ITC プロセスにおける情報システムの信頼性向上へのアプローチ

～「情報システムの信頼性向上に関するガイドライン」の超やさしい解説書～

2008年4月9日　Ver1.0

企業内 ITC・IT ガバナンス研究会

平成 20 年 6 月

企業内 ITC・IT ガバナンス研究会
「ITC プロセスにおける情報システムの信頼性向上へのアプローチ」
～「情報システムの信頼性向上に関するガイドライン」の超やさしい解説書～
ご紹介

経済産業省　商務情報政策局
情 報 処 理 振 興 課 長
八尋 俊英

現在、我が国の国民生活及び社会経済活動の IT 利用度は、かつて無いほど高まっており、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が深刻化してきており、情報システムの信頼性・安全性向上は喫緊の課題となっています。これを受けて、平成 18 年 6 月 15 日に経済産業省より公表された「情報システムの信頼性向上に関するガイドライン」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すべきことについて定めております。

また、ガイドラインの活用促進のための措置として、ガイドラインの遵守状況を測定するための評価指標の検討が重ねられ、平成 19 年 4 月 13 日に本検討結果を踏まえた「情報システムの信頼性向上に関する評価指標（試行版）」が公表されました。

この度、企業内 ITC・IT ガバナンス研究会にて、「情報システムの信頼性向上に関するガイドライン」の有効性を認識いただき、研究会有志の方々によりガイドラインの解説書を作成いただきましたので、ここにご紹介いたします。

「情報システムの信頼性向上に関するガイドライン」と併せて、本解説書をご活用いただき、情報システムの信頼性向上のために是非ともお役立ていただければ幸いです。

【参考】

① **「情報システムの信頼性向上に関するガイドライン」については、以下の経済産業省のホームページを参照。**
http://www.meti.go.jp/press/20060615002/20060615002.html

② **「情報システムの信頼性向上に関する評価指標（試行版）」については、以下の経済産業省のホームページを参照。**
http://www.meti.go.jp/press/20070413003/20070413003.html

はじめに

経済産業省が「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）を公表したのが、平成18年6月のことである。

公表するに当たって、「経済産業省では、情報システム障害の社会的影響が日々、深刻化してきていることを受け、「情報システムの信頼性向上に関するガイドライン」の検討を行ってきました。この度、案に対するパブリックコメントの結果を踏まえ、同ガイドラインを策定いたしましたのでその内容を公表いたします。」と、その趣旨を簡潔に述べている。

特に注目したいのが、社会的に影響が大きい情報システムの障害とその対策に苦慮している点であり、経済的損失への予防手段を講じる必要性に迫られていることを感じる。また、「ＩＴコーディネータプロセスガイドライン」と同様に経営者の参画、責任の重要性が明確に示されており、その活用における期待も大きい。

しかしながら、上記ガイドラインは多分に「在るべき論」的な内容であり、直ちに行動に移すにはやや理解しがたい内容となっていると感じられる。

本書は上記のような課題認識に基づいて、ＩＴコーディネータの視点から執筆者各自が蓄積してきた技術や見識をもとに、「情報システムの信頼性向上に関するガイドライン」を理解するうえでより噛み砕く必要があると考えられる部分について解説を試みたものであり、他のＩＴコーディネータへの参考書的な役割を果たすことを目的として作成されたものである。現時点では全ての項目を網羅しているのではないことをお断りしておくが、ひとつの読み物として繋がるよう集約してみた。

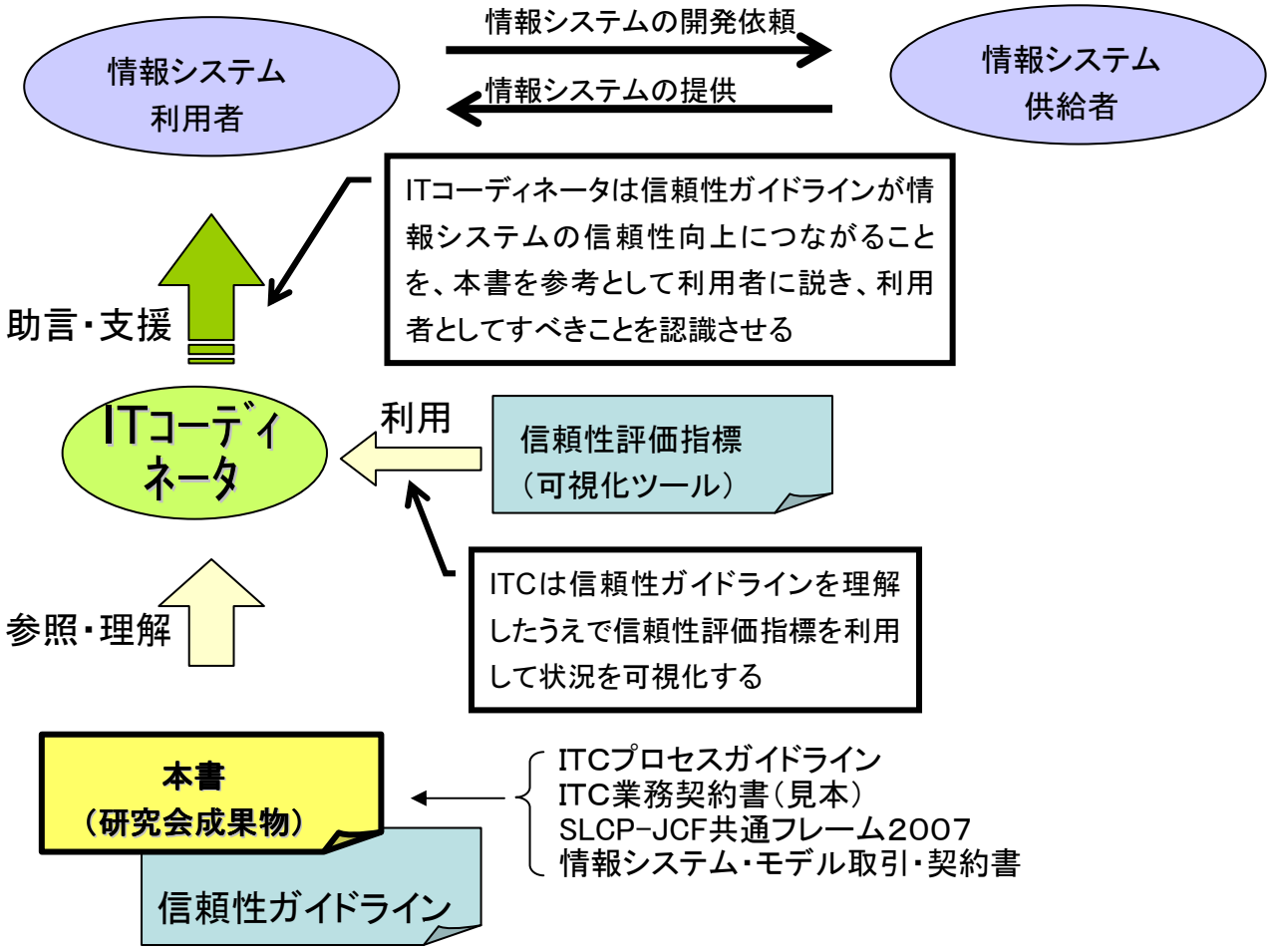
読者にとって、「情報システムの信頼性向上に関するガイドライン」をより深く理解し実務に活用する上での参考になれば幸いである。

２００８年４月
執筆者　一同

【執筆メンバー　ＩＴガバナンス研究会（アイウエオ順）】

久住　昭之　（ＮＴＴコミュニケーションズ株式会社　ＩＴﾏﾈｼﾞﾒﾝﾄｻｰﾋﾞｽ事業部）
瀬戸　昭彦　（日立ビジネスソリューション株式会社　第２業務システム事業部）
滝沢　　康　（三井造船株式会社　経営企画部　経営管理グループ）
千枝　和行　（アステラス製薬株式会社　健康保険組合出向）
古川　正紀　（住商情報システム株式会社　金融ソリューション事業部）
牧田　一雄　（日本アイビーエム株式会社　グローバルテクノロジーサービス）
山上　幸一　（日立ビジネスソリューション株式会社　第２業務システム事業部）
山﨑　直和　（ＮＴＴコミュニケーションズ株式会社　第二法人営業本部）

本書の位置付け（イメージ）



本書は次のように構成されている。

A．原文

「情報システムの信頼性向上に関するガイドライン」の原文そのもの

B．必要性・重要性

上記原文に記載されている項目がなぜ必要なのか、なぜ重要なのかについての解説

C．情報システム利用者の実施事項

情報システム利用者として実施しなければいけない事項について、「「情報システムの信頼性向上に関する評価指標（試行版）」の該当する部分の抜粋と追加解説

D．情報システム供給者への要求事項

情報システム供給者に対し、情報システム利用者が要求しなければいけない事項について、「「情報システムの信頼性向上に関する評価指標（試行版）」の該当する部分の抜粋と追加解説

E．その他の留意事項

ガイドラインの他項での指摘点、ITCとして注意すべき点などを必要に応じて記載

目次

Ⅰ．総論

（解説の対象外）

Ⅱ．信頼性・安全性向上に向けての全般的配慮事項

情報システムの信頼性・安全性を確保・維持していくための全般的配慮事項について述べる。

本「情報システムの信頼性向上に関するガイドライン」は、特に社会的基盤をなす重要インフラや社会的影響の大きい組込型システム（以下、重要インフラ等という）を担う情報システム等を中心にすえて検討されており、これらの情報システムは広範囲な相互依存度が高く、効果面に於いてもリスク面に於いても社会的な影響が大きいことから、一般の情報システム以上に配慮すべき点が多い。

それらの事情を考慮して、通常の情報システム構築・運用で、より強く認識すべき点をかい摘んで記述する。

１．関係者の責務

（１）情報システム利用者の責務

Ａ．ガイドライン原文

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、内部における利用部門及び開発・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。

また同時に、情報システムに内在する不完全性も自覚し、業務・サービスと情報システムの機能を峻別するとともに、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に努め、業務・サービス本体機能の維持の為に必要な資源（人的資源、金銭的資源等）及び技術等の動員を行わなければならない。

Ｂ．本項目の必要性・重要性

開発されたシステムは通常の利用範囲に於いて正常に稼動することを前提に運用されており、特に重要インフラ等を担う情報システムにおいては、想定外の動作をすることは社会的な影響が大きいと言える。そのことは、当該企業活動のみならず、相互依存している企業、更には、それらの企業からサービスを受ける一般利用者にも、波及的に大きな影響を及ぼすことを意味している。

重要インフラ等を担う企業はそのことを認識し、会社全体としての取り組みを行い、情報システムを正常に稼動させるために必要な資源の投入を行わなければならない。

今日考えられるシステム資源は自社に閉じたものではなく、ビジネスパートナーや委託先を含んでおり、それらを含めた大きな概念での捉え方と、推進のリーダーシップが要求されている。

Ｃ．情報システム利用者の実施事項

＜経営者が参画する要求品質の確保＞ 業務企画担当者は、アプリケーションの責任者として、また個々のプロジェクトの責任者として、情報システム部門、ベンダとともに要件を確定し、システムの検証をし、利用者に供給する必要があります。（第１章、１．３、（２）、①）

重要インフラ等の情報システムを構築・利用する企業は、次の事項に注意をしてシステム構築に

取り組む。

その情報システムが持つ必要な機能を要件に盛り込んで、一定以上の品質で開発・構築すること。

非機能要件、すなわち、運用、セキュリティ、バージョンアップ、機密保護などの要件も諸要素を考慮して洩れなく設計しておくこと。

情報システムの利用者や利害関係者（ステークホルダー）は、昔と違い広範囲にわたっているので、当該情報システムに関係する利用者・ステークホルダーを洗い出し、組織化し、それらの意見を洩れなく調整すること。

社内のステークホルダーと交わした取り決め内容は、文書化すること。

情報システムの設計・開発・運用を外部に委託する場合、要件を正確に供給者（委託先）に伝えること。

供給者への伝達は文書をもって行うこと。

供給者が誤った解釈をしそうな点を予め想定し、間違いなく伝わっていることをレビュー等の手段で確認すること。

情報システムの開発の結果もたらされる効果やリスクについては、経営者の承認を得ながら進めること。

D．その他の留意事項

今日の情報システムは複雑で、自社内に閉じたシステムとすることが出来ない。また、機能が複合化することにより情報システムが巨大化する傾向があり、利害関係者（ステークホルダー）も飛躍的に増加していて、実際の利用者やIT担当者のみで情報システムを構築することはできなくなってきている。組込型のシステムでも、自動車の場合などはリコールの対象になるので影響が大きい。

そのことは、

・システムのエラーや障害の発生時に影響を受ける範囲が広くなっている。

・それらの影響が自社内に閉じず、社外のステークホルダーへの影響も大きい。

・そのため、社会的な責任が発生し、経営者に説明責任が及ぶ。

などの現象を発生させており、システム利用の責任者及び経営者はそのことへの認識と、対応できる仕組みの整備が求められている。

（２）情報システム供給者の責務

Ａ．ガイドライン原文

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・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。

Ｂ．本項目の必要性・重要性

情報システムの開発・運用は、その多くは委託先（供給者）によって行われている。

情報システムの供給者（受託企業）は、利用者（委託企業）に代わって、その企画段階から、開発・運用段階までを受託し、情報システムが適正に構築され、正常に機能するよう支援することが強く求められている。

今日の利用者の業務環境は、コア業務に経営資源を集中させて、それ以外の部分は外部に委託したり、子会社化をはかるなど、効率化に走っている。従って、一昔前の様に、利用者自身が業務の要件定義をしたり、プログラム開発を行うなどは行われていない。それらの部分は供給者が担うことが期待されていて、プロジェクトマネジメントを始めとして、情報収集力・企画提案力・ソリューションの構築力・ジョイントベンチャーにおける調整力など、総合的なサービス提供力が求められる。

特に重要インフラ等を担う情報システムにおいては、供給者がその事業や当局の規制を理解し、必要な機能を提供するということが、ますます必要になってきている。

Ｃ．情報システム供給者への要求事項

＜経営者が参画する要求品質の確保＞

ベンダは顧客企業の IT 担当者とともに、企業のビジネス戦略実現を担う存在です。共に顧客企業のシステム開発を担い、顧客企業に IT 担当者がいない場合は、担当者に代わって、その役割を引き受ける必要があります。加えて、顧客企業の IT 担当者が、特定の産業に特化した存在とは違い、ベンダはシステム開発のプロとして、その技術力、構築力を用いて、顧客企業の戦略実現を支える役割を強く担っているといえます。（第１章、１．３、（４））

情報システムの供給者は、次の事項に注意をしてシステム供給に取り組む

- 利用者からの委託により、情報システムの構築・保守・運用を行うこと。
- 利用者がそれまでに使用してきた情報システムの調査・分析から始め、利用者が求める要求仕様のみならず、非機能要件である運用、セキュリティ、バージョンアップ、機密保護などの要件も加味し、構築すること。
- 前項に対応するため供給者は広範囲な技術を提供できる体制を整備すること。
- 利用者が適切に要求を出しているとは限らないので、業界動向や当局の規制、或いは利用者のインタビューなどから、適正なシステムを利用者に逆提案することも範囲に含めること。
- システム構築を含めた業務全体の構築マネジメント能力が発揮できるよう整備すること。
- 自社の経営資源のみでサービス提供できない場合は、他社の支援を得ながら総合的に調整してサービスを提供すること。

・ システム供給の経営者及び責任者はそれらの期待に応えられるよう、体制の整備を行うこと。

D．その他の留意事項

情報システムの供給者は幾つかの重要な問題を抱えている。例えば次のようなことが例として挙げられる。

・ 利用企業が業務の定義や要求仕様を作成しなくなった。
・ 要件を提示したのに、手直し・手戻りが発生する。
・ システム開発工程の標準化が進まず、人手に頼る部分が減らず、品質が安定しない。
・ プログラムが膨大化し、マネージャがフォローにまわるとプロジェクトのコントロールが失われて品質が落ちる。
・ 受託業務に追われ、要員の育成が手薄に成りがちである。

このことは、一企業の問題ではなく、システム供給側の業界全体の問題として捉えることが出来る。

ITスキル標準（ITSS）や共通フレーム2007等を制定しているのも、それらを解消する手段の一つとして活用されるためである。供給者は業界全体と歩調をとりながら、利用者に協力できる力を時代に合った形で提供できるよう継続努力が望まれる。

（3）共同作業であることの認識

A．ガイドライン原文

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。

B．本項目の必要性・重要性

今日の情報システムは、広範囲な影響、複雑な構成、不正からの防御、ステークホルダーへの説明責任等、業務を動かす以外の付随的な要素を満足させることが求められている。

規模の大きな情報システムや、重要インフラ等の情報システムの場合、更に当局による規制などもあり、利用者側の体制のみで対応することは合理的ではないし、また不可能に近い。適正な資源を持った供給者の支援を必要としている。

一方、システム供給者側も、利用者の多様な要求に応えねばならず、ＥＡ、データベース技術、セキュリティ技術、アジャイル開発法、IT 統制やＷｅｂ新機能対応など、新しい技術力が絶え間なく求められる。また、大規模システムや複雑なシステムの場合、1 社の対応ではなく複数会社のジョイントベンチャーになることが多く、情報システム構築上のプロジェクトマネジメントを総合的に進める役割も期待される。

これらの事情を踏まえ、情報システムの利用者及び情報システムの供給者双方が同じ方法論や同じ管理方式を共有することが求められている。また、信頼性の高いシステムを構築するためには、役割分担と責任範囲を明確にし、推進する必要がある。

情報システムの障害や期待された性能を発揮しない原因の多くが、仕様の確定不足、責任の所在の不明確さなどに求められることから、相互責任であることを自覚し、同じ価値観を共有しながら推進することが求められる。

C．情報システム利用者の実施事項

＜経営者が参画する要求品質の確保＞
プロセス標準は、意味定義、作業の位置付け、取引やサービス、あるいはプロセスアセスメントなどを行ううえで不可欠なものです。（第３章、３．１）

重要インフラの情報システムを利用し、一般利用者へ業務サービスを提供する企業の代表的取り組み項目を述べる。

- 業務全体として適正なサービスを継続して提供することが期待されていることを理解すること。
- この様なシステムを適正に継続するためには、機能の提供だけではなく、機密保持性や高い耐障害性を合わせて持っていなくてはならないことを理解すること。
- 情報システム利用の経営者は、適正な情報システムの維持と問題発生時の説明責任が課せられていることを理解すること。
- 自社内のみならず、協力者や利害関係者も含めた体制を整備するために、適正な経営資源を投入し、社会的使命の達成する様努めること。

D．情報システム供給者への要求事項

＜経営者が参画する要求品質の確保＞
　プロセス標準は、意味定義、作業の位置付け、取引やサービス、あるいはプロセスアセスメントなどを行ううえで不可欠なものです。（第３章、３．１）

重要インフラ等の重要システムの構築・運用を委託されている供給者の代表的取り組みを述べる。

・ その情報システムの適正な維持のために、最新の技術とサービスを提供しなければならないことを理解すること。
・ 情報システム供給の経営者は、今日の情報システムが複雑な要素と多数の利害関係者で成り立っていることを理解すること。
・ 自社内に閉じずに、広く協力者を求め、総合的なサービスを提供できる体制と環境の整備を行うこと。

Ｅ．その他の留意事項

利用者側から見て、情報システムに障害が発生することは問題ではあるが、発生した場合に、早急な回復と原因に対する説明を行うことが期待される。

一番問題なのは、供給者側がその対応に追われ、一般利用者に説明し理解を求めることを怠ることである。しかも、その説明が自社に閉じた都合のいい言い訳では納得が得られず、社会通念上、適正な説明を行うことが求められている。

この様な対応を行うためには、システムの構想段階から、利用者（委託者）、供給者（受託者）双方で、リスクを洗い出し、設計に折り込み、運用訓練に反映されている必要がある。これには、長期的な展望と、広範囲な視点をもって、情報システムを維持管理する必要があることを示しており、利用者（委託者）、供給者（受託者）双方の経営者を中心とした体制と環境整備を協力して行う必要がある。

２．経営層の責務

（１）経営資源の投入

Ａ．ガイドライン原文

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、必要な経営資源を投入しなければならない。

Ｂ．本項目の必要性・重要性

今日の情報システムはオープン化されたために、自社の中で閉じることが出来ず、外部との入り組んだ複雑なシステムとならざるを得ない。また、システムを利用する利害関係者（ステークホルダー）も大きく広がり、一部の関係者の考えだけでは情報システムの構築は不可能になっている。

この様な情報システムを開発し、サービスを提供するためには、経営者の明確な意思表示がなされている必要がある。全ての業務・サービスの提供は、この経営者の意思表示に基づいて行われている必要があり、経営者の意思こそが品質と信頼性実現の鍵を握っていると言える。

Ｃ．情報システム利用者の実施事項

＜経営者が参画する要求品質の確保＞
経営層は先入観を持つことなく、業務部門の声に耳を傾け、フラットな視点で判断する義務があるといえます。ヒト・モノ・カネという限りあるリソースを何処に対して投下すべきなのかは、経営層が投資効果を軸に判断する以外にありません。（４章、４．２、（２））

情報システムを利用しながら業務・サービスを提供する利用者の経営者の、システムの健全な維持のために行うことを述べる。

- 利用者の経営者は、情報システムに対して、自身の考えと、その考えを適正に実現するための、ポリシー（方針）とステートメント（指示事項）を明確に示すこと。
- 当該分野に於ける経営活動は、全てこのポリシーとステートメントを基準にして行われていることを報告と監査で確認すること。
- 経営者は適正な経営資源を投入し、その整備状況を報告と監査で確認すること。
- 経営資源の投入の適正さには、公的な客観的基準が存在している訳ではなく、経営者の意思として行われることを理解すること。
- 社会通念上必要とされる機能の実現が期待されることから、社内外のステークホルダー（利害関係者）と協議しながら進めること。
- 以上のようなプロセスで、業務統制、IT 統制の状況を把握し、ステークホルダーに対し説明責任を果たすこと。

Ｄ．情報システム供給者の要求事項

＜経営者が参画する要求品質の確保＞
経営層は先入観を持つことなく、業務部門の声に耳を傾け、フラットな視点で判断する義務があるといえます。ヒト・モノ・カネという限りあるリソースを何処に対して投下すべきなのかは、経営層が投資効果を軸に判断する以外にありません。（４章、４．２、（２））

情報システムを供給する供給者の経営者は、利用者の経営者と一体となって社会的責任を果たしていために行うことを述べる。

・ 供給者の経営者は、利用者のポリシーやステートメントに適合できる技術的な総合サービスを提供できるよう努めること。
・ 今日の複雑で進歩の速い技術環境を考え、自社内資源に留まらず、目的達成の為に広く協力関係を求めていくこと。
・ そのキーマンが経営者であることを理解し、責任者を指名すると共に推進計画と資源の投入を承認すること
・ 関係者に定期的な報告を求め、必要な措置を講じること。
・ 利用者の要求に合ったサービス体制と人材育成の整備は、経営者が率先して行うこと。

E．その他の留意事項

利用者・供給者共に、経営資源の投入と結果の評価は、その経営者によるステアリングコミッティー的な体制で推進することが望ましく、メンバーには関係組織を交え、推進のリスク評価と対策に洩れなく進める事が、品質の確保、維持に欠かせない。

（２）CIO（情報統括役員）の登用と活用

Ａ．ガイドライン原文

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、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。

Ｂ．本項目の必要性・重要性

今日の情報システムは、技術の進歩の速さ、範囲の広さ、複雑さ等が特徴といえる。

情報システム自身もホストと呼ばれる汎用大型コンピュータに始まり、ミニコンピュータ・オフィスコンピュータの様に小型化し、オープン型でスケーラビリティ（大小規模の融通性の高い）なシステムへと変化を遂げてきた。それに伴って、ソフトウェアやそれを実現する技術も大きく進歩を遂げている。

例えば、商売を行うにしてもホームページは不可欠であり、しかもその技術は情報発信に始まり、検索・連携に進み、最近では利用者が商品を考案して企業に提案し、企業がその商品を実現させるという、新しいプロダクトアウトの様な方式が普及し始めており、ただ単にホームページを立ち上げて情報発信する時代は終わりを告げている。

この様なめまぐるしい変化に対応するには、専門的な知識を備えた経営者の存在と指導が不可欠で、情報担当役員すなわちCIO を任命し、対処することが求められている。

CIO の様な専門性の高い経営者を自社だけに求めることは難しい場合があり、社外も含めて広く人材をスカウトして体制を整備することが求められている。

Ｃ．情報システム利用者の実施事項

＜経営者が参画する要求品質の確保＞
　システム開発に必要な要件としては、事業要件、業務要件、システム要件などがあり、それぞれに対応した役割（ロール）が考えられます。（４章、４．１）

情報システム利用の経営者が取り組むべきことを述べる。

- 情報システムはその特性を考えて活用を行えば十分な効果が期待できるが、一方、自社の経営戦略や業務推進と結びつけて機能を実現させなければ、無駄な投資に終る可能性が高い　ことを理解すること。
- 情報システムを活用するための技術や方法論は専門性が高く、しかも変化が速いという特性を理解し、継続的努力を行うこと。
- この重要な情報システムを現実の経営の場に活用するために、専任の情報担当役員（CIO）を指名してその任務に当たらせること。
- 任命された CIO は、情報システムの中期的計画を立案し、経営トップやステアリングコミッティーに図り、承認を得た後、体制を整備しておくこと。
- 中期計画立案には、情報システムに関する業務部門や情報システム部門のみならず、社内のステークホルダーも含めて検討すること。
- 個別の業務単位の情報システムは、中期計画に基づいて計画されていること。
- CIO はその開始のときから廃棄に至るまでのライフサイクルにつき、計画と報告を求め、必要の都度経営トップやステアリングコミッティーに報告し、必要な措置を講ずること。

・ 経営者は、CIOや情報システム責任者から、定期的な報告を求めること。
・ 経営者は、この様な体制整備やライフサイクルの管理を通じて、情報システムの信頼性・安全性の実現、情報システムの有効性とサービスの実現を図ることを、間接的に実施すること。

D．その他の留意事項

CIOは重要ではあるが、極めて専門性が高いために、自社内で選任できるとは限らない。高い専門性を備えた人材を広く求め、事業戦略の推進や一般利用者に支障が発生しないよう努めなければならない。

ITコーディネータ協会が公認しているITコーディネータの中には社外CIOの任務を実施している者もあり、選択肢の一つとして考えることが出来る。

（3）説明責任の認識

A．ガイドライン原文

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・サービスに対する双方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。

B．本項目の必要性・重要性

業務やサービスを一般の利用者に提供することは経営者の意思表示の現れであり、その結果責任も経営者に帰属することになる。

重要インフラ等の場合、その情報システムも含めて結果責任は重大であり、担当者に責任をなすりつけたり、自社内の閉じた論理で対応することは許されなくなってきている。

このことを踏まえ、経営者は方針を示し、計画を承認し、報告を求め、必要な措置をとることで説明責任を果たさなければならない。

C．情報システム利用者の実施事項

＜経営者が参画する要求品質の確保＞
「経営者の役割と責任分担」を明確にしていくことにしました。（第３章、３．１、（4））

情報システムを利用する経営者が取り組むべきことを述べる。

- 情報システムを通じて行われる業務・サービス提供の上で、社会通念上、期待される効果及び信頼性・安全性について、体制を整備し、説明責任を果たすこと。
- 説明責任の中には、経営者としての方針、推進するための体制の整備状況、進捗確認及び評価、協力を得ている委託先選定理由、予算的措置、監査体制とその評価結果等が含まれていることを理解すること。

D．情報システム供給者の要求事項

＜経営者が参画する要求品質の確保＞
「経営者の役割と責任分担」を明確にしていくことにしました。（第３章、３．１、（4））

情報システムを供給する経営者が取り組むべきことを述べる。

- 情報システムの供給に関し、社会通念上、期待される効果及び信頼性・安全性について、体制を整備し、説明責任を果たすこと。
- 説明責任の中には、情報システム供給にあたっての方針、体制の整備状況、予算的措置、採用した技術、監査体制とその評価結果、情報システム利用への責任等が含まれていることを理解すること。

E．その他の留意事項

説明責任が不十分であるとして責任を追及されるケースは、多くは自社内に閉じた都合の良い論理や、特定の業界でしか通用しない論理で対処されている等をあげることができる。

説明責任の程度は、その業界常識や社内の慣習のみ囚われず、その時点で社会的に何が要求されているかを情報収集し、分析し、責任の重さ等に応じて決められなければならない。

（４）保守・運用の重要性の認識

Ａ．ガイドライン原文

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、それらを行う保守・運用段階の重要性を認識しなければならない。

Ｂ．本項目の必要性・重要性

経営環境は絶えず変化を続けており、恒常的で不変な状況の継続を自己中心的に望んでも、その様な状況は現れてこない。特にニーズの変化に基づく対応、技術進歩に基づく対応は、適切な対応を行わないと経営を圧迫する事態を招きかねない。

情報システムもニーズ変化や技術進歩に合わせた対応をシステム内に組み込むことで、絶えず最新の状態に保つ必要がある。

それによって、一般利用者の利用離れを防止したり、不適切な機能により損害賠償による訴訟を防止したりし、社会的な信頼を定着していかなくてはならない。

Ｃ．情報システム利用者の実施事項

＜経営者が参画する要求品質の確保＞
システム障害リスクは経営リスクです。このことを正しく理解し、開発品質向上を実現し、システム障害リスクマネジメントを実現した経営者こそが、社会的責任を果たせる存在であるといえます。（１章、１．３、(1)、③）

情報システム利用者の経営者が取り組むべきことを述べる。

- 情報システムは設計通りに運用していくことは勿論、ニーズの変化、技術の進歩に合わせた改善を保守として継続をしなければならないことを理解すること。
- 変更は利用者を対象とした調査による意見収集、有効な新技術の取り入れ、情報システム自身の不具合改修などを原因として、適切に行うよう指示すること。
- 変更に当たっては広く情報を集め、ステークホルダーの意見を求めた上で、技術的実現性をコスト面も含めて満たすものであることを確認すること。
- 情報システムの運用・保守は、経営者の責任で実施すること。

Ｄ．その他の留意事項

重要インフラの情報システムでは、障害の発生を未然に防止することは勿論、障害発生時に早急な復旧、若しくは回避代替策で利用に支障をきたさない様にしないと、訴訟やマスコミなどによる社会的な責任を追及されかねない。

ベルトプラクティスを参考にするのも良いが、その業界で対応のベストプラクティスが無い場合は、他の業界で成功した例を手本にベンチマーキングなどを行い、改善の方向性を模索しておかなくてはならない。

（５）事業継続計画の策定と役割の認識

Ａ．ガイドライン原文

情報システム利用者の経営層は、提供する業務・サービスの事業継続計画（BCP：Business Continuity Plan）を策定し、情報システム障害等の緊急時における自らの役割を認識しなければならない。

また、情報システム供給者の経営層は、当該計画を理解し、同様に自らの役割を認識しなければならない。

Ｂ．本項目の必要性・重要性

重要インフラ等を構成する情報システムは、その社会的影響度から停止しないことが望ましいが、不幸にしてトラブルが発生した場合には、早期に復旧させるか、代替手段による回避策を実施できるように整備しなければならない。

特に社会インフラ分野（電気、ガス、水道、通信、交通機関、医療など）においては、停止による被害と損害賠償、復旧による経営資源の負担の発生などを、当該担当者のみならず、経営者を頂点として末端の従業員に至るまで、その社会的重要性と経営的負担について日頃から教育を行い、社会的責任達成の周知徹底を行わなければならない。

これらは、事業継続計画として計画的に準備されている必要があり、そのためには社内外のステークホルダーを含めた広範囲な影響と対策が網羅されている必要がある。

Ｃ．情報システム利用者の実施事項

＜経営者が参画する要求品質の確保＞
システム化が進んだ大企業ほどその影響が大きくなります。このことは、お客様にも影響を及ぼすことになります。（１章、１．３、（１）、③）
要求品質を確保することが事業を推進する鍵になります。（５章）

情報システム利用の経営者が取り組むべきことを述べる。

- 特に重要インフラ等の情報システムの場合、それ停止させないために、情報システム利用者の経営者は事業継続計画を策定し、その基本方針に基づいて整備を行い、教育訓練を実施すること。
- 事業継続計画は当該情報システムのみならず、情報システム以外の事業部分を含めて全体をフォーカスし、優先順位を付けて検討すること。
- 事業継続計画は、2000 年問題、事業拡大、事業分割、企業統合、システム基盤の更新など、機会あるごとに見直し、ローリングを行って最新の状態を保つこと。
- 事業継続計画手順は、事業継続の方針、対象となる機能の洗い出し、優先順位付け、優先順に基づいた対応のカテゴリー分け、カテゴリー毎の対策、全体推進の承認、予算化、アクションプランの立案と段階的実施、カテゴリー別に基づいた教育訓練の実施などを段階的に行うこと。
- 計画として取り組む項目や程度は、他社の事例などを参考に、ステークホルダーの意見、技術的可能性の見地などから検討を行い、場合によっては採算を超えた検討をせざるを得ない可能性も含めること。
- 事業継続計画の推進は、経営者の責任において行うこと。

Ｄ．その他の留意事項

重要インフラ等は他の事業分野に比較して、事前の基本的投資額が大きく、その割りに、投資額の回集に時間がかかる事業分野であると言える。そのため、急激な社会的変化に追従していくことが、コスト的にも難しい。

しかし、何らかの理由により停止や性能低下が発生した場合、それを利用している利用者の生活や利用企業の事業運営に影響を与える可能性が大きいので、対策を検討せざるを得ない。特にコスト的な負担が大きい事業継続計画の推進は簡単ではないが、実施しなかった場合の影響や社会的制裁を考えた場合、採算を超えた検討をせざるを得ない可能性もあり得る事を自覚しながら進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

Ａ．ガイドライン原文

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。

Ｂ．本項目の必要性・重要性

今日の様に情報システムに依存する社会では、障害リスクは直ちに経営リスクとなる。

情報システムの機能を適正に維持していくためには、環境に見合った継続的改善が必要となる。それによって、一般利用者に影響が及ばないようにしなければならない。

機能の改善の着眼点は「未然防止」と「事後対策」であるが、ISO9000 でいうところの CAPA（Corrective Action 是正措置、Priventive Action 予防措置）で考えることが出来る。

経営者は是正措置、予防措置が行えるような体制を整備しなければならない。

Ｃ．情報システム利用者の実施事項

情報システム利用者の経営者が取り組むべきことを述べる。

- 情報システムは、設計時点で全てのリスクを洗い出すことは困難で、また時間の経過と共に新たなリスクが発生することが見込まれ、定期的に改善を施さなければ正常な機能の維持は期待できないことを理解すること。
- そのためには、設計時にリスクを洗い出しておくのは勿論のこと、運用上の不具合や問題点の記録、環境変化のためのリスクとそれへの適用などをまとめ、優先順位付けを行い、経営者が承認し、計画的に適用していくこと。
- 不具合や障害への対応を、大きく是正措置と予防措置に分けること。
- 是正措置の場合、既に発生した障害や不具合に対応するもので、重要な案件若しくは比較的速く対応した方が良い案件に適用すること。
- 法律や規則の改正があって、既存の情報システム若しくは開発中の情報システムの法令適合が困難になった場合にも、是正措置を適用して対応すること。
- 予防措置は、既に発生した障害や不具合のうち、比較的時間をおいた対応でもかまわない案件、バージョンアップ等技術的理由で事前に計画できる案件、企画や設計段階で法改正が あり、開発に間に合わせることが出来る案件などに適用すること。
- 改善措置を行った場合には、経営者はそれをステークホルダーに連絡し、周知徹底させること。
- 是正措置や予防措置を行った場合は、その結果が構成管理に反映されるようにし、不整合が生じないように管理するよう指示すること。
- 経営者は、是正措置、予防措置の考え方を理解し、責任者を通じて体制を整備すること。

Ｄ．その他の留意事項

技術的には導入すれば効果が上がることが分かっていても、経済的理由、若しくは何らかの理由で導入が困難な場合が有り得る。その場合、中・長期的な計画に項目を織り込み、条件が満たされた場合に実行できるような整備を行うことが望ましい。

４．信頼性・安全性向上に向けた多面的取組の必要性

Ａ．ガイドライン原文

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・安全性の水準を認識及び決定した上で、情報システム障害に係る原因の種別（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。

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、合意すること。

Ｂ．本項目の必要性・重要性

重要インフラ等を担う情報システムは、障害が起きた場合に、その全てが解決されることが望ましいが、思い通りにならない場合もあり、多面的な取り組みが必要とされる。

情報システムの障害が発生した場合に、①直ぐに解決可能、②技術開発があれば解決可能、③直ぐには解決しないが時間が経過を待てば解決可能、④解決不可能なので他の運用手段や保険をかけるなど他の手段を講じる、などの対応が考えられる。

特に難しいのは障害が複合的にしかも同時に発生した場合である。構造の理解が難しく、範囲が広く、時間や費用がかかると想定され、円滑な業務推進を阻害しかねない。これらに対応するためには、日頃の情報整備と対策訓練がなされている必要がある。

他の障害を「他山の石」とすることが信頼性・安全性を確保する手段の一つではあるが、往々にして他人事で片付けてしまいがちになる。

経営者はそのことを理解し、関係者に定期的に障害リスクの洗い出しと対策の結果報告を求め、承認し、事態が発生した場合に対応しなければならない。

Ｃ）情報システム利用者の実施事項

＜経営者が参画する要求品質の確保＞
システム障害リスクは経営リスクです。このことを正しく理解し、開発品質向上を実現し、システム障害リスクマネジメントを実現した経営者こそが、社会的責任を果たせる存在であるといえます。（１章、１．３、(１)、③）

情報システム利用の経営者が取り組むべきことを述べる。

- 情報システムは、設計時点で全てのリスクを洗い出すことは困難で、また時間の経過と共に新たなリスクが発生することが見込まれる。また法令の改正などもリスクの一つと捉えることができるので、設計時にリスクを洗い出しておくのは勿論のこと、運用上の不具合や問題点の記録、環境変化のためのリスクとそれへの適用などをまとめ、優先順位付けを行い、経営者が承認し、計画的に適用していくこと。
- 障害や不具合のリスクを常時完全に捉えておくことは困難で、想定外のことが発生する事を予想しておくこと。
- 法令の改正も情報システム運用上はリスクの一つであり、国内だけではなく、海外の条約批准による影響なども想定外のリスクと捉えるておくこと。
- リスクは、重要度・緊急度のレベルによって、その影響度を社会的な面・コスト的な面などから計り、対策の優先順位とすること。
- 対応という視点からは、①現状の資源で解決できるレベル、②経営資源を追加投入すれば解決

できるレベル、③自社だけでは困難で業界等が共同で対応して解決できるレベル、④発明や技術革新があれば対応できるレベル、⑤解決不能なので保険や別の運用などで対応するレベルなどに分類すること。

・ 経営者は責任者を指名し、リスクの程度と対応手段の整備を行い、情報システムの正常運用の維持に努めること。

D．その他の留意事項

重要インフラ等に係る情報システムは、正常に機能するよう管理・維持されなければならないが、そのための技術的・人的対応のみでは不足する場合が考えられる。

災害や大規模な障害の場合、利用者企業、供給者企業に多大の負荷がかかるが、全ての復旧対応が可能な場合だけではなく、困難な場合を想定して保険をかけ、経済的な負担を和らげる措置なども検討しておく必要がある。また、新しい技術開発を待たなければならない事態も想定されるので、考え方の周知が必要になる。

重要インフラを担う企業が負担に耐えられなくなって消滅することは、それを利用する一般利用者にも多大の影響を与えることから、広範囲に継続策を検討することが望ましい。

５．情報システム障害に対する動作の基本

Ａ．ガイドライン原文

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3 つの観点からの措置を講じなければならない。

- **情報システム障害の原因・要因の除去**
- **情報システム障害の発現の防止**
- **情報システム障害による影響拡大の防止**

Ｂ．本項目の必要性・重要性

情報システムの障害対応は、適切に行われなければ利用者のみならず、一般の利用者にも影響が及び、その責任は利用者・供給者の経営者に及ぶことになる。

障害に対応するにはその発見と伝達ルート、判断レベル、対応者などが整備されている必要がある。特に、障害の程度・解決の難しさ、範囲の広さなどからエスカレーションルールを定めて適切に対応する必要がある。

障害は解決側の関係者、利用側の関係者など多くのステークホルダーが係わるので、年度計画ごとに体制の見直しを行なう。

障害の体制整備は経営者の責任において行われなければならない。

Ｃ．情報システム利用者の実施事項

＜経営者が参画する要求品質の確保＞
全ての業務がシステム上で動くようになった結果、システムが実現する機能、アウトプットに誤りが発生した場合、その影響は大きく、社会混乱をもたらし、企業の存続に機器をもたらすことも考えられます。（１章、１．３、（１）、③）

情報システム利用の経営者が取り組むべきことを述べる。

- 障害は、①障害の発見、②関係者への伝達、③初動処理、④拡大防止、⑤事後処理、⑥予防策の検討などからなることを理解すること。
- これらに関係するものは、保守・運用の関係者のみならず、利用者のステークホルダーにも及ぶことを理解すること。例えば、経理システムの障害の様な場合、システム停止によって資金の受け入れや支払が出来なくなるが、①関係者への伝達、②善後策の検討、③手作業処理（銀行の窓口に出向いて処理するなど)、④事後の検討などからなり、業務処理関係者だけではなく、取引先にも影響が及ぶ。
- 障害には、影響の度合いによって報告者や手段を変えていくエスカレーションの整備を行い、適切に対応していくこと。
- エスカレーションの度合いによって、招集される会議体が異なり、討議に参加するメンバーも変化する様に体制を整備すること。
- エスカレーションは全社リスク対策の一部として構成されていることが望ましく、その拡大の程度は経営層の段階と比例していること。
- 障害対応は是正措置・予防措置として中期計画に織り込まれていること。

D．その他の留意事項

障害対応のエスカレーションや体制作りは、自社内や業界内だけではなく、既に発生し、適切な対応を行った事例などを参考にしながら、構築していくことが望ましい。

今日的には、障害発生とその対応を隠すよりは、速めに公開し、一般利用者の理解を求めていく行為が必要となる。それらを怠って公表時間を遅らせると、社会的責任追によって売上低下などの社会的ダメージを蒙る損害につながりかねない。

業務分野によっては、事故・障害に対し、当局が関与する場合がある。その場合、障害の原因と対策の報告が求められるので、適切な体制の整備が必要となる。

Ⅲ．企画・開発および保守・運用全体における事項

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る為の企画・開発段階から保守・運用段階のシステムライフサイクルにわたる全般的配慮事項について述べる。

Ａ．ガイドライン原文

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・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。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。

Ｂ．本項目の必要性・重要性

特に重要インフラを担う様な社会的な影響が大きいシステムについて、通常の利用範囲に於いて正常に稼動するかどうかは、当該企業活動のみならず、相互依存している企業、更には、それらの企業からサービスを受ける一般利用者までも波及的に大きな影響を及ぼすことを意味している。

経営者の責務、利用者の責務、開発・運用者の責務について、本ガイドラインを参照しながら文書化を行い、関係者に周知徹底させることが必要である。

システムを開発・利用する責任者は、これらの事情をわきまえて体制を整備し、システムの利用に於けるシステムのプロセスを定め、ライフサイクルを確立し、文書化し、責任者の承認を得、これらの必要な基準を満たした開発・運用が出来るよう努めなければならない。

Ｃ．情報システム利用者の実施事項

経営の優先度と、スケジュール、経営資源など制約条件を考慮し

・人材育成
・組織・役割分担変更等を含む業務プロセス改革
・IT サービス
・セキュリティ＆リスク管理
・モニタリング＆コントロール

といった様な IT 調達・導入に関する前提条件、制約条件を確定する。

Ｄ．情報システム供給者への要求事項

例えば、現行の業務や情報システムからの移行方法時に

・役割と責任
・予算とスケジュール

といった様な前提条件や制約条件を明確にする（利用者との合意事項の確認）。

Ｅ．その他の留意事項

※）IT コーディネータが注意すべきこと

経営者の視点に立って、

・業務プロセス改革実現のための人材育成

・組織の役割の見直し

・経営戦略にそった経営資源の最適配置

・スリムな IT 環境構築

を経営の成熟度に応じて、経営者が理解できる形、表現で提案し、承認を受けることが必要となることに留意する。

1. 企画段階における留意事項

Ａ．ガイドライン原文

企画段階において、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。

その上で、当該の信頼性・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。

Ｂ．本項目の必要性・重要性

経営戦略の優先度、難易度、投入できる資源（ヒト・モノ・カネ)、人材育成に要する期間、ビジネスパートナーとの協力関係、投資対効果などを評価し、到達目標、新業務プロセス、IT サービスの範囲と機能、IT サービスレベルを決定しておくことが必要。

Ｃ．情報システム利用者の実施事項

例えば以下の様な

・ IT 化によって経営戦略を実現するために必要な範囲の抽出

・ 既存業務の見直し、組織や役割分担変更などの検討

といった項目についての検討を行い､あるべき業務プロセスの概要を策定しておくことが望ましい。

Ｄ．情報システム供給者への要求事項

・ ベストプラクティスなどを参考にして、目標業務プロセスを実現するために到達すべき IT 環境の概要を提案する。

・ IT サービス活用のレベルをどこに設定するかといった視点で、必要となる IT サービスと IT 資源を決定する。

Ｅ．その他の留意事項

※）IT コーディネータが留意すべきこと

個々のシステム企画時に

・IT サービス導入にあたって経営戦略との整合性を確保すること。IT 化はあくまで経営戦略の具現化が実現目標であり、経営戦略で要求していることと整合しているか常にチェックする必要があることに留意する。

・行き過ぎた IT 化や使い勝手の悪い IT サービスの導入により、人が振り回されたり、IT の活用不足により人に負担がかかりすぎないように留意する。

・システム構築と並行、協調して業務プロセス改革を進め、移行プロセスも含め、円滑な IT サービス活用がはかれるように留意する。

・企業の規模、業種業態の制約条件を考慮し、現状の IT 化の成熟度と遊離しすぎない様“身の丈にあった”IT サービスを導入できる様に留意すること。

・システムのことは担当者に任せるという態度をとることなく、率先してプロジェクトに関与し、トップダウンで成功に導かせる様なリーダーシップを経営者に取らせる様に仕向けることに留意する。

・情報システム構築前の企画・IT 調達段階から運用・廃棄までのライフサイクルを意識し、運用のキーマンを参画させるくことに留意する。

・投資効果を十分評価する為に、効果は極力数量的に把握し、運用・保守等の費用も含め

なるべく金額換算し、総額として把握しておくことが望ましい。

・事業継続の観点からもITサービス利用者もまじえ、合意事項を文書化しておくことが望ましい。

といった様な項目に留意することが望ましい。

（1）信頼性・安全性水準の利用者・供給者間での合意

A．ガイドライン原文

情報システム利用者及び情報システム供給者は、情報システムが具備すべき信頼性・安全性の水準及び目標とする品質基準等について定め、両者で合 意すること。

B．本項目の必要性・重要性

経営戦略で要求されていることを具現化し、維持する為に必要な情報システムに要求される信頼性・安全性（IT サービスの品質）について情報システム利用者と情報システム供給者間で合意を取り交わし、文書化し、運用しながら見直してゆくことが重要である。

リスク管理の観点からも、情報システムが停止した場合の社会的・経済的影響について洗い出しを行った上で情報システムが具備すべき信頼性・安全性の水準を定めることが必要。

C．情報システム利用者の実施事項

＜評価指標 U1＞

Q1. 信頼性・安全性の水準及び目標を明確化する際に、情報システムが停止した場合に与える社会的影響・経済損失を考慮に入れることを実施管理しているか。

Q2. 利用者が発生の可能性のある潜在的な危険要素について洗い出すこと（以下、潜在危険分析）を実施管理しているか。

a. 潜在危険分析を実施することを実施しているか。

b. 上記潜在危険分析の対象として当該システムで実現される業務・サービスを含んでいるか。

c. 上記潜在危険分析の対象としてハードウェアを含んでいるか。

d. 上記潜在危険分析の対象としてソフトウェアを含んでいるか。

e. 上記潜在危険分析の対象としてをヒューマンエラー(操作者等)含んでいるか。

Q3. Q2.で洗い出した危険要素について発生確率とその影響度を分析・評価すること（リスク分析・評価）を実施管理しているか。

Q4. 社会的影響・経済損失を考慮にいれて、システムの障害の許容度合を設定すること（安全水準の割付）を実施管理しているか。

Q5. 利用者が情報システムが具備すべき信頼性・安全性の水準について文書化することを実施管理しているか(安全機能要求仕様書等)。

Q6. Q5.の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを実施管理しているか。

＜評価指標 U2＞

Q1. 信頼性・安全性の水準及び目標を明確化する際に、情報システムが停止した場合に与える社会的影響・経済損失を考慮に入れているか。

Q2. 発生の可能性のある潜在的な危険要素について洗い出すこと（以下、潜在危険分析）を実施しているか。

a. 潜在危険分析を実施することを実施しているか。

b. 上記潜在危険分析の対象として当該システムで実現される業務・サービスを含んでいるか。

c. 上記潜在危険分析の対象としてハードウェアを含んでいるか。

d. 上記潜在危険分析の対象としてソフトウェアを含んでいるか。

e. 上記潜在危険分析の対象としてをヒューマンエラー(操作者等)含んでいるか。

Q3. Q2.で洗い出した危険要素について発生確率とその影響度を分析・評価すること（リスク分析・評価）を実施しているか。
Q4. 社会的影響・経済損失を考慮にいれて、システムの障害の許容度合を設定すること（安全水準の割付）を実施しているか。
Q5. 情報システムが具備すべき信頼性・安全性の水準について文書化しているか(安全機能要求仕様書等)。
Q6. Q5.の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認しているか。

・IT サービスの提供の実態がベンダーにアウトソーシングされている場合でも情報システムの信頼性・安全性についての責任は情報システム利用者にあることに留意。
・情報システムの信頼性・安全性の品質の維持は、情報システム利用者と情報システム供給者との共同作業である。このため、定期的な会議をあらかじめ設定するなど、両者のコミュニケーションが密になる施策がとられる様に留意すること。
・定期的に、企業における IT 化にかかわるすべての費用対効果を評価することにより、IT の有効な活用をめざす必要があることに様に留意すること。

といった事項について留意すること。

D．情報システム供給者への要求事項

＜評価指標 V1＞

Q1. 利用者が信頼性・安全性の水準及び目標を明確化する際に、情報システムが停止した場合に与える社会的影響・経済損失を考慮に入れることを支援することを実施管理しているか。
Q2. 利用者が発生の可能性のある潜在的な危険要素について洗い出すこと（以下、潜在危険分析）を実施することを支援することを実施管理しているか。
  a. 潜在危険分析を実施することを実施管理しているか。
  b. 上記潜在危険分析の対象として当該システムで実現される業務・サービスを含んでいるか。
  c. 上記潜在危険分析の対象としてハードウェアを含んでいるか。
  d. 上記潜在危険分析の対象としてソフトウェアを含んでいるか。
  e. 上記潜在危険分析の対象としてをヒューマンエラー(操作者等)含んでいるか。
Q3. Q2.を受けて利用者が洗い出した危険要素について発生確率とその影響度を分析・評価すること（リスク分析・評価）を支援することを実施管理しているか。
Q4. 利用者が社会的影響・経済損失を考慮にいれて、システムの障害の許容度合を設定すること（安全水準の割付）を支援することを実施管理しているか。
Q5. 利用者が情報システムが具備すべき信頼性・安全性の水準について文書化することを実施管理しているか。
Q6. Q5.の内容を利用者と供給者が合意した上で、利用者の適切な権限者の承認を確認することを実施管理しているか。

＜評価指標 V2＞

Q1. 利用者が信頼性・安全性の水準及び目標を明確化する際に、情報システムが停止した場合に与える社会的影響・経済損失を考慮に入れることを支援しているか。あるいはその

重要性を説明しているか。

Q2. 利用者が発生の可能性のある潜在的な危険要素について洗い出すこと（以下、潜在危険分析）を実施することを支援しているか。あるいはその重要性を説明しているか。

a. 潜在危険分析を実施することを支援しているか。

b. 上記潜在危険分析の対象として当該システムで実現される業務・サービスを含んでいるか。

c. 上記潜在危険分析の対象としてハードウェアを含んでいるか。

d. 上記潜在危険分析の対象としてソフトウェアを含んでいるか。

e. 上記潜在危険分析の対象としてをヒューマンエラー(操作者等)含んでいるか。

Q3. Q2.を受けて利用者が洗い出した危険要素について発生確率とその影響度を分析・評価すること（リスク分析・評価）を支援しているか。あるいはその重要性を説明しているか。

Q4. 利用者が社会的影響・経済損失を考慮にいれて、システムの障害の許容度合を設定すること（安全水準の割付）を支援しているか。あるいはその重要性を説明しているか。

Q5. 利用者が情報システムが具備すべき信頼性・安全性の水準について文書化することを支援しているか(安全機能要求仕様書等)。あるいはその重要性を説明しているか。

Q6. Q5.の内容を利用者と供給者が合意した上で、利用者の適切な権限者の承認を確認するしているか。

・上記の評価指標は、情報システム利用者にとって理解しやすい指標に設定し、情報システム供給者側での運用業務､運用管理業務をベースにIT専門用語が多用されない様に留意する。（**｢平均復旧時間｣や｢MTTR｣といった略語ではなく、例えば｢システム(端末)がまた使える様になるまでの予想時間｣などと利用者が理解しやすい様な表現で記述すること**）

・情報システムの信頼性・安全性の品質の維持は、情報システム利用者と情報システム供給者との共同作業である。このため、定期的な会議をあらかじめ設定するなど、両者のコミュニケーションが密になる施策がとられる様に留意すること。

といった事項について留意すること。

Ｅ．その他の留意事項

※）ITコーディネータが注意すべきこと

・現状のIT化の成熟度（ITガバナンス、ITリテラシー、ITサービス活用）と遊離しすぎないように配慮し、SLAを締結する。その際には、企業の規模、業種形態などの制約条件を考慮する事。

・経営者も含めた　ステークホルダー全体がIT化の価値、課題を認識することにより、ITの有効な活用をめざせる様に留意する。

・評価指標として、効果/費用の比、費用/売上の比など企業の実態にあった指標を決めて評価されていることを確認する。

・IT環境のライフサイクルの視点からだけでなく、根本的な見直しについても検討すること。

（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

Ａ．ガイドライン原文

情報システム利用者は、情報システムの企画に当たり、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前提条件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。

特に、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。

Ｂ．本項目の必要性・重要性

発注仕様の機能要件を明確にし､文書化して費用･作業内容を明確にしておくことは重要だが、以下の様な非機能要件についても明確にしておくこと

- ・セキュリティ対策
- ・現行システムから新システムへの移行(並行稼働が必須かどうか？等)
- ・現行システムの廃棄費用
- ・新・旧システムの並行稼働時の費用
  (原価償却費用、運用費用（ユーザー部門も含む)、保守費用)
- ・新システム教育費用
- ・瑕疵担保以外の新システムメンテ（稼働後　最低 6 か月は開発者を引っ張れる様な体制にしておくのが望ましい)
- ・ネットワーク（インターネット）環境
- ・電源・空調等のファシリティ（特に電源容量不足には注意すること）
- ・事業継続（災害対策）
- ・既存システムとの連携（データ交換）
- ・既存システム・インフラへの影響（例えばネットワークの帯域を圧迫してしまう等）

等について、必要なものは予算措置を講じておくことが必要と思われる。

特に情報システム供給者と情報システム利用者との運用・保守も含めた“責任分解点”を明確にし、合意の上文書化しておく必要がある。

Ｃ．情報システム利用者の実施事項

＜評価指標 U1＞

Q7. 情報システムに求める機能要件を明らかにすることを実施管理しているか 。

Q8. 情報システムに求める非機能要件を明らかにすることを実施管理しているか 。

- a. 上記で信頼性に関する要件を検討しているか。
- b. 上記で使用性に関する要件を検討しているか。
- c. 上記で効率性に関する要件を検討しているか。
- d. 上記で保守性に関する要件を検討しているか。
- e. 上記で移植性に関する要件を検討しているか。

Q9. 業務・システムの最適化を会社(組織)全体として整合性をもって進めてゆくための計画(全体最適化計画)との整合性を検討することを実施管理しているか 。

Q10. 運用環境(関連するほかの情報システムとの関係、システム運用形態、システム運用スケジュールなど)を明らかにすることを実施管理しているか。
Q11. 特に、非機能要件については見落としがちであることから、経営層を含めて十分に検討を行うことを実施管理しているか。
Q12. Q7-Q11 を踏まえて適切に、文書化することを実施管理しているか。
Q13. Q12 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを実施管理しているか。

＜評価指標 U2＞
Q7. 情報システムに求める機能要件を明らかにしているか 。
Q8. 情報システムに求める非機能要件を明らかにしているか 。
a. 上記で信頼性に関する要件を検討しているか。
b. 上記で使用性に関する要件を検討しているか。
c. 上記で効率性に関する要件を検討しているか。
d. 上記で保守性に関する要件を検討しているか。
e. 上記で移植性に関する要件を検討しているか。
Q9. 業務・システムの最適化を会社(組織)全体として整合性をもって進めてゆくための計画(全体最適化計画)との整合性を検討しているか 。
Q10. 運用環境(関連するほかの情報システムとの関係、システム運用形態、システム運用スケジュールなど)を明らかにしているか。
Q11. 特に、非機能要件については見落としがちであることから、経営層を含めて十分に検討を行っているか。
Q12. Q7-Q11 を踏まえて適切に文書化しているか。
Q13. Q12 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認理しているか。

システムライフサイクルを意識し、移行・システム運用費用等の非機能要件も含め（概算でもかまわないので）発生する費用をできるだけ明確することの重要性を経営者に説明し、必要なリソースを確保する様に様にする。

D．情報システム供給者への要求事項

＜評価指標 V1＞
Q7. 利用者が情報システムに求める機能要件を明らかにすることを支援することを実施管理しているか 。
Q8. 利用者が情報システムに求める非機能要件を明らかにすることを支援することを実施管理しているか 。
a. 上記で信頼性に関する要件を検討しているか。
b. 上記で使用性に関する要件を検討しているか。
c. 上記で効率性に関する要件を検討しているか。
d. 上記で保守性に関する要件を検討しているか。
e. 上記で移植性に関する要件を検討しているか。
Q9. 利用者が業務・システムの最適化を会社(組織)全体として整合性をもって進めてゆくための計画(全体最適化計画)との整合性を検討することを支援することを実施管理してい

るか 。

Q10. 利用者が運用環境(関連するほかの情報システムとの関係、システム運用形態、システム運用スケジュールなど)を明らかにすることを支援することを実施管理しているか。

Q11. 利用者が Q7-Q10 を踏まえて適切に文書化することを支援することを実施管理しているか。

Q12. Q11 の内容を利用者と供給者が合意した上で、利用者の適切な権限者の承認を確認することを実施しているか。

＜評価指標 V2＞

Q7. 利用者が情報システムに求める機能要件を明らかにすることを支援しているか。あるいはその重要性を説明しているか。

Q8. 利用者が情報システムに求める非機能要件を明らかにすることを支援しているか。あるいはその重要性を説明しているか。

a. 上記で信頼性に関する要件を検討しているか。

b. 上記で使用性に関する要件を検討しているか。

c. 上記で効率性に関する要件を検討しているか。

d. 上記で保守性に関する要件を検討しているか。

e. 上記で移植性に関する要件を検討しているか。

Q9. 利用者が業務・システムの最適化を会社(組織)全体として整合性をもって進めてゆくための計画(全体最適化計画)との整合性を検討することを支援しているか。あるいはその重要性を説明しているか。

Q10. 利用者が運用環境(関連するほかの情報システムとの関係、システム運用形態、システム運用スケジュールなど)を明らかにすることを支援しているか。あるいはその重要性を説明しているか。

Q11. 利用者が Q7-Q10 を踏まえて適切に文書化することを支援しているか。あるいはその重要性を説明しているか。

Q12. Q11 の内容を利用者と供給者が合意した上で、利用者の適切な権限者の承認を確認しているか。

特に情報システム利用者と供給者の“責任分解点”を明確にしておくことが重要。

具体的には、対象とするシステムの範囲（移行・システム運用費用等の非機能要件も含め）や、発生する費用を明確にしておくこと。

２．開発段階における留意事項

Ａ．ガイドライン原文

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。

Ｂ．本項目の必要性・重要性

情報システムの信頼性・安全性はその機能要件と非機能要件により成立するものである。しかし、その大部分は非機能要件が支えている。情報システム利用者にとって非機能要件はシステムが提供する機能を付帯的に満たすための要件であり、機能要件と比較すると非機能要件を明示的に要求事項としてまとめることは難しい。また機能要件を明確化・文書化することにスケジュールの大半を割くことにより、非機能要件が置き去りにされる傾向がある。これによって情報システムの信頼性・安全性水準が低下することを防ぐためにも適切なシステムライフサイクルプロセスを確立し、実行していくことが重要となる。

（1）システムライフサイクルプロセスの確立と文書化

Ａ．ガイドライン原文

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 98 及び ISO/IEC 20000 を参照し、ライフサイクルプロセスを確立し、文書化する。

Ｂ．本項目の必要性・重要性

システムを市場の取引として円滑に行うためには、情報システム利用者及び情報システム供給者が、共にシステム開発プロセスとその開発基準に関する共通の認識を持ち、文書化して確認する必要がある。求められる信頼性・安全性は開発プロセスの中で自ずと作りこまれるものであり、情報システム利用者及び情報システム供給者が、その水準を予め文書化して確認していることで共通の信頼性・安全性水準が維持可能となる。

システムの開発プロセスと開発の各時点に於ける確認基準に関しては以下のものが代表的である。

- ISO12207（SLCP，邦訳・共通フレーム 98)、
- IEEEE730（SQAP）
- SDLC 等
- 共通フレーム 2007
- システム監査基準
- プロセスガイドライン
- ISO5288（ソフトウェアライフサイクル）

Ｃ．情報システム利用者の実施事項

＜評価指標 U1＞
信頼性評価指標の該当記述なし。

＜評価指標 U2＞
信頼性評価指標の該当記述なし。

情報システム利用者が取り組むべきことを述べる。

・責任者による当該業務の開発・保守・運用に係るシステムライフサイクルを確立すること。
・システムライフサイクルと情報システム利用企業の開発・利用ポリシーの整合性を確認すること。
・システム開発・利用ポリシーと業界標準、監督官庁の規制・指示事項の整合を確認すること。
・経営者から責任者へシステム開発・保守・運用がシステム開発・利用ポリシーの遵守の指示をだすこと。
・責任者から関係者へシステム開発・利用ポリシーの周知徹底を図ること。
・下記の方法などによりシステムライフサイクルの遵守状況を確認すること。
　・プロジェクトレビュー

・情報システム利用者によるシステムバリデーション
・品質管理部門による内部業務監査
・外部第三者による監査

D．情報システム供給者への要求事項

＜評価指標 V1＞
Q13：文書化されたシステムライフサイクルプロセス（システムの開発から保守・運用に至るまでの一連の作業の過程）に定められたプロセスを実施管理しているか。
Q14：プロセスが適切に実施されているかどうかを評価する必要がある。
a. プロセスが適切に実施されているかどうかを評価するシステムがある。ただし当該システムには評価者、管理者（プロセスの実施の管理者）、監督者を置くこと。評価者、監督者は兼任可とする。
b. 適切な評価が実施されているか。
c. 適切な評価者が評価しているか。
Q15：評価した結果をもとに必要な是正措置がとられているか。
a. 是正措置の要否を判断しているか。
b. 必要な場合に是正措置を実施しているか。

＜評価指標 V2＞
Q13：文書化されたシステムライフサイクルプロセス（システムの開発から保守・運用に至るまでの一連の作業の過程）に従ってプロセスが実施されているか。

情報システム供給者が取り組むべきことを述べる。

・ 開発・保守・運用に関わる明確なシステムライフサイクルプロセスを確定すること。
・ システムライフサイクルプロセスに基づく業務運用を実施すること。
・ 下記方法などで責任者によるシステムライフサイクルプロセス遵守を確認すること。
  ・社内レビュー
  ・社内業務監査
  ・情報システム利用企業へのインタビュー
  ・外部第三者による監査

E．その他の留意事項

※IT コーディネータが注意すべきこと

IT コーディネータは当該業務の計画を策定するに当たって、情報システム利用企業のシステム開発ポリシーに基づくシステムライフサイクルプロセスが定義されていることを確認する。
利用企業にシステム開発ポリシーが策定されていない場合は、その制定を促し、経営者の承認を取っておくことが重要である。システムライフサイクルは、このポリシーの元に作成される必要がある。
システムライフサイクルは公的基準が基本になっていなければならないが、当該業務分野で業界標準や監督官庁の規制がある場合、ITC はそれらの内容をよく理解し、システムライフサイクルプロセスに反映されるよう、指導することが望ましい。
IT コーディネータの「プロセスガイドライン」は IT コーディネータの業務を視点に記述されているので、一般のシステムライフサイクルや品質基準と異なる部分がある。そのことをよく理解し、「プロセスガイドライン」に固執することなく、利用企業の適正なライフサイクル確立に寄与するよう心がける。

IT コーディネータは情報システム利用企業が利用するシステムの、開発・運用プロセスが適正なシステムライフサイクルに準拠して推進されていることを確認しなければならない。
システムライフサイクルが、公的基準に基づいているほか、情報システム利用企業が属する業界の標準、監督官庁の規制などを反映して作成されていること、責任者の承認を得て文書化されていることを確認しなければならない。

IT コーディネータは、システムライフサイクルが、情報システム利用企業・供給企業双方の合意の下に作成されるため、その橋渡し的な外部アドバイザーとして指導的を果たすことが期待されている。

情報システム利用者側のみに肩入れし過ぎても、情報システム供給者側に肩入れし過ぎても、望ましい結果に結びつかないことから、当該企業のみならず、競合他社とのベンチマーキングをするなど、第三者としての強みを発揮して、適正な方向に導いていくことが望ましい。

（２）役割分担・責任権限の利用者・供給者間での合意

Ａ．ガイドライン原文

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・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。

＜実施例＞

共通フレーム98 を参照し、個々のプロセスに関する双方の役割・責任を文書化し、合意する。

Ｂ．本項目の必要性・重要性

情報システム供給者および情報システム利用者はシステムを作るうえでの共同作業者であり、相互の協力が大変重要である。

しかしながら作業工程、作業項目の重複・不足およびその役割分担、責任権限は不明確になりがちである。不明確部分は作業が進むに連れて徐々に露呈してくる傾向にあるが、この対応により全体スケジュールに対する影響が出る可能性が大きくなる。

スケジュールの遅延は新規事業・業務・サービスなどの開始遅延へつながり、情報システム利用者の経営に大きな影響を与える。例えば社会インフラ・サービスが開始遅延した場合は、情報システム利用者、情報システムの社会的責任に発展することも考えられる。

これらを回避するためにはスケジュールどおりの情報システムの稼動が最優先となる一方で機能要件に譲歩できる部分は少ないために信頼性・安全性に関する作業工程・項目が置き去りにされる恐れがある。スケジュール重視、機能要件重視で完成した情報システムは運用面ではフェイルセーフ、フールプルーフなどの信頼性・安全性の考慮が少ないため、自ずとシステム障害が発生する確率が高くなる。システム障害が頻発することによりサービスの機能停止に波及し、回避・回復のために運用・保守面を人海戦術に頼らざるを得なくなり情報システム利用者、情報システム供給者ともに当初想定以上の費用負担を強いられることとなる。

このような事態に陥らないために情報システム供給者、情報システム利用者が役割分担及び責任権限を明確化しておくことが重要となる。

Ｃ．情報システム利用者の実施事項

＜評価指標 U1＞

Q14： 企画・開発から保守・運用に至る各プロセスにおける役割分担・責任権限を明確にし文書化することを実施管理しているか。

a. 組織で実施する全ての工程について、利用者・供給者間で役割分担・責任権限を明確にし文書化しているか。

b. 組織で実施する全ての作業項目について、利用者・供給者間で役割分担・責任権限を明確にし文書化しているか。

Q15： Q14 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを実施管理しているか。また、供給者の適切な権限者の承認を確認することを実施管理しているか。

＜評価指標 U2＞

Q14： 企画・開発から保守・運用に至る各プロセスにおける役割分担・責任権限を明確にし文書化しているか。

a. プロジェクトで実施する全ての工程について、利用者・供給者間で役割分担・責任権限を明確にし文書化しているか。

b. プロジェクトで実施する全ての作業項目について、利用者・供給者間で役割分担・責任権限

を明確にし文書化しているか。
Q15： Q14 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認しているか。また、供給者の適切な権限者が承認していることを確認しているか。

情報システム利用者が取り組むべきことを述べる。

・ 責任者による各プロセスにおける工程・作業項目を洗い出すこと。
・ 責任者による役割分担・責任権限を明確化、文書化すること。
・ 情報システム利用企業内部の関係者によるレビューおよび情報システム供給企業からのアドバイス、レビューを受けること。
・ 文書化された役割分担・責任権限の情報システム利用者および情報システム供給者間で合議を得ること。
・ 文書化された役割分担・責任権限の情報システム利用者および情報システム供給者間の適切な権限者による承認を受けること。

D．情報システム供給者への要求事項

＜評価指標 V1＞
Q16： 利用者が企画・開発から保守・運用に至る各プロセスにおける役割分担・責任権限を明確にし文書化することを支援することを実施管理しているか。
a. 組織で実施する全ての工程について、利用者・供給者間で役割分担・責任権限を明確にし文書化しているか。
b. 組織で実施する全ての作業項目について、利用者・供給者間で役割分担・責任権限を明確にし文書化しているか。
Q17： Q16 の内容を利用者と供給者が合意した上で、利用者の適切な権限者の承認を確認することを実施管理しているか。また、供給者の適切な権限者が承認することを実施管理しているか。

＜評価指標 V2＞
Q14： 利用者が企画・開発から保守・運用に至る各プロセスにおける役割分担・責任権限明確にし文書化することを支援しているか。あるいはその重要性を説明しているか。
a. プロジェクトで実施する全ての工程について、利用者・供給者間で役割分担・責任権限を明確にし文書化しているか。
b. プロジェクトで実施する全ての作業項目について、利用者・供給者間で役割分担・責任権限を明確にし文書化しているか。
Q15： Q14 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを確認しているか。また、供給者の適切な権限者が承認しているか。

情報システム供給者が取り組むべきことを述べる。

・ 情報システム利用者による各プロセスの工程・作業項目を洗い出しの支援を行うこと。
・ 情報システム利用者による各プロセスの役割分担・責任権限明確化、文書化の支援を行うこと。
・ 工程・作業項目の洗い出し、作業分担・責任権限の明確化に対する素案の提供を行うこと。
・ 文書化された役割分担・責任権限の情報システム利用者および情報システム供給者間での合議を得ること。
・ 文書化された役割分担・責任権限の情報システム利用者および情報システム供給者間の適切な権限者による承認を得ること。

E．その他の留意事項

※IT コーディネータが注意すべきこと
ITCPGL（IT導入フェーズ）に規定される導入詳細スケジュール作成と役割分担のアクティビティに従い、プロセスをWBS手法などによって作業工程、作業項目、作業分担、責任権限を明確化、文書化して情報システム利用者、情報システム供給者が合意・承認することを適切に支援する。

ITコーディネータは情報システム利用者が情報システム供給者から提示される作業分担・責任権限をよく解釈せずに、形式的に承認することがないように必ずレビューに参加して適切な確認・指摘をしなければならない。また、情報システム利用者が主体的に行わなければならない業務マニュアル作成、システム運用マニュアル作成、テスト計画策定などの作業は忘れがちになるため、これらの作業が計画に盛り込まれるよう留意しなければならない。

（３）機能要件の実現に向けた利用者・供給者間での合意

Ａ．ガイドライン原文

情報システム利用者及び情報システム供給者は、具体的な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下、精度の向上に努めること。

＜実施例＞

情報システム利用者及び情報システム供給者協力の下、発注仕様に基づき具体的な機能要件を明確化及び文書化する。

Ｂ．本項目の必要性・重要性

情報システム利用者は自分が実現したい情報システム機能の大部分をよく理解し、これを提示することができる。

しかし、情報システム利用者は言外の機能要求・要望を各種保持しているものである。それらの言外の要求は情報システムが当然保持しているべき機能との先入観等から明示的な要求として文書化されることは少ない。また、情報システム供給者は歴史的に情報システムの機能要件は情報システム利用者から提示されることを前提にしていることが多い。

一方で情報システムは完成間近にならないと目に見え、手で触れることができないという性質がある。情報システム利用者から噴出する各種の機能要求・要望を完成間近になってから取り込むことは開発スケジュールの見直し、開発費用の見直しに直結することが多くなる。

このようなことを極力発生させないことが情報システム開発を成功に導くこととなる。このためには情報システム利用者、情報システム供給者が具体的な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開発の企画段階から明確化及び文書化し、経営層を含め、合意しておくことが重要である。

Ｃ．情報システム利用者の実施事項

＜評価指標 U1＞

Q16： 具体的な要求事項(機能要件、非機能要件)を文書化することを実施管理しているか。

Q17： Q16 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを実施管理しているか。また、供給者の適切な権限者の承認を確認することを実施管理し

Q18： 要求事項及びその実現可能性のレビューは、事業継続計画及び、信頼性・安全性と実現・運用コストのトレードオフを考慮にいれて実施されているか。

a. 要求事項及びその実現可能性、実現・運用コスト等について、適切に合同レビューを実施しているか。

b. 合同レビューには運用部門、情報システム関係部門、経営者層等、必要な関係者が参加しているか。

c. 要求事項及びその実現可能性のレビューは、事業継続計画及び、信頼性・安全性と実現・運用コストのトレードオフを考慮にいれて実施されているか。

＜評価指標 U2＞

Q16： 具体的な要求事項(機能要件、非機能要件)を文書化しているか。

Q17： Q16 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認しているか。また、供給者の適切な権限者が承認していることを確認しているか。

Q18： 要求事項及びその実現可能性、実現・運用コスト等について、適切に合同レビューを実施し、すべての関係者の見解を統一しているか。

a. 要求事項及びその実現可能性、実現・運用コスト等について、適切に合同レビューを実施し

ているか。 b. 合同レビューには運用部門、情報システム関係部門、経営者層等、必要な関係者が参加しているか。 c. 要求事項及びその実現可能性のレビューは、事業継続計画及び、信頼性・安全性と実現・運用コストのトレードオフを考慮にいれて実施されているか。

情報システム利用者が取り組むべきことを述べる。

- 具体的な機能要件を要求事項として文書化すること。
- 要求事項の実現可能性、実現・運用コスト等を検討すること。
- 要求事項の運用部門、情報システム関係部門、経営者層等、必要な関係者による合同レビューを行うこと。
- 些細な要求事項も念には念を入れて明確化・文書化すること。
- 情報システム利用者、情報システム供給者間での確認・合意を得ること。
- 機能要求の優先順位付け、効果、実現できない場合の影響などによる機能要件の取捨選択基準を明確化すること。
- 文書化された要求事項の情報システム利用者・情報システム供給者間で合議、適切な権限者による承認を得ること。

D．情報システム供給者への要求事項

＜評価指標 V1＞ Q18： 利用者が具体的な要求事項(機能要件、非機能要件)を文書化することを支援することを実施管理しているか。 Q19： 具体的な実現性を考慮し、要求確認(機能要件、非機能要件)の文書を作成することを実施管理しているか。 a. 当該文書は要求事項に対するシステム方式設計の実現可能性について評価しているか。 b. 当該文書は要求事項に対する運用及び保守の実現可能性について評価しているか。 c. 当該文書は要求事項に対する実現・運用コストについて評価しているか。 d. 当該文書は要求事項に対して、利用者ニーズとの一貫性について評価しているか。 e. 当該文書は要求事項に対するテスト計画性について評価しているか。 f. 当該文書は要求事項と利用者の事業継続計画の整合性について評価しているか。 Q20： Q18, Q19内容を利用者と供給者が合意した上で、利用者の適切な権限者の承認を確認することを実施管理しているか。また、供給者の適切な権限者が承認することを実施管理しているか。 ＜評価指標V2＞ Q16： 利用者が具体的な要求事項(機能要件、非機能要件)を文書化することを支援しているか。あるいはその重要性を説明しているか。 Q17： 具体的な実現性を考慮し、要求確認(機能要件、非機能要件)の文書を作成しているか。 a. 当該文書は要求事項に対するシステム方式設計の実現可能性について評価しているか。 b. 当該文書は要求事項に対する運用及び保守の実現可能性について評価しているか。 c. 当該文書は要求事項に対する実現・運用コストについて評価しているか。 d. 当該文書は要求事項に対して、利用者ニーズとの一貫性について評価しているか。 e. 当該文書は要求事項に対するテスト計画性について評価しているか。 f. 当該文書は要求事項と利用者の事業継続計画の整合性について評価しているか。 Q18： Q16, Q17の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを確認しているか。また、供給者の適切な権限者が承認しているか。

情報システム供給者が取り組むべきことを述べる。

- 機能要件を要求事項として文書化することを支援すること。
- 要求事項のシステム方式設計・運用・保守の実現性、実現・運用コスト、情報システム利用ニーズとの一貫性、テスト計画性、情報システム利用者の事業継続計画との整合性の評価などを行

うこと。

・ 機能要件の丁寧な読み合わせを実施すること。
・ 情報システム利用者の隠された機能要件を引き出せるよう配慮すること。
・ 機能要件と実現・運用コストに見合った選択肢を提案し、明らかな過剰仕様がある場合、指摘すること。
・ 機能要件の多角的な検証によるシステム方式設計・運用・保守の実現性、実現・運用コスト、情報システム利用者ニーズとの一貫性、テスト計画性の確認を行うこと。
・ 文書化された要求事項を情報システム利用者・情報システム供給者間で合議し、適切な権限者による承認を得ること。

E．その他の留意事項

※IT コーディネータが注意すべきこと

情報システム利用者は機能要件の明確化の作業に着手すると情報システム開発の本来の目的を忘れて、近視眼的に目先の改善、操作性に深く入り込み、機能要件が肥大化していく傾向がある。

情報システム供給者は全体のスケジュール、費用を当初計画どおりに押さえ込むために機能要件を絞り込む傾向にある。IT コーディネータは両者の傾向をよく押さえた上で情報システム開発が経営戦略の実行であるという認識に立ち、情報システム開発の目的に合致しているか？経営戦略に合致しているか？を常に確認するようアドバイスをし、逸脱していることがあれば情報システム利用者が自ら気付くように支援する必要がある。

（４）非機能要件の実現に向けた利用者・供給者間での合意

Ａ．ガイドライン原文

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、ソフトウェアの品質に関する特性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―ドオフの関係にあり、高い水準の達成には相応のコスト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 で定められた品質に関する特性を参考に非機能要件を抽出し、文書化する。

Ｂ．本項目の必要性・重要性

情報システムは機能要件と非機能要件によって成り立っている。信頼性・安全性水準を達成するためには非機能要件が重要な役割を果たしている。

非機能要件の一例としてはコンピュータウィルスや不正アクセスなどのセキュリティ要件、ユーザ権限付与などのアクセス権限、災害時復旧のためのバックアップ要件、内部統制を実現するためのログ取得などの要件ある。これらの非機能要件が不十分な情報システムは情報システム利用者の誤った操作・運用や災害時などに基本的な機能要件を果たせない事態に陥る。従って機能要件を明確化、文書化するのと同等に非機能要件を明確化、文書化し情報システム利用者、情報システム供給者が合意をすることが重要となる。

Ｃ．情報システム利用者の実施事項

＜評価指標 U1＞

Q16： 具体的な要求事項(機能要件、非機能要件)を文書化することを実施管理しているか。

Q17： Q16 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを実施管理しているか。また、供給者の適切な権限者の承認を確認することを実施管理し

Q18： 要求事項及びその実現可能性のレビューは、事業継続計画及び、信頼性・安全性と実現・運用コストのトレードオフを考慮にいれて実施されているか。

a. 要求事項及びその実現可能性、実現・運用コスト等について、適切に合同レビューを実施しているか。

b. 合同レビューには運用部門、情報システム関係部門、経営者層等、必要な関係者が参加しているか。

c. 要求事項及びその実現可能性のレビューは、事業継続計画及び、信頼性・安全性と実現・運用コストのトレードオフを考慮にいれて実施されているか。

＜評価指標 U2＞

Q16： 具体的な要求事項(機能要件、非機能要件)を文書化しているか。

Q17： Q16 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認しているか。また、供給者の適切な権限者が承認していることを確認しているか。

Q18： 要求事項及びその実現可能性、実現・運用コスト等について、適切に合同レビューを実施し、すべての関係者の見解を統一しているか。

a. 要求事項及びその実現可能性、実現・運用コスト等について、適切に合同レビューを実施しているか。

b. 合同レビューには運用部門、情報システム関係部門、経営者層等、必要な関係者が参加して

いるか。
c. 要求事項及びその実現可能性のレビューは、事業継続計画及び、信頼性・安全性と実現・運用コストのトレードオフを考慮にいれて実施されているか。

情報システム利用者が取り組むべきことを述べる。

・ 非機能要件を具体的な要求事項として文書化すること。
・ 次のような非機能要件の間接的な提示を行うこと。
  ・システムの稼動がピークを迎えるタイミング・サイクル・アクセス量の提示
  ・事業継続計画の提示
  ・災害時に復旧すべき対象・復旧レベル・復旧に要する時間などの提示
・ 非機能要件の実現可能性、実現・運用コスト等を検討すること。
・ 非機能要件の運用部門、情報システム関係部門、経営者層等による合同レビューを行うこと。
・ 情報システム利用者・情報システム供給者間での合議および適切な権限者による承認を得ること。

D．情報システム供給者への要求事項

＜評価指標V1＞
Q18： 利用者が具体的な要求事項(機能要件、非機能要件)を文書化することを支援することを実施管理しているか。
Q19： 具体的な実現性を考慮し、要求確認(機能要件、非機能要件)の文書を作成することを実施管理しているか。
  a. 当該文書は要求事項に対するシステム方式設計の実現可能性について評価しているか。
  b. 当該文書は要求事項に対する運用及び保守の実現可能性について評価しているか。
  c. 当該文書は要求事項に対する実現・運用コストについて評価しているか。
  d. 当該文書は要求事項に対して、利用者ニーズとの一貫性について評価しているか。
  e. 当該文書は要求事項に対するテスト計画性について評価しているか。
  f. 当該文書は要求事項と利用者の事業継続計画の整合性について評価しているか。
Q20： Q18, Q19内容を利用者と供給者が合意した上で、利用者の適切な権限者の承認を確認することを実施管理しているか。また、供給者の適切な権限者が承認することを実施管理しているか。

＜評価指標V2＞
Q16： 利用者が具体的な要求事項(機能要件、非機能要件)を文書化することを支援しているか。あるいはその重要性を説明しているか。
Q17： 具体的な実現性を考慮し、要求確認(機能要件、非機能要件)の文書を作成しているか。
  a. 当該文書は要求事項に対するシステム方式設計の実現可能性について評価しているか。
  b. 当該文書は要求事項に対する運用及び保守の実現可能性について評価しているか。
  c. 当該文書は要求事項に対する実現・運用コストについて評価しているか。
  d. 当該文書は要求事項に対して、利用者ニーズとの一貫性について評価しているか。
  e. 当該文書は要求事項に対するテスト計画性について評価しているか。
  f. 当該文書は要求事項と利用者の事業継続計画の整合性について評価しているか。
Q18： Q16, Q17の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを確認しているか。また、供給者の適切な権限者が承認しているか。

情報システム供給者が取り組むべきことを述べる。

・非機能要件の文書化を支援すること。
・文書化支援のために処理性能、事業継続計画などの指標を提供すること。
・各種指標により間接的に提示された要求事項を要求確認書として文書化すること。
・非機能要件の実現性、実現・運用コスト、情報システム利用者ニーズとの一貫性、テスト計画性、情報システム利用者の事業継続計画との整合性を確認すること。

・情報システム利用者・情報システム供給者間で合議および適切な権限者による承認を得ること。

Ｅ．その他の留意事項

※IT コーディネータが注意すべきこと

ITコーディネータは情報システム利用者が非機能要件を適切かつ効率的に情報システム供給者に伝えることができるよう支援する必要がある。具体的には経営戦略策定によって既定した目標をモニタリング・ｺﾝﾄﾛｰﾙ項目としてSLM/SLAに落とし込みこれをもって非機能要件を明確化できるように支援する。情報システム供給者はSLM/SLAを実現するための要件を明確化することで非機能要件が明確かされ文書化を実現することが可能となる。

（５）利用者によるシステム要件に関する見解の統一

Ａ．ガイドライン原文

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。

Ｂ．本項目の必要性・重要性

情報システム開発において、そのシステム要件は特定の誰かが独善的に決定するわけではなく、情報システム利用者および運用部門、情報システム関連部門、経営層、情報システム供給者などが共同で決定すべきものである。その決定に至るプロセス・結果を情報システム利用企業の関係者全員が共有し、その総意として情報システム供給者に伝える必要がある。情報システム利用企業側の関係者の主張するシステム要件が統一されない場合は情報システム供給者が何を基準・根拠として情報システム開発を遂行していくべきかわからず、仮のシステム要件で情報システム開発を進めことが多々発生する。仮のシステム要件で進んだ情報システム開発が一定以上になると情報システム利用企業から明確な形でシステム要件が提示されてきて、開発の手戻りが発生することとなる。この場合には開発スケジュールの遅れ、費用の肥大化、信頼性・安全性水準の低下などのトラブルを招く恐れがある。

これらのトラブルを未然に防ぐ意味で情報システム利用者によるシステム要件に関する見解の統一が不可欠となる。

Ｃ．情報システム利用者の実施事項

＜評価指標 U1＞

Q16： 具体的な要求事項(機能要件、非機能要件)を文書化することを実施管理しているか。

Q17： Q16 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを実施管理しているか。また、供給者の適切な権限者の承認を確認することを実施管理し

Q18： 要求事項及びその実現可能性のレビューは、事業継続計画及び、信頼性・安全性と実現・運用コストのトレードオフを考慮にいれて実施されているか。

a. 要求事項及びその実現可能性、実現・運用コスト等について、適切に合同レビューを実施しているか。

b. 合同レビューには運用部門、情報システム関係部門、経営者層等、必要な関係者が参加しているか。

c. 要求事項及びその実現可能性のレビューは、事業継続計画及び、信頼性・安全性と実現・運用コストのトレードオフを考慮にいれて実施されているか。

＜評価指標 U2＞

Q16： 具体的な要求事項(機能要件、非機能要件)を文書化しているか。

Q17： Q16 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認しているか。また、供給者の適切な権限者が承認していることを確認しているか。

Q18： 要求事項及びその実現可能性、実現・運用コスト等について、適切に合同レビューを実施し、すべての関係者の見解を統一しているか。

a. 要求事項及びその実現可能性、実現・運用コスト等について、適切に合同レビューを実施しているか。

b. 合同レビューには運用部門、情報システム関係部門、経営者層等、必要な関係者が参加して

いるか。
c. 要求事項及びその実現可能性のレビューは、事業継続計画及び、信頼性・安全性と実現・運用コストのトレードオフを考慮にいれて実施されているか。

情報システム利用者が取り組むべきことを述べる。

・自社の企業風土、企業文化に立脚したシステム要件を経営者が承認ること。
・それを情報システム供給者へ提示すること。

D．情報システム供給者への要求事項

＜評価指標 V1＞
信頼性評価指標の該当記述なし。
＜評価指標 V2＞
信頼性評価指標の該当記述なし。

情報システム供給者が取り組むべきことを述べる。

・ 情報システム利用者から提示されたシステム要件が経営者により承認されたものとして扱うこと。
・ 情報システム利用者としての企業成熟度を見極め、システム要件に振れがでることを前提として情報システム開発を進めること。

（６）定量的見積りの実施

Ａ．ガイドライン原文

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（必要なソフトウェア、ハードウェア及び諸設備費用、要員、工数、工期、リスク等）とともに情報システム利用者に説明すること。

＜実施例＞

ファンクションポイント法等を活用した工数見積を実施し、価格の算出根拠の一つとする

Ｂ．本項目の必要性・重要性

情報システム利用者にとって、経営戦略に沿った情報システム導入と導入した情報システムの投資効果を測る上で客観的な尺度による見積値が必要である。情報システム供給者は、情報システム利用者が納得できる見積算出根拠と見積値を説明する必要がある。

特に、機能要件と非機能要件に基づいた見積とし算入項目とその実現レベルも明確化する必要がある。情報システム利用者と情報システム供給者とで、共通な指標（ファンクションポイント等）を介して見積内容での合意を行い、見積算出根拠や前提が変更となった場合には、プロジェクト計画やコストに影響がでることも合わせて合意する必要がある。見積時点での明確条件提示や合意を行うことにより、後日問題が発生することのないようにする必要がある。

Ｃ．情報システム利用者の実施事項

＜評価指標 U1＞
なし
＜評価指標 U2＞
なし

情報システム利用者は、情報システム供給者からの見積について、以下の点に注意して対応する必要がある。

- 機能要件と非機能要件を詳細かつ明確に伝えること。
- 情報システム利用者は RFP で提示した要件が網羅されているかをチェックし評価すること。
- ソフトウェアのコストと品質についての見積ノウハウを蓄積し、過去の事例（ベンチマーク）と比較するなどの評価を行うこと。
- 適正な評価方法として相見積を取る等して、公平に評価すること。

Ｄ．情報システム供給者への要求事項

＜評価指標 V1＞
Q21　情報システムの開発にかかる価格と根拠を情報システム利用者に説明することを実施管理しているか
Q22　必要なソフトウェア、ハードウェア及び設備費用、要員、工数、工期、リスク等を適切な見積手法を使って算出することを実施管理しているか
＜評価指標 V2＞
Q19　情報システムの開発にかかる価格と根拠を情報システム利用者に説明しているか
Q20　必要なソフトウェア、ハードウェア及び設備費用、要員、工数、工期、リスク等を適切な見積手法を使って算出しているか

情報システム利用者が取り組むべきことを述べる。

・ システム化要件をまとめて、必要な活動と成果物を見積ること。
・ 活動及び成果物は、そのシステム構成要素全体を見積り、当該プロジェクトの特性（工数に影響を及ぼす要因）を考慮して算定すること。
・ アプリケーションの開発の場合を例として、以下の手順で見積りを実施すること。

見積スコープの設定
見積根拠となる測定単位の設定
（画面数、データ項目数、プログラム行数、機能数、ドキュメントページ数）
規模の見積り（前項で設定した測定単位に基づく、対象規模の算出）
プロジェクトの特性に応じたぶれの取込み

E．その他の留意事項

※IT コーディネータが注意すべきこと
IT コーディネータはプロセスガイドラインを参照しつつ、その内容に照らし合わせて情報システム利用者と情報システム供給者が実施すべきことを実施しているかを確認する。

（7）情報システムの複雑化の回避

A．ガイドライン原文

情報システム供給者は、情報システムの大規模化及び複雑化を極力抑える設計を心掛けること。

＜実施例＞

標準に基づいた通信プロトコル、データフォーマットを採用する。

B．本項目の必要性・重要性

情報システムの大規模化と複雑化を抑えることにより、複雑なシステム運用や故障時の影響範囲の局所化や切り離し、機能のメンテナンス性向上を図ることができる。

情報システム供給者はその点について配慮した設計を心掛けるべきである。

そのために情報システム供給者は、情報システム内の各業務システムについて、標準的なアーキテクチャーを採用することとし、特殊な仕組みは採用しないようにするべきである。特に、システム間の連携やデータ交換が発生する場合、標準仕様による実装を心掛けるべきである。

C．情報システム利用者の実施事項

＜評価指標 U1＞
なし
＜評価指標 U2＞
なし

情報システム利用者が取り組むべきことを述べる。

- 情報システムの利便性を追求するあまり、機能要件を際限なく増大させることのないよう、配慮すること。
- 例えば、例外事項の網羅性について一定の基準で歯止めをかけるなど、情報システムでカバーできる範囲と人間系でカバーする範囲とを業務フローなどをベースに見極めること。
- 情報システムでカバーする範囲を絞り込むことで情報システムの複雑化・大規模化を抑えるように配慮すること。

D．情報システム供給者の実施事項

＜評価指標 V1＞
Q23　情報システムの大規模化及び複雑化を極力抑える設計とすることを実施管理しているか
＜評価指標 V2＞
Q21　情報システムの大規模化及び複雑化を極力抑える設計としているか

情報システム利用者が取り組むべきことを述べる。

- 情報システム化の要件全てを網羅できるよう努めること。
- 適正な費用・保守性・拡張性・安全性等の観点から複数の方式案を準備し、情報システムの利用者が選択できる形式をとること。
- 障害による影響を少なくし保守の容易性を重要視することで、システムの信頼性・安全性を高めるようシンプルな情報システムとなるよう設計時点で配慮すること。

E．その他の留意事項

Ｅ．１　情報技術に関する留意事項

情報システム供給者が留意する点として、「Ⅳ．技術に関する事項」「２.信頼性・安全性向上にむけた技術の活用及び留意事項」を参照する。

※IT コーディネータが注意すべきこと

IT コーディネータはプロセスガイドラインを参照しつつ、その内容に照らし合わせて情報システム利用者と情報システム供給者が実施すべきことを実施しているかを確認する。

（８）情報システムの障害対応能力の向上

Ａ．ガイドライン原文

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り、フェイルセーフ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二重化・多重化を設計に織り込む。

Ｂ．本項目の必要性・重要性

企業内外の業務が情報システム上で実現されるようになった結果、情報システムが止まると業務が停滞することとなる。社会インフラを支える部分の情報システムの場合、ネットワークを含む情報システムのダウンは社会的な影響を及ぼすこととなる。そのため、システム開発の品質向上はもとより、障害発生を抑え込む措置を行うとともに万一障害が発生した場合は、その影響範囲を極力おさえられるようにサーバ機の２重化や設置場所を別地域に分散配置するなどを検討する必要がある。

Ｃ．情報システム利用者の実施事項

＜評価指標 U1＞ Q19　フェイルセーフ（システムが何らかの事情でトラブルを発生した場合にもシステム障害の影響を最小限に食い止めるという視点から、システムを安全側に帰着させるという考え方）のメカニズムを検討することを実施管理しているか ＜評価指標 U2＞ Q19　フェイルセーフ（システムが何らかの事情でトラブルを発生した場合にもシステム障害の影響を最小限に食い止めるという視点から、システムを安全側に帰着させるという考え方）のメカニズムを検討しているか

情報システム利用者が取り組むべきことを述べる。

- 情報システムが正常に稼動し続けることが必要であるが、万が一障害による停止が発生した場合の復旧時間や、復旧させる業務機能の優先順位付け・障害箇所の切り分け等を準備しておくこと。
- システム障害の影響を最小限に食い止める視点から、システムを安全に帰着させる設計となっているかを確認すること。
- 設計時点で、発生し得るリスクを洗い出し、復旧時間やシステム停止の許容範囲も含めて要件を代替手段も含めて纏めておくこと。

Ｄ．情報システム供給者への要求事項

＜評価指標 V1＞ Q24　利用者がフェイルセーフ（システムが何らかの事情でトラブルを発生した場合にもシステム障害の影響を最小限に食い止めるという視点から、システムを安全側に帰着させるという考え方）のメカニズムを検討することを支援することを実施管理しているか。 ＜評価指標 V2＞ Q22　利用者がフェイルセーフ（システムが何らかの事情でトラブルを発生した場合にもシステム障害の影響を最小限に食い止めるという視点から、システムを安全側に帰着させるという考え方）のメカニズムを検討することを支援しているか。あるいはその重要性を説明しているか。

情報システム供給者が取り組むべきことを述べる。

・設計時点で想定し得る障害について、障害発生時の発生箇所の切り離しによる縮退運用や、システム装置の系切替によるシステム運用継続の検討をシステム要件として検討すること。

・日常のデータバックアップ方式や障害からの復旧方式、障害発生時にシステム管理者への通報の方法や、障害時の対応方法などもルール化しておき、業務への影響を最小とするようにシステム設計やシステム運用設計に織り込むこと。

・上記システム要件については、情報システムが対象とする業務の重要性や扱うデータのリアルタイム性等を考慮し、業務要件にあったシステム形態を情報システム利用者へ提供すること。

Ｅ．その他の留意事項

Ｅ．１　障害対応に関する留意事項

障害発生時の対応については、「４．障害対応に関する留意事項」を参照する。

※IT コーディネータが注意すべきこと

IT コーディネータはプロセスガイドラインを参照しつつ、その内容に照らし合わせて情報システム利用者と情報システム供給者が実施すべきことを実施しているかを確認する。

（9）誤操作等防止への配慮

A．ガイドライン原文

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ース等の設計に当り、フールプルーフの観点から、誤操作等の防止に努めること。

＜実施例＞

画面設計において、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。

B．本項目の必要性・重要性

データ入力にあたり、金額等の不正な数値が登録されることや操作ミスによるデータ破壊等、情報システム利用者の意図しないミスから情報システムならびに企業を防御する必要がある。

情報システムとしては、データを直接操作する際の画面等のユーザインタフェース機能で、直感的な操作が可能な画面配置とするなど正確な情報入力を保証できる仕組みを実現する必要がある。

C．情報システム利用者の実施事項

＜評価指標 U1＞

Q20　フールプルーフ（システム利用者が誤った操作などをした場合にも、直接的なシステム障害にならないようにする、あるいは系としての安全性を保持するようにする考え方）を検討することを実施管理しているか。

Q21　システム利用者の視点に立ったユーザビリティ（利用者の使い勝手）を検　討することを実施管理しているか。

＜評価指標 U2＞

Q20　フールプルーフ（システム利用者が誤った操作などをした場合にも、直接的なシステム障害にならないようにする、あるいは系としての安全性を保持するようにする考え方）を検討しているか。

Q21　システム利用者の視点に立ったユーザビリティ（利用者の使い勝手）を検討しているか。

情報システム利用者が取り組むべきことを述べる。

- システムに利用者が誤った操作などをした場合に、直接的なシステム障害にならないようにすること。
- 或いは系としての安全性を保持するような設計となっているか確認すること。
- 情報システム利用者が、実際の業務で使用する上での使い勝手が考慮されているかを、事前検証するなどの対応を行うこと。

D．情報システム供給者への要求事項

＜評価指標 V1＞

Q25　利用者がフールプルーフ(システム利用者が誤った操作などをした場合にも直接的なシステム障害にならないようにする、あるいは系としての安全性を保持するようにする考え方）のメカニズムを検討することを支援することを実施管理しているか。

Q26　システム利用者の視点に立ったユーザビリティ（利用者の使い勝手）を検討することを支援することを実施管理しているか。

＜評価指標 V2＞

Q23　利用者がフールプルーフ(システム利用者が誤った操作などをした場合にも直接的なシステム障害にならないようにする、あるいは系としての安全性を保持するようにする考え方）のメカニズムを検討することを支援しているか。あるいはその重要性を説明しているか。

Q24　システム利用者の視点に立ったユーザビリティ（利用者の使い勝手）を検討することを支援しているか。あるいはその重要性を説明しているか。

情報システム供給者が取り組むべきことを述べる。

・情報システム利用者が操作ミスを起こさないような画面設計や、操作ミスをした場合のメッセージ表示による正しい操作へのガイダンスを行うなど、利用者側に立った操作性を確保するように配慮すること。
・データを入力する際のチェック機能を付加することにより、不正なデータが情報システムに登録されないような機能とすること。

E．その他の留意事項

※IT コーディネータが注意すべきこと
IT コーディネータはプロセスガイドラインを参照しつつ、その内容に照らし合わせて情報システム利用者と情報システム供給者が実施すべきことを実施しているかを確認する。

（１０）テスト及びレビューの徹底

Ａ．ガイドライン原文

情報システム供給者は、情報システム利用者との協力の下、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テスト及びレビューを行い、当該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利用可能性の確認に向け、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。

Ｂ．本項目の必要性・重要性

情報システムの機能要件及び非機能要件及び実現機能について、情報システム利用者と供給者とでレビューを行い漏れがないかを相互に確認する必要がある。

また、テスト方法・テスト項目・テストデータ、発見不具合の目標等を事前に検討・レビューしその妥当性を相互に確認する必要がある、またテスト結果、発見不具合についてもその内容と対策が妥当であるかをレビューで情報システム利用者と供給者とで相互に確認する。情報システム供給者任せとならないように、情報システム利用者もレビューで現物確認を行うべきである。

Ｃ．情報システム利用者の実施事項

＜評価指標 U1＞
なし
＜評価指標 U2＞
Q22　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テスト及びレビューを実施しているか。
Q23　Q22 により、当該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をおこなっているか。
Q24　実環境に近い適切な環境でテストを実施しているか。
a.　テスト項目には確認すべきユーザ要求事項をテストする項目が全て含まれている
b.　確認すべきユーザ要求事項をテストする環境を定義しているか
c.　実環境における利用可能性の確認に向け、供給者に協力してテスト及び試行等を実施しているか
d.　ユーザ受入テストは実務に精通したユーザが参画しているか。
e.　ユーザ受入テストは本番運用を想定してテストケースを設定しているか。

情報システム利用者が取り組むべきことを述べる。

・情報システムの機能要件及び非機能要件についての適合性確認や信頼性・安全性の水準に応じたテスト及びレビューを行い結果の承認を行うこと。
特に業務機能については、上流工程での品質確保の関連からもレビューによる品質作りこみを行うこと。
・本番環境でテストを実施するための計画策定と本番環境での確認項目を策定するおこと。
・性能要件を設計段階で明確にし、性能要件を満たしているかを確認する項目がテスト計画に盛り込まれているかを確認すること。

Ｄ．情報システム供給者への要求事項

＜評価指標 V1＞
Q27　適切なテストが行われることを実施管理しているか。
a.　安全性、信頼性の水準に応じたテスト工程を規定しているか
b.　安全性、信頼性の水準に応じた適切なテスト項目が設計されているか

c. テスト項目に対して、適切なレビューを行っているか
d. テスト結果を適切に確認しているか
Q26 適切なレビューが行われることを実施管理しているか。
a. 安全性、信頼性の水準に応じたレビュー工程を規定しているか
b. 安全性、信頼性の水準に応じた適切なレビュー項目が設計されているか
c. レビュー方法に対して適切な評価を行っているか
Q27 情報システム利用者の協力の下、実環境に近い適切な環境でテストが行われることを実施管理しているか。
a. テスト項目には確認すべきユーザ要求事項をテストする項目が全て含まれている
b. 確認すべきユーザ要求事項をテストする環境を定義しているか
c. 実環境における利用可能性の確認に向け、情報システム利用者に対してテスト及び試行等の協力を依頼しているか。
＜評価指標 V2＞
Q25 適切なテストを実施しているか。
a. 安全性、信頼性の水準に応じたテスト工程を規定しているか
b. 安全性、信頼性の水準に応じた適切なテスト項目が設計されているか
c. テスト項目に対して、適切なレビューを行っているか
d. テスト結果を適切に確認しているか
Q26 適切なレビューを実施しているか。
a. 安全性、信頼性の水準に応じたレビュー工程を規定しているか
b. 安全性、信頼性の水準に応じた適切なレビュー項目が設計されているか
c. レビュー方法に対して適切な評価を行っているか
Q27 情報システム利用者の協力の下、実環境に近い適切な環境でテストを行っているか。
a. テスト項目には確認すべきユーザ要求事項をテストする項目が全て含まれている
b. 確認すべきユーザ要求事項をテストする環境を定義しているか
c. 実環境における利用可能性の確認に向け、情報システム利用者に対してテスト及び試行等の協力を依頼しているか。

情報システム供給者が取り組むべきことを述べる。

・テスト計画について、顧客とのレビュー議事録などがあり、承認印を貰うなどして合意（承認）を情報システム利用者から得るようにすること。
・テスト計画の策定では、テスト実施に必要な環境（テスト機、本番環境、テストデータ、ドライバ等のテスト用プログラムなど）の準備を行い、必要があれば情報システム利用者にも協力をお願いする等、漏れのないようにすること。
・テストの実施結果についても、レビューを通じて情報システム供給者と利用者双方で結果検証を行うなど、実施方法・体制なども計画時点で明確にすること。

E．その他の留意事項

※IT コーディネータが注意すべきこと
IT コーディネータはプロセスガイドラインを参照しつつ、その内容に照らし合わせて情報システム利用者と情報システム供給者が実施すべきことを実施しているかを確認する。

（１１）検収基準の明確化

Ａ．ガイドライン原文

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を行い積極的に支援すること。

＜実施例＞

検収基準として、「ピーク時の応答時間５秒以内」及び「データ破損時の復旧時間１時間以内」等、評価及び判断可能な目標値を設定する。

Ｂ．本項目の必要性・重要性

情報システムへの機能要件についての約束事項を数値化・指標化することにより、情報システム利用者・供給者が相互に同一の目標値を設定してその達成度を測ることで検収条件とすることができる。またその条件を文書化して情報システム利用者と供給者とで、契約時点で合意をしておくことが重要である。

Ｃ．情報システム利用者の実施事項

＜評価指標 U1＞
Q25　定量的な検収基準を明確にし、文書化することを実施管理しているか。
Q26　Q25 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを実施管理しているか。
＜評価指標 U2＞
Q25　定量的な検収基準を明確にし、文書化しているか。
Q26　Q25 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認している

情報システム利用者が取り組むべきことを述べる。

・定量的な検収基準を明確・文書化し、情報システム供給者と合意すること。

・利用者側での適切な権限者が承認すること。

Ｄ．情報システム供給者への要求事項

＜評価指標 V1＞
Q30　利用者が定量的な検収基準を明確にし、文書化することを支援することを実施管理しているか。
Q31　Q28 の内容を利用者と供給者が合意した上で、利用者の適切な権限者の　承認を確認することを実施管理しているか。
＜評価指標 V2＞
Q28　利用者が定量的な検収基準を明確にし、文書化することを支援しているか。
Q29　Q28 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が　承認することを確認しているか。

情報システム供給者が取り組むべきことを述べる。

・ 情報システム利用者から提示された検収基準について、利用者側と情報技術等の観点から実現可能な条件かを検討し、利用者側と合意すること。

Ｅ．その他の留意事項

※ITC が注意すべきこと

ITC はプロセスガイドラインを参照しつつ、その内容に照らし合わせて情報システム利用者と情報システム供給者が実施すべきことを実施しているかを確認する。

３．保守・運用段階における留意事項

Ａ．ガイドライン原文

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、共同して適切な保守・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。

Ｂ．本項目の必要性・重要性

情報システムは国民の生命の安全や社会経済活動に大きな影響を与えるものから、一般企業の社内業務で利用されるもの、さまざまな機器に実装される組込みシステムなど、社会の隅々まで入り込んでいる。

これらの情報システムはその重要性が様々であるが、いまや情報システムが関与しない活動はほとんどないといっても過言ではなく、それぞれの情報システムはその目的に応じて信頼性・安全性水準が明確に定められているべきである。

そのため、情報システム利用者に対するサービス提供水準を、定めた信頼性・安全性水準以上に維持できるよう、障害時の影響や損害等を最小化するための保守・運用業務を明確に定義し、適切に実施できるようにしておくことが重要である。

上記により、単にサービス提供を継続するだけでなく、サービス品質の向上と長期的な観点からのコスト削減といったことを実現することにつなげることができる。

（１）保守･運用に関する体制等の利用者･供給者間での合意

A. ガイドライン原文

情報システム利用者及び情報システム供給者は、保守・運用に係る活動全般について、双方の推進体制（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文書化し、両者で合意すること。

＜実施例＞

運用保守体制図及び運用フロー図を作成し、合意する。

Ｂ．本項目の必要性・重要性

保守運用全般に渡り、その推進体制と業務フローを明確にしておくことは、情報システムが企業活動の中で重要な位置付けを占めている状況においては、きわめて重要である。なぜならば、情報システムが停止することにより、企業活動そのものが停止に陥り、結果的に大きな損失の発生やその企業の社会的信頼の失墜につながるからである。

したがって、情報システムによるサービス提供が継続的・安定的に行えるように、その適切な維持管理だけでなく、障害発生時における迅速な復旧をはかることを可能とする推進体制と業務フローを定め、関係者が十分習熟しておくことは必須事項と言える。

また、このようなことが個々の情報システムすべてについて均一的に行われていることが重要であり、全体として一定の水準を維持できていなければならない。

上記を実現する上では、情報システムに対する運用面からの要件をあらかじめ明確にしておき、シンプルな体制で負荷の少ない通常のシステム運用業務が実施できるようにするとともに、障害発生時における運用面での対応も考慮しておくことが重要である。保守運用の推進体制と業務フローについては、システム設計と並行した運用設計を進め、開発終了の時点で整備が完了していることが必要である。

C. 情報システム利用者の実施事項

＜評価指標 U1／U2＞

Q27　事業継続計画に基づいた情報システム障害発生時の対応手順・マニュアルを元に、適切な教育訓練を行うことを実施管理しているか。／教育訓練が実施されているか。

Q28　保守・運用に係る活動全般について、利用者・供給者それぞれの推進体制及び承認手順を含む業務フロー等を文書化することを実施管理しているか。／文書化しているか。

a. 組織で実施されている保守運用の全ての工程（作業プロセス）に対応した推進体制を文書化しているか。

b. 組織で実施されている保守運用の全ての工程（作業プロセス）に対応した業務フローを文書化しているか。

ただし、業務フローの中には、信頼性・安全性などを意識した作業が含まれなくてはいけない。

Q29　不具合や保守の重要性を段階的に定め、それぞれのランクに応じた対応内容を文書化することを実施管理しているか。／文書化しているか。

a. 保守の種類（是正保守、予防保守、適用保守、完全化保守）に応じた対応が文書化されているか。

b. 保守の量（修正量、修正費用、修正時間）に応じた対応が文書化されているか。

c. 保守の重大性（性能、安全性、セキュリティ、影響範囲等）に応じた対応が文書化されているか。

Q30　リリースに際して、特にリリース手順及び問題発生時の緊急対応等のマニュアル化、現場への徹底及び適切なテストを実施管理しているか。／テストを実施しているか。

a. リリース手順及び問題発生時の対応手順・マニュアルが作成されているか。

b. a の対応手順・マニュアルを基に適切な教育訓練が実施されているか。

Q31　構成管理及び変更管理について手順等（ツールを含む）を確立しているか。

Q32　Q28,Q29,Q30,Q31 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認しているか。また、供給者の適切な権限者が承認していることを確認することを実施管理しているか。／確認しているか。

情報システム利用者は、自らの実施事項として以下の事項を実施する必要があることを認識すべきである。

・ 保守・運用に係る情報システム利用者及び供給者の実施する業務内容と、それらの相互関係を理解すること。
・ 情報システム供給者が実施する保守・運用業務範囲の認知と文書化を行うこと。
・ 情報システム利用者と情報システム供給者内の保守・運用組織体制、作業の役割分担、責任者の明確化、責任範囲の理解と文書化を行うこと。
・ 保守・運用業務の業務フロー及び業務遂行上必要となる書式等の文書化を行うこと。
・ 情報システム利用者が承認すべき事項の明確化と承認手続き、書式の文書化を行うこと。
・ 情報システム供給者との間でのコミュニケーションルールの文書化、窓口とツールの明確化を行うこと。
・ 文書化されていない保守・運用作業の発生時における対応方法を明文化すること。
・ 情報システム供給者との合意事項を承認すること。
・ 上記各事項についての実施管理すること。

D. 情報システム供給者への要求事項

＜評価指標 V1／V2＞

Q32　利用者が保守・運用に係る活動全般について、利用者・供給者それぞれの推進体制及び承認手順を含む業務フロー等を文書化することを支援することを実施管理しているか。／Q30　支援しているか。あるいはその重要性を説明しているか。

a.　組織で実施されている保守運用の全ての工程（作業プロセス）に対応した推進体制を文書化しているか。

b.　組織で実施されている保守運用の全ての工程（作業プロセス）に対応した業務フローを文書化しているか。

ただし、業務フローの中には、信頼性・安全性などを意識した作業が含まれなくてはいけない。

Q33　利用者が不具合や保守の重要性を段階的に定め、それぞれのランクに応じた対応内容を文書化することを支援することを実施管理しているか。／Q31　支援しているか。あるいはその重要性を説明しているか。

a.　保守の種類（是正保守、予防保守、適用保守、完全化保守）に応じた対応が文書化されているか。

b.　保守の量（修正量、修正費用、修正時間）に応じた対応が文書化されているか。

c.　保守の重大性（性能、安全性、セキュリティ、影響範囲等）に応じた対応が文書化されているか。

Q34　リリースに際して、特にリリース手順及び問題発生時の緊急対応等のマニュアル化、現場への徹底及び適切なテストを実施することを支援することを実施管理しているか。／Q32　支援しているか。あるいはその重要性を説明しているか。

a.　適切なテストを行った上、リリース手順及び問題発生時の対応手順・マニュアルが作成されているか。

b.　a の対応手順・マニュアルを基に適切な教育訓練が実施されているか。

Q35　利用者が構成管理及び変更管理について手順等（ツールを含む）を確立することを支援することを実施管理しているか。／Q33　支援しているか。あるいはその重要性を説明しているか。。

Q36　Q32,Q33,Q34,Q35 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを実施管理しているか。また、供給者の適切な権限者が承認することを実施管理しているか。／Q34　Q30,Q31,Q32,Q33 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを確認しているか。また、供給者の適切な権限者が承認しているか。

情報システム供給者は、自らの実施事項として以下の事項を実施する必要があることを認識すべきである。

・保守・運用に係る情報システム利用者及び供給者の実施する業務内容とそれらの相互関係についての情報システム利用者へ説明すること。

・以下の点についての情報システム利用者に対する説明と合意内容の文書化、情報システム利用者承認を受領すること。

情報システム供給者が実施する保守・運用業務範囲

情報システム利用者と情報システム供給者内の保守・運用組織体制、作業の役割分担、責任者の明確化と責任範囲

保守・運用業務の業務フロー及び業務遂行上必要となる書式等

情報システム利用者が承認すべき事項の明確化と承認手続き、書式

情報システム供給者との間でのコミュニケーションルール、窓口とツール

グレーゾーン作業発生時における対応方法

・上記各事項について実施管理すること。

E. その他の留意事項

※IT コーディネータが注意すべきこと

・情報システム利用者に対して、ITIL などのベストプラクティスを紹介するなど、情報システム利用者が保守・運用業

務に関する理解を深めることができるような情報提供を行う。
・情報システム利用者に対して、情報システム利用者の実施事項について適切な保守・運用体制とその業務プロセスの仕組み作りが適切に実施されるように必要な助言または支援を行う。
・情報システム利用者の実施事項が保守・運用体制に基づき適切に実施されているか、組織的にその実施管理が行われているかをモニタリングし、問題点・改善点があれば経営者に対して助言または支援を行う。

（2）企画・開発・保守・運用の全体を通じたリスク管理

A．ガイドライン原文

情報システムに対する要求仕様については、企画・開発の段階で合意されたものが保守・運用段階において変化していく可能性があるため、情報システム利用者と情報システム供給者は協力し、業務をとりまく環境の変化及び技術的問題（機能、性能、容量、拡張等）等に関するリスク管理を恒常的に実施し、必要に応じて対応策をとること。

＜実施例＞

リスクマネジメントのためのチェックリストを作成し、リスクレビュー会議等で定期的にチェックを行う。

B．本項目の必要性・重要性

企画・開発段階から保守・運用を考慮した要求仕様を作成することは、保守・運用を効率的・効果的に実施するうえで極めて重要なことである。しかしながら、実際に保守・運用を開始して初めて明らかになる事項があったり、保守・運用体制の変更等によって当初仕様では対応しきれなくなったりすることがある。また、時間の経過に伴うシステム規模の拡大や機器等の劣化、セキュリティ上の脅威の発生等も見込まれる。更に、ビジネスそのものが変化することにより、情報システムに対する要求も変化していくことも想定できる。

従って、様々な観点から情報システムに関わるリスク分析とその見直しを行い、監視対象とすべきリスクを明確にした上で、そのモニタリングを実施していくことが必要である。

例えば、保守・運用にとって必要な機能の不足や改善事項の有無、体制変更に対応した機能追加や変更の必要性の有無、データ量や利用者数の増加などによる性能劣化や容量不足によるサービスレベルの低下の有無や予測、セキュリティ上の脆弱性評価など、定期的なチェックを定性的・定量的両面から行い、コスト増加や障害発生の未然防止を図り、信頼性・安全性を維持し続けることが重要である。

C．情報システム利用者の実施事項

＜評価指標 U1／U2＞

Q33　業務を取り巻く環境の変化及び技術的問題（機能、性能、容量、拡張等）等に関するリスク管理を恒常的に実施することを実施管理しているか。／実施しているか。

a.　リスクを特定しているか。

b.　リスクの分析をしているか。

c.　リスクの対応計画を立てているか。

Q34　情報システムの運用状況に関するデータを取得し監視を行い、また必要に応じてしかるべき対応を行うことを実施管理しているか。／対応を行っているか。

情報システム利用者は、自らの実施事項として以下の事項を実施する必要があることを認識すべきである。

・リスク管理の必要性の理解、及び認識すべきリスク項目を認知すること。
・リスク項目の監視方法を文書化すること。
・リスクの顕在化による影響度を文書化すること。
・リスクの防止・抑制対策、リスクが顕在化した場合の対応方法を文書化すること。
・上記に基づくリスク管理を実施すること。
・上記各事項についての実施管理を行うこと。

D．情報システム供給者への要求事項

＜評価指標 V1／V2＞
Q37　利用者が業務を取り巻く環境の変化及び技術的問題（機能、性能、容量、拡張等）等に関するリスク管理を恒常的に実施することを実施管理しているか。／Q35　支援しているか。あるいはその重要性を説明しているか。
a.　リスクを特定しているか。
b.　リスクの分析をしているか。
c.　リスクの対応計画を立てているか。
Q38　利用者が情報システムの運用状況に関するデータを取得し監視を行い、また必要に応じてしかるべき対応を行うことを支援することを実施管理しているか。／Q36　支援しているか。あるいはその重要性を説明しているか。

情報システム供給者は、自らの実施事項として以下の事項を実施する必要があることを認識すべきである。

・リスク管理の必要性、及び認識すべきリスク項目の情報システム利用者へ説明すること。
・以下の点についての情報システム利用者に対する説明と合意内容の文書化、情報システム利用者承認を受領すること。
　リスク項目の監視方法
　リスクの顕在化による影響度評価
　リスクの防止・抑制対策、リスクが顕在化した場合の対応方法
・情報システム利用者のリスク管理の支援を行うこと。
・上記各事項についての実施管理を行うこと。

E．その他の留意事項

※IT コーディネータが注意すべきこと
・情報システム利用者に対して、情報システム利用者がリスク管理に関する理解を深めることができるような情報提供を行う。
・情報システム利用者に対して、情報システム利用者の実施事項について初期の枠組み作りが適切に実施されるように必要な助言または支援を行う。
・情報システム利用者の実施事項が保守・運用体制に基づき適切に実施されているか、組織的にその実施管理が行われているかをモニタリングし、問題点・改善点があれば経営者に対して助言または支援を行う。

（3）保守・不具合の取扱方針の利用者・供給者間での合意

A．ガイドライン原文

情報システム利用者と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、それぞれについて両者で合意すること。

＜実施例＞

不具合や保守の重要性を段階的に定め、それぞれのランクに応じた対応内容を文書化しておく。

B．本項目の必要性・重要性

情報システムは当初から完璧なものはあり得ず、必ずソフトウェア不具合等が潜在的にあると考えるべきである。これらは、インシデントとして適切に管理／解決／復旧が行われる必要があるとともに、その根本原因が対処されなければならないが、こういった、「本来あるべき状態とは異なる状態のものを是正する」という訂正に係る保守と、「時間の経過とともに当初の要件が現実に合わなくなってくることに対応する」ための改良に係る保守は原則としてその責任所在もまったく異なるものである。

従って、情報システム利用者は、これらの保守は明確にその責任所在の違いとそれに伴う取り扱い方の違いがあることを認識し、両者の関係を良好に維持し続けるためにもそれぞれの取り扱い方について情報システム供給者と合意する必要がある。また、どのような保守がそれぞれに該当するのかといった判断基準についても明確にすることが重要である。

一方、あらゆる不具合事象や保守対象事象について、すべて保守作業を実施する必要はなく、最低限の保守・運用コストにより適切な信頼性・安全性水準を維持するうえでは、費用対効果において実施可否を判断することが重要である。具体的に、どのような事象のときにどのような保守作業をどの程度実施するかを明確に基準として定めることで、スムーズな保守対応判断とその実施を実現することが可能となる。

その結果として、最適なサービスの維持と長期的なコスト削減が実現できる。

なお、瑕疵期間経過後においては、通常は訂正に係る保守であっても契約上は改良に係る保守として扱われるべきであるが、組織体の成熟度レベルにより、情報システムの保守に対する認識には違いがでることが多く、前述の判断基準の合意等が重要となってくる。

C．情報システム利用者の実施事項

＜評価指標 U1／U2＞

Q27　事業継続計画に基づいた情報システム障害発生時の対応手順・マニュアルを元に、適切な教育訓練を行うことを実施管理しているか。／教育訓練が実施されているか。

Q28　保守・運用に係る活動全般について、利用者・供給者それぞれの推進体制及び承認手順を含む業務フロー等を文書化することを実施管理しているか。／文書化しているか。

a.　組織で実施されている保守運用の全ての工程（作業プロセス）に対応した推進体制を文書化しているか。

b.　組織で実施されている保守運用の全ての工程（作業プロセス）に対応した業務フローを文書化しているか。
ただし、業務フローの中には、信頼性・安全性などを意識した作業が含まれなくてはいけない。

Q29　不具合や保守の重要性を段階的に定め、それぞれのランクに応じた対応内容を文書化することを実施管理しているか。／文書化しているか。

a.　保守の種類（是正保守、予防保守、適用保守、完全化保守）に応じた対応が文書化されているか。

b. 保守の量（修正量、修正費用、修正時間）に応じた対応が文書化されているか。
c. 保守の重大性（性能、安全性、セキュリティ、影響範囲等）に応じた対応が文書化されているか。
Q30 リリースに際して、特にリリース手順及び問題発生時の緊急対応等のマニュアル化、現場への徹底及び適切なテストを実施管理しているか。／テストを実施しているか。
a. リリース手順及び問題発生時の対応手順・マニュアルが作成されているか。
b. a の対応手順・マニュアルを基に適切な教育訓練が実施されているか。
Q31 構成管理及び変更管理について手順等（ツールを含む）を確立しているか。
Q32 Q28,Q29,Q30,Q31 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認しているか。また、供給者の適切な権限者が承認していることを確認することを実施管理しているか。／確認しているか。

情報システム利用者は、自らの実施事項として以下の事項を実施する必要があることを認識すべきである。

・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）を理解すること。
・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）の判断基準と取り扱い方法を文書化すること。
・情報システム供給者が実施する保守業務の責任範囲を理解し文書化すること。
・情報システム供給者の保守業務の組織体制、作業の役割分担を理解し文書化すること。
・保守業務の業務フロー及び業務遂行上必要となる書式等を文書化すること。
・情報システム利用者が承認すべき事項の明確化と承認手続き、書式を文書化すること。
・情報システム供給者との合意事項を承認すること。
・情報システム供給者に対する保守対象情報の提供依頼、判断基準に基づく保守作業実施の可否判断を行うこと。
・上記各事項についての実施管理を行うこと。

D. 情報システム供給者への要求事項

＜評価指標 V1／V2＞
Q32 利用者が保守・運用に係る活動全般について、利用者・供給者それぞれの推進体制及び承認手順を含む業務フロー等を文書化することを支援することを実施管理しているか。／Q30　支援しているか。あるいはその重要性を説明しているか。
a. 組織で実施されている保守運用の全ての工程（作業プロセス）に対応した推進体制を文書化しているか。
b. 組織で実施されている保守運用の全ての工程（作業プロセス）に対応した業務フローを文書化しているか。
ただし、業務フローの中には、信頼性・安全性などを意識した作業が含まれなくてはいけない。
Q33 利用者が不具合や保守の重要性を段階的に定め、それぞれのランクに応じた対応内容を文書化することを支援することを実施管理しているか。／Q31　支援しているか。あるいはその重要性を説明しているか。
a. 保守の種類（是正保守、予防保守、適用保守、完全化保守）に応じた対応が文書化されているか。
b. 保守の量（修正量、修正費用、修正時間）に応じた対応が文書化されているか。
c. 保守の重大性（性能、安全性、セキュリティ、影響範囲等）に応じた対応が文書化されているか。
Q34 リリースに際して、特にリリース手順及び問題発生時の緊急対応等のマニュアル化、現場への徹底及び適切なテストを実施することを支援することを実施管理しているか。／Q32　支援しているか。あるいはその重要性を説明しているか。
a. 適切なテストを行った上、リリース手順及び問題発生時の対応手順・マニュアルが作成されているか。
b. a の対応手順・マニュアルを基に適切な教育訓練が実施されているか。
Q35 利用者が構成管理及び変更管理について手順等（ツールを含む）を確立することを支援することを

実施管理しているか。／Q33　支援しているか。あるいはその重要性を説明しているか。 Q36 Q32,Q33,Q34,Q35 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを実施管理しているか。また、供給者の適切な権限者が承認することを実施管理しているか。／Q34 Q30,Q31,Q32,Q33 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを確認しているか。また、供給者の適切な権限者が承認しているか。

情報システム供給者は、自らの実施事項として以下の事項を実施する必要があることを認識すべきである。

・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）の情報システム利用者へ説明すること。

・以下の点についての情報システム利用者に対する説明と合意内容の文書化、情報システム利用者の承認を受領すること。

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）の判断基準と取り扱い方法

情報システム供給者が実施する保守業務の責任範囲の理解と文書化

情報システム供給者の保守業務の組織体制、作業の役割分担の理解と文書化

保守業務の業務フロー及び業務遂行上必要となる書式等の文書化

情報システム利用者が承認すべき事項の明確化と承認手続き、書式の文書化

・情報システム利用者に対する保守対象情報の提供、保守作業実施判断に基づく保守作業を実施すること。

・上記各事項についての実施管理を行うこと。

E．その他の留意事項

※IT コーディネータが注意すべきこと

・情報システム利用者に対して、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）についての理解を深めることができるような情報提供を行う。

・情報システム利用者に対して、情報システム利用者の実施事項について初期の枠組み作りが適切に実施されるように必要な助言または支援を行う。

・情報システム利用者の実施事項が保守・運用体制に基づき適切に実施されているか、組織的にその実施管理が行われているかをモニタリングし、問題点・改善点があれば経営者に対して助言または支援を行う。

（４）恒常的な運用状況の把握

Ａ．ガイドライン原文

情報システム供給者は、保守・運用契約により、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、情報システム利用者との間で共有すること。

また、不具合及びシステム能力の不足等が認められる場合には然るべき対応を行うこと。

＜実施例＞

システムの稼働状況を日・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。

Ｂ．本項目の必要性・重要性

情報システムが定められた信頼性・安全性水準を満たしてサービス提供を維持しつづけるためには、その稼動状態を常時モニターし、ボトルネックがどこかに生じていないかを監視することが重要であるとともに、その稼動状態に関するデータを時系列的に分析するなどし、潜在的な問題を検知して問題が顕在化する前の予防措置に役立てることが重要である。

こういった、日常の監視および監視データの分析を踏まえ、前項（２）で定められた基準に照らし合わせ、保守対応判断を行っていくことで、最適なサービスの維持と長期的なコスト削減につなげることができる。

Ｃ．情報システム利用者の実施事項

＜評価指標 U1／U2＞

Q33　業務を取り巻く環境の変化及び技術的問題（機能、性能、容量、拡張等）等に関するリスク管理を恒常的に実施することを実施管理しているか。／実施しているか。

a.　リスクを特定しているか。

b.　リスクの分析をしているか。

c.　リスクの対応計画を立てているか。

Q34　情報システムの運用状況に関するデータを取得し監視を行い、また必要に応じてしかるべき対応を行うことを実施管理しているか。／対応を行っているか。

情報システム利用者は、自らの実施事項として以下の事項を実施する必要があることを認識すべきである。

・恒常的な運用状況把握の必要性の理解、及び認識すべき運用状況に関するデータ項目を認知すること。

・運用状況に関するデータ項目の監視方法を文書化すること。

・不具合及びシステム能力の不足等の顕在化による影響度を文書化すること。

・不具合及びシステム能力の不足等の防止・抑制対策、不具合及びシステム能力の不足等が顕在化した場合の対応方法を文書化すること。

・上記に基づく、情報システム供給者に対する運用状況に関するデータの収集・分析指示、基準に照らし合わせたアクション判断とアクションの実施を行うこと。

・上記各事項についての実施管理を行うこと。

Ｄ．情報システム供給者への要求事項

＜評価指標 V1／V2＞

Q37　利用者が業務を取り巻く環境の変化及び技術的問題（機能、性能、容量、拡張等）等に関するリスク管理を恒常的に実施することを支援することを実施管理しているか。／Q35　支援しているか。あるいはその重要性を説明しているか。
a.　リスクを特定しているか。
b.　リスクの分析をしているか。
c.　リスクの対応計画を立てているか。
Q38　利用者が情報システムの運用状況に関するデータを取得し監視を行い、また必要に応じてしかるべき対応を行うことを支援することを実施管理しているか。／Q36　支援しているか。あるいはその重要性を説明しているか。

情報システム供給者は、自らの実施事項として以下の事項を実施する必要があることを認識すべきである。

・恒常的な運用状況把握の必要性についての情報システム利用者へ説明を行うこと。
・以下の点についての情報システム利用者に対する説明と合意内容の文書化、情報システム利用者の承認を受領すること。
　認識すべき運用状況に関するデータ項目
　運用状況に関するデータ項目の監視方法
　不具合及びシステム能力の不足等の顕在化による影響度
　不具合及びシステム能力の不足等の防止・抑制対策、不具合及びシステム能力の不足等が顕在化した場合の対応方法
・情報システム利用者に対する運用状況に関するデータの収集・分析結果の提供、判断結果に基づくアクションの実施を行うこと。
・上記各事項についての実施管理を行うこと。

E．その他の留意事項

※IT コーディネータが注意すべきこと
・情報システム利用者に対して、恒常的な運用状況把握の必要性、及び認識すべき運用状況に関するデータ項目についての理解を深めることができるような情報提供を行う。
・情報システム利用者に対して、情報システム利用者の実施事項について初期の枠組み作りが適切に実施されるように必要な助言または支援を行う。
・情報システム利用者の実施事項が保守・運用体制に基づき適切に実施されているか、組織的にその実施管理が行われているかをモニタリングし、問題点・改善点があれば経営者に対して助言または支援を行う。

（５）リリース手順等の整備と訓練

Ａ．ガイドライン原文

情報システム利用者及び情報システム供給者は協力し、リリース手順及び問題発生時の緊急対応等のマニュアル化、現場への徹底及び十分なテストを行うこと。

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。

＜実施例＞

マニュアルに基づく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。

Ｂ．本項目の必要性・重要性

保守作業に伴う、情報システムのリリースを行う場合には、事前に十分な確認を行ってあるリリース手順を準備するとともに、リリース時点での確認テストで、その作業に伴いサービス停止が発生しないようにすることが重要である。

また、万が一に備え、あらかじめ発生しうる問題を想定しておき、それが発生した場合における対応体制と実施すべき措置を決めておくとともに、その措置手順についても検証し、対応要員のスキル等になるべく依存しないようにマニュアルとして整備しておく必要がある。

更に、マニュアルを用いての訓練を定期的に実施することにより、保守要員が日常とは異なる作業手順についての理解を深めるとともに、体制が機能するか、作業手順が対象となる情報システムの変更等を反映しているかの確認もあわせて実施し、問題発生時に影響や損失を最小化するための迅速な対応を図れるように備えておくべきである。

これにより、サービス中断による損失を最低限に抑制することが可能となる。

Ｃ．情報システム利用者の実施事項

＜評価指標 U1／U2＞

Q27　事業継続計画に基づいた情報システム障害発生時の対応手順・マニュアルを元に、適切な教育訓練を行うことを実施管理しているか。／教育訓練が実施されているか。

Q28　保守・運用に係る活動全般について、利用者・供給者それぞれの推進体制及び承認手順を含む業務フロー等を文書化することを実施管理しているか。／文書化しているか。

a.　組織で実施されている保守運用の全ての工程（作業プロセス）に対応した推進体制を文書化しているか。

b.　組織で実施されている保守運用の全ての工程（作業プロセス）に対応した業務フローを文書化しているか。

ただし、業務フローの中には、信頼性・安全性などを意識した作業が含まれなくてはいけない。

Q29　不具合や保守の重要性を段階的に定め、それぞれのランクに応じた対応内容を文書化することを実施管理しているか。／文書化しているか。

a.　保守の種類（是正保守、予防保守、適用保守、完全化保守）に応じた対応が文書化されているか。

b.　保守の量（修正量、修正費用、修正時間）に応じた対応が文書化されているか。

c.　保守の重大性（性能、安全性、セキュリティ、影響範囲等）に応じた対応が文書化されているか。

Q30　リリースに際して、特にリリース手順及び問題発生時の緊急対応等のマニュアル化、現場への徹底及び適切なテストを実施管理しているか。／テストを実施しているか。

a.　リリース手順及び問題発生時の対応手順・マニュアルが作成されているか。

b.　a の対応手順・マニュアルを基に適切な教育訓練が実施されているか。

Q31　構成管理及び変更管理について手順等（ツールを含む）を確立しているか。

Q32　Q28,Q29,Q30,Q31 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認しているか。また、供給者の適切な権限者が承認していることを確認することを実施管理しているか。／確認しているか。

情報システム利用者は、自らの実施事項として以下の事項を実施する必要があることを認識すべきである。

・リリース手順等の整備と確認及びその承認を得ること。
・リリース時における緊急時のビジネスに対する影響度とビジネス復旧・対応方法を文書化すること。
・緊急時の訓練の必要性の理解、及び実施すべき項目を認知すること。
・緊急時の訓練計画と実施手順を文書化すること。
・上記に基づく、情報システム供給者からのマニュアルに基づくシステムの導入訓練や緊急対応訓練の指示と実施を行うこと。
・上記各事項についての実施管理を行うこと。

D．情報システム供給者への要求事項

＜評価指標 V1／V2＞

Q32　利用者が保守・運用に係る活動全般について、利用者・供給者それぞれの推進体制及び承認手順を含む業務フロー等を文書化することを支援することを実施管理しているか。／Q30　支援しているか。あるいはその重要性を説明しているか。

a.　組織で実施されている保守運用の全ての工程（作業プロセス）に対応した推進体制を文書化しているか。

b.　組織で実施されている保守運用の全ての工程（作業プロセス）に対応した業務フローを文書化しているか。

ただし、業務フローの中には、信頼性・安全性などを意識した作業が含まれなくてはいけない。

Q33　利用者が不具合や保守の重要性を段階的に定め、それぞれのランクに応じた対応内容を文書化することを支援することを実施管理しているか。／Q31　支援しているか。あるいはその重要性を説明しているか。

a.　保守の種類（是正保守、予防保守、適用保守、完全化保守）に応じた対応が文書化されているか。

b.　保守の量（修正量、修正費用、修正時間）に応じた対応が文書化されているか。

c.　保守の重大性（性能、安全性、セキュリティ、影響範囲等）に応じた対応が文書化されているか。

Q34　リリースに際して、特にリリース手順及び問題発生時の緊急対応等のマニュアル化、現場への徹底及び適切なテストを実施することを支援することを実施管理しているか。／Q32　支援しているか。あるいはその重要性を説明しているか。

a.　適切なテストを行った上、リリース手順及び問題発生時の対応手順・マニュアルが作成されているか。

b.　a の対応手順・マニュアルを基に適切な教育訓練が実施されているか。

Q35　利用者が構成管理及び変更管理について手順等（ツールを含む）を確立することを支援することを実施管理しているか。／Q33　支援しているか。あるいはその重要性を説明しているか。。

Q36　Q32,Q33,Q34,Q35 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを実施管理しているか。また、供給者の適切な権限者が承認することを実施管理しているか。／Q34 Q30,Q31,Q32,Q33 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを確認しているか。また、供給者の適切な権限者が承認しているか。

情報システム供給者は、自らの実施事項として以下の事項を実施する必要があることを認識すべきである。

・リリース手順等の整備と訓練の必要性、及び実施すべき項目の情報システム利用者へ説明すること。
・以下の点についての情報システム利用者に対する説明と合意内容を文書化し、情報システム利用者の承認を受領しておくこと。

リリース手順、緊急時の影響度と対応方法

訓練計画と実施手順

・情報システム利用者に対する、マニュアルに基づくシステムの導入訓練や緊急対応訓練の指導を行うこと。
・上記各事項についての実施管理を行うこと。

E．その他の留意事項

※IT コーディネータが注意すべきこと
・情報システム利用者に対して、リリース手順等の整備と訓練の必要性、及び実施すべき項目についての理解を深めることができるような情報提供を行う。
・情報システム利用者に対して、情報システム利用者の実施事項について初期の枠組み作りが適切に実施されるように必要な助言または支援を行う。
・情報システム利用者の実施事項が保守・運用体制に基づき適切に実施されているか、組織的にその実施管理が行われているかをモニタリングし、問題点・改善点があれば経営者に対して助言または支援を行う。

（６）問題追跡性の確保

Ａ．ガイドライン原文

情報システム供給者及び情報システム利用者は、構成管理及び変更管理等を確実に実施し、問題の追跡性を確保すること。

＜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。

Ｂ．本項目の必要性・重要性

情報システムで発生する問題の多くは、情報システムに対する何らかの変更により発生していることが経験上明らかとなっている。従って、情報システムを変更する場合においては、システム変更の内容を十分に確認するとともに、変更内容をシステム構成情報にきちんと反映し、システム構成情報を常に最新状態に維持しておくことが必要である。

システム構成情報の適切な更新が行われないことにより、次回のシステム変更時に障害が発生し、その原因追究が迅速に行えないといった弊害、つまり問題追跡性の欠如が生じる。例えば、保守者が認識していない変更等がシステムに加えられていた場合には、変更等の履歴をすべてトレースしたうえで、履歴として残されていない変更があることを知るまでに多大な時間を要し、結果的に復旧に長時間を要するということにつながる。

従って、障害を防止するだけでなく、障害復旧時間をできるだけ短くするためには、システムの変更がシステム構成情報に正確に反映され、常に最新の構成情報を把握できるようにしておくとともに、変更がどのように行われたかを的確に把握できることが重要である。これにより、問題発生時における変更の追跡、原因の究明が迅速に可能となる。

このようなことから、構成管理や変更管理等については、その実施プロセスを明確に定義しマニュアル化するとともに、漏れや抜けがないようにチェックする体制を設けることが必要である。

Ｃ．情報システム利用者の実施事項

＜評価指標 U1／U2＞

Q27　事業継続計画に基づいた情報システム障害発生時の対応手順・マニュアルを元に、適切な教育訓練を行うことを実施管理しているか。／教育訓練が実施されているか。

Q28　保守・運用に係る活動全般について、利用者・供給者それぞれの推進体制及び承認手順を含む業務フロー等を文書化することを実施管理しているか。／文書化しているか。

a.　組織で実施されている保守運用の全ての工程（作業プロセス）に対応した推進体制を文書化しているか。

b.　組織で実施されている保守運用の全ての工程（作業プロセス）に対応した業務フローを文書化しているか。
ただし、業務フローの中には、信頼性・安全性などを意識した作業が含まれなくてはいけない。

Q29　不具合や保守の重要性を段階的に定め、それぞれのランクに応じた対応内容を文書化することを実施管理しているか。／文書化しているか。

a.　保守の種類（是正保守、予防保守、適用保守、完全化保守）に応じた対応が文書化されているか。

b.　保守の量（修正量、修正費用、修正時間）に応じた対応が文書化されているか。

c.　保守の重大性（性能、安全性、セキュリティ、影響範囲等）に応じた対応が文書化されているか。

Q30　リリースに際して、特にリリース手順及び問題発生時の緊急対応等のマニュアル化、現場への徹底及び適切なテストを実施管理しているか。／テストを実施しているか。

a.　リリース手順及び問題発生時の対応手順・マニュアルが作成されているか。

b.　a の対応手順・マニュアルを基に適切な教育訓練が実施されているか。

Q31　構成管理及び変更管理について手順等（ツールを含む）を確立しているか。

Q32　Q28,Q29,Q30,Q31 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認しているか。また、供給者の適切な権限者が承認していることを確認することを実施管理しているか。／確認

しているか。

情報システム利用者は、自らの実施事項として以下の事項を実施する必要があることを認識すべきである。

・問題追跡性の確保の必要性の理解、及び実施すべき項目を認知すること。
・構成管理および変更管理手順を文書化すること。
・管理ツールの明確化と使用方法を文書化すること。
・上記に基づく、構成管理および変更管理を実施すること。
・上記各事項についての実施管理を行うこと。

D．情報システム供給者への要求事項

＜評価指標 V1／V2＞

Q32　利用者が保守・運用に係る活動全般について、利用者・供給者それぞれの推進体制及び承認手順を含む業務フロー等を文書化することを支援することを実施管理しているか。／Q30　支援しているか。あるいはその重要性を説明しているか。

a.　組織で実施されている保守運用の全ての工程（作業プロセス）に対応した推進体制を文書化しているか。

b.　組織で実施されている保守運用の全ての工程（作業プロセス）に対応した業務フローを文書化しているか。

ただし、業務フローの中には、信頼性・安全性などを意識した作業が含まれなくてはいけない。

Q33　利用者が不具合や保守の重要性を段階的に定め、それぞれのランクに応じた対応内容を文書化することを支援することを実施管理しているか。／Q31　支援しているか。あるいはその重要性を説明しているか。

a.　保守の種類（是正保守、予防保守、適用保守、完全化保守）に応じた対応が文書化されているか。

b.　保守の量（修正量、修正費用、修正時間）に応じた対応が文書化されているか。

c.　保守の重大性（性能、安全性、セキュリティ、影響範囲等）に応じた対応が文書化されているか。

Q34　リリースに際して、特にリリース手順及び問題発生時の緊急対応等のマニュアル化、現場への徹底及び適切なテストを実施することを支援することを実施管理しているか。／Q32　支援しているか。あるいはその重要性を説明しているか。

a.　適切なテストを行った上、リリース手順及び問題発生時の対応手順・マニュアルが作成されているか。

b.　a の対応手順・マニュアルを基に適切な教育訓練が実施されているか。

Q35　利用者が構成管理及び変更管理について手順等（ツールを含む）を確立することを支援することを実施管理しているか。／Q33　支援しているか。あるいはその重要性を説明しているか。。

Q36　Q32,Q33,Q34,Q35 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを実施管理しているか。また、供給者の適切な権限者が承認することを実施管理しているか。／Q34 Q30,Q31,Q32,Q33 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを確認しているか。また、供給者の適切な権限者が承認しているか。

情報システム供給者は、自らの実施事項として以下の事項を実施する必要があることを認識すべきである。

・問題追跡性の確保の必要性、及び実施すべき項目の情報システム利用者への説明を行うこと。

・以下の点についての情報システム利用者に対する説明と合意内容の文書化し、情報システム利用者の承認を受領しておくこと。

構成管理および変更管理手順

管理ツールと使用方法

・情報システム利用者に対する、マニュアルに基づく構成管理および変更管理の指導を行うこと。

・上記各事項についての実施管理を行うこと。

E．その他の留意事項

※IT コーディネータが注意すべきこと

・情報システム利用者に対して、問題追跡性の確保の必要性、及び実施すべき項目についての理解を深めることができるような情報提供を行う。

・情報システム利用者に対して、情報システム利用者の実施事項について初期の枠組み作りが適切に実施されるように必要な助言または支援を行う。

・情報システム利用者の実施事項が保守・運用体制に基づき適切に実施されているか、組織的にその実施管理が行われているかをモニタリングし、問題点・改善点があれば経営者に対して助言または支援を行う。

４．障害対応に関する留意事項

Ａ．ガイドライン原文

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。

Ｂ．本項目の必要性・重要性

この項では障害対応および事業継続について、個別プロジェクトまたは個別アプリケーションという視点ではなく、企業レベルの視点つまり事業全体における事業継続という信頼性安全性から障害対応および事業継続に取り組むことを説明している。ここでの信頼性安全性とは、ステークホルダーから見た場合の、事業が情報システムに強く依存している企業の信頼性安全性のことを意味している。従って、経営層は経営戦略の中で経営リスクへ対応として障害対応および事業継続を位置づけ、経営戦略の実行において、それと対を成す情報システムが有効性を発揮するように構築・運用を推進できるように改革を進めていく責任がある。

前文の前半では障害対応の視点から述べている。情報システムの障害対応は、情報システムを構成する要素が内包するリスクをすべて洗い出し、それらが顕在化した場合、機能要件および非機能要件がどのように阻害されるかを分析し、対応方法（手順や組織など）を検討、作成する。そして、作成された対応方法を運用して、実施管理をおこなう。

後半は事業継続の観点から述べている。業務において情報システムの使用している最終利用者や取引先などの間接影響者が業務を中断しないような手立てを検討し、作成する。

障害対応に関連する規格としては ITSMS（IT サービスマネジメントシステム）:ISO2000-1 がある。この中の「マネジメントシステム要求事項」および「サービスマネジメントの計画立案及び導入」、「サービス継続および可用性の管理」、「問題管理」が深く関連している。事業継続に関連する規格としては事業継続マネジメント：BS25999 がある。BS25999 は 2 つのパートに分かれており、BS25999-1 は BCM の実践規範であり、BS25999-2 は認証のための規格である。BS25999 は情報システムのみの範囲ではなく、企業や組織レベルで潜在的な脅威を認識し、その脅威が現実となった場合に引き起こされる事業運営への影響を特定するための継続的な管理と統制のプロセスである。

これらの規格に基づいてプロセスを実施し、認証を取得することは、ステークホルダーに対して信頼性安全性を目に見える形で提示することになる。しかし、認証を取得し継続していくには、成熟度の高さが必要で、一朝一夕には実現できない。従って、これらの規格に準拠しつつ、力量にあったプロセスを実施し、問題認識と改善を繰り返し、成熟度の高いプロセスへレベルアップしていくことが現実的である。

（1）緊急時対応の利用者・供給者間での合意

A．ガイドライン原文

情報システム利用者及び情報システム供給者は、事業継続計画に基づき、情報システム障害等の緊急時の経営層まで含めた指揮命令系統及び影響度に応じた対応手順等を文書化及びマニュアル化し、双方で合意し、共有すること。その際、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。

また、緊急時には双方の緊密な協力の下、業務・サービス維持及び情報システム維持の両面からの対策を講じること。

＜実施例＞

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。

B．本項目の必要性・重要性

緊急時対応について情報システム利用者と供給者の間で合意が、事業継続計画に基づいているためには、情報システム利用者が事業継続計画を策定している必要がある。事業継続計画は事業継続を脅かす状況での使用に備えての文書化された一連の手順や情報である。事業継続計画が事業継続を脅かす状況で有効性を発揮するためには、事業継続管理の構築が必要である。事業継続管理を運用することにより、事業継続計画が最新の経営戦略や経営環境に合致した状態に維持するとともに、経営者および社員、取引先、ステークホルダーが最新の事業継続計画に基づいて的確に行動できるためのトレーニングおよびリハーサル、レビューを実施する。情報システム供給者は、情報システム利用者の事業継続管理に参画することにより、情報システム利用者の事業継続計画を理解し、情報システム共有者としての役割を合意して、手順や情報を共有できた状態になる。

BS25999-1 に準拠する事業継続管理は次のマネジメントプロセスで構築および維持される。

- 事業継続管理方針とプログラムマネジメント
- 組織の理解
- 事業継続戦略の決定
- 事業継続管理を実現する手法の開発と実装
- 訓練、維持管理およびレビュー
- 事業継続管理の組織文化への浸透

事業継続計画と情報システム障害対応の関係はどのようになっているがここで検討する。

事業継続管理の特性は、

- ビジネス影響分析
- 影響と時間
- 重大な事業混乱を発生させる事象
- 規模に関係なく生存を脅かすインシデント
- 事業のコアコンピテンシーの範囲を超えたインシデント管理に注目
- 突然または急激な事象

である。また、情報システムの障害対応はリスクマネジメントとして考えることができ、その特性は、

- リスク分析
- 影響と発生確率

・すべてのタイプの事象
・すべての規模の事象
・コアの事業目標に対するリスクの管理に注目
・徐々にから突然までのすべてに事象
である。

リスクマネジメントとしての情報システム障害対応は、コンポーネント障害影響分析（CFIA）などの手法を使って情報システムが内包するリスクを特定し、影響度と発生の可能性からから評価する。評価により対応すべきリスクは、リスクを減少させるため、回避、低減、移転、保有などの対策を組み合わせて対応する。情報システムにおける対策の例として、

・回避：戦略の実行に対して情報システムに依存しない
・低減：ハードウェアおよびソフトウェア、ファシリティ、ユーティリティに冗長化などの解決案を適応する、データセンターなどの外部のサービスを利用する
・移転：保険などのリスクファイナンスを利用する、SLA に基づくペナルティを含む契約によりアウトソーシングやサービスプロバイダーを利用する
・保有：発生したらそのとき対応を考える、予め準備した対応手順で対応する
が考えられる。

これらの対策を実行することによりリスクを減少させることはできるが、ゼロにはならず残留リスクが存在する。残留リスクが企業として容認できる水準になっているかを評価し、容認できない場合、リスクの評価や対策の選択、さらには戦略実行における情報システム化の方針および範囲、予算を見直す必要がある。

情報システム障害の観点から見ると事業継続計画の発動は、

・見逃されていた影響度が高いリスク
・リスク低減のための対策が稼動しなかった影響度が高いリスク
・発生可能性が低いと評価し保有したが、発生してしまった影響度が高いリスク
・影響度が低いと評価し保有したが、実際には影響度が高かったリスク
などが顕在化することにより、事業継続を脅かすと経営層が判断する。

また、情報システム障害のリスク分析では特定されないリスクですが、事業継続計画の策定の対象となるリスクがある。これらのリスクが顕在化したときに情報システムがどのような影響を受けるか評価し、必要な対策を準備し、対応する。

リスクマネジメントの有効性を高めるためには、影響度の大きなリスクに対して保持という対策を組み合わせ、情報システムを利用できないことを想定した手順を準備し、リスクが顕在化したと時に対応できるようにしておくことが重要である。

C．システム利用者の実施事項

＜評価指標 U1＞

Q35 情報システム障害等の緊急時の双方の経営層まで含めた指揮命令系統及び影響度に応じた対応手順等を文書化及びマニュアル化し、供給者と合意することを実施管理しているか。

a. 影響度に応じた報告経路及び体制などが定められているか。
b. 報告経路は運用責任者及び利用部門の責任者が承認しているか。
c. 報告経路について関係者に周知徹底しているか。
d. 報告経路は環境に応じて定期的に見直しを行っているか。

Q36 Q35 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認しているか。また、供給者の適切な権限者の承認を確認することを実施管理しているか。

＜評価指標 U2＞

Q35 情報システム障害等の緊急時の双方の経営層まで含めた指揮命令系統及び影響度に応じた対応手順等を文書化及びマニュアル化し、供給者と合意しているか。

a. 影響度に応じた報告経路及び体制などが定められているか。

b. 報告経路は運用責任者及び利用部門の責任者が承認しているか。

c. 報告経路について関係者に周知徹底しているか。

d. 報告経路は環境に応じて定期的に見直しを行っているか。

Q36 Q35 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認しているか。また、供給者の適切な権限者が承認していることを確認しているか。

情報システム利用者が取り組むべきことを述べる。

・PMBOK に準拠した情報システムが内包するリスクを検討すること。

1.リスク管理計画

2.リスクの特定

3.リスクの定性分析

4.リスクの定量分析

5.リスク対応計画

6.リスクの監視と管理

・コンポーネント障害影響分析(CFIA)による障害対策を検討すること。

7.格子分析

8.詳細分析

9.分析結果への対応

・BS25999-1 に準拠した事業継続管理を構築すること。

10. 事業継続方針

11. 事業継続管理のプログラムマネジメント

12. 組織の理解

13. 事業継続戦略の決定

14. 事業継続管理を実現する手法の開発と実装

15. 事業継続管理への取組みに関する訓練、維持管理、レビュー

16. 事業継続管理の組織文化への導入

・システム供給者を含めた訓練を実施すること。

・システム供給者を含めたレビューを実施すること。

・システム供給者を含めた維持管理を実施すること。

D．システム供給者への要求事項

＜評価指標 V1＞

Q39 情報システム障害等の緊急時の双方の経営層まで含めた指揮命令系統及び影響度に応じた対応手順等を文書化及びマニュアル化し、利用者と合意することを実施管理しているか。その際、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を実施管理しているか。

a. 響度に応じた報告経路及び体制などが定められているか。

b. 報告経路は運用責任者及び利用部門の責任者が承認しているか。

c. 報告経路について関係者に周知徹底しているか。
d. 報告経路は環境に応じて定期的に見直しを行っているか。

Q40 Q39 の内容を利用者と供給者が合意した上で、利用者の適切な権限者の承認を確認することを実施管理しているか。また、供給者の適切な権限者が承認することを実施管理しているか。

＜評価指標 V2＞

Q37 情報システム障害等の緊急時の双方の経営層まで含めた指揮命令系統及び影響度に応じた対応手順等を文書化及びマニュアル化し、利用者と合意しているか。その際、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しているか。あるいはその重要性を説明しているか。

a. 影響度に応じた報告経路及び体制などが定められているか。
b. 報告経路は運用責任者及び利用部門の責任者が承認しているか。
c. 報告経路について関係者に周知徹底しているか。
d. 報告経路は環境に応じて定期的に見直しを行っているか。

Q38 Q37 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを確認しているか。また、供給者の適切な権限者が承認しているか。

情報システム供給者が取り組むべきことを述べる。

・ システム供給者のリスクマネジメントや事業継続計画に対応した体制確立を依頼すること。
・ システム供給者のリスクマネジメントによる障害対策の検討や事業継続管理の構築へ参画すること。
・ 訓練へシステム供給者も参画すること。
・ レビューへシステム供給者も参画すること。
・ 維持管理へシステム供給者が協力すること

E．その他の留意事項

※IT コーディネータが注意すべきこと

障害対策や事業継続のための ITSMS や事業継続管理の実施管理は、ITC プロセスと親和性が非常に高い。

親和性の１つ目のポイントは、ITC プロセスの経営戦略の展開と実行（プロセス改革）におけるダブルループコントロールと同じプロセス管理を ITSMS や事業継続管理でモデルとして参照している。

ITC プロセスの「3-8 経営戦略実行」において、「従来の枠組みに基づいた PDCA（計画・実行・統制・改善）サイクルを正確に回すだけでなく、経営戦略に基づいた抜本的な改革をおこなうために、ステイクホルダーの知の共有し学習する組織活動に基づいた SPDLI（Strategy：戦略・Plan：計画・Do：実行・Learning：学習・innovation：改革）のサイクルを回し、抜本的なベストプラクティスを構築することが重要である。」と述べています。ITC プロセスでは、経営戦略フェーズに続く経営戦略実行を経営全般のプロセス改革、IT 戦略策定フェーズから IT サービス活用フェーズまでを IT 領域のプロセス改革として、それぞれの領域の経営課題について SPDLI サイクルを実行することにより解決を図り、改革の実現を目指している。また、これらの SPDLI サイクルによるプロセス改革を確実に推進するために、PDCA サイクルをプロセス＆プロジェクトマネジメントおよびモニタリング＆コントロールをとおして実行している。

先に示した BS25999-1 に準拠した事業継続管理は、SPDLI サイクルを実行することにより、事業継続の脅威を特定し、その影響と対処の導入を図っている。また、BS25999-2 では、マネジメントシステムとして PDCA サイクルの実行を求めている。また、ITSMS では、「サービスマネジメントの計画(Plan)」および「サービスマネジメントの実施及びサービスの提供(Do)」、「監視、測定およびレビュー(Check)」、「継続的改善(Act)」が記述されており、PDCA サイクルによるプロセス管理を要求している。

２つ目のポイントは、経営戦略とのリンクと経営層のリーダーシップである。ITC プロセスの特徴として、「「経営戦略」の重要性の認識」および「指導原理は「経営戦略との整合性」」であり、IT コーディネータの立場は「経営者の経営改革推進を支援する」ことである。戦略策定フェーズの「リスク評価」において抽出された情報システム障害や事業継続に関連する経営リスクは、経営戦略実行や IT 戦略策定フェーズ以降で回避、低減のための要件として具体化される。経営層は、モニタリング＆コントロールを通して、それらの経営戦略との整合性を確認し、経営戦略達成に対して有効性を持つように導く責任がある。

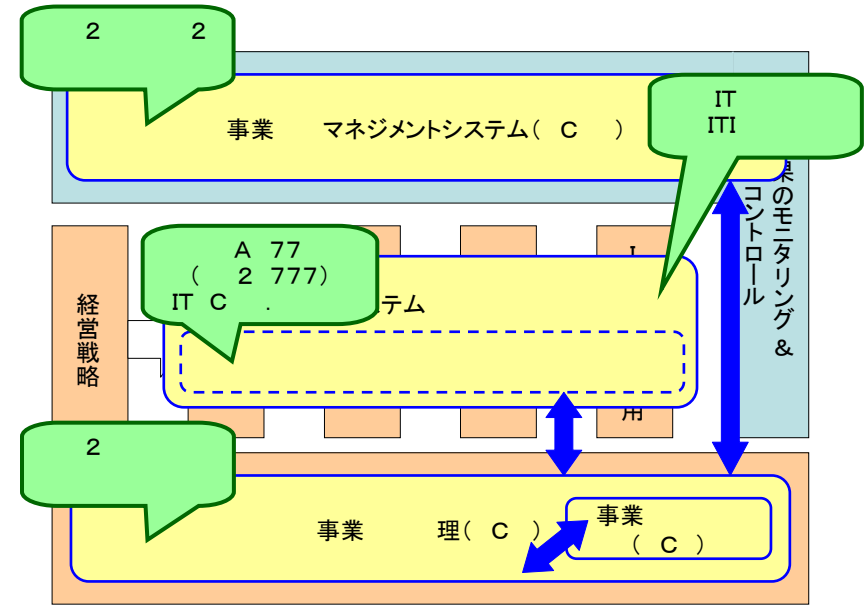
ITSMS は、情報システム障害などのリスクに対して、必要な安全性信頼性を確保した情報システムの運用をするためのマネジメントシステムで、計画、導入、監視、レビューおよび改善について、経営層は最終的な責任を負う。ITSMS では「経営陣の責任」として、経営層の責任を次のように規定している。

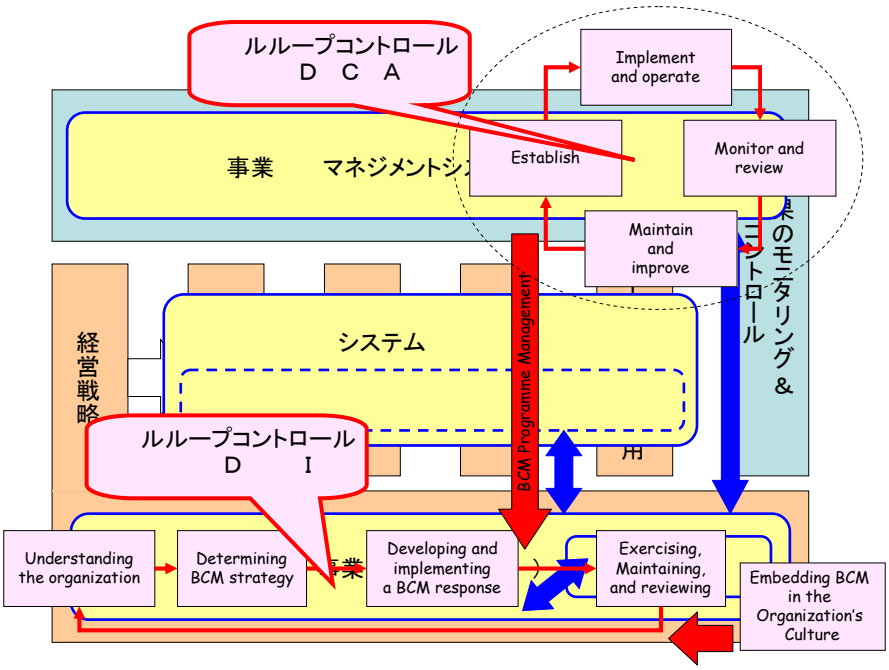
「経営陣は、サービスマネジメントの能力を事業上の要求事項および顧客要求事項との関連におい開発、実装及び改善することへのコミットメントの証拠を、リーダーシップ及び活動を通じて示さなければならない。」

つまり、経営層は ITSMS についての方針、目標を設定し、実践のための計画と実施を明確に指示します。これらに必要

な役割や責任を持つ役員を選出し、実施に必要な経営資源を提供しなければならない。また、意図した通り有効に機能しているかマネジメントレビューにより把握しなければならいとしている。

この項で述べられている「緊急時対応の利用者・供給者間での合意」は、システム利用者の経営層が障害対策や事業継続にたいして、リーダーシップを持ち活動を牽引することにより実現できることは、以上の説明から明白である。


2 2
事業 マネジメントシステム(C)
IT
ITI
A 77
(2 777)
IT C .
経営戦略
2
事業 理(C)
事業
(C)
のモニタリング &
コントロール


ルループコントロール
D C A
Implement and operate
事業 マネジメントシ
Establish
Monitor and review
Maintain and improve
BCM Programme Management
のモニタリング &
コントロール
経営戦略
システム
ルループコントロール
D I
Understanding the organization
Determining BCM strategy
Developing and implementing a BCM response
Exercising, Maintaining, and reviewing
Embedding BCM in the Organization's Culture

（２）原因究明手順等の明確化

Ａ．ガイドライン原文

情報システム利用者及び情報システム供給者は、情報システム障害を引き起こした欠陥の究明並びにその欠陥が作られた原因及び見逃されてしまった原因等を客観的な方法等を用いて究明する手順を定め、文書化し、共有すること。

＜実施例＞

情報システム障害に対する原因究明手順書及び様式類を整備し、情報システム利用者及び情報システム供給者間で共有する。

Ｂ．本項目の必要性・重要性

情報システムの障害は、事業に構成する業務に対して、情報システムのサービス提供が停止だけではなく、低下により業務に支障をきたす状態をいう。ハードウェアの故障やソフトウェアの不具合は欠陥と認識するべきか検討する。1 つの考え方として、ハードウェアの故障やソフトウェアの不具合を直接的な欠陥と認識して、それらを顕在化させてしまった原因の究明する考え方がある。この場合、多くの場合、ハードウェアの信頼性やソフトウェアのテストのカバレッジの中に原因を求めることになる。しかし、ハードウェアの信頼性を高くする構成にしたり、不具合の総数がわからないソフトウェアに対してテストを増加させたとしても、コストは急増するが、ハードウェアの信頼性を 100%にしたり、ソフトウェアの不具合がゼロにすることはできない。もう 1 つの考え方として、ハードウェアの信頼性やソフトウェアの不具合を制約条件として、障害により情報システムのサービス提供が停止もしくは低下して発生した業務への支障に対応する対策が作成されていなかった、またはうまく機能しなかったことを運用の欠陥と認識して、このような状態を見逃してきた構築プロセスまたは運用プロセスの中に原因を求めることができる。

ハードウェアは欠陥が引き金となって機能停止した時、エラーログ、メモリーダンプなど客観的な情報を記録する機能があり、そのような機能がある製品を選択することにより、製造メーカーに欠陥の再発の防止を求めることは可能だろう。しかし、製造メーカーになぜ欠陥が完全に除去できなかったのかと原因の究明させることは現実的ではないことは容易に想像がつく。ソフトウェアも同様に異常時の情報や異常に至るまでのログやジャーナルを記録する機能を持つソフトウェア製品を選択したり、そのような機能を仕様としたソフトウェアを開発する必要がある。ネットワークについてもトレースやトラップなどのツールを使用することで客観的な情報を取得することができる。

構築プロセスや運用プロセスにおける客観的な方法について検討する。一般にこのようなプロセスは成果物が定義され、必要な手順・手続きが決められている。そして、成果物のレビューが完了することで一連の手順・手続きが完了することになる。レビューにおいて成果物の内容に抜けや漏れがなく、必要な品質であることが確認される。不十分なところがあれば課題点としてリストアップされ、改善を実施して課題がなくなるまで繰り返される。構築プロセスや運用プロセスでは、成果物、レビュー結果、改善結果を文書として残すことで、情報システムの障害が発生したときに、欠陥を作りこんでしまった原因を客観的に究明することができる。プロセスを遵守して成果物を作成しレビューを受け、適切に対応したにもかかわらず欠陥を作りこんでしまった場合は、プロセスを見直したり、レビューの確認項目や基準を改定して再発を防止する。また、プロセスを遵守しなかったり、課題に適切に対応しなかったことで欠陥を見逃ししまった場合は、プロセスの実効性を高めるための手順・手続きの改善が必要になる。

企業経営や経営環境は市場へ対応して、急速に変化している。情報システムの構築時に完全を目

指して、要件を確定し、設計を行い、テストを完了させたとしても、変化によりギャップが発生してしまっていることがある。IT サービス活用フェーズにおいても、市場の変化や経営戦略の修正に伴い発生したギャップから発生が予測される障害を認識して、それらへの対応を始動させるプロセスが必要である。

C．システム利用者の実施事項

＜評価指標 U1＞
Q37 障害に関して報告・記録の手順と、これを共有する仕組みを整えているか。
a. 事故及び障害の発生時に報告書を作成し、運用の責任者が承認しているか。
b. 報告書は、事故及び障害の状況、影響、原因を記載しているか。
c. 事故及び障害発生時にあらかじめ定めた連絡体制が機能しているか。
d. a，b，c を経営層等、情報システム関係者以外にも共有する仕組みがあるか。
Q38 障害に関して原因を客観的な方法により究明する手順を定めているか。
＜評価指標 U2＞
Q37 障害に関して報告・記録の手順と、これを共有する仕組みを整えているか。
a. 事故及び障害の発生時に報告書を作成し、運用の責任者が承認しているか。
b. 報告書は、事故及び障害の状況、影響、原因を記載しているか。
c. 事故及び障害発生時にあらかじめ定めた連絡体制が機能しているか。
d. 上記を経営層等、情報システム関係者以外にも共有する仕組みがあるか。
Q38 障害に関して原因を客観的な方法により究明する手順を定めているか。

情報システム利用者が取り組むべきことを述べる。

・情報システム障害の影響の重大性に応じて、経営層を含めた調査委員会を設置して、原因の究明に必要な経営資源の割り当てること。
・障害の検知から初動対応までの対応を分析し、改善すること。
・障害を引き起こした直接の欠陥を特定し、改善すること。
・欠陥を作り込んだ、または見逃した本当の原因を特定し、改善すること。
・調査結果について報告書にまとめ、情報公開すること。

D．システム供給者への要求事項

＜評価指標 V1＞
Q41 利用者が障害に関する報告・記録の手順と、これを共有する仕組みを整えることを支援することを実施管理しているか。
a. 事故及び障害の発生時に報告書を作成し、運用の責任者が承認しているか。
b. 報告書は、事故及び障害の状況、影響、原因を記載しているか。
c. 事故及び障害発生時にあらかじめ定めた連絡体制が機能しているか。
d. a，b，c を経営層等、情報システム関係者以外にも共有する仕組みがあるか。
Q42 利用者が障害に関して原因を客観的な方法により究明する手順を定めることを支援することを実施管理しているか。
＜評価指標 V2＞
Q39 利用者が障害に関する報告・記録の手順と、これを共有する仕組みを整えることを支援しているか。あるいはその重要性を説明しているか。
a. 事故及び障害の発生時に報告書を作成し、運用の責任者が承認しているか。
b. 報告書は、事故及び障害の状況、影響、原因を記載しているか。
c. 事故及び障害発生時にあらかじめ定めた連絡体制が機能しているか。
d. a,b,c を経営層等、情報システム関係者以外にも共有する仕組みがあるか。
Q40 利用者が障害に関して原因を客観的な方法により究明する手順を定めることを支援しているか。あるいはその重要性を説明しているか。

情報システム供給者が取り組むべきことを述べる。

・情報システム障害の影響の重大性に応じて、情報システム供給者の経営層を含めた情報システム利用者の調査委員会に参画すること。
・障害の検知から初動対応までの対応状況についての情報を提供し、改善に協力すること。
・障害を引き起こした直接の欠陥の特定と改善に協力すること。
・欠陥を作り込んだ、または見逃した本当の原因の特定と改善に協力すること。

E．その他の留意事項

※IT コーディネータが注意すべきこと

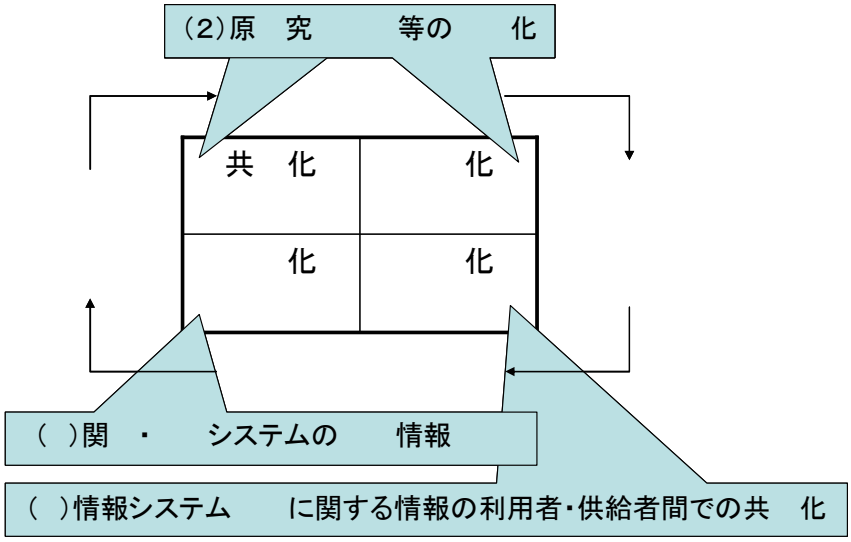
ITC プロセスには「経営者責務の原則」があり、「経営者は IT サービスを活用したプロセス改善が遂行できるよう、リーダーシップををとる」という基本原則がある。情報システム障害、つまり IT サービスを活用したプロセス改善の遂行が阻害される欠陥や原因を除去は、経営層はリーダーシップを持って遂行されなければならない。情報システム障害を単なる責任問題として、担当者に任せて責任の回避となすり合いするのではなく、今後、同じ障害の再発や同様な障害の発生を回避するために、本当の原因を見つけ出し、欠陥の排除するように率先することが重要である。

情報システム障害は、ハードウェア故障の発生など客観的なデータが比較的とりやすい欠陥だけでなく、それに対する人間の不適切な対応なども含めて顕在化する。操作卓から入力されたコマンドなどはログに記録され客観的なデータとして利用できあるが、人間系で行われた情報伝達や指揮・命令、判断などは記録が残らない。当事者や関係者の記憶を証言として収集し、経緯を分析することにより、人間系に内在する原因を突き止めなければならない。重大な情報システム障害では、経営層を含めた調査委員会を設置して原因の究明にあり、懲罰とは別の次元であることをコミットメントし、当事者間の利害関係を排除して、信憑性の高い証言を収集する必要がある。

情報システム障害の影響の重大性は、ITC プロセスの観点では「IT 戦略達成度評価」に関連してくる。つまり、IT 戦略達成度の評価をしたときに情報システム障害がどのように影響したか評価されるが、この評価は時間的にはかなりのタイムラグの後の結果の評価である。この評価は「継続的な IT 環境の改善と業務プロセス改善の提言」に受け継がれ、IT 化の成熟度の向上のための活動になる。

一方、情報システム障害は直接的には、情報システムのサービス停止や低下を引き起こし、業務の中断や事業継続への危機を引き起こすことになる。情報システム障害への対応は、欠陥や原因を 100%除去できないことを前提に策定されるされるので、障害発生後のリアクティブな対応だけでなく、発生の予防に重点が置かれるべきである。そのため、情報システムの重要度に応じて、適切なサービスレベル項目と管理値を設定し、モニタリングすることが必要となる。ITC プロセスでは、「SLM の実施」を行い、評価と改善活動を実施していく。障害対策の不備や不具合の顕在化の先行指標として、それらが変動に反映するようなサービスレベル項目を選択し、管理値を設定することにより、予防的な改善などのプロアクティブな対応が策定され、障害に備えられ、サービスレベルの改善活動につながっていく。

また、障害に至らずに表面化しなかったヒヤリ・ハットも記録と分析は、将来偏在化する可能性がある情報システム障害の重要な兆候を示しており、これらについてもモニタリングをおこないプロアクティブな対応につながっていく。


(2)原　究　　等の　　化
共　化
化
化
化
(　)関　・　システムの　　情報
(　)情報システム　　に関する情報の利用者・供給者間での共　化

（３）情報システム障害に関する情報の利用者・供給者間での共有化

Ａ．ガイドライン原文

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）及びその原因等の事柄は確実に記録し、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。

特に、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或いは広く経済的、社会的影響を与えるものである場合、原因究明を体系的に行い、その結果については、秘密保持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されることが望ましい。

＜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。

Ｂ．本項目の必要性・重要性

情報システム障害に関する情報をシステム利用者と提供者間で共有するということは、発生してしまった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）及びその原因等の事柄を障害情報として単に知るというだけではない。障害の再発防止や影響の最小化などの障害対応を確立するために、そこから得た経験や知識を共有して活かしていくことである。したがって、情報システム障害を忌み嫌うのではなく、障害の発生から得たものを生かそうという企業風土や情報活用のための仕組み作りをして初めて実現することができる。企業風土については、「（４）関連・類似システムの障害情報収集」で説明をする。ここでは仕組みについて検討する。

ITSMS ではと問題管理のプロセスで管理される範囲のリアクティブな活動の一部ですが、問題管理の要求事項の中に

・予防処置をとること

・問題解決の有効性を監視・レビュー・報告すること

とある。問題を発生させないためのプロアクティブな事前予防の活動を要求しており、この項のテーマの共有化はこれらへの対応と考えることができる。

情報システム障害は発生してしまった事実として、結果として目に触れることになる。多くの場合、原因や経過は簡単に記録され、経験や知識を活かすことができていない。本当に障害情報を活かして役立てるためには、起こるに至った脈絡を結末まで把握し、障害全体を理解できることと、その中から学んだ経験を将来使える知識としてまとめることが不可欠である。障害を「事象」、「経過」、「原因」、「対処」、「総括」などの項目ごとに記述することにより、脈絡を正しく表現し、情報を活用する人に障害全体をクリアにすることができる。さらに「知識化」の項目として、さまざまな視点からこの障害を見て、そこから得た知識や教訓、知恵、創造の種などを記述する。後からその障害を振り返って活用しようというときに、事実だけが記録された障害情報に比べて、障害情報の有効性が高くなる。

このように記述された障害情報が有効に活用されるためには、利用し易い形に記録されなければならない。報告書のような紙の媒体では倉庫で眠ってしまう。情報システム障害を共有するためには、障害情報を「知りたい人」に「知りたい時」、「知りたい中身」を「欲しい形」で示せることが必要である。ガイドラインの実施例にある「情報システム障害管理データベース」のようなデータベースを社内 LAN システム上に構築することにより、このような環境を整備することが可能になる。情

報システム障害管理データベースをより効果的なものにするためにいくつかの注意が必要である。

ITSMS の問題管理で記録された情報をそのままデータベース化しても、情報システム障害の共有の目的に利用できない。問題管理の情報は、原因の究明のために決められたプロセスの管理を目的としている。まだ明らかになっていない障害に至るまでの脈絡を試行錯誤して解明する作業の記録だからである。情報システム障害の共有のためには、前述した項目に従って、問題管理の記録を整理する必要がある。

また、ITSMS の問題管理により記録された障害すべてをデータベースに登録すれば良いわけではない。障害情報を活用するためには、情報システムの特徴に合わせて、代表的な障害事例に集約し、同種のものをグループ化して登録する必要があります。集約やグループ化は原因の種類と階層により分類するのが一般的であるが、技術的な原因の他に経済的背景や心理的背景など強く影響している要因を検索の軸に加えることにより活用し易くなる。

情報システム障害に関する情報の「知識化」により、データベースを利用して共有化を図ることを説明してきた。この方法は、記録された知識がデータベースを利用した人へ伝達される。つまり、先人から後人へ経験や知識を伝承していることと同じである。データベースから知識を得た人は障害の原因を回避することができますが、データベースを利用しない人は原因を回避せずに障害を繰り返すことになる。これは、企業全体で情報や知識がうまく伝達されていないし、共有されていないことである。データベースの整備だけでは「暗黙知」から「形式知」へ変換されただけで不十分なのである。

企業全体で情報や知識を共有するためには、「暗黙知」から「形式知」へ変換された知識を、企画段階、開発段階、保守・運用段階の中にそれらを活用できるような仕組みをとして埋め込むことが必要である。「（２）原因究明手順等の明確化」で説明した「欠陥が作られた原因」及び「見逃されてしまった原因」は、企画段階、開発段階、保守・運用段階の成果物の作成や各段階を完了するためのガイドや手順を見直して、欠陥が作り込まれたり、見逃されたりする原因を排除しなければならない。つまり、成果物の作成のためのチェックリストや完了レビューの手順や基準を改定して、欠陥や原因を排除しなければならない。この結果、改定されたガイドや手順を遵守することにより、情報システム障害の経験や知識を共有し、企業全体として同じような情報システム障害を減少させることが可能となる。

「形式知」は成熟期を迎えると形骸化する傾向があり、障害抑止の実効性が低下する。標準、基準、手順の継続的な改定と運用、およびデータベースに登録された障害事例についての情報伝達の双方が重要になる。

標準、基準、手順の改定は、ITSMS の変更管理のプロセスによって行われる。

この項では事業継続管理という観点では説明をしていないが、上記の説明と同様に考えることができる。

「（２）原因究明手順等の明確化」と同様に、情報システム障害に関する情報の利用者・供給者間での共有化に対しても経営層は重要な役割を果たす。経営会議や全体会議、社内報などの冒頭で情報システム障害も含め事業継続に関するテーマを取り上げ、企業全体として再発防止を優先する姿勢を示すことが重要である。

経営層は情報システム障害を発生してしまったことの最終的な責任を持つことはいうまでもないが、障害を発生させないための予兆に対する注意も経営層の責任である。そのために小さな事故の情報収集ができるような施策を実行し、将来の重大な障害の可能性を察知しなければならない。情報の中から課題を拾い出し、課題解決の PDCA のサイクルをまわすことを実施し、解決がうまく進

んでいるかをレビューし、現状を把握しなければならない。

C．システム利用者の実施事項

＜評価指標 U1＞
Q37 障害に関して報告・記録の手順と、これを共有する仕組みを整えているか。
a. 事故及び障害の発生時に報告書を作成し、運用の責任者が承認しているか。
b. 報告書は、事故及び障害の状況、影響、原因を記載しているか。
c. 事故及び障害発生時にあらかじめ定めた連絡体制が機能しているか。
d. a,b,c を経営層等、情報システム関係者以外にも共有する仕組みがあるか。
Q38 障害に関して原因を客観的な方法により究明する手順を定めているか。
＜評価指標 U2＞
Q37 障害に関して報告・記録の手順と、これを共有する仕組みを整えているか。
a. 事故及び障害の発生時に報告書を作成し、運用の責任者が承認しているか。
b. 報告書は、事故及び障害の状況、影響、原因を記載しているか。
c. 事故及び障害発生時にあらかじめ定めた連絡体制が機能しているか。
d. 上記を経営層等、情報システム関係者以外にも共有する仕組みがあるか。
Q38 障害に関して原因を客観的な方法により究明する手順を定めているか。

情報システム利用者が取り組むべきことを述べる。

- 月例会議を開催し、障害に関する情報を共有し、情報システム提供者へ参画を要請すること。
- 重大な情報システム障害については個別に報告会を開催し、障害に関する情報を共有し、情報システム提供者へ参画を要請すること。
- 経営会議などで障害に関する情報を取り上げ、経営層で共有すること。
- 全体会議や社内報などで障害に関する情報を取り上げ、全社で共有すること。
- 障害情報を記録するための情報システム障害管理データベースを構築すること。
- 調査委員会により問題管理で記録された資料から障害を記述し、知識化すること。
- 情報システム障害管理データベースへ障害情報を記録すること。
- 情報システム障害管理データベースの利用を推進すること。
- 情報システム障害管理データベースの有効性をレビューし、必要なアクションをとること。
- 知識化された情報により、企画段階、開発段階、保守・運用段階の標準、基準、手順の改定を推進すること。
- 改定された標準、基準、手順の有効性をレビューし、必要なアクションをとること。
- 経営層は情報システム障害や事業の中断の重大度を鑑みて、情報公開を行うこと。

D．システム供給者への要求事項

＜評価指標 V1＞
Q41 利用者が障害に関する報告・記録の手順と、これを共有する仕組みを整えることを支援することを実施管理しているか。
a. 事故及び障害の発生時に報告書を作成し、運用の責任者が承認しているか。
b. 報告書は、事故及び障害の状況、影響、原因を記載しているか。
c. 事故及び障害発生時にあらかじめ定めた連絡体制が機能しているか。
d. a, b, c を経営層等、情報システム関係者以外にも共有する仕組みがあるか。
Q42 利用者が障害に関して原因を客観的な方法により究明する手順を定めることを支援することを実施管理しているか。
＜評価指標 V2＞
Q39 利用者が障害に関する報告・記録の手順と、これを共有する仕組みを整えることを支援しているか。あるいはその重要性を説明しているか。
a. 事故及び障害の発生時に報告書を作成し、運用の責任者が承認しているか。

b. 報告書は、事故及び障害の状況、影響、原因を記載しているか。
c. 事故及び障害発生時にあらかじめ定めた連絡体制が機能しているか。
d. a，b，c を経営層等、情報システム関係者以外にも共有する仕組みがあるか。
Q40 利用者が障害に関して原因を客観的な方法により究明する手順を定めることを支援しているか。あるいはその重要性を説明しているか。

情報システム供給者が取り組むべきことを述べる。

・ 情報システム利用者が開催する月例会議に参画し、障害に関する情報を共有すること。
・ 情報システム利用者が開催する重大な情報システム障害についての個別に報告会に参画し、障害に関する情報を共有すること。
・ 情報システム供給者の経営層は、利用者の経営層と面談し、障害に関する情報について認識を共有すること。
・ 情報システム障害管理データベースの構築を支援すること。
・ 調査委員会に参画すること。
・ 改定された標準、基準、手順に準拠してプロジェクトを進めること。

E．その他の留意事項

※IT コーディネータが注意すべきこと

この項の内容は、経営戦略フェーズの基本原則である「知の共有と成長の原則」に述べられている「知の共有・活用に立脚した経営をおこなうことにより、個人と組織の能力向上をはかり、経営改革を促進し、企業を成長発展させる」に実施するものである。経営層はリーダーシップをもってこの基本原則を実行しなければならない。

情報システム障害に関する情報を共有するために、経営層が具体的におこなうことは、データベースなどの共有のためのインフラや仕組みを整備することと、そこに情報を有効な形での蓄積と活用の推進ことである。

インフラや仕組みを整備するためには、プロジェクトを実行し、必要な人材や資金などの経営資源を割り当てる意思決定をしなければならない。また、活用の推進は、蓄積された情報を経営層の立場で活用してみることである。

また、情報システム障害や事業中断に対する企業責任の関連からは、経営層は「CSR(Corporate Social Responsibility:社会的責任)と継続企業の原則」に述べられている「企業は社会システムの一員であり、社会的に認められる存在でなければならない。企業の目的は、ステイクホルダーの価値を向上させることいであり、社会的価値を維持することが企業存続の条件である」の実行も必須である。経営層は「(2) 原因究明手順等の明確化」に基づいて究明された真実を情報公開しなければならない。自己弁護することなく、社会からコンプライアンスおよび企業倫理への背任があれば厳しく反省し、責任をもって改善計画の策定と実施を実行することが重要である。

（4）関連・類似システムの障害情報収集

A．ガイドライン原文

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。

＜実施例＞

情報システム障害管理データベースに、関連する情報システム障害を登録する。

B．本項目の必要性・重要性

原文で述べられているように他のシステムの障害の情報を収集し、そこから教訓を得ることができる情報システムの利用者および提供者は、この点において非常に成熟度の高い企業または組織と言える。障害管理データベースに障害情報を登録し管理することは、日常の運用の中で問題管理として実施される。ここでは単に障害情報を収集することだけではなく、そこから改善すべきことを発見し、経営戦略を実施し目標を実現するための改革を、具体的に推進する人材の育成や、それに対応することができる企業風土の醸成や社員への教育が重要である。さらに、これらの実現には、経営層が取組を企業理念として表明し、リーダーシップを持って進めていくことが最も重要なことである。

障害対応や事業継続の体制を構築するためには、この章で紹介している ITSMS や事業継続管理のフレームワークを参照または導入して、連絡体制などの社内体制や社内手続きを策定する。そして、これらを実行する専門職が不可欠である。この専門職は、社内外の過去の事故・障害事例を分析し、統計データなどに基づいて障害対応や事業継続計画を策定する。それには、重要業務の選定したり、複数箇所における複合事故、障害の同時発生や連鎖発生を想定したり、確かな知識と豊かな経験が求められる。

最初の段階では、組織全体が“問題に気づいている状態”になることが重要である。組織内の人に障害対応や事業継続の重要性や、各持ち場での対応について“問題意識”を持ってもらうために、研修や体験などの普及活動や啓発活動を展開する。次の段階では、引続き研修や訓練を重ねて行きます。組織内に障害対応や事業継続を率先する資質を持つ人材が浮上してきた場合、その人材を本人のキャリア・プランも含めて、専門職への育成を検討すべきである。多くの事例から障害対応や事業継続の推進には、このような資質やスキルが不可欠である。最終段階では、専門職として抽出された人材は、ITSMS 審査員や英国 BCI など専門資格を取得したり、業界団体などを通じて外部との交流をして、より専門性を高める。組織内の障害対応や事業継続に関わる戦略立案、研修や訓練の計画と実施などを、PDCA サイクルとして回す。組織全体については、引続き研修や訓練を続けることで、実行力をより高いレベルで向上させることができる。その際の重要なポイントは、組織内で発生したシステム障害や事業中断の事例やヒヤリ・ハットの分析を積極的に取組み、また他企業で発生したような事例であっても、自らの組織に反映することが重要である。

C．システム利用者の実施事項

＜評価指標 U1＞
Q39 障害に関する情報を収集し、活用することを実施管理しているか。
＜評価指標 U2＞
Q39 障害に関する情報を収集し、活用しているか。

情報システム利用者が取り組むべきことを述べる。

・ITSMS および事業継続管理(BCM)の専門職を設置すること。

（1） 専門職を専任する

（2） 組織文化の中への ITSMS および BCM の定着を実施する

（3） 達成状況を把握し、必要な措置を実施する

・組織文化の中への ITSMS および BCM の定着を実施すること。

（4） ITSMS および BCM への問題意識と訓練のレベルをアセスする

（5） 組織文化の中の ITSMS および BCM を開発する

（6） 定着のための活動を実施する

D．システム供給者への要求事項

＜評価指標 V1＞

Q43 障害に関する情報を収集し、活用することを実施管理しているか。

＜評価指標 V2＞

Q41 障害に関する情報を収集し、活用しているか。

情報システム供給者はなし。

E．その他の留意事項

※IT コーディネータが注意すべきこと

この項の「関連・類似システムの障害情報収集」で述べられているような「自らに直接関係のない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」がすぐに実現可能ではないことは明白である。

この章の前２項で説明したように、自社で発生した情報システム障害や事業継続に関わるインシデントから、本当の原因の発見やそこから学び取ったことを情報システム利用者全体で共有し、さらに情報システム供給者も含めて共有を目指すことが第一歩である。

この一連の活動は、ITC プロセスの基本となる SPDLI サイクルの D の結果を受けた L および I にあたり、自社で発生した障害や事業継続の危機への対応の中から、多くを学び、改革へ結びつける部分である。経営層はリーダーシップをこれに対して持って取り組み、この項の説明にもあるが、資質も持った人材を発掘し、専門職として育成していくことが重要である。また、全社的に問題意識を高めるための努力も継続的におこなうことも重要である。このような継続的な努力の結果、専門職を中心として、自らに直接関係のないシステムの障害を含めて、情報の収集を集め、その中から得た教訓を共有して、プロセス改革として、具体的に実現することができる。

BS25999-1 による事業継続管理では、この章の第一項で紹介したように、「事業継続管理の組織文化への浸透」を 1 つの大項目としている。そのために、「事業継続の問題意識と習熟のアセス」、「組織文化の中の事業継続の開発」、そして「文化の変化のモニタリング」の手順を規定している。また、ITSMS では、ITSMS の計画および導入、運用、管理を実現するため、役割を割り当てられたすべての人が、要求された職務を実施することを確実にするために、必要な網力を持つことが重要だと考えている。そのために、経営層は教育や訓練を実施させる責任がある。教育や訓練の内容は、すべての人が ITSMS の活動の意味と重要性を認識し、ITSMS の目的達成にどのような貢献ができるかを考え、実践するという動機になるようなものである。

このように、各リファレンスモデルでは、「自らに直接関係のない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」ということが自らおこなえるような成熟度が高い組織へ変化するため、問題意識や能力を継続的に高めることを要求しており、経営層の責任とリーダーシップを求めている。

ITC プロセスの「人間系、IT 系調和の原則」でいう「IT 化は経営戦略にのっとり、業務を遂行する人間系と、業務遂行に必要なサービスを提供する IT 系の調和によって具現化する」および「IT 化の成熟度の原則」でいう「IT 化の成熟度に見合った IT サービスの導入をはかる」、「業務プロセス改革並行実施の原則」でいう「業務プロセス改善は、「IT 化実行プロジェクト」での推進と、日常業務部門での推進を並行、協調して実施する」という基本原則と対応する部分と考えられる。

参考文献

１．佐藤允一『新版図解問題解決入門』ダイヤモンド社，2003 年
２．野中郁次郎，竹中弘高『知識創造企業』東洋経済新報社，1996 年
３．畑村洋太郎『失敗学のすすめ』講談社，2000 年
４．日本経営品質賞委員会『日本経営品質賞アセスメントガイドブック【2006 年度版】』2006 年
５．内閣府防災担当『事業継続ガイドライン　第一版』2005 年
６．経済産業省情報セキュリティ政策室『事業継続計画(BCP)策定ガイドライン』2005 年
７．経済産業省中小企業庁『中小企業 BCP 策定運用方針』2006 年
８．Business ContinuITy InstITute『GOOD PRACTICE GUIDELINES 2007 Section 1-6』2007
９．日本情報処理開発協会『ITSMS ユーザーズガイド』2007 年
１０．　National InstITute of Standards and Technology（情報処理推進機構訳）『IT システムにおける緊急時対応計画ガイド』2005 年

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

Ａ．ガイドライン原文

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。

Ｂ．本項目の必要性・重要性

本節では、システムライフサイクルプロセス全体を通しての横断的な留意事項が記述されている。以降、ここで記述されている５つの具体的な方策は、プロジェクトの成否を直接左右する重要な事項である。多くのステークホルダーが関与するプロジェクトにおいて、「共通の尺度」で「一貫した管理」が行えるようにするための共通的な基盤作りの重要性が述べられている。ついては、情報システム利用者、情報システム供給者ともに、本節を理解し、確実に実践していただきたい。

（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

Ａ．ガイドライン原文

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＞

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※等）を導入する。

※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。

Ｂ．本項目の必要性・重要性

一般的にプロジェクトマネジメントには様々な手法が存在する。そして、それらの多くは様々なプロジェクトの実践に基づく経験則によって培われるものである。したがって、経験則によるプロジェクトマネジメントも極めて有効な手法であるが、経験則のみによるプロジェクトマネジメントでは不十分である。経験則によるプロジェクトマネジメントの場合、どうしても個人差が生じてしまうからである。

そこで、経験則による個人差を吸収すべく、品質・コスト・進捗・リスク等のプロジェクトマネジメント項目に関して、関係するステークホルダーが共通の尺度でプロジェクトマネジメントを行えるように網羅的かつ定量的手法を取り入れながら開発されたのが、近代プロジェクトマネジメント手法である。近代的プロジェクトマネジメント手法は、1950 年代後半に米国防総省が大規模プロジェクトを管理するためにマネジメント手法を体系化したのが始まりとされる。その後、大学や研究機関等での研究を経て、現在ではアメリカの非営利団体ＰＭＩ(Project Management Institute)が、「PMBOK」としてまとめた知識体系が事実上の標準として世界中の様々な分野で広く受け入れられている。

ちなみに、実施例として記載されている「アーンドバリューマネジメント（EVM)」とは、「PMBOK」でも推奨している定量的なコスト及び進捗の管理手法の一つであり、プロジェクトのコストとスケジュールを「バリュー」という共通の尺度を使って一元的に管理できるという点で非常に有効なツールである。

他に、品質管理手法としての「ISO9000」や、リスク管理手法としての「PMBOK のリスク管理」等も近代的プロジェクトマネジメント手法の一つとして有効なツールである。

C．情報システム利用者の実施事項

＜評価指標 U1＞
Q40.　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を確立しているか。
Q41.　品質、コスト、進捗及びリスクに関し、定量的な測定方法を定めているか。
Q42.　Q41 に関連するデータを収集及び共有し、プロジェクト管理及び目標達成に向けた活動に活用しているか。
Q43.　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・支援体制を整備しているか。
＜評価指標 U2＞
Q40.　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を確立しているか。
Q41.　品質、コスト、進捗及びリスクに関し、定量的な測定方法を定めているか。
Q42.　Q41 に関連するデータを収集及び共有し、プロジェクト管理及び目標達成に向けた活動に活用しているか。

情報システム利用者が取り組むべきことを述べる。

- 情報システム供給者に対して、最適な「近代的プロジェクトマネジメント手法」を採用するように指示すること。
- プロジェクトマネジメントは、全て情報システム供給者任せにせず、主体的に実施すること。（例えば、情報システム供給者よりプロジェクトに係る進捗報告を定期的に受けるようし、進捗状況を確認し必要に応じて是正措置を講じる等）

D．情報システム供給者への要求事項

＜評価指標 V1＞
Q44.　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を確立しているか。
Q45.　品質、コスト、進捗及びリスクに関し、定量的な測定方法を定めているか。
Q46.　Q45 に関連するデータを収集及び共有し、プロジェクト管理及び目標達成に向けた活動に活用しているか。
Q47.　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・支援体制を整備しているか。
＜評価指標 V2＞
Q42.　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を確立しているか。
Q43.　品質、コスト、進捗及びリスクに関し、定量的な測定方法を定めているか。
Q44.　Q43 に関連するデータを収集及び共有し、プロジェクト管理及び目標達成に向けた活動に活用しているか。

情報システム供給者が取り組むべきことを述べる。

- 「PMBOK」若しくは、同等の一般に認められた考え方に基づく、近代的プロジェクトマネジメント手法を採用すること。
- 採用した近代的プロジェクトマネジメント手法に基づき、的確にプロジェクトを推進すると。
- 品質管理においては、「ISO9000」もしくは、同等の一般に認められた品質管理手法を採用すること。

E．その他の留意事項

※IT コーディネータが注意すべきこと
プロジェクトマネジメントの重要性については、「ITC プロセスガイドライン：第一部第一章」にて、10 ページを割いて、詳しく述べられている。ITC は、その内容を把握し、プロジェクトマネジメントの重要性を強く認識したうえで、情報システム利用者に対する啓蒙活動を積極的に行う必要がある。

（2）定量データを活用した管理

A．ガイドライン原文

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＞

テストに関する定量的な指標を活用し、品質目標の達成に向けた管理を行う。

B．本項目の必要性・重要性

情報システムの開発においては、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して、個々の指標に関する定量的な測定法を情報システム利用者及び情報システム供給者間で合意のうえ定め、データ収集を行い、目標達成に向けた管理を行うことが重要である。指標を使うことにより、以下のメリットが享受できるためである。

(a) 状況を数値で把握できる。

(b) 過去と比較できる。

(C) 基準と比較して状況の良悪を判断できる。

また、一般的に、プロジェクトの工程管理や品質管理ほど難しいものはない。この最大の原因は、各工程の仕上り具合を目に見える形で確認しづらいためである。定量的な指標を定めていないプロジェクトの場合、情報システムの仕上り具合がどのようなレベルにあるのか、適宜把握することは非常に難しい。特に泥沼状態に陥ってしまったプロジェクトの場合、そのプロジェクトの問題点すら把握できない。また、一見、優良そうに見えるプロジェクトにおいても実態をリアルタイムに把握できているわけではないため、あたかもスケジュールどおりに進捗しているように見えながら、結局、最後の段階で火を噴く、ということも往々にして発生してしまうのである。このような苦い経験を積んだ優秀なプロジェクトマネージャは、いかに定量的な評価指標の設定が必要かを経験から学び実践していくのである。

ちなみに実施例として記載されているテストに関する定量的な品質指標としては、主に以下のようなものがあるが、プロジェクトの特性や過去の類似プロジェクトを考慮して、適宜必要な指標を設定することが望ましい。

【参考】テストに関する定量的な品質指標の例

・テスト項目数（テスト密度）

・バグ密度

・バグ修正率

C．情報システム利用者の実施事項

＜評価指標 U1＞
Q40.　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を確立しているか。
Q41.　品質、コスト、進捗及びリスクに関し、定量的な測定方法を定めているか。
Q42.　Q41 に関連するデータを収集及び共有し、プロジェクト管理及び目標達成に向けた活動に活用しているか。
Q43.　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・支援体制を整備しているか。
＜評価指標 U2＞
Q40.　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を確立しているか。
Q41.　品質、コスト、進捗及びリスクに関し、定量的な測定方法を定めているか。
Q42.　Q41 に関連するデータを収集及び共有し、プロジェクト管理及び目標達成に向けた活動に活用しているか。

情報システム利用者が取り組むべきことを述べる。

・情報システム供給者が設定する品質指標の妥当性を確認すること。
・情報システム供給者が常に指標データを取得し、管理しているか確認すること。
・情報システム供給者から提示される実績データを適宜把握し、品質目標を達成しているかを確認すること。

D．情報システム供給者への要求事項

＜評価指標 V1＞
Q44.　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を確立しているか。
Q45.　品質、コスト、進捗及びリスクに関し、定量的な測定方法を定めているか。
Q46.　Q45 に関連するデータを収集及び共有し、プロジェクト管理及び目標達成に向けた活動に活用しているか。
Q47.　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・支援体制を整備しているか。
＜評価指標 V2＞
Q42.　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を確立しているか。
Q43.　品質、コスト、進捗及びリスクに関し、定量的な測定方法を定めているか。
Q44.　Q43 に関連するデータを収集及び共有し、プロジェクト管理及び目標達成に向けた活動に活用しているか。

情報システム供給者が取り組むべきことを述べる。

・あらかじめ品質指標を設定し、定量データを用いて品質管理を行うこと。
・各工程で設定した品質指標について、データ収集が確実に行われ、管理されていること。
・収集されたデータを分析し、絶えずフィードバックする仕組みが出来ていること。
・各工程終了時には、実績データ並びに、その分析結果の提出が行えること。

E．その他の留意事項

※IT コーディネータが注意すべきこと
　ITC は、情報システム利用者に対して、情報システム供給者が「定量データを活用した品質管理」を確実に行っているかを確認するように指導し、必要に応じて情報システム利用者をフォローする必要がある。　「ITC プロセスガイドライン」では、「第一部第三章　モニタリング＆コントロール」にて、広義の解釈で、この「定量データを活用した管理」の重要性を述べている。

（３）健全なプロジェクト運営に向けた活動の実施

Ａ．ガイドライン原文

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＞

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。

Ｂ．本項目の必要性・重要性

健全なプロジェクト運営を行うには、個々のプロジェクトへの支援環境の整備や恒常的な労働環境のモニタリングや改善等の活動を行うことが重要である。このことは、至極当たり前のことと思われるが、一旦プロジェクトの中に入ってしまうと客観的な目でモニタリング等が出来なくなることから、なかなか実践することは難しい。そこで、これを実現するための一つの手段として、最近実践されているのが、実施例にあるような「PMO の設置」である。それでは、何故、PMO のような個々のプロジェクトを横断的に支援する組織を別途設置することが必要なのか。

PMO を設置しない場合、往々にして以下のような問題点が発生してしまうためである。

(a)プロジェクト運営方法がばらばらで、経営層に状況が見えない。
(b)プロジェクトマネージャが雑用に追われていて、重要な意思決定に時間が使えない。
(c)同じような失敗がいくつものプロジェクトで起こってしまう。
(d)プロジェクト間でのリソース配分がうまくいっていない。

⇒これらの結果として、プロジェクトのスケジュール遅延、コスト超過等が発生し、健全なプロジェクト運用が困難になってしまう。

開発プロセスの標準化や開発ツールの整備等は開発マネジメント側の問題であるが、整備したプロセス等をいかに確実に実行させるか、というのはプロジェクトマネジメント側の問題である。その確実な実行のためには、プロジェクトレビュー、ファシリティマネジメント、チームマネジメント、リソースインテグレーション、リスクマネジメント等、様々なマネジメントが随所で必要であり、それらを専門的に推進するために PMO 等の組織的支援が必要不可欠なのである。つまり、各プロジェクトの成功率を高め、プロジェクト統合マネジメント力を一層高めるためにも、PMO を設置し、全体支援体制の強化を推し進めることが望ましい。

C．情報システム利用者の実施事項

＜評価指標 U1＞
Q40.　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を確立しているか。
Q41.　品質、コスト、進捗及びリスクに関し、定量的な測定方法を定めているか。
Q42.　Q41 に関連するデータを収集及び共有し、プロジェクト管理及び目標達成に向けた活動に活用しているか。
Q43.　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・支援体制を整備しているか。
＜評価指標 U2＞
Q40.　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を確立しているか。
Q41.　品質、コスト、進捗及びリスクに関し、定量的な測定方法を定めているか。
Q42.　Q41 に関連するデータを収集及び共有し、プロジェクト管理及び目標達成に向けた活動に活用しているか。

情報システム利用者が取り組むべきことを述べる。

・情報システム供給者における支援環境／支援体制が組織的に整備されているか確認すること。
・ＰＭＯによる審査活動報告をふまえ、必要に応じて適宜対応すること。

D．情報システム供給者への要求事項

＜評価指標 V1＞
Q44.　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を確立しているか。
Q45.　品質、コスト、進捗及びリスクに関し、定量的な測定方法を定めているか。
Q46.　Q45 に関連するデータを収集及び共有し、プロジェクト管理及び目標達成に向けた活動に活用しているか。
Q47.　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・支援体制を整備しているか。
＜評価指標 V2＞
Q42.　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を確立しているか。
Q43.　品質、コスト、進捗及びリスクに関し、定量的な測定方法を定めているか。
Q44.　Q43 に関連するデータを収集及び共有し、プロジェクト管理及び目標達成に向けた活動に活用しているか。

情報システム供給者が取り組むべきことを述べる。

・当該プロジェクトに対する支援環境／支援体制が組織的に整備されていること。
・ＰＭＯによるプロジェクトレビュー（チェック）が定期的に実施され、改善活動等も機能していること。

E．その他の留意事項

※IT コーディネータが注意すべきこと
ITC は、情報システム利用者に対して、情報システム供給者側に「組織的な支援環境・支援体制の整備」を要求し実現させるように指導する必要がある。また、情報システム利用者側にも情報システム供給者側の体制を評価できる仕組みを構築するように指導する必要がある。
例として挙げている PMO の採用は、PMO に「プロジェクトの妥当性評価とプロセス管理」といった役割を期待しているものであるため、PMO の策定したプロセスやポリシーに準拠してプロジェクトが推進されていない状況であれば、ITC としては、適宜是正を求め、健全に機能するよう指導する必要がある。

（４）第三者によるレビュー及び監査の実施

Ａ．ガイドライン原文

情報システム利用者及び情報システム供給者は、企画・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。

Ｂ．本項目の必要性・重要性

プロジェクトを滞りなく推進するためには、企画・開発及び保守・運用の各局面において、その信頼性・安全性を担保するために、客観的視点を持つ第三者（専門家、部門、企業・機関等）によるレビューおよびシステム監査等を受けることが重要である。それでは、何故、客観的視点を持つ第三者によるレビューやシステム監査等を受ける必要があるのか。

仮に、あるプロジェクトマネージャが「本プロジェクトは、企画・開発及び保守・運用段階全体における各局面において、プロジェクトマネジメントに万全を期しているので、第三者によるシステム監査を行う必要はない。」と考えていたとする。本当にそれで良いのだろうか。まさに、その「プロジェクトマネジメントに万全を期している」という状態そのものが、本当にそれで良いのかを客観的な立場で第三者的に点検・評価し、その結果で良否を判断するというのがシステム監査に他ならない。したがって、システム監査とは、マネジメント状態が良いから必要ない、悪いから必要、といった単純なものではなく、情報システムに関するプロジェクトにおいては原則実施すべきものなのである。その上で問題等が検出されれば問題の所在を明確にし、改善すべき点があれば改善勧告を出す等により、さらなるプロジェクトの健全化が期待できる。

一般的にシステム監査等の第三者チェックは、情報システムの開発等に関する直接的なマネジメントと異なり、それらの状況を客観的な立場で点検・評価するという間接的なマネジメントとして位置づけられる。複雑化する今日の情報化社会・IT 環境においては、むしろ直接的なマネジメントだけでは十分と言えず、間接的なマネジメントによりその不足分を補完するという傾向が強まってきている。

C．情報システム利用者の実施事項

＜評価指標 U1＞
Q44.　第三者（専門家、部門、企業・機関等）によるレビュー及びシステム監査等を行うことを実施管理しているか。
＜評価指標 U2＞
Q43.　第三者（専門家、部門、企業・機関等）によるレビュー及びシステム監査等が実施されているか。

情報システム利用者が取り組むべきことを述べる。

・ 情報システム供給者が実施する第三者レビューもしくは監査の報告を受け、情報システム供給者が善処している実態を確認すること。

D．情報システム供給者への要求事項

＜評価指標 V1＞
Q48.　第三者（専門家、部門、企業・機関等）によるレビュー及びシステム監査等が行われることを実施管理しているか。
＜評価指標 V2＞
Q45.　第三者（専門家、部門、企業・機関等）によるレビュー及びシステム監査等が実施されているか。

情報システム利用者が取り組むべきことを述べる。

・ 第三者（システム監査人等）による定期的なレビューもしくは監査を受け、改善勧告等に従い改善活動を実施すること。

E．その他の留意事項

【ITC の役割】

ITC は、IT システムに対する監査の重要性を認識し、情報システム利用者に対して、最適なシステム監査を実施するように指導する必要がある。なお、ITC としては、COBIT を標準として使いたいところではあるが、COBIT は網羅性が高い反面、個別要件への合致度は、必ずしも高くないので、対象企業の固有性、独自性を充分勘案した上で適用することが望ましい。また、近年の IT 環境は高度化／複雑化し、コンプライアンス要件も厳しさを増していること、大手企業の多くが日本版 SOX 法施行を視野に IT 統制／監査体制の見直しを行っていること、等の影響で監査に対するニーズが質的／量的にも年々拡大してきていることも留意しておく必要がある。

（５）仕様変更の取扱に関する利用者・供給者間での合意

Ａ．ガイドライン原文

情報システム利用者及び情報システム供給者は、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すること。

Ｂ．本項目の必要性・重要性

情報システムの開発においては、勿論、一旦仕様が固まったら完全に仕様を凍結させ、その後の仕様変更は一切認めない、というのが理想的である。ただし、実態としては、多かれ少なかれ何らかの変更が後になって必要になってくるものであり、どんなに時間をかけて最初の仕様を固めたからといって、「今後、仕様の変更が発生するはずがない」と考えるのは過ちである。したがって、どのようなプロジェクトであっても仕様を変更する際の取扱（仕様変更を行う場合の細かい手続きや費用分担等）について双方で合意し、契約書等で明文化しておくことが必要である。仮に、仕様変更に関する取扱が曖昧なままプロジェクトが進行してしまった場合、いざ仕様変更が発生した際、責任分界や費用分担等の面において確実にトラブルの素になると考えるべきである。

それでは、仕様変更に関する取扱だけを決めておけば、後は自由に仕様変更を認めてしまって良いのだろうか。特に、情報システム供給者は、情報システム利用者からの要求を何でも受け入れるのではなく、何故仕様の変更が必要か、仕様変更によりどのような効果があるのか、変更しなければどのような不都合があるのか、等を双方でよく吟味し、変更するか否かの最終決定を行う必要がある。また、仕様変更を決定した場合は、仕様変更に伴うリスクを確実に洗い出し、慎重に対応しなければならない。

また、往々にして、開発フェーズの後半、特に最終的なテスト工程において仕様上の欠点等が見つかり、仕様変更をせざるを得ないというケースが発生する。所謂、テストを行ってみて初めて明らかになった仕様上の不備というものである。この場合、仕様を変更する箇所は必要最小限に抑え、できるだけ影響箇所を小さくすべきである。特に、優秀なシステムエンジニアほど、ついでに他の関連箇所も直してしまおう、と思いがちであるが、常に全体品質の確保を最上位に考え変更する箇所を決めることが肝要である。

C．情報システム利用者の実施事項

＜評価指標 U1＞
Q45.　供給者とプロジェクト運営途中における仕様変更プロセスについて明確化し文書化することを実施管理しているか。
Q46.　Q45 の内容を利用者と供給者が合意した上で、利用者の適切な権限者の承認を確認することを実施管理しているか。　また、供給者の適切な権限者の承認を確認することを実施管理しているか。
＜評価指標 U2＞
Q44.　供給者とプロジェクト運営途中における仕様変更プロセスについて明確化し文書化しているか。
Q45.　Q44 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認しているか。　また、供給者の適切な権限者が承認していることを確認しているか。

情報システム利用者が取り組むべきことを述べる。

- 情報システム供給者との間で、プロジェクト運営途中における仕様変更プロセスについて、明確化されていること。
- 情報システム利用者主導で仕様変更を行う場合も、「変更記述書」相当を作成し、管理（変更管理/構成管理）すること。

D．情報システム供給者への要求事項

＜評価指標 V1＞
Q49.　利用者とプロジェクト運営途中における仕様変更プロセスについて明確化し文書化することを支援することを実施管理しているか。
Q50.　Q49 の内容を利用者と供給者が合意した上で、利用者の適切な権限者の承認を確認することを実施管理しているか。　また、供給者の適切な権限者が承認することを実施管理しているか。
＜評価指標 V2＞
Q46.　利用者とプロジェクト運営途中における仕様変更プロセスについて明確化し文書化しているか。
Q47.　Q46 の内容を利用者と供給者が合意した上で、利用者の適切な権限者が承認することを確認しているか。　また、供給者の適切な権限者が承認しているか。

情報システム利用者が取り組むべきことを述べる。

- 仕様変更を行う場合は、経緯・事由等を含む「変更記述書」相当を作成し、情報システム利用者の合意を得ること。
- 過去履歴を含めた変更管理台帳（データベース）を管理（変更管理/構成管理）すること。

E．その他の留意事項

※IT コーディネータが注意すべきこと
ITC は、情報システム利用者が情報システム供給者との間で締結された契約に基づく「変更管理」や「構成管理」を滞りなく行っているかを適宜確認することが必要である。

Ⅳ．技術に関する事項
（解説の対象外）

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・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

Ａ．ガイドライン原文

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・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。

Ｂ．本項目の必要性・重要性

本ガイドラインの第Ⅲ章、及び第Ⅳ章では、「情報システムのライフサイクルにおいて、個々の事象ごとになすべき事柄を、タイミング、内容、手段などの切口」で述べられてきたが、そこには具体的にその実行主体、即ち「人材・組織」について、深くは触れられていない。

そこで本第Ⅴ章において、その第１項では「人材」に関して、「人材育成・教育の実施」の観点から、第２項では「組織」に関して、「組織の整備」の観点から、掘り下げて述べられている。

情報システム利用者、並びに供給者ともに従来より各社其々に、独自の基準を設けて、情報システム要員の育成・教育の実施を行ってきている。しかし、一般常識的な入門レベルから個別専門的な上級レベルまで、組織的体系的に確立された形態で実施できているところは、稀といわざるを得ない。

情報システム供給者側は未だしも、「人的資産」が主要なコンピタンスであるがゆえに、ある程度確立されたものを持つのが一般的ではあるが、その育成・教育結果である「人材の持つスキル・レベル」を客観的に判断するのは難しい。　ましてや情報システム利用者側では、計画的継続的に運用するのは、いささか困難であろう。

しかしながら、情報システム利用者がその要求するところを、情報システム供給者に正しく伝え、且つ履行状況を正しく把握し、履行結果を正しく評価するには、情報システム利用者及び供給者が、同質の基盤で物事が判断できることが肝要と言える。

そのためになすべき人材育成・教育を、本項では解説している。

（１）人材の育成・教育

Ａ．ガイドライン原文

情報システム利用者と情報システム供給者は、情報処理技術者試験及び IT スキル標準等を活用し、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・開発、保守・運用及び管理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及び IT スキル標準等を活用し、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。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。

Ｂ．本項目の必要性・重要性

益々複雑化、細分化される情報システム分野において、一人の個人が習得できる技術領域には自ずと限界があるので、個々に最適なキャリアパスを設定して、それに沿った教育計画の下に、ある程度の期間を掛けて計画的に要員育成してゆくことが必要とされる。

IPA では、共通キャリア・スキルフレームワークの下で客観的な人材評価メカニズムを構築するため、情報処理技術者試験を抜本的に改定し、IT スキル標準、 組込みスキル標準、情報システムユーザースキル標準の各人材スキル標準との整合化を図り、同フレームワークを参照モデルとしてレベル判定の尺度に利用できるよう、新しい試験制度の具体的な設計を進めてきた。

平成２１年度春期試験から、すべての試験区分を新試験制度で実施される(注１)ことになるため、今後は客観的評価尺度としてのこれらの活用が有効となろう。

一般的に、利用者側企業で求められているのは、現場で責任を持ってプロジェクトを動かしていける「IT リーダ」である。「経営に資するシステム」「コスト削減」といった高い要求には、ベンダー任せや事業部門任せの人材では応えられない。

ところが、利用者側企業の IT 部門では、以下のような傾向にあるため、企業側の高い要求レベルとは大きなギャップが生まれている。

- IT に携わる各自の役割が不明確である。
- IT 組織の機能や役割と人材が合っていない。
- IT 部門のキャリアパスが不明確なため、モチベーションを維持できない。
- 経営者は IT 部門の能力に不満があり、IT 部門を高く評価していない。 等々

このような現象を放っておくと、次のような経営上の大きな問題を引き起こすことにつながる。

- 最適なビジネスモデルを構築できず、古い体質から抜け出せない。
- 最適なガバナンスが構築できず、毎回の監査で指摘されるという構図が当たり前になってしまう。
- 個人情報の漏洩、企業機密の漏洩などの「情報事故」を発生させる可能性が高い。

これらは、そもそも IT 人材の育成プロセスを描けない実情から、計画すら策定できないところからスタートしている。

自社の IT 組織に必要な人材構造を明確にすると共に、必要な役割と機能を定義し、IT 人材の教育計画の策定を進めなければならない。

「中長期的に有能な IT 人材を確保し、IT ガバナンスを確立するだけでなく、経営目的を実現するためのビジネスモデルを運営するための最適な IT を維持することができる」人材を育成してゆくことは、極めて重要な経営課題でもある。

反面、供給者企業の多くは、従来から IT スキル標準、情報システムユーザースキル標準などのフレームを活用してきている。

但し必要スキルに対する供給が追いつかず、慢性的に需給バランスの是正が課題となっているように思われる。

IT 人材の需要(利用)側と供給側との間には、スキルレベルの達成度で乖離が見られ、この乖離は特に顕著となっており問題視されている。この問題に対する取り組みを強化することが供給者にとって重要な課題である。

供給者にとっても共通キャリア・スキルフレームワークに連携した、情報処理技術者試験の抜本的改定は有利に働く。

スキルマップの棚卸しから、必要スキルモデルの再構成など、変革の契機となりうるので、計画的早期の要員育成をはかり、需給ギャップの解消に繋げられたい。

(注１)現行試験区分のうち初級システムアドミニストレータ試験については、平成２１年度春期試験まで継続実施される。

C．情報システム利用者の実施事項

＜評価指標 U1＞
Q47 人材の育成に向けた仕組みがあるか。
Q48 人員の育成計画が存在し実施されているか。

情報システム利用者側の経営者が取り組むべきことを述べる。

- 会社の経営方針の中に、情報システム部門に対する責務並びに求める人材像を明確にする。
- 情報システム部門には、求める人材を育成する仕組みを具備させる。
- さらに、その人材を育成する仕組みが有効に機能しているか、定期的に監査する仕組みを持つ。

D．情報システム供給者への要求事項

＜評価指標 V1＞
Q55 人材の育成に向けた仕組みがあるか。
Q56 人員の育成計画が存在し実施されているか。

情報システム供給者側の経営者が取り組むべきことを述べる。

- 会社の経営方針の中に、各部門の責務並びに、その要員に求める人材像を明確にする。
- 会社として、求める人材を育成する仕組みを具備させる。
- さらに、その人材を育成する仕組みが有効に機能しているか、定期的に監査する仕組みを

持つ。

E．その他の留意事項

※IT コーディネータが注意すべきこと
　IT コーディネータとしては、利用者と供給者の役割分担を明確に把握して、ギャップを埋める意味でも、利用者を代弁する形で供給者側に要求事項を伝えられることが肝要。
　人員の要求スキル等に関しても、RFP の中に織り込まれ伝えられることになるが、その意図するレベル感に差異を生じさせない配慮が必要である。
　供給者側の要員のスキルレベルを的確に把握して、配員ミスを起させない様、指導すべきである。
　また、一般的に利用者側企業では、IT 人材の育成計画が体系立ってなされ、全社的にマップ展開されているところは稀である。しかし、本件は「極めて重要な経営課題である」ことを充分経営者が理解し、率先して本課題に取り組まれるよう指導すべきである。

２．組織の整備

Ａ．ガイドライン原文

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・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。

Ｂ．本項目の必要性・重要性

前項では「信頼性・安全性の水準を満たす情報システムの企画・開発、保守・運用及び管理を遂行できる人材」の育成について解説したが、本項では「遂行できる組織」整備について述べられている。

個々の人材がばらばらに動いても目標が達成されることは困難であり、そこに統一された組織力が働いて、目標に近付くことが可能となる。そのための組織整備であるから、人材育成と対にしてバランスよく進めることが必要となる。

さらに、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与する組織には、「組織が有機的に機能しているか否かを、モニタリング＆コントロールする機能」が必要とされる。即ち組織的成熟度としては、４以上の高レベルが要求されることになる。そのためには、当該組織体が、正しく標準プロセスを遵守し、運営されていることを監査・監督できる体制も保有しなければならない。

（1）知識・スキルに応じた人材登用・配置

A．ガイドライン原文

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、適切な知識及びスキルを備えた人材のメンバ及びリーダ等への適切な登用及び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。

B．本項目の必要性・重要性

適材適所は、どのような組織体においても重要なことであるが、「人に起因する障害の防止」という切り口から言えば、仕組みとしての歯止め（次項にて解説）と言う対策のほかに、専門家の配置と言う人的対策も重要である。

必要な人材予測に基く個人の育成計画から、育成経緯を含めたスキルマップまでを情報として整理し蓄え、各種シミュレーションにも供せる状態に置くことは、期待される成果に対しての信頼性向上に役立つものである。

従来にも増して戦略性の高い情報システム構築が要求されている今日、しかしその一方では、情報システムの複雑化や IT 市場の多様化によって、専門技術も高度化され、日々進化している状況下では、情報システム利用者側企業としては、自社に必要な情報技術領域を見極め、それに応じた人材の確保に努めなければならない。

しばしば問題になるところの、「適切にベンダーを統制できない」、「選定や交渉が円滑に行えない」といった、ベンダー・マネジメント上の問題を抱える利用者側企業は、この点がないがしろにされていると言えよう。

人材のスキル領域を定める基準としては、IT スキル標準等を活用して、さらにそのスキルレベルを客観的に判断するために、情報処理技術者試験を活用するのは合理的な方法である。

適切な知識及びスキルを備えた人材を確保した上で、その最適配置を行い、利用者側企業として果たすべき役割分担を担いたい。

また、情報システム供給者側企業は、自社のコンピタンスに従って、そのカバーする情報システムのライフサイクルにおける領域を定めているが、先ずもってその領域を明示することによって、利用者側要求にミスマッチングな要員を割り振り、人に起因する障害を発生させる危険を、未然防止しなければならない。

更に利用者側要求に応じて最適要員を割り振る場合には、利用者側に要員のスキルレベルを的確に伝え、合意を得ることが必要である。そのためには、自社の要員を客観的判断基準で事前評定しておく必要があるので、スキル領域を IT スキル標準等を活用して定め、そのスキルレベルを情報処理技術者試験を活用して評定しておくことが望まれる。

C．情報システム利用者の実施事項

＜評価指標 U1／U2＞
Q49　人材の活用の仕組みがあるか。

a. 適切な知識及びスキルを備えた人材を確保しているか。
b. 適切な知識及びスキルを備えた人材のメンバ及びリーダ等への適切な登用及び配置を行っているか。

情報システム利用者側の経営者が取り組むべきことを述べる。

- 自社の情報システム部門に、情報システム部門が果たすべき責務を遂行するに足る人材を確保する。
- さらにその人材を最適に登用、配置させる。

D．情報システム供給者への要求事項

＜評価指標 V1＞
Q57　人材の活用の仕組みがあるか。
a. 適切な知識及びスキルを備えた人材を確保しているか。
b. 適切な知識及びスキルを備えた人材のメンバ及びリーダ等への適切な登用及び配置を行っているか。

情報システム供給者側の経営者が取り組むべきことを述べる。

- 顧客に対して、自社の果たすべき責務を遂行するに足る人材を確保する。
- さらにその人材を最適に登用、配置させる。

E．その他の留意事項

※IT コーディネータが注意すべきこと
情報システム利用者側企業は自社に必要な情報技術領域を見極め、それに応じた人材を必要な役割に配置しようとする。また、情報システム利用者側要求に応じて、供給者側企業は最大限努力して最適要員を割り振るが、それぞれ本当に適合しているか否かを、客観的に見極める必要がある。
IT コーディネータとしてはこの局面において、利用者側要件に必要なスキルレベルを見極め、配置された要員がその任に適うスキルを保有しているか、実地判断すべきである。
利用者側要員、供給者側要員ともに、インタビュー等を交えレベルを捕捉し、判断することが望ましい。

（２）独立した品質保証部門の設置

Ａ．ガイドライン原文

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。

Ｂ．本項目の必要性・重要性

開発サイクルの早い時期にエラーを取り除くことで節約できるコストは膨大である。逆に、システムが稼動してから不具合や利用者の不満に対処する消火型の対応では、利用者満足度は低下し、手戻り作業によるコストや工数は増大する一方である。最終的に品質問題は、システムのトータルコストと緊密に関係する。開発ライフサイクルの前工程であればあるほど、不具合１件あたりに要する対応コストは小さくなる傾向にあるため、システム構築の計画段階で利用者の視点に立った品質検証を行うための期間と予算を確保することが肝要である。

品質確保のための予算措置などが常態となるには、品質基準・開発標準・管理標準類等が体系立って整備されている必要がある。

品質検証の実現手段としては、自動テストツールや第三者検証機関の採用を検討し、ソフトウェア品質保証プロセスを確立する方法がある。その上で、社内で組織的に対応する品質監査部門や品質保証部門が設置されることが望ましい。過渡的手段としては、システム評価やソフトウェア品質の検証を専門の機関に委託することも多く行われるようになってきている。

一般企業において、情報システムの品質を確保するために、独立した組織を構成させるのはハードルが高い対応と考えられるが、中立な立場での品質評価は必須の事項であるため、何らかの体制は持つべきである。

通常、情報システム部門の管理セクションにて、各種基準類・標準類を維持管理されているが、過渡期においては、この部門が客観的に品質を管理する職掌を併せ持つことも、考えられる。　いずれにしても、品質基準・開発標準等で定められたプロセスを間違いなく履行することを徹底することから品質確保は始まるので、必須のプロセスとして考えるべきである。

さらにこのプロセスは、委託している情報システム供給者へのチェックも含まれる。委託契約において、品質担保の方法の妥当性確認や、履行状況のチェックは欠かしてはならないプロセスである。

情報システム供給者は、持ち得る品質の水準自体がその企業力と判断されるため、各社ともに力点が置かれ、高品質を保つ方策を採用している。

各種標準を整備し、管理部門としての品質保証部門を設置するのは、大手供給者では一般的と言える。

品質保証部門では、レビューの形でアプリケーションテストの実態等を監査し、形式チェックから内容チェックまで、証跡をベースに綿密に実施することが多い。この検査報告書の添付が、契約上の検収条件になっている場合も多く、実際的にも組織化された体制で対応しなければ、発注者側

利用者の要求に応えきれないものとも思われる。

C．情報システム利用者の実施事項

＜評価指標 U1／U2＞
Q50　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ているか。
Q51　契約の妥当性・遵守状況のチェック方法が確立しているか。
Q52　 Q50，Q51 により、チェックが実施されているか。

情報システム利用者側の経営者が取り組むべきことを述べる。

- 自社の情報システム部門の外部組織として、情報システム部門を監査する組織（監査部門の一組織等）を持つ。
- その監査部門の責務として、情報システムの品質基準・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。
- 更に、上記仕組みが確実に機能していることを、定期的に監査する。

D．情報システム供給者への要求事項

＜評価指標 V1＞
Q58　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ているか。
Q59　契約の妥当性・遵守状況のチェック方法が確立しているか。
Q60　Q58，Q59 により、チェックが実施されているか。

情報システム供給者側の経営者が取り組むべきことを述べる。

- 顧客対応を行う事業部門の外部組織として、事業部門の成果物品質、並びにそのプロセス品質を保証する組織（独立した品質管理部門が望ましい）を持つ。
- その品質保証部門の責務として、事業部門の品質基準・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。
- 更に、上記仕組みが確実に機能していることを、定期的に監査する。

E．その他の留意事項

※IT コーディネータが注意すべきこと
品質レベルと費用とは相関関係にあるので、アプリケーション要件(機能要件)を確定する段階で、充分抑えておくべき事項である。　必要以上の品質を求めることは、利用者側にも利益を損ねる場合があるので、最適レベルの品質を担保するために、利用者・供給者が実施すべき事柄を整理するのも、IT コーディネータの重要な役割である。
詳細な品質情報の開示を避けたがる情報システム供給者も多いため、品質を担保するデータの開示を契約上織り込むなどの配慮を、情報システム利用者にアドバイスすることも必要であろう。

（３）契約の妥当性・遵守状況のチェック体制の構築

Ａ．ガイドライン原文

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、社内法務部門による契約書レビューを行う。

Ｂ．本項目の必要性・重要性

企業では、毎年ソフトウェア調達に多額の投資を行っている。

利用者側とすれば、求める機能を備えた高品質のソフトウェアを、より安価に調達したいというニーズが高い反面、実際に完成したソフトウェアあるいは参画したＳＥに対しては、思い通りでないが故に不満の声は多い。これは調達に関する社内規定が整備されておらず、場当たり的に実施されている場合が多いからと思われる。　また、見積りの根拠も十分に確認しないまま発注するということも見受けられることから、情報システム利用者はソフトウェア調達のあり方を見直し、あるべき姿に変革していく必要がある。

契約の締結は、すべての信頼関係のベースとなる事柄であるにも拘らず、情報システム利用者側企業は、時間的な制約やノウハウの不足から、細かな交渉を十分に行わないまま契約締結を優先するケースが意外にも多い。

その結果、契約後に発生する不具合としては、追加費用の発生や料金見直しの制限などコストに関わることが主に発生する。

この様なリスクを回避するために、サービスの対象範囲、内容、価格、契約条件など多岐に及ぶ交渉すべきテーマを事前にしっかりと捉え、法律専門家の目も通して、事前に適切な交渉を行うことが肝要である。

法律専門家としては、社内法務部門がこの任を担うことが妥当と思われる。

但し、アウトソース契約の場合等の契約書には、サービス内容の詳細は示されないことが多い。そこで契約書の条文だけではなく、サービス内容と価格について詳細に示されるサービス仕様書や見積書などのドキュメントを包括的にチェックする必要がある。

そこで、一般的には法的判断を得意とする社内法務部門には、契約事項全般に関して、サービス内容と価格についての詳細は、情報システム要員が着実にチェックする体制を構築することが必要となる。

反対に情報システム供給者も、内容に不備な点のある契約を締結したが故に、予想以上の工数や費用が発生し、採算を悪化させたり、対応不能に陥ったりすることも起こりうる。

本項では、この様な場合における組織的対応策の一つとして、「社内法務部門」の採用を提案している。

情報システム供給者側企業には、情報システム関連取引専門の法務部隊もしくは、法律専門家を擁していることが一般的であるので、標準プロセスの取り決め事項などで、法務部門の関与を仕組みに取り込み、更に監視プロセスなども織り込んで運営することによって、リスクの少ない運用が可能である。

尚、契約締結には、供給者側企業の方が経験も豊富であるため、利用者に対して契約書において

は要点を網羅しつつも、条項や条文をできるだけ簡素化し、具体的なサービス内容などは、サービス仕様書などの参照先を設けて、契約書文面には契約管理上必要なことのみを記述する等の配慮を行うべきである。

C．情報システム利用者の実施事項

＜評価指標 U1／U2＞
Q50　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ているか。
Q51　契約の妥当性・遵守状況のチェック方法が確立しているか。
Q52　 Q50，Q51 により、チェックが実施されているか。

情報システム利用者側の経営者が取り組むべきことを述べる。

- 自社の情報システム部門が情報システム構築や運用等に係り、外部企業と交わす契約の妥当性・遵守状況のチェックを、法務部門がその責務として行う等の仕組みを確立させる。
- 更に、上記仕組みが確実に機能していることを、定期的に監査する。

D．情報システム供給者への要求事項

＜評価指標 V1＞
Q58　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ているか。
Q59　契約の妥当性・遵守状況のチェック方法が確立しているか。
Q60　Q58，Q59 により、チェックが実施されているか。

情報システム供給者側の経営者が取り組むべきことを述べる。

- 顧客対応を行う事業部門が顧客の情報システム構築や運用等に係り、顧客と交わす契約の妥当性・遵守状況のチェックを、法務部門がその責務として行う等の仕組みを確立させる。
- 更に、上記仕組みが確実に機能していることを、定期的に監査する。

E．その他の留意事項

※IT コーディネータが注意すべきこと
法務スペシャリストを置くことがまれな中堅中小にあっては、IT コーディネータはユーザ企業より、サービス内容を十分把握したうえで、供給者見積りの妥当性を確認することが求められるであろう。
往々にして契約時点においても、未だサービス内容が固まっていないことが多く、いくつかの見積り対象外の項目や見積り条件が必ず存在する。特に第一版の見積書においては、すべての要求が網羅的に反映されているわけではないと考えた方がよい。
IT コーディネータとしては、主観的な判断により対象や範囲が設定されていることもあるので、文面だけでは見通せない部分もあることから、いろいろな過去事例を踏まえ、本来検討しておくべき事柄の抜け落ちがないか、しっかりチェック出来ることが必要である。

Ⅵ. 商慣行・契約・法的要素に関する留意事項
（解説の対象外）

Ⅶ. 実効性に冠する担保措置
（解説の対象外）

Ⅷ. その他の関連事項
（解説の対象外）

A1. 用語の定義
（解説の対象外）