

第1章 COBIT5のITガバナンスの捉え方

1. COBIT5のITガバナンスの定義

COBIT5は従来のITガバナンスを事業体のガバナンスに取り込みました。IT視点にあった従来のITガバナンスは事業体に焦点を当てた「事業体のITガバナンス」という表現に変更しました。

COBIT5の目的は、この事業体のITガバナンスに対して「効果の実現と、リスクレベルやリソース活用の最適化とのバランスを保つことによって、事業体がITから最適な価値を生み出すことを支援するものである。」と述べています。

つまり、COBIT5でいう事業体のITガバナンスとは、「効果の実現と、リスクレベルやリソース活用の最適化とのバランスを保つことによって、事業体がITから最適な価値を生み出すこと」ということになります。

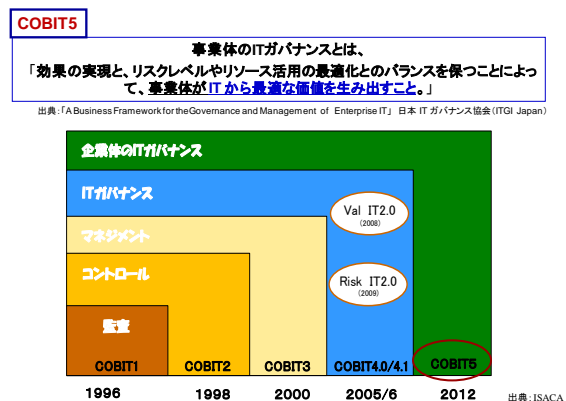
この定義の意味するところを、少し説明を加えましょう。

「事業体」とは、事業の利害関係者であるステークホルダーに向けて価値を創出するために存在します。この価値創出が事業体のITガバナンスの目標です。ステークホルダーは事業活動の構成要因である「顧客」、「仕入先」、「銀行」等を考えればよいでしょう。つぎに、

「価値創出」とは、事業利益を最大化することですが、事業には事業活動を阻害するリスクが存在します。例えば、セキュリティリスク、粉飾決算リスク、経営戦略リスク等様々です。リスク対策はより精度の高い対策を講じるほど投資予算は拡大します。それらのリスクを事業目標に照らし、最適なリソースコストで効果を実現することが必要になります。つまり、事業の「価値創出」とは、「リスクを最適化」し、より良い事業活動に向けたヒト、モノ、カネ、情報といった経営資源の「資源最適化」を図り、事業の「効果の実現」を作り出すということです。

「ガバナンス」とは、異なるステークホルダー間の価値の利害を調節し決定することです。利害を調整し統制がとれる状態にするには、その責任者である「誰が」に焦点を当

図1-1 COBIT5のITガバナンス定義



て設定することが必要になります。

もう一度、事業体のITガバナンスに戻ってみましょう。事業体のITガバナンスには「IT」が加えられていますので、「事業体がITから最適な価値を生み出すことを支援するもの」と置き換えることができます。

2. COBIT5フレームワークの特性

COBIT5のフレームワークは、事業体のITガバナンスを確立するためのフレームワークです。このフレームワークの特性は2つの要点としてまとめることができます。

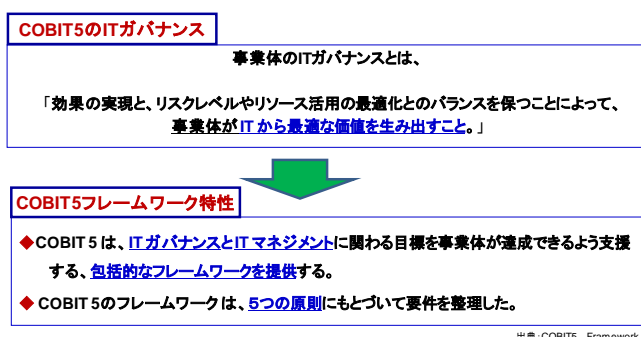
◆要点1: COBIT 5は、ITガバナンスとITマネジメントに関わる目標を事業体が達成できるよう支援する、包括的なフレームワークを提供する。

従来のCOBIT4.0フレームワークと大きく異なるのは、COBIT5が事業体のITガバナンスを「ITガバナンス」と「ITマネジメント」の2つの領域に分類し、各領域のプロセスを統治する構成にしました。「ITガバナンス」の領域に含まれるプロセスを「ITマネジメント」領域に含まれるプロセスの上位に置き、上下関係で事業体のITガバナンスを構造化しました。

ITガバナンスとは、ステークホルダーのニーズや、条件、選択肢を「評価」し、優先順位の設定と意思決定によって「方向性」を定め、合意した方向性と目標に沿ってパフォーマンスや準拠性を「モニター」することです。これらの方策は事業体の目標のもとにバランスを取り、合意の上で決定し、達成されることを保証するものでなければなりませんと述べています。ITガバナンスプロセスは「評価」、「方向付け」、「モニター」で構成しています。事業体においては取締役会長のリーダーシップのもと、取締役会が事業体のITガバナンス全体の実行責任を負うこととなります。一方、

ITマネジメントとは、事業体の目標の達成に向けてガバナンス主体が定めた「方向付け」と整合するようにアクティビティを計画、構築、実行し、評価することとなります。マネジメントプロセスは、「計画」、「構築」、「実行」、「モニター」のプロセスで構成することに

図1-2 COBIT5フレームワークの特性



出典: COBIT5 Framework

なります。

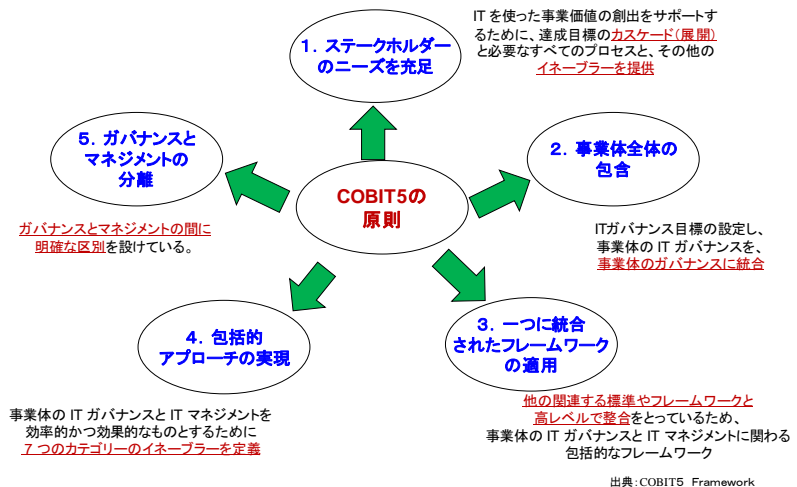
このITマネジメントは事業体において最高経営責任者(CEO)のリーダーシップのもとに、経営幹部がマネジメントの実行責任を負うこととなります。詳細記述は第2章で行います。

◆要点2: COBIT 5のフレームワークは、5つの原則にもとづいて構築した。

COBIT5のフレームワーク要件は、5つの原則のもとに構成されていますので、この原則を要約をしておきましょう。(図1-3-1)

5つの原則とは、「ステークホルダーのニーズを充足」、「事業体全体の包含」、「一つに統合されたフレームワークの適用」、「包括的アプローチの実現」、「ガバナンスとマネジメントの分離」です。

図1-3-1 ITガバナンスに向けたCOBIT5の原則



① 原則1:ステークホルダーのニーズを充足

事業体は、ステークホルダーに向けて

価値を生み出すために存在しています。COBIT 5は、ステークホルダーニーズにもとづく事業価値の創出をガバナンス目標として設定しました。価値創出とは「リスクを最適化しつつ、最適なリソースコストで効果を実現すること」と定義しています。

また、達成目標のカスケード(展開)で、事業体のステークホルダーにニーズから事業達成目標を、ITの達成目標へ変換し、プロセス、実践手法に絞り込む手続きを提供しました。この提供される達成目標カスケードはあらゆる事業体がITガバナンス導入のカスタマイズにおいて、実施作業(タスク)までの絞り込みを容易にしました。

② 原則2:事業体全体の包含

COBIT 5はITガバナンスを、事業体のガバナンスに統合しましたが、この意味するところは、

a.COBIT 5は「IT機能」のみに焦点を合わせるのではなく、「情報とそれに関わる技

術を、他の資産と同様に事業体の全員が関与すべき資産として扱う。」。つまり、情報とそれに関わる技術を事業価値創出に向けた重要イネーブラーとして取り扱うということです。

b.COBIT 5 は、すべての IT に関わるガバナンスとマネジメントのすべてのプロセスを提供し、事業体の全体に亘る活動として包括的なものとして捉えている。

事業体のITガバナンスおよびITマネジメントプロセスの実施で、関与する7つのイネーブラーである「原則、ポリシーおよびフレームワーク」、「プロセス」、「組織構造」、「文化、倫理および行動(個人と事業体の行動)」、「情報」、「サービス、インフラストラクチャおよびアプリケーション」、「人材、スキルおよび遂行能力」は、IT 機能の定義だけではなく事業価値創出の観点で捉えることを前提としていることです。

③ 原則 3:一つに統合されたフレームワークの適用

COBIT 5 は、他の関連する標準やフレームワークと整合をとっているため、事業体の IT ガバナンスと IT マネジメントに関わる包括的なフレームワークとなっている。

この意味するところは、

事業体の IT ガバナンスに係る標準やガイド、例えば ISACA で発行された COBIT 以外の他の標準やフレームワークである ValIT、RiskIT などを取り込み統合したこと、および ISACA 発行以外の ISO 標準、ITIL や TOGAF などとも整合性を取ったことを述べている。COBIT5 は IT ガバナンスに係る標準およびフレームワークを統合し、その中核に位置づけようとしている意図がよく表れています。

④ 原則 4:包括的アプローチの実現

COBIT5 は事業体の IT ガバナンスと IT マネジメントを効率的かつ効果的なものとするために 7 つのカテゴリーのイネーブラーを定義しています。イネーブラーとは、広義には、事業体の目標達成を支援する影響要因を指します。

これらのイネーブラーを定義することで事業体の目標達成を支援する IT ガバナンス要因を定義することになるということです。7 つのカテゴリーのイネーブラーとは、以下の通りです。詳細は 2 章で解説します。

- 原則、ポリシーおよびフレームワーク
- プロセス
- 組織構造

- 文化、倫理および行動
- 情報
- サービス、インフラストラクチャおよびアプリケーション
- 人材、スキルおよび遂行能力

⑤原則 5:ガバナンスとマネジメントの分離

COBIT 5 フレームワークは、ガバナンスとマネジメントの間に明確な区別を設けています。「ガバナンス」と「マネジメント」の区分を明確にしておきましょう。(図 1-3-2)

「ガバナンス」とは、ITマネジメントのフレームワークに対するステークホルダーのニーズや、条件、選択肢を「評価」し、優先順位の設定と意思決定によって方向性を定める。そして、合意した「方向性」と目標に沿ってパフォーマンスや準拠性を「モニター」することで事業体の目標が達成されることを保証する全体監理の統治プロセスです。

ほとんどの事業体においては取締役会長のリーダーシップのもと、取締役会がガバナンス全体の実行責任を負います。

「マネジメント」とは、事業体の目標の達成に向けてガバナンス主体が定めた方向性に沿ってアクティビティを計画、構築、実行し、評価する実働の管理プロセスです。

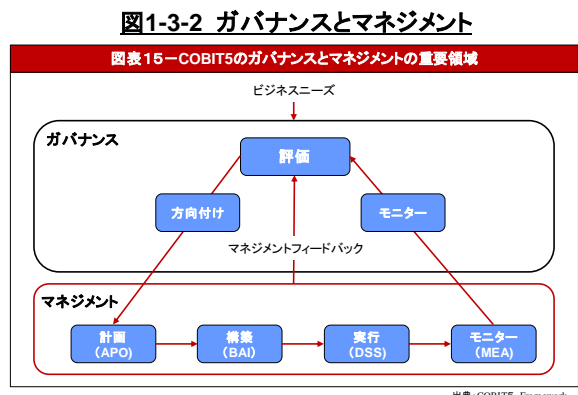
ほとんどの事業体において、最高経営責任者(CEO)のリーダーシップのもとに、経営幹部がマネジメントの実行責任を負います。

以上の定義を踏まえると、事業体のITガバナンスでは社内でのステーク

ホルダーのすべてが関係することになります。経営者はガバナンスプロセスの統治、そして管理者と従業員はマネジメントプロセスの統治という活動における役割が出てきます。「ガバナンス」と「マネジメント」領域の統治の対象となるプロセスを以下に概説します。

a. 評価、方向づけおよびモニタリング (evaluate, direct and monitor: EDM)

ガバナンス領域での統治プロセスです。ビジネスニーズを受けて、経営者(取締役会)がITガバナンスの現状を「評価」し、「方向付け」をして、マネジメントプロセスの成果を「モニタリング」するドメイン(領域)です。このドメインはすべてのステークホルダーに向



【第1章 COBIT5 の IT ガバナンスの捉え方】

けた目標達成のプロセス統治活動を経営者が保証することになりますので、「ガバナンス」とカテゴリーしました。COBIT5 では EDM ドメインといいます。

事業体の IT ガバナンスのマネジメントプロセスは、管理者と従業員で実践する「マネジメント」カテゴリーになり、4 つのプロセスドメインがあります。

b. 整合、計画および組織化 (Align, Plan and Organise : APO)

EDM ドメインの「方向付け」のもとに、IT 化業務プロセスの計画を立案し、プロジェクトの組織化を行うプロセスを統治するドメインです。「APO ドメイン」といいます。

c. 構築、調達および導入 (Build, Acquire and Implement : BAI)

APO ドメインの計画にもとづいて、構築、調達および導入を実践するプロセスを管理するドメインです。「BAI ドメイン」といいます。

d. 提供、サービスおよびサポート (Deliver, Service and Support : DSS)

BAI ドメインの完了を受けて、IT システムによってサービスとその管理を行うプロセスを統治するドメインです。「DSS ドメイン」になります。

e. モニタリング、評価およびアセスメント (Monitor, Evaluate and Assess : MEA)

DSS ドメインの定着化時に APO ドメインの計画目標の達成をモニタリングし、評価し、EDM ドメインへの報告するプロセスを統治するドメインです。MEA ドメインといいます。

「ガバナンス」と「マネジメント」の各ドメインとプロセスに関しては第 2 章で詳述します。