（参考資料 3）システム管理基準ガイドライン（案）抜粋

注意：以下のガイドライン（案）は未定稿であり、記載内容は修正の可能性がある。

Ⅰ　IT ガバナンス編

Ⅰ.1　IT ガバナンスの実践

ステークホルダーのニーズに基づき、組織体の価値及び組織体への信頼度を向上させるために、組織体における IT システムの利活用のあるべき姿を示す IT 戦略を策定し、組織体の IT に関するパフォーマンスを含めた IT ガバナンスの状況を確認して必要な是正措置を指示することによって、組織体の目標を達成する。

Ⅰ.1.1　経営戦略とビジネスモデルの確認

組織体の目的（パーパス）を実現するためのビジネスモデルと、それを実現するための経営戦略を支援するための IT 戦略ビジョンを策定する。

なお、ビジネスモデルとは、組織体が、顧客や社会に価値を提供し、持続的に価値を向上させていくビジネスの仕組みのことをいう。

＜達成目標＞

1. 組織体を取巻く自然環境、社会的・経済的な状況に応じて、組織体の目的を達成するための経営戦略とビジネスモデルと達成すべきビジネス成果が明確にされ、組織体全体に周知されている。
2. 経営戦略とビジネスモデルを実現するための IT の役割と重要性が認識されている。
3. 経営戦略とビジネスモデルを実現するための IT 戦略ビジョンが策定されている。
4. IT ソリューションや新技術等が経営戦略とビジネスモデルに及ぼす影響が定期的に評価され、経営戦略とビジネスモデルについて、必要な見直しを行っている。

＜ガバナンス活動の例：1＞（IT 戦略ビジョンの策定）経営戦略とビジネスモデルにおける IT の役割を明確にし、組織体の IT 戦略ビジョンを策定する。

＜リスク＞

IT の戦略ビジョンは、経営戦略とビジネスモデルを支える IT の役割を示すものであり、ビジネスモデルとの整合が取れていないと IT の役割とビジネスの成果がつながらない。

＜着眼点＞

（指示と承認）

① IT 戦略ビジョンについて、適切な執行責任者等に策定を指示する。
② IT 戦略ビジョンについて承認する。
③ ガバナンスの運営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、必要に応じてガバナンス運営委員会等運営組織を設置する。

（参考資料 3）システム管理基準ガイドライン（案）抜粋

（策定）

① 経営戦略とそれに基づくビジネスモデルについて確認する。

② IT 戦略ビジョンでは、組織体が目指すべき IT システムの利活用の姿（形態）をモデル化手法等により明確にする。※5

③ IT 戦略ビジョンでは、組織体の価値を向上させる革新的サービス等の実現のために IT エコシステムや人材を含むデジタル活用能力を活用する。

④ ビジネスモデルにおける IT システムの利活用に関する方向性について検討する。

（方向性の例示）

（ア）「変革又は差別化戦略」顧客への多様なサービス又は革新的なサービスの提供※4

（イ）「コストリーダーシップ戦略」コスト最小化の実現※4

（ウ）「安定した顧客サービス戦略」顧客指向サービスの安定的提供※4　等

⑤ IT 戦略ビジョンの検討では、競争環境、将来の技術動向、ステークホルダーのニーズ等を考慮する。

⑥ IT 戦略ビジョンでは IT システムの利活用による変革が、組織体のビジネスモデルにもたらす機会と脅威について評価する。

⑦ IT 戦略ビジョンでは、組織体のリスク、必要なリソース、スケジュール等について記載する。

⑧ IT 戦略ビジョンに基づき実施する組織体や業務の新設、改変や廃止及びビジネスプロセスの見直し等、組織体と業務の変革方針を明確にする。（DX）

＜ガバナンス活動の例：2＞（ビジネス成果の設定）IT 戦略ビジョンでは、経営戦略とビジネスモデルにより達成すべきビジネス成果を設定する。

＜リスク＞

IT 戦略ビジョンは経営戦略とビジネスモデルを支える IT の役割を示すものであり、IT 戦略ビジョンにビジネスモデルの戦略目標として具体的なビジネス成果が設定されていないと、事業活動が適切であるか評価が困難となる。

＜着眼点＞

（指示と承認）

① 具体的なビジネス成果の目標の設定を指示する。

② 具体的なビジネス成果の目標を承認する。

（策定）

① 組織体の目的と存在価値を満たすと判断できる具体的なビジネスの成果を検討する。

② 目標とするビジネスの成果は、経営戦略、外的環境要因、ステークホルダーのニーズ等を適切に評価したうえで設定する。*5

③ ビジネス成果の例

(ア)製品やサービスの利用者数、製品シェア

(イ)製品やサービスによる利益、ROI 等

(ウ)新製品やサービスの提供開始までの期間

(エ)組織体の目的である存在意義の実現に伴う、組織体のブランディング、社会的信頼性の向上

(オ)持続可能性のための IT エコシステムを含む、デジタル活用能力を含む IT インフラの整備

＜ガバナンス活動の例：3＞（ステークホルダーのニーズの反映）IT 戦略ビジョンには、ステークホルダーのニーズを反映する。

＜リスク＞

IT 戦略ビジョンにステークホルダーのニーズが反映されていないと、ステークホルダーや市場等から評価されないリスクがある。

＜着眼点＞

（ニーズの反映）

① IT 戦略ビジョンに関連するステークホルダーを特定する。

② ステークホルダーの期待やニーズを明らかにする。

③ ステークホルダーの期待やニーズに応える目的と優先順位付けをする。

（ステークホルダーへの対応）

① IT 戦略ビジョンは、関連するステークホルダーに報告する。

② その他「Ⅰ.2.1 ステークホルダーへの対応」を参照のこと

＜ガバナンス活動の例：4＞（新技術等の定期的評価）新しい IT ソリューションや新技術が IT 戦略ビジョンに及ぼす影響を定期的に評価する。

＜リスク＞

新しい IT ソリューションや新技術に対する影響を定期的に評価していないと、IT 戦略ビジョンが陳腐化してしまい、ビジネス成果を達成できなくなる。

＜着眼点＞

（指示）

①IT 戦略ビジョンで評価の実施を明示する。

（新技術等に関する定期的評価）

（参考資料 3）システム管理基準ガイドライン（案）抜粋

①IT 戦略ビジョンで、以下の評価を実施することを検討する。

（ア）新しいソリューション、新技術に関する情報について定期的に収集する。

（イ）他社のソリューション活用事例等について定期的に確認する。

（ウ）新しいソリューションや新技術がビジネスモデルに与える影響について、機会と脅威等の観点から定期的に評価する。

（エ）評価の結果は取締役会等に報告する。

＜ガバナンス活動の例：5＞（市場変化の定期的評価）市場の変化が経営戦略とビジネスモデルに及ぼす影響を定期的に評価する。

＜リスク＞

経営戦略とビジネスモデルについて、市場の変化に対する影響を評価していないと、ビジネスモデルが陳腐化してしまい、ビジネス成果を達成できなくなる。

＜着眼点＞

（指示）

① 定期的な評価を指示する。

（ビジネスモデルに関する定期的評価）

① 自社で提供している製品やサービスの顧客の満足度を定期的に確認する。

② 顧客のニーズの変化を定期的に確認する。

③ ターゲット市場の成長性について確認する。

④ 競合他社の動向を定期的に確認する。

⑤ 現在のビジネスモデルについて定期的に評価した結果を取締役会等に報告する。

＜ガバナンス活動の例：6＞（IT 戦略ビジョン等の見直し）事業環境等の評価を実施し、その結果に基づいて、ビジネスモデルと IT 戦略ビジョンの見直しを行う。

＜リスク＞

変化する事業環境に合わせて、経営戦略とビジネスモデル等を変化させないと、市場等からの支持を失ってしまう。

＜着眼点＞

（IT 戦略ビジョンやビジネスモデルの見直し検討）

① 新しいソリューションや新技術の影響に関する定期的な評価の結果により、新しいソリューションや新技術の自社での取込みの可能性等について検討する。

② 顧客やターゲット市場の変化に対して、自社で提供している製品やサービスの対応を検討する。

（参考資料 3）システム管理基準ガイドライン（案）抜粋

③ 新しいソリューションや新技術等の変化の内容によっては、IT 戦略ビジョンを見直する。
④ 市場等の変化の内容によっては、ビジネスモデルとそのビジネス成果を見直しする。

＜モデル組織体制での実施主体とステークホルダー＞

ガバナンス活動の例	実施主体	ステークホルダー
1. IT 戦略ビジョンの策定	指示と承認：取締役会等 策定：経営者／委員会	市場、顧客、従業員、取引先、投資家等
2. ビジネス成果の設定	指示と承認：取締役会等 策定：経営者／委員会	
3. ステークホルダーのニーズの反映	ステークホルダーへの対応：取締役会等 ニーズの反映：経営者／委員会	
4. 新技術等の定期的評価	指示：取締役会等 評価実施内容の検討：経営者／委員会等	
5. 市場変化の定期的評価	指示：取締役会等 定期的評価の検討：経営者／委員会	
6. IT 戦略ビジョン等の見直し	検討：取締役会等	

※以降省略

（参考資料3）システム管理基準ガイドライン（案）抜粋

Ⅱ　ITマネジメント編

Ⅱ.6　保守プロセス

Ⅱ.6.1　保守体制の整備

情報システムの性能・機能を維持するために、保守に関する方針、手順を定め、保守体制を整備する。

＜達成目標＞

1. **保守方針及び手順が定められ、周知されている。**
2. **保守対象が明確にされている。**
3. **保守実施体制が整備されている。**
4. **開発プロセス及び運用プロセスから保守に必要な情報が連携されている。**
5. **保守の実施に必要なシステム環境や保守用ツールが整備されている。**
6. **保守業務を外部委託する場合、外部委託先との間で契約が締結されている。**

＜管理活動の例：1＞（保守方針）保守方針（外部委託方針を含む）を定めて、周知する。

＜リスク＞

保守の方針が明確化され組織内の関係者に周知されていないと、組織内の保守についての認識が統一されない。

＜着眼点＞

① 保守の方針を明確化する。
② 保守の方針は、保守のための費用や要員に関する組織としての方針と整合性をとる。
③ 保守の方針を組織として承認する。
④ 保守の方針を組織内の関係者に周知する。
⑤ 保守の方針の見直しに関する手順を定める。

＜管理活動の例：2＞（保守対象）保守方針に従って、情報システム、ハードウェア、ソフトウェア等の保守対象を明確にする。

＜リスク＞

保守対象が明確に設定され、組織内の関係者に周知されていないと、保守計画策定段階及び保守作業実施段階で混乱が生じる。

＜着眼点＞

① 保守の方針に従って、保守対象を明確にし、承認する。

② 保守対象には、ハードウェア（情報機器、ネットワーク、電源系統を含む設備など）及びソフトウェアを含める。
③ 保守対象のソフトウェアには、以下のものを含める。
・自社で開発したアプリケーション、Web サイト、データベース　など
・外部のソフトウェアメーカから調達した OS、ミドルウェア、パッケージソフト　など
・サービス提供事業者から調達した SaaS などのクラウドサービス
後の２つを合わせて、外部調達ソフト等と呼ぶ。
④ 保守対象について、自社で保守を行うものと外部委託先に保守を委託するものに区分する。
⑤ 保守対象を上記③及び④を含めて可視化(一覧化)する。
⑥ 保守対象を組織内の関係者に周知する。

＜管理活動の例：3＞（保守手順書）保守方針に従って、保守手順書を作成し、周知する。

＜リスク＞
保守手順書が作成されていないと、保守の実施手順についての理解が保守実施体制または保守担当者によって異なってしまう。

＜着眼点＞
① 保守手順書を策定し、承認する。
② 保守手順書には、保守の方針・戦略、保守対象、保守体制、保守において想定されるリスクと対応策などを記載する。
③ 保守手順書には、保守依頼の受領、保守実施の決定、保守作業実施計画の策定、保守の実施、保守作業実施結果の検証、保守によって変更された構成要素の本番環境への適用、保守作業実施内容の記録と報告などについての標準的な手順を記載する。
④ 特に迅速な対応が要求される緊急保守の基準及び対応手順を、保守手順書の中で明確にする。
⑤ 必要に応じて、保守手順書を詳細化した保守マニュアルを作成する。保守マニュアルは、例えば、保守対象の特性、保守の規模や期間などを考慮したものである。
⑥ 作成した保守手順書及び保守マニュアルを、関係者に周知する。
⑦ 保守手順書の見直しについての手順を定める。
⑧ 標準的保守手順書及び保守マニュアルの最新版を、関係者が必要な時に参照可能な状態で管理する。

＜管理活動の例:4＞(情報セキュリティ対策)情報セキュリティ管理基準等を参考にして、保守方針に、保守作業に係る情報セキュリティ対策を構築することを明確にする。

＜リスク＞

保守作業に係る情報セキュリティインシデントへの対応策が不十分だと、保守作業実施中に情報セキュリティインシデントが発生する。

＜着眼点＞

① 保守対象や保守実施環境などを考慮し、想定される情報セキュリティリスクを明確化する。
② 情報セキュリティリスクに対する予防対策、発見対策、復旧対策を策定・実施する。
③ 情報セキュリティ対策の策定に当たって、情報セキュリティ管理基準を参考にする。
④ 策定・実施する情報セキュリティ対策の実効性を検証する。
⑤ 保守作業実施中に情報セキュリティインシデントが発生した場合の連絡・報告手順を明確化し、関係者に周知する。

＜管理活動の例：5＞（必要情報の連携）保守対象のハードウェアやソフトウェアの構成管理情報、システム構成図、プログラム一覧等含む保守で必要な情報を、開発プロセスや運用プロセスから連携する。

＜リスク＞

保守対象に関する情報･データ･文書が確実に引き渡されていないと､保守計画策定段階、保守作業実施段階で再調査・再確認が必要になる。

＜着眼点＞

① 保守対象ごとに保守に必要な情報・データ・ドキュメント（例えば、ハードウェアの仕様、開発プロセスで作成されたソースコードやシステム設計書、業務運用マニュアルなどのドキュメント、開発プロセスの検証段階で作成されたテストデータやテスト結果報告書などのドキュメント）を明確化する。
② 保守に必要な情報・データ・ドキュメントに、保守対象の構成管理情報を含める。
③ 保守に必要な情報・データ・ドキュメントに、保守における制約事項（システムアーキテクチャに係る制約、システム設計上の制約など）を含める。
④ 保守に必要な情報・データ・ドキュメントが開発プロセスや運用プロセスから漏れなく引き渡されていることを記録する。
⑤ 保守に必要な情報・データ・ドキュメントの管理体制を明確化する。
⑥ 保守に必要な情報・データ・ドキュメントの管理方法を、安全性の確保を含めて明確化する。
⑦ 保守に必要な情報・データ・文書の管理体制・管理方法を承認する。

（参考資料 3）システム管理基準ガイドライン（案）抜粋

＜管理活動の例：6＞（保守環境等の整備）保守の実施に必要な保守環境、保守支援システム、保守用ツール等を整備し、使用可能な状態に維持する。

＜リスク＞

保守を実施するために必要な保守環境、保守支援システムや保守用ツールが必要な時に使用可能な状態に維持されていないと、保守計画策定段階や保守作業実施段階で改めて整備が必要になる。

＜着眼点＞

① 保守の実施に必要な保守環境、保守支援システムや保守用ツールを明確化し、可視化（一覧化）し、承認する。
② 保守作業の実施に必要な保守環境、保守支援システムや保守用ツールを導入あるいは提供元と契約し、使用可能な状態にする。
③ 保守作業の実施に必要な保守環境、保守支援システムや保守用ツールが使用可能であることを確認する。
④ 保守作業の実施に必要な保守環境、保守支援システムや保守用ツールの使用方法を、保守作業要員に周知する。

＜モデル組織体制での実施主体と関係者＞

管理活動の例	実施主体	関係者
1. 保守方針	IT 部門長	利用部門（調整・周知対象）
2. 保守対象	保守管理者	IT 部門長（承認） IT 部門担当（調整・周知対象） 利用部門（周知対象）
3. 保守手順書	保守管理者	IT 部門長（承認） IT 部門担当（周知・遵守対象） 利用部門（調整・周知対象）
4. 情報セキュリティ対策	保守管理者	IT 部門長（方針の承認） IT 部門担当（対策の策定、周知・遵守対象）
5. 必要情報の連携	保守管理者	IT 部門長（管理体制・管理方法の承認） IT 部門担当（管理体制・管理方法の周知・遵守対象） IT 部門開発・運用担当（必要情報・データ・ドキュメントの引渡し）
6. 保守環境等の整備	保守管理者	IT 部門長（承認） IT 部門担当（稼働確認、使用方法の周知対象）

（参考資料 3）システム管理基準ガイドライン（案）抜粋

※以降省略