システム管理基準（骨子）

経済産業省

平成 30 年 4 月 20 日

前文(システム管理基準の活用にあたって)

システム管理基準は、平成 16 年のシステム監査基準の改訂において、それまでの「一般基準」、「実施基準」、「報告基準」で構成されるシステム監査基準の「実施基準」の主要部分を抜き出すとともに、当時の情報技術環境の進展を踏まえて修正・追加を行うことによって、システム監査基準の姉妹編として策定された。その主旨は、システム監査とシステム管理の実践規範を明確に切り分けることによって、システム監査実践の独立性・客観性を明確に位置づけるとともに、監査の効率的・効果的遂行を可能にする判断の尺度として有効活用されることを企図するものであった。

今回の改訂の主旨は、前回の改訂の後に生じた情報通信技術環境と情報化実践の大きな変化を踏まえて、さらに次の点を企図している。

第 1 に、大企業のみならず中小企業においても情報システム化戦略、情報システム化実践に関わる適切な自己診断及び監査実践を可能にすること。

第 2 に、情報システムにまつわるリスクを適切にコントロールしつつ、これまで以上に IT ガバナンスの実現に貢献すること。

本基準は、どのような組織体においても情報システムの管理において共通して留意すべき基本的事項を体系化・一般化したものである。したがって、本基準の適用においては、基準に則って網羅的に項目を適用するような利用法は有効ではない。事業目的、事業分野における特性、組織体の業種・業態特性、情報システム特性などに照らして、適切な項目の取捨選択や各項目における対応内容の修正、情報システムの管理に関連する他の基準やガイドから必要な項目を補完するなど、監査及び管理の主旨が実現できるように独自の管理基準を策定して適用することが望ましい。

なお、情報セキュリティの確保に焦点をおいて情報システムの監査・管理を実施する場合には、当基準でも情報セキュリティの確保に関連する最小限の項目で体系化しているが、それぞれの項目については、「情報セキュリティ管理基準（平成 28 年改正版」(経済産業省)等を活用して独自の管理基準を策定することが望ましい。

さらに、独自に策定する管理基準については、情報システムに影響を与える情報技術の発展動向、関連する法令や規範の制定・改定状況、情報システム管理プロセスの要員の知識と技能の蓄積度などに絶えず注意を払い、定期的に管理項目の追加・削除などの修正を行うことにより基準の有用性を高めることが必要である。

なお本基準では、「情報セキュリティ管理基準」における要求事項との対応関係の理解を容易にするために、「情報セキュリティ管理基準参照表」を付してある。これを参照して各企業のリスク特性を勘案して独自の管理基準の策定に利用されたい。

本基準で使用した用語は、JIS 及び ISO、その他の標準規格に可能な限り留意するとともに、本基準の理解を容易にするために、理解が困難であったり、意味の特定化が必要と思われたり、やや専門的であったりする基本用語については「用語説明表」として基準の末尾に収録している。適宜、参照されたい。

システム管理基準の枠組み

1. IT ガバナンスの定義

あらゆる組織は、顧客、従業員、取引先、投資家その他を含む、ステークホルダに対して価値を創出することが求められる。一方、IT(情報技術)は事業戦略に欠かせないものとなっており、IT によって実現される情報システムの巧拙が経営に大きな影響を及ぼすようになっている。

情報システムの企画、開発、保守、運用といったライフサイクルを管理するためのマネジメントプロセスが IT マネジメントであり、経営陣はステークホルダに対して IT マネジメントに関する説明責任を有する。

IT ガバナンスとは経営陣がステークホルダのニーズに基づき、組織の価値を高めるために実践する行動であり、情報システムのあるべき姿を示す情報システム戦略の策定及び実現に必要となる組織能力である。また、経営陣は IT ガバナンスを実践する上で、情報システムにまつわるリスク（以下「情報システムリスク」という。）だけでなく、予算や人材といった資源の配分や、情報システムから得られる効果の実現にも十分に留意する必要がある。

なお、今日では、クラウドサービスやアウトソーシング等、外部の資源を組み合わせる手法が一般化していることから、本基準では情報システムをハードウェア、ソフトウェア、ネットワークに加えて、外部のサービスや業務プロセスを含む概念として用いている。そのため、本基準における IT ガバナンスとは情報システムのガバナンスであり、IT マネジメントとは情報システムのマネジメントである。すでに IT ガバナンス及び IT マネジメントという用語が定着している事を反映して、本基準ではこれらの用語を用いている。

2. IT ガバナンスにおける EDM モデル

本ガイドラインでは、前節の IT ガバナンスの定義における経営陣の行動を、情報システムの企画、開発、保守、運用に関わる IT マネジメントとそのプロセスに対して、経営陣が評価し、指示し、モニタすることとする。また、IT ガバナンスにおける国際標準である ISO/IEC 38500 シリーズ及び日本での規格である JIS Q 38500 より、評価（Evaluate)、指示（Direct)、モニタ（Monitor）の頭文字をとって EDM モデルと呼ぶ。

- 評価とは、現在の情報システムと将来のあるべき姿を比較分析し、IT マネジメントに期待する効果と必要な資源、想定されるリスクを見積もることである。
- 指示とは、情報システム戦略を実現するために必要な責任と資源を組織へ割り当て、期待する効果の実現と想定されるリスクに対処するよう、IT マネジメントを導くことである。
- モニタとは、現在の情報システムについて、情報システム戦略で見積もった効果をどの程度満たしているか、割り当てた資源をどの程度使用しているか、及び、想定した

リスクの発現状況についての情報を得られるよう、IT マネジメントを整備すると共に、IT マネジメントの評価と指示のために必要な情報を収集することである。

3. IT ガバナンスにおける 6 つの原則

IT ガバナンスを成功に導くため、経営陣は、次の 6 つの原則を採用することが望ましい。

① 責任

役割に責任を負う人は、その役割を遂行する権限を持つ。

② 戦略

情報システム戦略は、情報システムの現在及び将来の能力を考慮して策定し、現在及び将来のニーズを満たす必要がある。

③ 取得

情報システムの導入は、短期・長期の両面で効果、リスク、資源のバランスが取れた意思決定に基づく必要がある。

④ パフォーマンス

情報システムは、現在及び将来のニーズを満たすサービスを提供する必要がある。

⑤ 適合

情報システムは、関連する全ての法律及び規制に適合する必要がある。

⑥ 人間行動

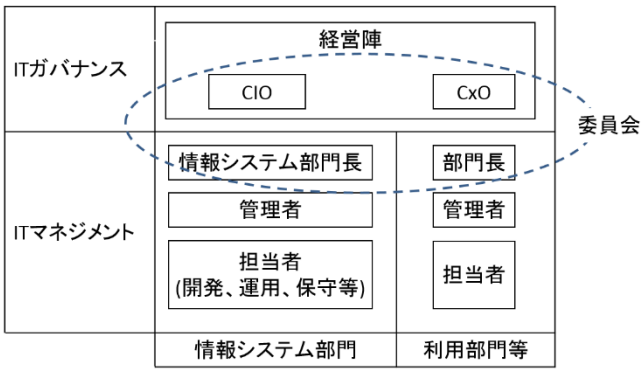
情報システムのパフォーマンスの維持に関わる人間の行動を尊重する必要がある。

4. システム管理基準の前提となる組織体制

本基準は判りやすく具体化したものとするために、モデル化した組織体制を前提とした記述となっている。

そのため、本基準を利用する際に、自らの組織に適合するように読み替える必要がある。

本基準が想定する組織体制を右図に示す。



本基準が想定する組織体制と、自らの組織への適合について以下に述べる。

(1) CIO

情報システムから価値を得るためには、IT に関する専門的知識が求められることから、経営陣は CIO を任命し、必要な権限を委譲する。そのため、CIO も経営陣に含まれる。

なお、小規模な組織、あるいは経営陣が十分な専門的知識を有している場合には CIO を任命しないことがある。その場合には、本基準において、CIO に関する記述は経営陣として読み替えることとなる。

(2) 委員会（情報システム戦略委員会，プロジェクト運営委員会等）

情報システム戦略の策定や大規模プロジェクト等では組織全体にまたがる利害関係者の調整が必要となる。経営陣は CIO を含む複数の CxO、あるいは後述する部門長を含む委員会を組成し、必要な権限を委譲する。そのため、委員会も経営陣の一部とする。

なお、小規模な組織、あるいは組織内の調整が容易な場合には、委員会を組成しないことがある。その場合には、本基準において、委員会に関する記述は経営陣として読み替えることとなる。

(3) 情報システム部門

IT マネジメントは経営陣の指示に従うと共に、経営陣によるモニタに必要な情報を提供する。

組織内で IT マネジメントを実施する体制を、本基準では、「情報システム部門」と呼ぶ。

情報システム部門は、情報システムに関する「企画」、「開発」、「保守」、「運用」を実施する「担当者」、及び担当者を管理する「管理者」、そして情報システム部門の長である「情報システム部門長」で構成される。

なお、組織によって、経営陣、あるいは CIO が情報システム部門長を兼務することがある。その場合には、本基準において、情報システム部門長に関する記述は経営陣あるいは CIO として読み替えることとなる。

また、小規模な組織では、「担当者」及び「管理者」が少数であり、情報システム部門長を任命しないことがある。その場合には、本基準における情報システムに関する記述は該当する管理者として読み替えることとなる。

(4) 利用部門等

組織内において、「情報システム部門」以外の体制を「利用部門等」と呼ぶ。

情報システム部門と同様、経営陣は必要に応じて CxO 及び「部門長」を任命し、必要な権限を委譲する。CxO あるいは部門長を任命しない場合には、情報システム部門と同様に、本基準の該当箇所を、経営陣、あるいは管理者として読み替えることとなる。

Ⅰ．IT ガバナンス

1．情報システム戦略の方針及び目標設定

(1) 経営陣は、情報システム戦略の方針及び目標の決定の手続を明確化していること。

(2) 経営陣は、経営戦略の方針に基づいて情報システム戦略の方針・目標設定及び情報システム化基本計画を策定し、適時に見直しを行っていること。

(3) 経営陣は、情報システムの企画、開発とともに生ずる組織及び業務の変革の方針を明確にし、方針に則って変革が行われていることを確認していること。

2．情報システム戦略遂行のための組織体制

(1) 経営陣は、CIO（Chief Information Officer）を任命すること。CIO は最高情報責任者 / 情報統括役員としての職務を担うこと。

(2) 経営陣は、情報戦略を統括する役割を明確に規定し、適切な権限及び責任の付与のもとに情報システム戦略委員会等を設置し、適切に機能させていること。

(3) 情報システム戦略委員会等は、組織における情報システムに関する活動全般について、モニタリングを実施し、必要に応じて是正措置を講じること。

(4) 情報システム戦略委員会等は、情報技術の動向に対応するため、技術採用指針を明確にしていること。

(5) 情報システム戦略委員会等は、活動内容を経営陣に報告していること。

(6) 情報システム戦略委員会等は、経営戦略の計画･実行･評価に関わる意思決定を支援するための情報を経営陣に提供していること。

3．情報システム部門の役割と体制

(1) 経営陣は、CIO の配下に情報システム部門をおき、情報システム部門の役割を明確にし、適切な権限及び責任を与えていること。

(2) 情報システム部門長は、経営陣の承認を得て、組織の規模及び特性に応じて、情報システム部門における職務の分離、専門化、権限付与、外部委託等を考慮した体制を構築していること。

4. 情報システム戦略の策定の評価・指示・モニタ

(1) 経営陣は、情報システム戦略の策定を情報システム戦略委員会等に、指示していること。

(2) 経営陣は、情報システム戦略について利害関係者の合意を得ることを指示していること。

(3) 経営陣は、情報システムで目指すべき情報システムの将来像を、中長期の情報システム化基本計画として明確にしていること。

(4) 経営陣は、経営計画で示した事業の方針及び目標に基づいて、情報システム戦略を評価していること。

(5) 経営陣は、情報システム戦略においてコンプライアンスを考慮することを指示していること。

(6) 経営陣は、情報システムの企画、開発及び運用、保守のための標準化の方針、並びに品質確保の方針を含めたルールを明確にすること。

(7) 経営陣は、個別の開発計画の優先順位及び順位付けのルールを明確にしていること。

(8) 経営陣は、情報システム戦略を関係者への周知徹底を指示することと、その結果をモニタすること。

(9) 経営陣は、情報システム戦略の実行状況について、定期的及び経営環境等の変化に対応して適時モニタリングを行い、必要なアクションをとること。

5. 情報システム投資の評価・指示・モニタ

(1) 経営陣は、情報システム投資計画を経営戦略との整合性を評価して策定すること。

(2) 情報システム投資計画の決定に際して、経営陣は、影響、効果、期間、実現性等の観点から複数の選択肢を評価すること。

(3) 経営陣は、情報化投資に関する予算を適切にモニタしていること。

(4) 経営陣は、情報システム投資の方針及び確保すべき経営資源を明確にすることと、その投資状況及び経営資源の状況をモニタリングしていること。

(5) 経営陣は、情報システム投資に関する投資効果の算出及びリスク算定の方法を明確にしていること。

(6) 経営陣は、情報システムの全体的な実績及び個別プロジェクトの実績を財務的な観点からモニタリングして、問題点に対して対策を講じること。

(7) 経営陣は、投資した費用が適正な使用であったかについてモニタリング及び評価をすること。

6. 情報システムの資源管理の評価・指示・モニタ

(1) 経営陣は、情報システムに関する資源管理の対象を明確にしていること。

(2) 経営陣は、情報資産に対する管理方針及び体制を明確にしていること。

(3) 経営陣は、情報システム戦略において外部資源の活用を考慮していること。

(4) 経営陣は、情報資産の効率的で有効な活用を指示し、その結果をモニタすること。

(5) 経営陣は、情報資産の共有化による生産性向上を考慮し、その結果をモニタすること。

(6) 経営陣は、人的資源に関する現在及び発展するニーズを考慮し、人間行動を尊重することを指示し、その結果をモニタすること。

(7) 経営陣は、情報技術に関する人的資源の現状及び必要とされる人材を明確にすること。

(8) 経営陣は、人的資源の調達及び育成の方針を明確にしていること。

7. コンプライアンスの評価・指示・モニタ

(1) 経営陣は、情報システムに関する法令及び規制の遵守のための管理体制を確立するとともに、管理者を定めていること。

(2) 経営陣は、情報システムに関して遵守すべき法令及び規範を識別し、関係者への教育及び周知徹底を指示し、その結果をモニタしていること。

(3) 経営陣は、情報倫理規程を定め、関係者への教育及び周知徹底を指示し、その結果をモニタしていること。

(4) 経営陣は、個人情報の取扱い、知的財産権の保護、外部へのデータ提供等に関する方針を定めて指示し、その結果をモニタしていること。

8. 情報セキュリティの評価・指示・モニタ

(1) 経営陣は、情報セキュリティの現在及び予想される環境変化を考慮し評価すること。

(2) 経営陣は、情報セキュリティの目的及び戦略を明確にして指示すること。

(3) 経営陣は、情報セキュリティ対策の有効性をモニタしていること。

9. リスクマネジメントの評価・指示・モニタ

(1) 経営陣は、情報システムリスクについて、情報システム戦略と情報システムに関わるリスクを管理する体制と役割を明確にしていること

(2) 経営陣は、情報資産に対するリスクの抽出とその対策についてモニタリングし、評価すること。

(3) 経営陣は、情報資産に対するリスクマネジメントの方針を明確に指示すること。

(4) 経営陣は、策定したリスクマネジメントの方針を、関係各部門への周知徹底を指示することと、その結果をモニタすること。

10. 事業継続管理の評価・指示・モニタ

(1) 経営陣は、情報戦略及び情報システムに関連した事業継続の方針を策定していること。

(2) 事業継続計画は、利害関係者を含んだ組織的体制で立案し、経営陣が評価して承認していること。

(3) 経営陣は、事業継続計画を、関係各部門への周知徹底を指示することと、その結果をモニタすること。

Ⅱ.企画フェーズ

1. プロジェクト計画の管理

(1) 経営陣は、プロジェクト運営委員会を設置すること。

(2) プロジェクト運営委員会は、プロジェクトマネージャ(PM)を任命すること。

(3) PM は、プロジェクト計画を策定し、プロジェクト運営委員会の承認を得ること。

(4) PM は、要件定義に必要な体制を確保すること。

2. 要件定義の管理

(1) プロジェクト運営委員会は、要件定義の作業内容を定めるよう PM に指示すること。

(2) PM は、利害関係者の要求を収集・分析・調整すること。

(3) プロジェクト運営委員会は、優先順位付けの適切性を検証すること。

(4) PM は、開発方針を策定すること。

(5) PM は、プロジェクトのリスクを分析し、対策を検討すること。

(6) PM は、要件定義書を作成し、プロジェクト運営委員会の承認を得ること。

3. 調達の管理

(1) プロジェクト運営委員会は、システムにかかる調達方法を明確にするよう PM に指示すること。

(2) PM は、プロジェクト計画に基づき、調達の要求事項を作成すること。

Ⅲ．開発フェーズ

1. 開発ルールの管理

(1) 情報システム部門長は、事前にシステム開発部署とシステム運用部署の責任を分離すること。

(2) PM は、プロジェクト標準を策定し、文書化し、プロジェクト運営委員会の承認を得ること。

2. 基本設計の管理

(1) PM は、基本設計を作成し、文書化すること。

(2) プロジェクト運営委員会は、基本設計を承認すること。

3. 詳細設計の管理

(1) PM は、詳細設計を作成し、文書化すること。

(2) PM は、テストの要件を検討すること。

(3) プロジェクト運営委員会は、詳細設計を承認すること。

4. 実装の管理

(1) PM は、プロジェクト計画、プロジェクト標準に従い、プログラミング及び実装を実施すること。

(2) PM は、単体テスト計画を作成し、単体テストを実施すること。

5. システムテスト（総合テスト）の管理

(1) PM は、システムテスト計画を作成し、文書化すること。

(2) プロジェクト運営委員会は、システムテスト計画を承認すること。

(3) PM は、情報システム部門に、システムテスト環境を準備させること。

(4) PM は、システムテストの状況を収集し、結果を評価し、文書化すること。

(5) プロジェクト運営委員会は、システムテストの結果を承認すること。

6. ユーザ受入テストの管理

(1) PM は、ユーザ受入テスト計画を作成すること。

(2) プロジェクト運営委員会は、ユーザ受入テスト計画を承認すること。

(3) システム部門は、ユーザ受入テスト環境を準備すること。

(4) PM は、ユーザ受入テストを実施し、経過を報告し、結果を文書化すること。

(5) プロジェクト運営委員会は、ユーザ受入テストの結果を承認すること。

7. 移行の管理

(1) PM は、移行計画を作成し、文書化すること。

(2) プロジェクト運営委員会は、移行計画を承認すること。

(3) プロジェクト運営委員会は、移行結果を承認すること。

8. プロジェクト管理

(1) PM は、プロジェクトの進捗をモニタリングする手法を定義すること。

(2) PM は、プロジェクトの進捗管理を継続的に実施すること。

(3) PM は、プロジェクトのリスクを管理すること。

(4) プロジェクト運営委員会は、プロジェクト終了時にレビューを実施すること。

9. 品質管理

(1) CIO は、開発・運用で求められる品質目標を定めること。

(2) CIO は、品質管理に責任と権限を明確にすること。

(3) CIO は、品質維持・向上に関する活動を周知すること。

Ⅳ. アジャイル開発

従来のウォーターフォール型の開発だけでなく、アジャイル開発による開発手法も増加しており、その必要性に鑑みて、従来の取扱いに加えて、特にアジャイル開発において留意するべき取扱いについて示すものである。

1. アジャイル開発の概要

(1) 利用部門と情報システム部門・ビジネス部門が一体となったチームによって開発を実施すること。

(2) アジャイル開発では、反復開発を実施すること。

2. アジャイル開発に関係する人材の役割

(1) プロダクトオーナーは、開発目的を達成するために必要な権限を持つこと。

(2) 開発チームは、複合的な技能と、それを発揮する主体性を持つこと。

3. アジャイル開発のプロセス（反復開発）

(1) プロダクトオーナーと開発チームは、反復開発によって、ユーザが利用可能な状態の情報システムを継続的にリリースすること。

(2) プロダクトオーナーと開発チームは、反復開発を開始する前にリリース計画を策定すること。

(3) プロダクトオーナー及び開発チームは、緊密なコミュニケーションの構築ためのミーティングを実施すること。

(4) プロダクトオーナー及び開発チームは、イテレーション毎に情報システム、及びその開発プロセスを評価すること。

(5) プロダクトオーナー及び開発チームは、利害関係者へのデモンストレーションを実施すること。

Ⅴ．運用・利用フェーズ

所定の運用環境で、情報システム及びソフトウェア製品を運用し、情報システム及びソフトウェア製品の利用部門への支援を運用管理者が提供するフェーズである。運用管理手順書は、開発管理者より引継ぎを受けて、運用管理者及び情報システム部門長が承認している。その際、リスクの高い情報システムについては、運用部門と開発部門等との職務が分離されていることを確認する。但し、開発部門と運用部門等が協働してソフトウェアのリリースを迅速かつ頻繁に、あるいは反復的･継続的に実施する方法等を駆使する場合は、各部門は各々の職務遂行について常に情報を共有し、意思疎通及び相互チェックが可能な仕組みを確立して、透明性を実現する。

運用・利用フェーズで情報システムの運用を円滑に行うための活動には、情報システム運用部門が主体となる活動に限らず、情報システムの利用部門が主体となる活動を含む。

1. 運用管理ルール

(1) 運用管理者は、運用管理ルールを、開発フェーズで作成した運用設計に基づいて作成すること。

(2) 情報システム部門長は、運用管理ルールを承認すること。

(3) 運用管理者は、運用手順を承認すること。

(4) 運用管理者は、作業手順を標準化し、明文化すること。

2. 運用管理

(1) 運用管理者は、年間運用計画を策定すること。

(2) 運用管理者は、年間運用計画に基づいて、月次、週次、日次等の運用計画を策定すること。

(3) 運用管理者は、運用管理ルールの遵守状況を確認すること。

(4) 運用管理者は、ジョブスケジュールを、業務処理の優先度を考慮して設定すること。

(5) 運用管理者は、例外処理のオペレーションを、運用管理ルールに基づいて行うこと。

(6) 運用管理者は、運用管理ルールに基づいてオペレータの交代を行うこと。

(7) 運用管理者は、指示書とオペレーション実施記録の差異分析を実施すること。

(8) 運用管理者は、オペレーション実施記録を、運用管理ルールに基づいて一定期間保管すること。

(9) 運用管理者は、利用部門の情報システム利用を支援すること。

(10) 運用管理者は、情報システムの稼動実績を把握し、性能管理、リソース管理、及び資源の有効活用を図ること。

3. 情報セキュリティ管理

3. 1 情報セキュリティ管理ルール

(1) 運用管理者は、組織の情報セキュリティ方針に基づいて運用の情報セキュリティ管理ルールを作成し、遵守状況を確認すること。

(2) 運用管理者は、サイバー攻撃への対処策を作成し、有効性を保つこと。

(3) 上記以外の情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

3. 2 アクセス管理

(1) 運用管理者は、情報セキュリティ方針に基づいて、運用システムへのアクセス管理ルールを作成し、情報システム部門長の承認を得て、適切に運用すること。

(2) 運用管理者は、データへのアクセスコントロール及びモニタリングを、実施すること。

(3) 上記以外のアクセス管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

4. データ管理

(1) 運用管理者は、データ管理ルールを定め、遵守状況を確認すること。

(2) 運用管理者は、データの知的財産権を、管理すること。

(3) 運用管理者は、データのインテグリティ（完全性）を、維持すること。

(4) 運用管理者は、データの利用状況を記録し、定期的に分析すること。

(5) 運用管理者は、データのバックアップの範囲、方法及びタイミングを、業務内容、処理形態及びリカバリの方法を考慮して決定すること。

(6) 運用管理者は、データのバックアップの処理単位をデータ構造に基づいて定めること。

(7) 運用管理者は、データの授受、保管、確認及び返却を、データ管理ルールに基づいて行わせること。

(8) 運用管理者は、データの交換の形態に応じた、不正防止及び機密保護の対策を講じること。

(9) 運用管理者は、データの保管、複写及び廃棄に、誤びゅう防止、不正防止及び機密保護の対策を講じること。

(10) 利用部門の管理者は、データの入力管理ルールを作成し、遵守状況を管理すること。

(11) 利用部門の管理者は、出力管理ルールを作成し、遵守状況を管理すること。

(12) データ管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

5. ログ管理

(1) 運用管理者は、ログを取得し、定期的に分析すること。

(2) 運用管理者は、情報セキュリティ方針に基づいて、適切なツールを利用するなどして、全てのログを一元管理し、即時に分析して、可及的速やかにセキュリティインシデントの予兆や痕跡を取得し、対策を講じること。

(3) ログ管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

6. 構成管理

6. 1 機器の構成管理

(1) 運用管理者は、構成管理ルールを作成し、遵守状況を確認すること。

(2) 運用管理者は、管理するソフトウェア、ハードウェア及びネットワークを明確にして管理すること。

(3) 運用管理者は、ソフトウェア、ハードウェア及びネットワークの構成、調達先、サポート条件等を明確にした管理台帳を作成して構成を管理すること。

(4) 運用管理者は、ソフトウェア、ハードウェア及びネットワークの導入及び変更について、影響を受ける範囲を検討して決定すること。

(5) 運用管理者は、ソフトウェア、ハードウェア及びネットワークの導入及び変更について、計画を作成して実施すること。

(6) 機器の構成管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

6.2 ハードウェア管理

(1) 運用管理者は、ハードウェア管理ルールを作成し、遵守状況を確認すること。

(2) 運用管理者は、ハードウェアの保管、移設及び廃棄の際の、不正防止及び機密保護の対策を講じること。

(3) 運用管理者は、ハードウェアを、想定されるリスクに対応できる環境に設置すること。

(4) 運用管理者は、ハードウェアの、定期的保守を行うこと。

(5) 運用管理者は、ハードウェアの障害対策を講じること。

(6) 運用管理者は、ハードウェアの利用状況を記録し、定期的に分析して改善を図ること。

(7) ハードウェア管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

6.3 ネットワーク管理

(1) ネットワークの管理者は、ネットワーク管理ルールを定め、遵守状況を確認すること。

(2) ネットワークの管理者は、ネットワークを利用した外部サービスを、ネットワーク管理ルールに基づいて管理すること。

(3) ネットワークの管理者は、ネットワークへのアクセスコントロール及びモニタリングを実施すること。

(4) ネットワークの管理者は、ネットワーク監視ログを定期的に分析すること。

(5) ネットワークの管理者は、ネットワークの障害対策を講じること。

(6) ネットワークの管理者は、ネットワークの利用状況を記録し、定期的に分析すること。

(7) ネットワーク管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

7. ファシリティ管理

(1) ファシリティの管理者は、建物及び関連設備を、想定されるリスクに対応できる環境に設置すること。

(2) ファシリティの管理者は、建物及び室への入退の管理について、不正防止及び機密保護の対策を講じること。

(3) ファシリティの管理者は、関連設備について、適切な運用を行うこと。

(4) ファシリティの管理者は、関連設備について、定期的に保守を行うこと。

(5) ファシリティの管理者は、関連設備について、障害対策を講じること。

(6) ファシリティの管理者は、建物及び室への入館及び入室を記録し、定期的に分析すること。

(7) ファシリティ管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

8. サービスレベル管理

(1) 運用管理者は、提供するサービスについて、サービスの要求事項に基づいて実行可能

なサービスメニューを作成し、実施すること。

(2) 利用部門の管理者は、定期的にサービスをレビューし、変更を管理すること。

(3) 運用管理者は、サービスを継続的に改善すること。

9. インシデント管理

9. 1 インシデント対応の管理

(1) 運用管理者は、すべてのインシデントを、優先度をつけて、またインシデント管理手順を用いて、効率的かつ効果的に体系的な管理をすること。

(2) 運用管理者は、インシデントのエスカレーションの手続を定めること。

(3) 運用管理者は、インシデントの終了の手続を定めること。

(4) 運用管理者は、重大なインシデントを専用に取り扱うための手順を文書化すること。

(5) 運用管理者は、インシデント管理プロセスの体系的な記録を作成し、報告すること。

(6) 運用管理者は、インシデント管理プロセスで必要となる要員と、その権限及び責任を適切に割り当てること。

(7) 利用部門の管理者は、インシデント発生後可能な限り早く、インシデント対応の優先度を運用管理者と合意すること。

(8) 利用部門の管理者は、インシデントの終了を判断すること。

(9) インシデント管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

9. 2 問題管理

運用管理者は、問題を識別し、問題管理手順を整備して問題を適切に管理し、再発防止の措置を講じること。

9. 3 変更管理

(1) 運用管理者は、変更計画を作成して変更を適切に管理すること。

(2) 利用部門の管理者は、変更管理を情報システム運用部門と合意し、変更を適切に管理すること。

9. 4 リリース管理

運用管理者は、リリース計画を策定し、リリース管理手順を作成してリリースを適切に管理すること。

10. サービスデスク管理

(1) 運用管理者は、情報システム運用部門と利用部門とをつなぐ単一窓口(SPOC : Single Point of Contact)のサービスデスクを設置すること。

(2) サービスデスクは、利用部門からの問合せ及び対応を記録し、レビューし、文書化すること。

(3) 利用部門は、情報システム運用部門への連絡にサービスデスクを活用すること。

Ⅵ. 保守フェーズ

1. 保守ルール

(1)情報システム部門長は、保守フェーズにおける保守対象を明確にすること。

(2) 情報システム部門長は、保守を実施する体制とその役割を明確にすること。

(3) 保守管理者は、自社開発ソフトの保守に必要な開発の成果物を、開発フェーズから引き継ぐこと。

(4)保守管理者は、保守フェーズ全体の基本的枠組みをまとめた「保守手順書」を作成し、最新状態に維持すること。

(5) 保守管理者は、「保守手順書」の基本手順を詳細化した「保守作業マニュアル」を作成し、最新状態に維持すること。

2. 保守計画

(1) 保守管理者は、保守依頼部門管理者から提出された保守依頼の内容について確認、調査及び分析を行うこと。

(2) 保守管理者は、保守依頼に対してソフトウェアの修正を実施するかどうかを決定すること。

(3) 保守管理者は、修正を実施することを決定した場合、保守フェーズに従うのか、開発フェーズに従うのかを決定すること。

(4) 保守管理者は、修正を実施することを決定した場合、「修正計画」を作成すること。

(5) 保守管理者は、「修正計画」を承認するとともに、保守依頼部門管理者の了解を得ること。

(6) 保守依頼部門管理者は、修正されたソフトウェアの「受入計画」を作成すること。

3. 情報セキュリティ管理

(1) 保守管理者は、外部調達ソフトに関するぜい弱性情報及び修正コード情報の収集に努めること。

(2) 保守管理者は、収集したぜい弱性情報及び修正コード情報について、自社システム環境への適用の必要性を調査・分析し、適用の是非を決定すること。

(3) 保守管理者は、OS などの自動適用可能なソフトウェアの修正コードについて、適用方針を決め確実な適用を行うこと。

(4) 保守管理者は、コンピュータウイルス対策ソフトウェア（以下「ウイルス対策ソフト」という。）及びパターン定義ファイル（以下「パターンファイル」という。）の更新の適用を実施すること。

(5) 上記以外の情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

4. 変更管理

保守管理者は、仕様変更に伴うソフトウェアの修正に対応すること。

5. 保守の実施

(1) 保守管理者は、「修正計画」を再確認し、必要であれば詳細化すること。

(2) 保守管理者は、「修正計画」に従って修正作業を実施し、実施状況を管理すること。

(3) 保守管理者は、「修正計画」に従って、修正したソフトウェアのテストを実施すること。

(4) 保守管理者は、ソフトウェアの修正に伴って関連するドキュメントの修正が必要かどうかを調査し、必要なドキュメントの修正を行うこと。

(5) 保守管理者は、修正実施結果、テスト結果、最終的な修正内容、及びドキュメント修正内容を承認すること。

(6) 保守依頼部門管理者は、「受入計画」に従って、修正されたソフトウェアの受入テストを実施すること。

(7) 保守依頼部門管理者は、受入を決定したソフトウェアの修正について、運用管理者に本番システム環境へのリリースを依頼する。

6. ソフトウェア構成管理

(1) 保守管理者は、ソフトウェア構成管理として管理する項目を決定すること。

(2) 保守管理者は、ソフトウェア構成管理実施体制を確立すること。

(3) 保守管理者は、ソフトウェア構成管理の実施手順を定めること。

(4) 保守管理者は、本番システムで使用しているソフトウェアについて、修正コードの本番システム環境へのリリース履歴を管理すること。

(5) 保守管理者は、ソフトウェアのバージョンアップを行った場合における、ソフトウェアの旧バージョンの扱いを明確にすること。

(6) ソフトウェア構成管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

7. ライフサイクル管理

(1) 保守管理者は、外部調達ソフトについて、ソフトウェアメーカのバージョンアップ計画、サポート計画に関する情報を収集すること。

(2) 保守管理者は、(1)で収集した情報に基づいて、自社における外部調達ソフトの保守計画を作成すること。

(3) 保守管理者は、外部調達ソフトの保守計画に従って保守を実施し、実施結果を記録すること。

(4) 保守管理者は、バージョンアップや他のソフトウェアへの移行を行った後の旧ソフトウェアの廃棄計画を立て、廃棄を行い、記録を残すこと。

Ⅶ. 外部サービス管理

1. 外部サービス利用計画

(1) 外部委託元部門長は、情報システム戦略計画にもとづき、外部サービス利用計画を策定し、情報システム戦略委員会が承認すること。

(2) 外部委託元部門長は、外部サービス利用計画で、目的、対象範囲、予算、体制等を明確にすること。

2. 委託先選定

(1) 外部委託元部門長は、委託先の選定基準を明確にすること。

(2) 外部委託元管理者は、委託候補先に対して必要な要求仕様を提示し、その内容を合意すること。

(3) 外部委託元管理者は、可能な限り、複数の候補先が提示した提案内容の比較検討を行ったうえで、委託先を選定すること。

3. 契約と管理

3. 1 契約

(1) 外部委託元管理者は、「外部サービス利用計画」に基づき、契約を締結すること。

(2) 外部委託等契約書には、必要な事項を盛り込むこと。

(3) 契約締結後の委託業務内容に追加及び変更が生じた場合、外部委託元管理者は契約内容の再検討を行うこと。

(4) システム監査に関する方針を明確にすること。

3. 2 委託先管理

(1) 外部委託元管理者は、委託業務の実施内容が、契約内容と一致することを確認すること。

(2) 外部委託元管理者は、契約に基づき、必要な要求仕様、データ、資料等を提供すること。

(3) 外部委託元管理者は、契約に基づき、委託先より業務報告書に基づく報告を定期的に受けていること。

(4) 外部委託元管理者は、業務報告書の内容を分析・評価し、必要な対策を講ずること。

(5) 外部委託元管理者は、情報システム戦略委員会で定めた「委託先に対する立入監査又はモニタリングの実施対象の選定基準」に該当する場合、立入監査又はモニタリングを実施すること。

(6) 委託業務において事故等が発生した場合は、外部委託元管理者は、委託先に対して速やかに報告を求めること。

(7) サービスや成果物の検収は、契約に基づいて外部委託元管理者が実施し、検収結果は外部委託元部門長が承認すること。

(8) 外部委託元管理者は、業務終了後、委託業務で提供したデータ、資料等の回収及び廃棄の確認を行うこと。

(9) 外部委託元管理者は、外部委託終了後、委託業務の結果について、評価すること。

(10) 外部委託元管理者は、労働者派遣法等関連法規を遵守して、委託先の管理を行うこと。

4. サービスレベル管理(SLM)

(1) 外部委託元管理者は、サービスの品質を維持するために、外部委託契約に SLA (Service Level Agreement：サービスレベル合意）の締結を検討すること。

(2) SLA 締結の場合は、外部委託元管理者は必要な事項を盛り込むとともに、外部委託元部門長の承認を得ていること。

(3) 外部委託元管理者は、外部委託業務が SLA を満たしているかを定期的に確認し、その結果を外部委託元部門長に報告すること。

(4) 外部委託元管理者は、サービスレベル未達成の場合に備え、リソース増強や代替手段の適用など具体的な対応方法を検討していること。

(5) 外部委託元管理者は、委託業務内容に変更が生じた場合は、必要に応じて SLA の内容の見直しを行うこと。

Ⅷ. 事業継続管理

IT ガバナンス及び情報システム戦略委員会の方針に基づく。

1. リスクアセスメント

(1) 情報システム部門長は、自然災害等のリスク及び情報システムに与える影響範囲を明確にすること。

(2) 情報システム部門長は、情報システムの停止等により組織体が被る損失を分析すること。

(3) 情報システム部門長は、業務の復旧許容時間及び復旧優先順位を定めること。

2. 業務継続計画の管理

(1) 情報システム部門長は、リスクアセスメントの結果に基づき、経営陣が定めた事業継続計画と整合を取った情報システムの業務継続計画を策定すること。

(2) 情報システム部門長は、情報システムに係る災害及び重大事故発生時に対応した業務継続計画を作成し、承認を得ること。

(3) 情報システム部門長は、情報システムに係る業務継続計画の実現可能性を確保すること。

(4) 情報システム部門長は、業務継続計画の中で、従業員の教育訓練及びリスクコミュニケーションの方針を明確にすること。

(5) 情報システム部門長は、業務継続計画を関係各部に周知徹底すること。

(6) 情報システム部門長は、業務継続計画を必要に応じて見直すこと。

3. システム復旧計画の管理

(1) 情報システム部門長は、情報システム、データ及び関連設備のバックアップ方法及び手順を業務の復旧目標に対応して定めること。

(2) 情報システム部門長は、情報システムにかかわるバックアップ方法及び手順を検証すること。

(3) 情報システム部門長は、復旧までの代替処理手続及び体制を定め、検証すること。

(4) 情報システム部門長は、復旧手続及び体制を定め、検証すること。

4. 訓練の管理

(1) 情報システム部門長は、情報システムにかかわる適切な業務継続手順・計画が、事業継続目的に合致していることを確かにするために、手順に基づき訓練を実施すること。また、訓練は、策定後の維持管理のために、定期的に訓練の目的に応じて適切な訓練を実施、継続していること。

(2) 情報システム部門長は、訓練の実施手順に則り実施し、マネジメントレビューを行い、マネジメントサイクル（PDCA）を回すこと。

5. 計画の見直しの管理

(1) 情報システム部門長は、情報システムにかかわる業務の中断・阻害を引き起こす事故が発生し、業務継続計画の発動に至った場合、事故発生後に業務継続計画の評価及び見直しを行うこと。

(2) 情報システム部門長は、業務継続計画が、引き続き、適切かつ有効であることを確実にするために、あらかじめ定められた間隔で、業務継続計画の評価及び見直しを行うこと。

Ⅸ. 人的資源管理

IT ガバナンス及び情報システム戦略委員会で定められている方針に基づく。

1. 責任と権限の管理

(1) 情報システム部門長は、業務の特性及び業務遂行上の必要性に応じて、要員の責任及び権限を定めること。

(2) 情報システム部門長は、要員の責任及び権限は、業務環境及び情報環境の変化に対応した見直しを行うこと。

(3) 情報システム部門長は、要員の責任及び権限を関係者に周知徹底すること。

2. 業務遂行の管理

(1) 要員は、責任を果たし、権限を遵守すること。

(2) 管理者は、作業分担及び作業量を、要員の知識、能力等から検討すること。

(3) 管理者は、要員の計画的及び不測な交替に備え、交替要員の育成をすること。

(4) 管理者は、要員の交替にあたっては、業務の適切な遂行、誤謬防止、不正防止及び機密保護を考慮すること。

(5) 管理者は、不測の事態に備えた代替要員を日常的に確保すること。

3. 教育・訓練の管理

(1) 管理者は、教育及び訓練に関する計画及びカリキュラムを、システム化計画及び人的資源管理の方針に基づいて作成及び見直しを行うこと。

(2) 管理者は、教育及び訓練に関する計画及びカリキュラムについて、技術力の向上、業務知識の習得、情報システムの情報セキュリティ確保等から検討すること。

(3) 情報システム部門長は、教育及び訓練を、計画及びカリキュラムに基づいて定期的かつ効果的に行うこと。

(4) 情報システム部門長は、要員に対するキャリアパスを確立し、業務環境及び情報環境の変化に対応した見直しを行うこと。

4. 健康管理

(1) 管理者は、身体的及び精神的に健康を保ち、企画、開発、運用及び保守業務を健全に遂行するため、健康管理を考慮した作業管理を整えること。

(2) 管理者は、システム関連する業務の従事者の健康を維持する対策を講ずるため、健康診断及びカウンセリングを行うこと。

(3) 情報システム部門長は、職業病、成人病等、要員の物理的、肉体的管理のみならず、メンタルヘルスケアとして、精神的ないしは心の側面における健康管理を行うこと。

(4) 情報システム部門長は、重大な疾病や災害につながらないようにするために、予防管理体制として、健康診断やカウンセリングも結果に基づいて、作業量の軽減、職種の変更、配置転換等、適切な予防管理体制がとられなければならない。

X. ドキュメント管理

1. ドキュメントの作成

(1) 利用部門長及び情報システム部門長は、情報システム戦略委員会で定めた方針に従い、ドキュメントの作成ルールを定めること。

(2) 利用部門及び情報システム部門の管理者は、ドキュメントの作成計画を策定すること。

(3) 利用部門及び情報システム部門の管理者は、ドキュメントの種類、目的、作成方法等を明確にすること。

(4) 利用部門及び情報システム部門の管理者は、ドキュメントの作成計画に基づいて作成すること。

(5) 利用部門長及び情報システム部門長が、作成したドキュメントを承認すること。

(6) 利用部門長及び情報システム部門長は、定期的にドキュメント作成ルールの見直しをすること。

2. ドキュメントの管理

(1) 利用部門長及び情報システム部門長は、情報システム戦略委員会で定めた方針に従い、ドキュメント管理ルールを定め、遵守すること。

(2) 利用部門及び情報システム部門の管理者は、利用する情報システムや情報サービスの変更に伴い、ドキュメントの内容を更新し、更新履歴を記録すること。

(3) 利用部門長及び情報システム部門長が、ドキュメントの更新内容を承認すること。

(4) 利用部門及び情報システム部門の管理者は、ドキュメントの保管、複写及び廃棄の際の不正防止及び機密保護の対策を講じること。

(5) 利用部門長及び情報システム部門長は、定期的にドキュメント管理ルールの見直しをすること。

用語定義

章	用語	定義・説明
	情報システム	組織体の活動を支えるデータ･情報の収集、蓄積、処理、伝達、利用に関わる仕組み･体系の総称である。情報通信技術、人間、制度･ルールなどで構成される。
	経営陣	業務執行に責任を有する経営者を含むガバナンスに責任を有する者。具体的には、取締役（会）、経営者、非営利法人の理事等のことを指し、経営者は一人とは限らないため、このような表現を用いた。
Ⅱ	プロジェクト運営委員会	経営者からの権限移譲を受け、開発プロジェクトに対する IT ガバナンスの職務（指示、モニタリング、評価）の遂行責任を有する。プロジェクトの立ち上げ、進捗、完了について経営者への説明責任を有する。調整を容易にするため、プロジェクトの利害関係者及び専門家を構成メンバーに加えることが望ましい。
Ⅱ	プロジェクトマネージャー（PM）	プロジェクト運営委員会からの権限移譲を受けて、プロジェクトの企画立案、運営管理の遂行責任を有する。 自らが担当するプロジェクトの進捗状況についてプロジェクト運営委員会に説明責任を有する。
Ⅱ	フィットアンドギャップ分析	情報システムを導入する際に、情報システムに対するニーズと、情報システムの機能がどれだけ適合(フィット)し、どれだけ乖離(ギャップ)しているかを分析すること。
Ⅲ	プロジェクト標準	プロジェクトの品質を確保するため、プロジェクト担当者が順守すべきガイドライン
Ⅲ	プロジェクト支援ツール	プロジェクトの管理を支援するために用いられるソフトウェアの総称。 主要なものとして以下のものがあり、PM はプロジェクトに適したプロジェクト支援ツールを購入又は開発する必要がある。 ・進捗管理ツール プロジェクトの進捗状況を収集し、見える化するためのツール ・テスト支援ツール テスト計画から実施までを効率化し、品質・進捗・問題管理を容易にするためのツール ・バージョン管理ツール プログラムやドキュメントの変更箇所を管理するためのツール ・デプロイツール 開発環境・テスト環境・本番環境へのプログラム配布を自動化するため

		のツール ・問題管理ツール
Ⅲ	インフラストラクチャー	情報システムにおいて、アプリケーションを実行するために必要なハードウェア、ネットワーク、及びソフトウェアの総称
Ⅲ	CIO（最高情報責任者）	経営者によって任命された、組織全体の情報化推進の最高責任者であり、経営戦略と情報システム戦略の整合性を確保し、その実現に関する統括責任を持つ。 IT 要員の確保や、情報システムに関する組織共通のルールの策定を情報システム部門またユーザ部門に対して指示する必要がある。
Ⅳ	プロダクトオーナー	情報システムの総責任者(ないしは実権限を委譲された代行者)であり、プロジェクトの対象情報システムの利用者・ユースケース・機能・品質・リリース等の決定権をもち、名目ではなく実際に開発チームと一体となってイテレーションに参加できることが必要。
Ⅳ	イテレーション	1～数週の期間を設け、その期間分の計画・分析・設計・実装・テストを実施して、その期間分の情報システムをリリースする活動。1 プロジェクトの中でこの活動を複数回反復する。
Ⅳ	フィードバック	利用者や利用部門からの情報システムに対する改善及び提案要望。
Ⅴ	利用部門	情報システムの利用部門（従来のユーザ）。
Ⅴ	アクセスコントロール	アクセスできるシステムや機能、データなどを利用者の属性に応じて設定して、認可された利用者がアクセスし、認可されていないアクセスを防止するなど、システムの利用を制御すること。
Ⅴ	特権的アクセス権	システム上のあらゆる作業を可能にする、高いレベルの操作権限。
Ⅴ	ログ	システムの利用状況の履歴の記録。例えばシステム作動記録のシステムログ、情報システム運用部門の作業ログ、利用者の活動ログ、アクセスログなど。情報セキュリティインシデント管理の観点からは、イベントログ、障害の内容ログ、原因ログ等となる。
Ⅴ	情報セキュリティインシデント	情報セキュリティを脅かす事件や事故、及びセキュリティ上好ましくない状況。
Ⅴ	ペネトレーション（侵入）テスト	ネットワークに接続されているシステムに対して実際に既知の技術を用いて侵入を試みることで、システムに脆弱性がないかどうかをテストする手法のこと。侵入テスト。
Ⅴ	ファシリティ	情報システムが稼動する機器を格納する設備や施設、建物など。
Ⅴ	サービスレベル管理	運用管理サービスの品質や成果を、サービス利用者とサービス提供者の双方が適切な管理指標に基づいて具体的、定量的に把握することで、コストや要求に見合ったサービスを維持する管理手法。SLM(Service Level Manegement)と略す。

Ⅴ	インシデント管理	インシデント(事故や事件に繋がる不測の事態）に対応するプロセスには、問題を識別し、原因を特定する問題管理、問題を解決するための変更管理、変更結果を適用するリリースのプロセスを含む。
Ⅴ	エスカレーション	利用部門からの連絡、問合わせや要求にサービスデスクでは対応できないときに、運用管理者などの上位者やインシデント対応管理者等の専門家に連絡して対応してもらう、又は上位者の指示を仰ぐこと。
Ⅵ	レグレッションテスト（退行テスト）	システムに修正や機能の追加を行ったことで、関連する他のシステムに影響が及んでいないか確認するためのテスト
Ⅶ	アウトソーシング	企業の事業戦略の達成を支援し、業務及び管理の有効性と効率性をより高めるために、外部組織のリソースを活用し、企業内業務の遂行を外部組織に委託することをいう。
Ⅶ	クラウド	共用可能なコンピューティングリソース（ネットワーク、サービス、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスして利用することを可能とする形態の総称である。クラウドコンピューティングを略した表現である。
Ⅶ	ASP	アプリケーションソフトウェアをインターネットを介してユーザに提供するサービス形態。(Application Service Provider）の略語。
Ⅶ	データ消去証明書	データが消去されたことを証明する書類（作業場所、消去方法、作業期間、作業担当者名等を記載）のこと。
Ⅶ	（ソフトウェア）エスクロー	委託先の倒産等に備え、ソフトウェアのソースコードや技術情報等を第三者（エスクロー・エージェント）に預託すること
Ⅶ	SLA	委託元（サービス利用者）と委託先（サービス提供者）の間で結ばれたサービスレベルに関する書面による合意。Service Level Agreement の略語
Ⅶ	立入監査	委託元が、委託業務を実施している委託先の作業場所、又は委託元のデータを保管している委託先のデータセンタ等に立ち入って、必要な監査を実施すること。
Ⅷ	復旧許容時間/目標復旧時間	復旧許容時間/目標復旧時間（RTO：Recovery Time Objective）は、インシデント発生後、次の処理/事業までに要する時間。①製品又はサービスの事業が再開されなければならない、又は②事業活動が事業が再開されなければならない、又は③資源が復旧されなければならない。
Ⅷ	事業継続（BC）	事業の中断・阻害を引き起こすインシデントに対応し、事前に定められた事業の許容水準/レベルで製品/商品又はサービスの提供/供給を継続する組織/企業の能力/事業力。
Ⅷ	インシデント	事業の中断・阻害、損失、非常事態、危機となり得るか、又はこれらを導き得る状況。

Ⅷ	事業継続マネジメント（BCM）	組織/企業への潜在的な脅威、及びそれが顕在化した場合に引き起こされる可能性がある事業活動への影響を特定し、主な利害関係者の利益、組織の評判、ブランド力、及び価値創造を保護する効果的な対応のための能力/組織力を備え、組織のレジリエンス*を構築するための枠組みを提供するマネジメントプロセス。 （* レジリエンス：情報システムがあらゆるレベルにおいて備えておくべきリスク対応能力・危機管理能力）
Ⅷ	事業継続計画（BCP）	事業の中断・阻害に対応し、事業を復旧、再開し、あらかじめ定められた事業水準に復旧するように導く文書化された手順。
Ⅷ	業務継続計画	IT ガバナンスの事業継続計画に基づき、情報システム部門の長などが作成する情報システムを復旧、再開するための手順。
Ⅷ	事業影響度分析	事業または業務の中断・阻害の与える影響を分析する手順/プロセス。
Ⅷ	リスクコミュニケーション	あるリスクについて利害関係者間で情報交換をしたり、対話をすることによって意思疎通をはかり、相互理解や信頼を構築すること。
Ⅸ	人的資源管理	情報システムの利活用は、組織にとって重要課題であり、組織全体の人的資源の活用とも密接な関係を有している。情報システムに係る人的資源管理として、情報システムの適切な利活用を推進する上で必要な事項を定める。

参考文献

- 一般財団法人日本情報経済社会推進協会(JIPDEC)，ITSMS ユーザーズガイド　JIS Q 20000(ISO/IEC 20000)対応，2012 年
- 経済産業省，情報セキュリティ管理基準（平成 28 年度改正版），2016 年
- 経済産業省商務情報政策局，新版 システム監査基準／システム管理基準解説書－平成 16 年度基準改訂版，2005 年
- 独立行政法人情報処理推進機構(IPA)，アジャイル型開発におけるプラクティス活用事例調査 調査報告書 ガイド編，2013 年
- 独立行政法人情報処理推進機構(IPA)，共通フレーム 2013，2013 年
- 独立行政法人情報処理推進機構(IPA), 情報システムに係る政府調達への SLA 導入ガイドライン，2004 年
- NPO 日本システム監査人協会，情報システム監査実践マニュアル（第 2 版），2005 年
- ISACA，COBIT 5 Framework(日本語訳)，2012 年
- ISACA，COBIT 5 Enabling Processes(日本語訳)，2012 年
- ISACA，Self-Assessment Guide：Using COBIT 5(日本語訳)，2013 年

- JIS Q 38500:2015，情報技術－IT ガバナンス
- JIS Q 22301:2013，社会セキュリティー事業継続マネジメントシステム－要求事項
- JIS X 0161:2008，ソフトウェア技術－ソフトウェアライフサイクルプロセス－保守
- JIS Q 20000-1:2012，情報技術－サービスマネジメント－第 1 部：サービスマネジメントシステム要求事項
- JIS Q 20000-2:2013，情報技術－サービスマネジメント－第 2 部：サービスマネジメントシステムの適用の手引