、ユーザ企業ソフトウェアメトリックス調査[JUAS3]、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[JISA1]等を参照し、各フェーズに関する定量的な指標を活用し、EPM(Empirical Project Monitor)等のツールも利用しつつ、品質目標の達成に向けた管理を行う。

（３）健全なプロジェクト運営に向けた活動の実施

情報システム利用者及び情報システム供給者は、健全なプロジェクト運営に向け、個々のプロジェクトへの支援環境の整備並びに恒常的な労働環境のモニタリング及び改善等の活動を行うこと。

＜実施例＞

PMBOK[PMBOK]を参照し、社内にプロジェクトを横断的に支援する組織（PMO：Project Management Office 等）を設置する。

（４）第三者によるレビュー及び監査の実施

情報システム利用者及び情報システム供給者は、企画・要件定義・開発及び保守・運用段階全体における各局面において、品質保証部門及び技術部門等、情報システム関係者から見て第三者（専門家、部門、企業・機関等）に

[9] プロジェクトにおける進捗及び達成度等を金額（アーンドバリュー）に換算し、定量的に管理する手法。

よるレビュー及びシステム監査等を実施すること。実施レベルについては、求められる信頼性・安全性の水準によって判断すること。

＜実施例＞

システム監査基準及びシステム管理基準を活用したシステム監査を実施する。また監査結果については、監査者と被監査者の間で事実確認及び十分な意見交換を行い、問題があると認められた点について適切な改善を行う。

（５）仕様変更の取扱に関する利用者・供給者間での合意

情報システム利用者及び情報システム供給者は、仕様変更の必要性と仕様変更に伴う影響（開発規模、テスト量、見積りの前提条件の変化等）とのバランスに十分留意するとともに、プロジェクト運営途中における仕様変更の取扱について両者で合意し、仕様の変更管理を徹底すること。

＜実施例＞

情報システム利用者と情報システム供給者は、仕様変更の認定基準、仕様変更に伴う量（変更追加量、変更棄却量など)、変更回数及び変更タイミングなどを明確にし、両者で合意する。(ソフトウェアテスト見積りガイドブック［IPA5］の「仕様変更と開発量」を参照)

（６）情報セキュリティ対策の実施

情報システム利用者及び情報システム供給者は、情報システムで扱う情報資産を洗い出し、リスクを特定した上で分析・評価し、適切な情報セキュリティ対策を講じること。また、情報セキュリティ対策の効果の確認と見直しを継続的に実施すること。

＜実施例＞

JIS Q 27001、JIS Q 27002、情報セキュリティ管理基準を参考に情報セキュリティ対策を実施する。また、定期的に情報セキュリティ監査基準及び情報セキュリティ管理基準を活用した第三者による情報セキュリティ監査を実施し、発見された問題点について適切な改善を行う。

Ⅳ．技術に関する事項

情報システム利用者及び情報システム供給者は、利用者・供給者間で合意した情報システムの信頼性・安全性の水準の達成に向け、的確に標準・規格、技術及び製品等を活用すること。

１．開発手法・ツールの活用及びテスト環境の整備

求められる信頼性・安全性の水準を達成するため、必要と考えられる開発手法及びツール等を活用し、テスト環境を整備すること。新規の手法やツールを採用する際には、事前の適用評価を行うこと。以下に具体的な方策を示す。

（１）利用者・供給者間での情報共有

情報システム供給者及び情報システム利用者の間で、設計情報及び中間成果物等に関する情報の共有化に向け、各種手法及びツール等を活用すること。

その際、円滑な情報の共有化に向け、必要に応じ、情報システム供給者は情報システム利用者に対し教育等の支援を行うこと。

＜実施例＞

要求仕様定義ガイドライン[JUAS1]等を参考に情報システム利用者及び情報システム供給者共通の要件定義記法を定めるとともに、モデル化言語等により設計文書の記法及び書式等を統一し、グループウェア等を利用して情報システム関係者間で共有する。

（2）各種開発手法・ツール等の活用

情報システム供給者及び情報システム利用者は、要件定義の曖昧性やソフトウェア設計及びソフトウェアコード作成時の不具合など、各フェーズにおける人手による作業の誤りを極力排除するため、各種開発手法やテスト手法、開発環境及びツール、プロジェクト管理用ツール等を評価の上、活用すること。また、高品質なフレームワーク、クラスライブラリなどの再利用を進め、プログラムの品質を高めること。

＜実施例＞

要件定義・設計時にモデリングツールを活用する。特に高水準の信頼性・安全性が求められるソフトウェアには形式手法の活用も検討する。テスト時には単体テストツールを始め、負荷テストツール、コードインスペクションツール等、求められる信頼性・安全性に応じて各種テストツールを活用する。

（3）テスト環境の整備

情報システム利用者は情報システム供給者の協力のもと、本番稼動環境と完全に切り離したうえで、本番稼動環境に近いテスト環境を用意すること。

＜実施例＞

ハードウェア、ソフトウェア、ネットワーク、データ、パラメータ設定値等、本番稼動環境と近い条件のテスト環境を用意する。本番稼動後の保守における検証評価環境やリリース時のテスト環境としても活用する。

２．信頼性・安全性向上に向けた技術の活用及び留意事項

情報システム利用者及び情報システム供給者は、利用者・供給者間で合意した情報システムの信頼性・安全性水準の達成に向け、信頼性・安全性の向上を実現するメカニズム（機構）を情報システムに組み込むこと。

また、当該メカニズムが想定する動作環境下において情報システム障害を未然に防ぐ、又は、障害が発生した際の影響を最小化する効果があることを確認しておくこと。以下に具体的な方策を示す。

（1）アーキテクチャの確立

情報システム利用者は、情報システム供給者の協力のもと、将来にわたるシステム全体の効率化及び最適化に向け、信頼性、効率性、拡張性及び保守性等の観点から、アーキテクチャの確立又は実績のあるアーキテクチャの活用を行うこと。

＜実施例＞

EA 策定ガイドライン[METI2]を参照し、アーキテクチャを確立する。IPA が提供するオープンな標準に関する適合性評価機能等を活用することで、システム間の相互運用性を確保し、開放的で柔軟な情報システムの構築を図るべく、オープンな標準の活用を検討する。

（2）インターネット経由のアクセスへの対処

家庭用インターネット環境及びインターネットアクセス機能付き携帯電話等の普及により、一般利用者向け Web システムへのアクセスは急激に増加及び多様化している。これに伴い、個人情報やクレジットカード情報等の流出のリスクも増大している。

これに対処するため、情報システム供給者及び情報システム利用者は、性能・容量及び情報セキュリティ等に関するリスクを十分検討の上、技術面及び運用面を含めた多面的な対策を講じること。その際、マルウェア等悪意のある第三者からの攻撃に対しては、攻撃手法が日々進化していることに留意すること。また、情報システム障害及び情報セキュリティ上の問題等の発生時には、事業継続計画に従い、業務・サービスへの影響を最小限に抑えること。

＜実施例＞

システム負荷の分散機能及び負荷・容量過多等による障害発生時の縮退機能等を設計に追加する。さらに IT サービス継続ガイドライン[METI5]等を参考に技術的対策及び運用的対策を実施する。情報セキュリティ確保のために、IPA セキュリティセンターや JPCERT/CC 等で公開されているガイドライン、ツール類を活用し、情報セキュリティ対策を定期的、継続的に実施する。

（3）信頼性・安全性に関する評価技術の活用

情報システム利用者は、情報システム供給者の協力のもと、開発段階において故障分析等の手法を活用し、情報システムの信頼性・安全性について評価の上、予防に向けた対策を講じること。

＜実施例＞

ソフトウェア品質知識体系ガイド[SQuBOK]で指摘されている信頼性予測、品質進捗管理、障害分析、データ解析・表現などに関する各種技法を評価し、活用を検討する。また、安全水準の設定方法については JIS C 0508:2000 を参考に設定する。

（4）信頼性・安全性の向上に向けた先端技術の活用

情報システム供給者は、自律分散の考え方を応用したシステム負荷の分散方式等、性能・容量等の確保及び向上並びにそれらの拡張性向上に寄与する先端技術を利用することのリスクを勘案し、事前に十分適用評価した上で、活用を検討すること。

Ⅴ．人・組織に関する事項

情報システム利用者及び情報システム供給者は、求められる信頼性・安全性の水準を満たす情報システムの企画・要件定義・開発、保守・運用及び管理を実施するため、効果的な人材育成及び組織づくりを行わなければならない。

１．人材育成・教育の実施

情報システム利用者及び情報システム供給者は、本ガイドライン「Ⅲ．企画・要件定義・開発及び保守・運用全体における事項」、「Ⅳ．技術に関する事項」に記載した対策を確実に計画・実行できる人材の育成と、これに向けた仕組を整備しておくこと。以下に具体的な方策を示す。

（１）人材の育成・教育

情報システム利用者と情報システム供給者は求められる信頼性・安全性の水準を満たす情報システムの企画・要件定義・開発、保守・運用及び管理を実現するために、利用者と供給者の各作業範囲及び責任を明確にした上で、各分担を遂行できる人材の育成を行うこと。それに向け、情報システムに携わる人員に対し、関連する教育を行うこと。

＜実施例＞

情報処理技術者試験[METI3]及びITスキル標準[METI4]、情報システムユーザースキル標準[JUAS4]等を活用し、社内の人材育成マップ等の作成とこれに基づく社内教育コースの整備を行う。情報システム利用者側は、企業内のデータの全体整合性を確保するデータベース管理者を育成する。また、過去の社内事例や類似システムの事故事例に基づく安全教育を実施する。

２．組織の整備

情報システム利用者及び情報システム供給者は、求められる信頼性・安全性の水準を満たす情報システムの企画・要件定義・開発、保守・運用及び管理を遂行できる組織の整備に努めること。特に、極めて高度な信頼性・安全性の水準が求められる情報システムに関係する情報システム利用者及び情報システム供給者は、これらの組織整備状況及び実施状況等を客観的に確認及び検証できるようにしておくこと。以下に具体的な方策を示す。

（１）知識・スキルに応じた人材登用・配置

情報システム利用者及び情報システム供給者は、人に起因する障害の防止に向け、情報処理技術者試験及びITスキル標準等を活用し、メンバ及びリーダの知識やスキル等、人的資源と稼動状況を正確に把握した上で、プロジェクトに応じて適切な人材及び人員数の配置に努めなければならない。

＜実施例＞

情報処理技術者試験、IT スキル標準及び情報システムユーザースキル標準等に基づいて作成した社内人材データベースを活用し、プロジェクト編成や組織編成を行う。

（2）独立した品質保証部門の設置

情報システム利用者及び情報システム供給者は、事業部門から独立し、品質基準・開発標準・管理標準類等の整備及び品質監査・システム監査・プロジェクト監査等の機能を持つ品質保証部門を設置するなどし、業務・サービス及び情報システムの品質向上に向けた仕組及び体制づくりに努めること。

＜実施例＞

経営者・CIO 直轄の品質監査部門や品質保証部門を設置する。社会的に大きな影響のあるミッションクリティカルシステムに対しては、第三者視点で集中監視し、開発・運用体制の是正権限を持つ組織を設置する。

（3）契約の妥当性・遵守状況のチェック体制の構築

情報システム利用者及び情報システム供給者は、組織内に法的観点・リスク管理の観点から契約の妥当性、遵守状況をチェックする体制を構築する。

＜実施例＞

契約書案作成段階において、社内法務部門及び必要に応じて弁護士と契約対象となる情報システムの関係者による契約書レビュー体制を整備し、レビューなしには契約を締結できない業務プロセスを構築する。

（4）開発部門と運用部門の相互チェック体制の構築

情報システム利用者は、開発部門と運用部門が相互に牽制可能な体制を構築し、開発した情報システムが一定の基準を満たした上で運用部門の承認なしにはサービスを開始できないプロセスを構築し、品質確保の実効性を高めなくてはならない。

＜実施例＞

運用部門の承認なしには、サービスを物理的に開始できないようなプロセスを構築する。また、本番稼動環境の変更や操作は、開発部門を含め運用部門以外によるオペレーションを禁止するルールを適用し、障害抑制性を高める。

Ⅵ．商慣行・契約・法的要素に関する事項

情報システム利用者と情報システム供給者は、情報システム・モデル取引・契約書[METI6]等を参考に本ガイドラインの遵守を前提とした契約を予め結び、当該契約を遵守しなければならない。特に、情報システム利用者及び情報システム供給者は、システムライフサイクルプロセスの円滑な実施及び管理のためには両者の協力が重要であるとの認識に立ち、役割及び責任について一方に偏った契約を避けるべきである。

契約で規定されるもののうち、一般的に個別契約で定められるような個別業務に関する事項については、システムライフサイクルプロセスが進展する中で変化しうることから、情報システム利用者と情報システム供給者は、合意の上、それぞれのフェーズにおいて最大限明確な契約の内容とするよう心掛ける。

１．契約における重要事項の明確化

情報システム利用者と情報システム供給者は、要件や委託内容が曖昧なまま一括契約を結ぶことを避けるべきである。特に、下記の事項については明確に契約において規定すべきである。

（１）システムライフサイクルプロセス全体における重要事項の規定の明確化

本ガイドライン「Ⅲ．企画・要件定義・開発及び保守・運用全体における事項」に掲げられている、情報システム利用者と情報システム供給者が明確化・共有すべき事項については、原則として契約において規定する。

（２）仕様変更の取扱に関する規定の明確化

本ガイドライン「Ⅲ．５．（５）仕様変更の取扱に関する利用者・供給者間での合意」における合意内容に基づき、仕様変更の取扱を契約において規定する。

（３）障害発生時の対応手順等の規定の明確化

「Ⅲ．４．障害対応に関する留意事項」の考え方に基づき、情報システム関係者の間で予め合意された情報システム障害発生時の対応手順及び原因究明手順等を契約において規定する。

（４）障害発生時の責任関係に関する規定の明確化

情報システム障害により生じる損害は、情報システム及び業務・サービスの性格により大きく異なる。また、障害の種別・当初合意されていた信頼性・安全性水準によって、情報システム利用者及び情報システム供給者の責任の度合いは大きく異なる。情報システム利用者及び情報システム供給者は、これらの点を十分に考慮して、損害賠償の範囲・賠償上限額等の損害の負担のあり方及び瑕疵担保責任の範囲・期間等の瑕疵への対応を契約において規定する。

（５）事業継続計画における分担及び責任の明確化

情報システム利用者と情報システム供給者は、IT サービス継続ガイドライン[METI5]等を参考に、緊急事態発生時の事業継続に関して、双方の分担及び責任を契約において規定する。

２．情報システム構築の分業時の役割分担及び責任関係の明確化

（１）情報システム利用者を含めた複数のシステム供給者間での責任明確化

情報システムの企画・要件定義・開発・保守・運用の各フェーズを異なる情報システム供給者が担当している場合等に、情報システム供給者と情報システム利用者は、それぞれの担当した部分の統合に係るリスクを認識した上で、協力して不具合の原因を特定する旨及び原因の所在と重みに応じて、応分の責任を分担することを予め明確化する。

＜実施例＞

契約類型（売買、準委任、請負）を契約書において明らかにしておくとと

もに、共通フレーム 2007[IPA1]や情報システム・モデル取引・契約書[METI6]等を参考にし、分担及び責任を定め、その内容を契約書に明記する。

（2）一部分を供給するシステム供給者の責任明確化

情報システムの開発を複数の情報システム供給者で担当している場合（パッケージを活用している場合を含む）、情報システム供給者と情報システム利用者は、各情報システム供給者の担当分（モジュール）の統合に係るリスクを認識した上で、協力して不具合の原因を特定する旨及び原因の所在と重みに応じて、応分の責任を分担することを予め明確化する。

＜実施例＞

契約類型（売買、準委任、請負）を契約書において明らかにしておくとともに、共通フレーム 2007[IPA1]等や情報システム・モデル取引・契約書[METI6]を参考にし、分担及び責任を定め、その内容を契約書に明記する。

（3）再委託先発注時のシステム供給者間の責任明確化

情報システム供給者が一部の業務を再委託している場合には、役割分担・責任関係を、上記情報システム利用者・情報システム供給者の間と同様、契約において明確化する。元請情報システム供給者は情報システム利用者に対しては再委託先の担当した業務についても信頼性・安全性水準の確保に責任を有することを情報システム利用者との間の契約で規定する。

また、元請情報システム供給者は再委託先に対し、法令遵守及び情報漏えい等に必要な措置を講ずることについて監督責任を持つことを情報システム利用者との間の契約で規定する。

＜実施例＞

情報システム利用者と元請情報システム供給者は、情報システム・モデル取引・契約書[METI6]等を参考に、再委託に係る事項を合意し、その内容を契約書に明記する。

3．着実な契約履行

情報システム利用者及び情報システム提供者は、役割分担や責任関係の明確化のための十分な協議のもと、予め合意した契約上の責務を確実かつ誠実に履行することに務めなければならない。その際、情報システム利用者及び情報システム提供者は、自らの責任遂行の能力を十分に精査した上で、役割分担の判断を行う必要がある。

Ⅶ．実効性に関する担保措置

ガイドラインの実効性を担保するための取組を示す。

1．モデル契約の見直し・活用

本ガイドラインの考え方を反映し、情報システム利用者団体（JUAS 等）及び情報システム供給者団体（JISA、JEITA 等）と協力して標準的な契約のあり方を定めた情報システム・モデル取引・契約書[METI6]の定期的な見直しを行う。情

報システム利用者及び情報システム供給者は本モデル取引・契約書を最大限尊重し、本ガイドラインにおいて定められた対策及び留意事項の実施を前提として契約を締結する。

２．政府調達における活用

経済産業省は、本ガイドラインの内容及び情報システム・モデル取引・契約書[METI6]の内容を積極的に調達に活用する。また、政府調達における本ガイドラインの活用方策も検討する。

３．信頼性評価指標及び診断（ベンチマーキング）方法の整備

経済産業省及び IPA（独立行政法人 情報処理推進機構）/SEC（ソフトウェア・エンジニアリング・センター）は、情報システムの信頼性・安全性の向上に向け、本ガイドラインへの遵守度合いを測るための信頼性評価指標、及び本指標を用いた情報システム供給者及び情報システム利用者両者に対する情報システムの開発及び運用状況の診断（ベンチマーキング）方法を整備する。

Ⅷ．その他の関連事項

１．開発プロセスの共有化

経済産業省及び IPA/SEC は、情報システム供給者及び情報システム利用者間の開発プロセスの共有化に向け、共通フレーム 2007[IPA1]の普及を促進する。

２．障害事例データベースの公開

経済産業省及び IPA/SEC は、重要な情報システム障害について関係者の同意を得た上で原因の究明に当たり、状況の改善に向けてデータベース化及び外部への提供を行う。データベースの整備に当たっては、稼動直後に発生する障害と安定稼動中に発生する障害、オープン系システムで発生する障害とメインフレームで発生する障害など、原因と対策が異なる様々な障害が存在することに配慮する。

３．事例・定量データの蓄積・公開

経済産業省及び IPA/SEC は、システム開発・運用事例並びに見積り及び品質等に関するデータの蓄積及び外部への提供を行う。

４．組込みシステムの信頼性確保

IC カード乗車券による自動改札やモバイル決済システムなど、組込み機器が情報システムの端末として利用されている。携帯電話、車載機器等、大規模ソフトウェアを搭載した組込み機器がインターネット等を通じて情報システムと接続される一方で、これらの組込みシステムの大規模化・複雑化に起因する障害が、接続対象のサービス全体に重大な影響を及ぼす事例も現れている。こうした現状から、組込みシステムの信頼性向上は非常に重要な課題となっている。

組込みシステムはハードウェア/ソフトウェア両面の開発が必要であること、製品固有の国際規格が存在する場合があること、要求定義から製造・試験までをメーカーが一貫して行う製造工程など、固有の特性を持つ。組込みシステム

の信頼性向上の取り組みを実施するに当たっては、組込みシステム固有の特性を勘案の上、本ガイドラインで活用可能な事項の検討を行い、積極的な活用を進めることが望ましい。

５．ガイドラインの定期的見直し

経済産業省は、本ガイドラインの定期的な見直しを行う。

６．安全基準等策定時における活用

重要インフラの所管省庁は安全基準等の策定に際し、必要に応じ、本ガイドラインを参照することが望まれる。

参考：本ガイドラインに関係する法令、国際規格及び日本工業規格等

本ガイドラインの遵守に当たっては、下記の法令、国際規格、日本工業規格及び基準・指針・資格類等を参考にすること。*はガイドライン本文の中から引用されている文献である。

１．法令

・民法、商法、製造物責任法等

２．国際規格及び日本工業規格

【信頼性・安全性】
- JIS C 0508:2000 電気・電子・プログラマブル電子安全関連系の機能安全*
- JIS X0134：1999 システムおよびソフトウェアに課せられたリスク抑制の完全性水準*

【プロセス】
- JIS X 0160: 2007 ソフトウェアライフサイクルプロセス及びその追補1、2
- JIS X 0170:2004 システムライフサイクルプロセス
- JIS X 0145:2008 情報技術―プロセスアセスメント

【品質、プロジェクトマネジメント】
- JIS X 0129:2003 ソフトウェア製品の品質
- ISO/IEC 25000:2005 Software Engineering - Software product Quality Requirements and Evaluation (SQuaRE)-Guide to SQuaRE
- JIS Q 9001:2000 品質マネジメントシステム - 要求事項

【運用】
- JIS Q 20000:2007 情報技術サービスマネジメント*

３．基準・指針・資格類

【信頼性・安全性、ＢＣＰ】
- [FISC1] 金融機関等コンピュータシステムの安全対策基準（財団法人 金融情報システムセンター、1998 年）
- [METI5] IT サービス継続ガイドライン（経済産業省、2008 年）*
  http://www.meti.go.jp/press/20080903001/20080903001.html
- [METI7] 事業継続計画策定ガイドライン（経済産業省、2005 年）*
  http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html

【プロセス】
- [IPA1] 共通フレーム 2007（IPA/SEC、2007 年）*
- [ITC1] IT コーディネータプロセスガイドライン（特定非営利活動法人 IT コーディネータ協会、2006 年）
  http://www.itc.or.jp/about/guideline/index.html

【要件定義】
- [JUAS1] 要求仕様定義ガイドライン UVC 報告書（JUAS、2007 年）*
- [JUAS2] 非機能要求仕様定義ガイドライン UVCⅡ（JUAS、2007 年）*
- [IPA6] 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（IPA/SEC、2006 年）

【品質、プロジェクトマネジメント】
・ [IPA2] ソフトウェア開発見積りガイドブック（IPA/SEC、2006 年）*
・ [IPA3] ソフトウェア改良開発見積りガイドブック（IPA/SEC、2007 年）*
・ [IPA4] 定量的品質予測のススメ（IPA/SEC, 2008 年）*
・ [IPA5] ソフトウェアテスト見積りガイドブック（IPA/SEC, 2008 年）*
・ [JISA1] 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（JISA、2008 年）*
・ [JUAS3] ユーザ企業ソフトウェアメトリックス調査（JUAS、2007 年）*
・ [JUAS5] システム・リファレンス・マニュアル（JUAS、2006 年）*
・ [PMBOK] プロジェクトマネジメント知識体系ガイド第 3 版（Project Management Institute、2004 年）*
・ [SQuBOK] ソフトウェア品質知識体系ガイド（SQuBOK Guide、2007 年）*
【運用】
・ [ITIL1] ITIL V3 - Information Technology Infrastructure Library（英国商務省、2007 年）
【監査】
・ [METI1] システム監査基準、システム管理基準（経済産業省、2004 年）
http://www.meti.go.jp/policy/it_policy/press/0005668/index.html
【人材育成】
・ [METI3] 情報処理技術者試験（経済産業省）*
http://www.jitec.jp/
・ [METI4] IT スキル標準/組込みスキル標準（経済産業省、独立行政法人 情報処理推進機構） *
http://www.ipa.go.jp/jinzai/itss/index.html
http://sec.ipa.go.jp/ETSS/download.html
・ [JUAS4] 情報システムユーザースキル標準 Ver.1.2 （JUAS、2008 年）*
http://www.ipa.go.jp/about/press/20080331-2.html
【契約】
・ [METI6] 情報システム・モデル取引・契約書（経済産業省、第一版 2007 年、追補版 2008 年）*
http://www.meti.go.jp/policy/it_policy/keiyaku/index.html
【政府調達】
・ [METI2] EA 策定ガイドライン（経済産業省、2003 年）*
http://www.meti.go.jp/policy/it_policy/itasociate/it.associate.htm

情報セキュリティに関する規格及び基準類

１．規格
・JIS X 5070:2000 セキュリティ技術 - 情報技術セキュリティの評価基準
・JIS Q 27001:2006 セキュリティ技術 - 情報セキュリティマネジメントシステム－要求事項*
・JIS Q 27002:2006 セキュリティ技術 - 情報セキュリティマネジメントの実践のための規範*

２．基準類
・ コンピュータ不正アクセス対策基準（通商産業省、2000 年）
http://www.ipa.go.jp/security/ciadr/guide-crack.html

・ 情報システム安全対策基準（通商産業省、1995 年）
http://www.meti.go.jp/policy/netsecurity/downloadfiles/esecu03j.pdf
・ コンピュータウイルス対策基準（通商産業省、2000 年）
http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm
・ 情報セキュリティ監査基準、情報セキュリティ管理基準（経済産業省、2003 年）*
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.pdf
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex01.pdf

表　1

情報システム障害に係る原因の種別

種別	障害原因の例
(1) 要件の誤り	発注仕様の誤り、システム動作環境、運用環境（前提条件等）の認識誤り、システム対象業務分析ミス、非機能要件の評価誤り、セキュリティ機能要件の誤り　等
(2) ソフトウェアの誤り	機能不適合、データ加工・処理ミス、条件判定ミス、 処理タイミング・ミス、情報の誤表示等、コーディング・ミス（脆弱性）　等
(3) 調達ソフトウェアの不具合	調達ライブラリの仕様不適合、ミドルウェアの不安定稼動、ドライバソフトウェアの不具合、調達ソフトウェアの脆弱性　等
(4) ハードウェア故障・性能低下等	ハードウェア故障（周辺装置・機器、制御装置を含む）、故障時の代替機の調達困難、 ハードウェア処理能力の低下、想定状況外での不安定動作、製造プロセスにおけるマルウェアの混入　等
(5) 製品間インターフェイスの誤り	ハードウェア及びソフトウェア製品単体の機能としては問題ないが、それぞれの組合せの不整合等により発生するトラブル 等
(6) 性能・容量等の不足	トランザクションや処理の集中に伴う処理速度の低下、データ量増大に伴うデータ記憶領域の不足、不正アクセス等による過負荷　等
(7) 移行時の誤り	ソフトウェア修正時のデグレード発生、データ移行の失敗、機器及びソフトウェアの設定ミス等
(8)運用・保守方法・手順等の誤り	マニュアル等の誤りや過信、操作手順に関する誤解や誤り、慣れに伴う操作の誤解や誤り、脆弱性対応手順の誤り（パターンファイルの不適用等）　等
(9) 情報システム障害発生時の対応の誤り・遅れ	情報システム障害発生時の復帰手順の整備不足、復帰操作の誤解や誤り、縮退運転機能の欠落、関係者への周知不足、対応の遅れ 等

表　2　信頼性・安全性の水準に応じた必須・推奨事項及び関連規格等

実施項目	必須／推奨区分			実施分担例			活用できる規格･標準･基準･指針･資格等
	システムA	システムB	システムC	情報システム利用者が実施	情報システム供給者が実施	情報システム利用者･供給者両者が合意	
Ⅱ．　信頼性・安全性向上に向けての全般的配慮事項							
1．関係者の責務							(12)、(17)、(25)、(29)、(31)、(39)
（1）情報システム利用者の責務	◎	◎	◎	◎			
（2）情報システム供給者の責務	◎	◎	◎		◎		
（3）共同作業であることの認識	◎	◎	◎	●	●		
2．経営層の責務							
（1）システム障害が経営リスクの問題であることの認識	◎	◎	○	◎	○		
（2）経営資源の投入	◎	◎	○	◎	○		
（3）CIO（情報統括役員）の登用と活用	◎	◎	○	◎			
（4）説明責任の認識	◎	◎	○	●	●		
（5）保守・運用の重要性の認識	◎	◎	○	◎	○		
（6）事業継続計画の策定と訓練の実施	◎	◎	－	◎	○		
3．未然防止と事後対策の両側面からの対策の実施	◎	◎	○	◎	○		
4．信頼性・安全性向上に向けた多面的取組の必要性	◎	◎	○	●	●		
5．情報システム障害に対する動作の基本	◎	◎	○	●	●		
Ⅲ．企画・要件定義・開発及び保守・運用全体における事項							
1．企画・要件定義段階における留意事項							(1)、(2)、(3)、(4)、(5)、(6)、(7)、(8)、(9)、(10)、(11)、(12)、(13)、(14)、(15)、(17)、(18)、(19)、(20)、(21)、(22)、(24)、(25)、(26)、(33)、(34)、(35)、(36)、(37)、(38)、(39)
（1）信頼性・安全性水準の定義と利用者・供給者間での合意	◎	◎	◎			●	
（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	◎	◎	◎	◎			
（3）設計等上流工程における品質確保の重要性の認識	◎	◎	◎	●	●		
（4）機能要件の実現に向けた利用者・供給者間での合意	◎	◎	◎			●	
（5）非機能要件の実現に向けた利用者・供給者間での合意	◎	◎	◎			●	
（6）利用者によるシステム要件に関する見解の統一	◎	◎	◎	◎			
2．開発段階における留意事項							(1)、(2)、(3)、(4)、(5)、(6)、(7)、(8)、(9)、(10)、(12)、(13)、(15)、(18)、(19)、(20)、(21)、(22)、(24)、(25)、(26)、(33)、(34)、(35)、(36)、(37)
（1）システムライフサイクルプロセスの確立と文書化	◎	◎	◎	○	◎		
（2）役割分担・責任権限の利用者・供給者間での合意	◎	◎	◎			●	
（3）定量的見積りの実施	◎	◎	○	○	◎		
（4）情報システムの複雑化の回避	◎	◎	○	●	●		
（5）情報システムの障害対応能力の向上	◎	◎	○	●	●		
（6）誤操作等防止への配慮	◎	◎	○	●	●		
（7）テスト及びレビューの徹底	◎	◎	◎			●	
（8）検収基準の明確化	◎	◎	◎			●	
3．保守・運用段階における留意事項							(1)、(2)、(3)、(5)、(7)、(8)、(9)、(10)、(12)、(14)、(18)、(19)、(22)、(24)、(25)、(29)、(31)、(35)、(37)
（1）保守・運用機能を果たす体制・業務フロー等の整備および利用者・供給者間での合意	◎	◎	○			●	
（2）保守の取扱方針の利用者・供給者間での合意	◎	◎	○			●	
（3）ニーズや環境の変化へのシステム仕様の適切な適応	◎	◎	○	◎	○		
（4）保守に伴う変更作業・リリース手順等の整備と訓練	◎	◎	○	●	●		
（5）情報システムの構成情報の完全性確保	◎	◎	◎	○	◎		
（6）恒常的な運用状況の監視と管理	◎	◎	○	●	●		
（7）定量的見積りの実施	◎	◎	○	○	◎		
4．障害対応に関する留意事項							(6)、(8)、(9)、(10)、(18)、(19)、(22)、(24)、(25)、(29)、(31)、(35)、(37)
（1）障害発生事象の検知と対応の整備	◎	◎	◎	●	●		
（2）問題の診断と根本原因の究明	◎	◎	◎	●	●		
（3）再発防止に向けた障害に係る各種情報の保持と活用	◎	◎	◎	●	●		
（4）重大な障害に対するリスクの把握と緊急対応の利用者・供給者間での合意	◎	◎	－			●	
（5）関連・類似システムの障害情報の活用と情報公開	◎	○	－	●	●		
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)、(5)、(8)、(9)、(12)、(13)、(14)、(15)、(19)、(22)、(24)、(25)、(30)、(32)、(33)、(37)
（1）経験則のみによらないプロジェクトマネジメントの導入	◎	◎	◎	○	◎		
（2）定量データを活用した管理	◎	◎	○	○	◎		
（3）健全なプロジェクト運営に向けた活動の実施	◎	◎	◎	●	●		
（4）第三者によるレビュー及び監査の実施	◎	○	○	◎	○		
（5）仕様変更の取扱に関する利用者・供給者間での合意	◎	◎	◎			●	
（6）情報セキュリティ対策の実施	◎	◎	◎	●	●		
Ⅳ．技術に関する事項							
1．開発手法・ツールの活用及びテスト環境の整備							(1)、(2)、(6)、(7)、(12)
（1）利用者・供給者間での情報共有	◎	◎	○	●	●		
（2）各種開発手法・ツール等の活用	◎	◎	◎	●	●		
（3）テスト環境の整備	◎	◎	○	◎	○		
2．信頼性・安全性向上に向けた技術の活用及び留意事項							(4)、(6)、(7)、(26)、(34)、(35)、(36)
（1）アーキテクチャの確立	◎	◎	◎	◎	○		
（2）インターネット経由のアクセスへの対処	◎	◎	◎	●	●		
（3）信頼性・安全性に関する評価技術の活用	◎	◎	◎	●	●		
（4）信頼性・安全性の向上に向けた先端技術の活用	－	－	－	●	●		
Ⅴ．人・組織に関する事項							
1．人材育成・教育の実施							(5)、(8)、(9)、(23)、(24)、(25)、(27)、(28)、(37)
（1）人材の育成・教育	◎	◎	○	●	●		
2．組織の整備							
（1）知識・スキルに応じた人材登用・配置	◎	◎	◎	●	●		
（2）独立した品質保証部門の設置	◎	○	○	●	●		
（3）契約の妥当性・遵守状況のチェック体制の構築	◎	◎	○	●	●		
（4）開発部門と運用部門の相互チェック体制の構築	◎	◎	○	●	●		
Ⅵ．商慣行・契約・法的要素に関する事項							
1．契約における重要事項の明確化							(10)、(12)、(18)、(24)、(25)、(29)、(30)、(31)
（1）システムライフサイクルプロセス全体における重要事項の規定の明確化	◎	◎	○			●	
（2）仕様変更の取扱に関する規定の明確化	◎	◎	◎			●	
（3）障害発生時の対応手順等の規定の明確化	◎	◎	○			●	
（4）障害発生時の責任関係に関する規定の明確化	◎	◎	○			●	
（5）事業継続計画における分担及び責任の明確化	◎	◎	－	●	●		
2．情報システム構築の分業時の役割分担及び責任関係の明確化							
（1）情報システム利用者を含めた複数のシステム供給者間での責任明確化	◎	◎	○			●	
（2）一部分を供給するシステム供給者の責任明確化	◎	◎	○			●	
（3）再委託先発注時のシステム供給者間の責任明確化	◎	◎	○		◎		

〔必須／推奨区分凡例〕

◎：必須事項
○：推奨事項
－：参考

システムA：重要インフラ等システム
システムB：企業基幹システム
システムC：その他のシステム

〔実施分担例の凡例〕

◎：主体的な立場で実施
○：支援的な立場で実施
●：双方が各自の立場で実施あるいは対等の立場で実施

〔活用できる規格・標準・基準・指針・資格等〕

(1)　JIS X 0160:1996 ソフトウェアライフサイクルプロセス及びその追補1、2
(2)　JIS X 0170:2004 システムライフサイクルプロセス
(3)　ISO/IEC 15504 Information technology - Process assessment
(4)　JIS X 0129:2003 ソフトウェア製品の品質
(5)　JIS Q 9001:2000 品質マネジメントシステム - 要求事項
(6)　JIS C 0508:2000 電気・電子・プログラマブル電子安全関連系の機能安全
(7)　JIS X 5070:2000 セキュリティ技術 - 情報技術セキュリティの評価基準
(8)　JIS Q 27002:2006 セキュリティ技術 - 情報セキュリティマネジメントの実践のための規範
(9)　JIS Q 27001:2006 セキュリティ技術 - 情報セキュリティマネジメントシステム－要求事項
(10)　ISO/IEC 20000:2005 Information technology - Service management
(11)　金融機関等コンピュータシステムの安全対策基準（財団法人 金融情報システムセンター、1998年）
(12)　共通フレーム2007（IPA/SEC、2007 年）
(13)　ソフトウェア開発見積りガイドブック（IPA/SEC、2006年）
(14)　ソフトウェア改良開発見積りガイドブック（IPA/SEC、2007年）
(15)　定量的品質予測のススメ（IPA/SEC，2008年）
(16)　ソフトウェアテスト見積りガイドブック（IPA/SEC，2008年）
(17)　ITコーディネータプロセスガイドライン（特定非営利活動法人 ITコーディネータ協会、2006年）
(18)　ITIL V3 - Information Technology Infrastructure Library（英国商務省、2007年）
(19)　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（JISA、2008年）
(20)　要求仕様定義ガイドラインUVC報告書（JUAS、2007年）
(21)　非機能要求仕様定義ガイドラインUVCⅡ（JUAS、2007年）
(22)　ユーザ企業ソフトウェアメトリックス調査（JUAS、2007年）
(23)　情報システムユーザースキル標準Ver.1.2 （JUAS、2008年）
(24)　システム・リファレンス・マニュアル（JUAS、2006年）
(25)　システム監査基準、システム管理基準（経済産業省、2004年）
(26)　EA策定ガイドライン（経済産業省、2003年）
(27)　情報処理技術者試験（経済産業省）
(28)　ITスキル標準/組込みスキル標準（経済産業省、独立行政法人 情報処理推進機構）
(29)　ITサービス継続ガイドライン（経済産業省、2008年）
(30)　情報システム・モデル取引・契約書（経済産業省、第一版2007年、追補版2008年）
(31)　事業継続計画策定ガイドライン（経済産業省、2005年）
(32)　プロジェクトマネジメント知識体系ガイド第3版（Project Management Institute、2004年）
(33)　ソフトウェア品質知識体系ガイド（SQuBOK Guide、2007年）
(34)　コンピュータ不正アクセス対策基準（通商産業省、2000年）
(35)　情報システム安全対策基準（通商産業省、1995年）
(36)　コンピュータウイルス対策基準（通商産業省、2000年）
(37)　情報セキュリティ監査基準、情報セキュリティ管理基準（経済産業省、2003年）
(38)　JIS X 0134:1999 システムおよびソフトウェアに課せられたリスク抑制における完全水準
(39)　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（IPA/SEC、2006年）