DISCUSS THIS ARTICLE

東京海上日動システムズにおけるCOBIT 5を活用した価値の創出

Yuichi (Rich) Inaba, CISA 著

COBIT Focus | 24 November 2014 Japanese | English

東京海上日動システムズ（以下、「システムズ」と略す）は COBIT 5 に基づくガバナンス・リスク管理・コンプライアンス（GRC）態勢を構築した。これにより、当社はステークホルダーへ大きな価値の提供をもたらすと共に、価値創出に向けたリスクとリソースの最適化を実現した。COBIT のコンセプトが IT ガバナンスから事業体 IT ガバナンスへ進化したことにより、当社は COBIT 5 をガイダンスとして活用するように導かれた。

システムズは東京海上グループの IT サービス提供会社であり、グローバルに広範囲の各種保険サービスを提供する企業グループである。システムズは 1983 年に設立され現在約 1400 名の従業員から構成される。システムズが IT サービスを提供する相手先の主要な東京海上グループ会社は、損害保険会社の東京海上日動火災保険株式会社および生命保険会社での東京海上日動あんしん生命保険株式会社である。東京海上グループは日本における最大規模の有名な保険グループである。システムズが提供する IT サービスの範囲は、グループ会社のためのシステム開発および運用業務を含んでいる。システムズはそれらグループ会社のシステム企画業務やモニタリング業務の一部についてもサポートしている。

価値創出を目指したGRC態勢

システムズはさまざまなリスクやコンプライアンスへの対応ニーズに直面していた。従来、経営者の関心はリスク管理やコンプライアンスへの受け身の対応が中心であった。経営者は、IT サービスの業務委託契約や日本の法規制等を順守するためにリスクやコンプライアンスへの対応をすることだけであれば、これほど楽なことはないと考えていたが、このアプローチだけでは会社の将来への不安もステークホルダーと共に感じていた。

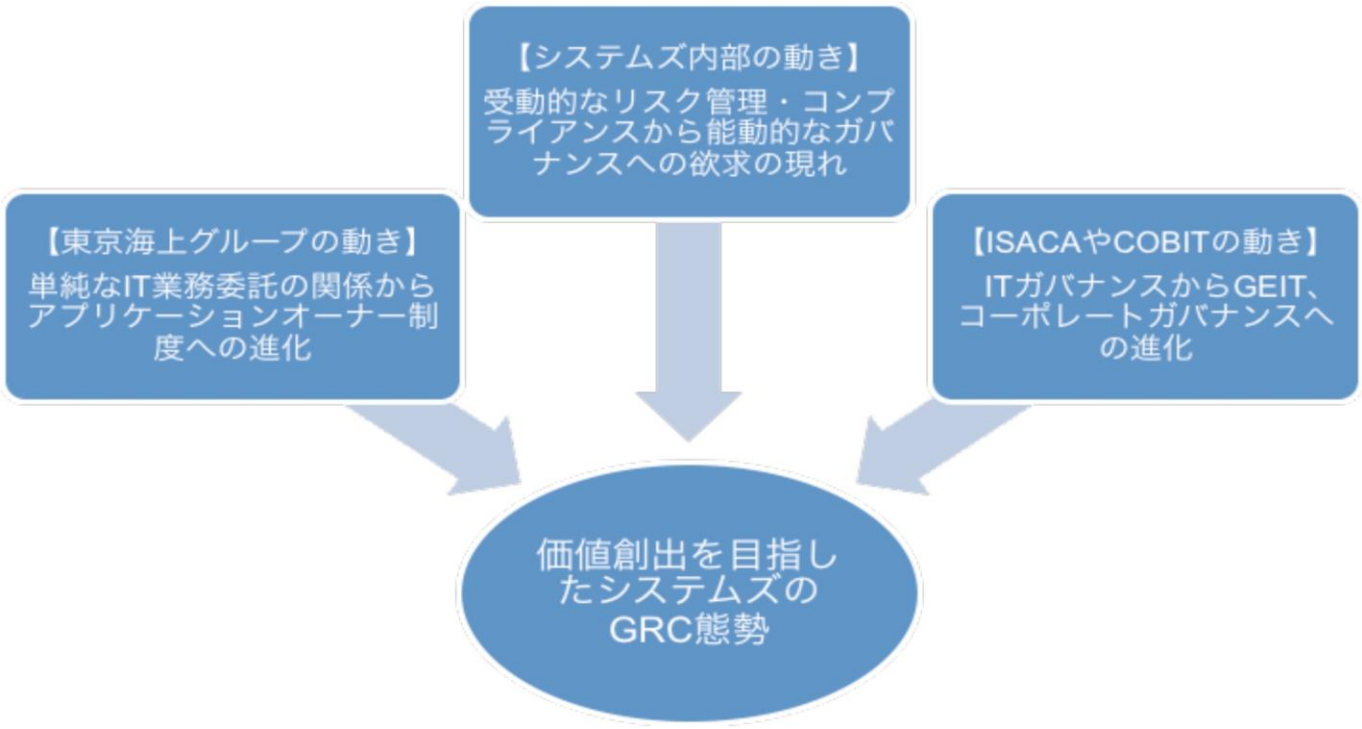
一方で、東京海上ホールディングスにより導入された東京海上グループの IT ガバナンス態勢に従い[1]、グループ会社にはビジネス部門と IT 部門が適切な役割と責任を分担する対等なパートナーシップの関係を構築することが求められていた。その結果がアプリケーションオーナー制度であり、当社はステークホルダーへの価値創出に寄与するものであると確信していた。

さらに、COBIT については、COBIT 5 のアプローチにより事業体 IT ガバナンス（GEIT）へと進化し、CIO や IT 部門の視点から CEO や取締役会への視点を含めるように視野が広げられた。

システムズは受動的なリスク管理やコンプラアンスばかりによる将来への不安を解消し、主要なステークホルダー（お客様である東京海上日動火災保険やその他のグループ会社）の価値を一緒になって創出することを切望していた。これを実現するために、当社はグループのアプリケーションオーナー制度と COBIT 5 を活用することを決定した。

結果として、システムズはステークホルダーへの価値創出を目指した GRC 態勢を必然的に導入した。

図表１ーGRC態勢への歴史的必然性



出典：Yuichi (Rich) Inaba、許諾による掲載

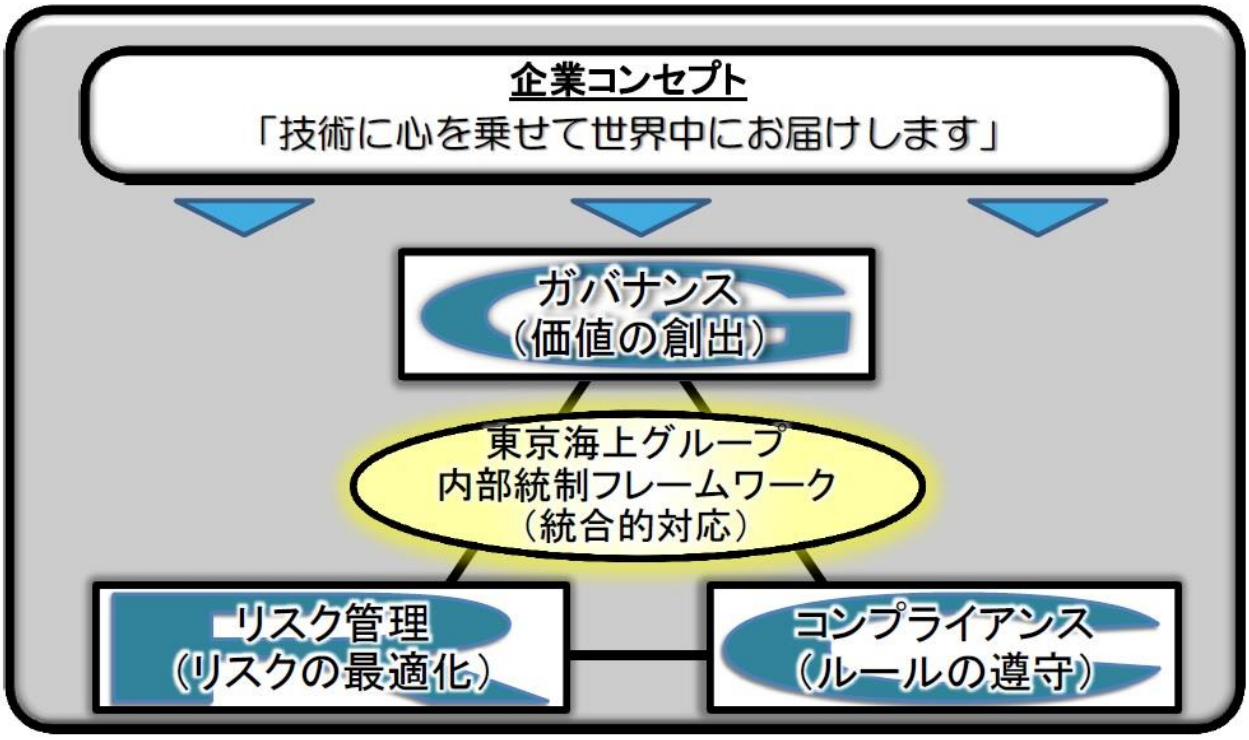
システムズのGRCの概念

システムズは企業コンセプトとして「技術に心を乗せて世界中にお届けします」と宣言している。この企業コンセプトや経営理念、経営ビジョンに従い、システムズは３つの重要なガバナンスとマネジメントに関する分野として、ガバナンス、リスク管理、コンプライアンスの３つを定義した。

ガバナンス目標は「価値創出」と設定。さらに、それぞれのガバナンスとマネジメントの分野に対し、ガバナンスの目標は価値を創出すること、リスク管理の目標はリスクを最適化すること、コンプライアンスの目標はルールを順守すること、というようにそれぞれの目標を決定した。

これらの３つの分野は、G、R、Cに対し個別最適で業務を行うと、ややもすると非効率になったり時には矛盾したりしてしまう。業務を効果的かつ効率的に行うために、システムズは G、R、C を１つのガバナンスとマネジメントのフレームワークへ統合した。これを東京海上グループの内部統制フレームワークを活用した GRC 態勢と呼んでいる（図表２）。

図表２ーシステムズにおけるGRC態勢の概念



出典： Yuichi (Rich) Inaba、許諾による掲載

東京海上グループの内部統制フレームワーク

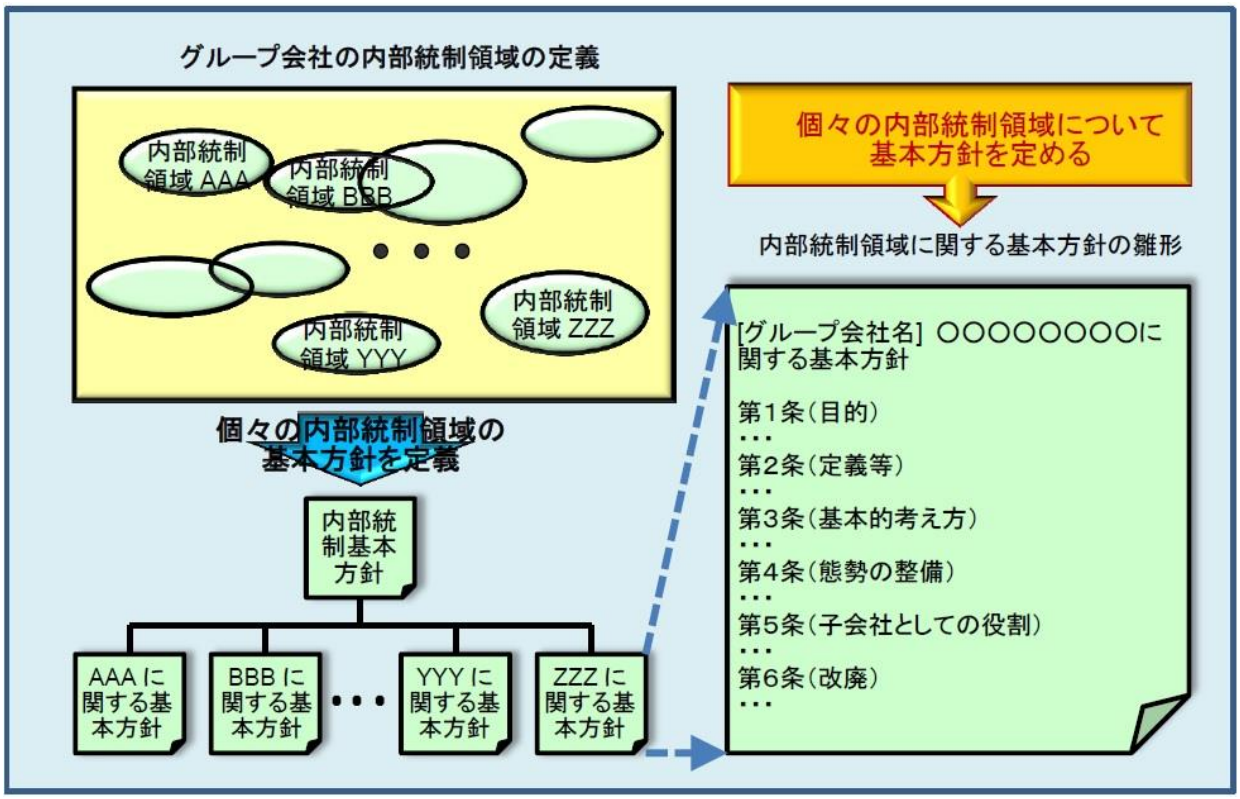
COBIT 5 の原則3「1つに統合されたフレームワークの適用」に従って、システムズは東京海上グループの内部統制フレームワーク（以下、「内部統制フレームワーク」と略す）を 1 つに統合されたフレームワークとして採用した。

内部統制フレームワークは、日本の会社法に準拠するために東京海上ホールディングスにより確立された。 東京海上ホールディングスは、東京海上グループ会社に対し、この内部統制フレームワークを使って内部統制管理態勢を構築することを義務づけた。

内部統制フレームの概要を図表３に記載する。東京海上グループ会社は以下の対応を行わなければならないとしている。

1. 会社の業務形態に応じて、会社の内部統制領域を定義する。
2. 定義した個々の内部統制領域について、あらかじめ定義されている形式に従い、東京海上ホールディングスがガイダンスとして提供する個々の内部統制領域の雛形を参考にして、内部統制に関する基本方針を定める。

図表３－東京海上グループの内部統制フレームワーク



出典： Yuichi (Rich) Inaba、許諾による掲載

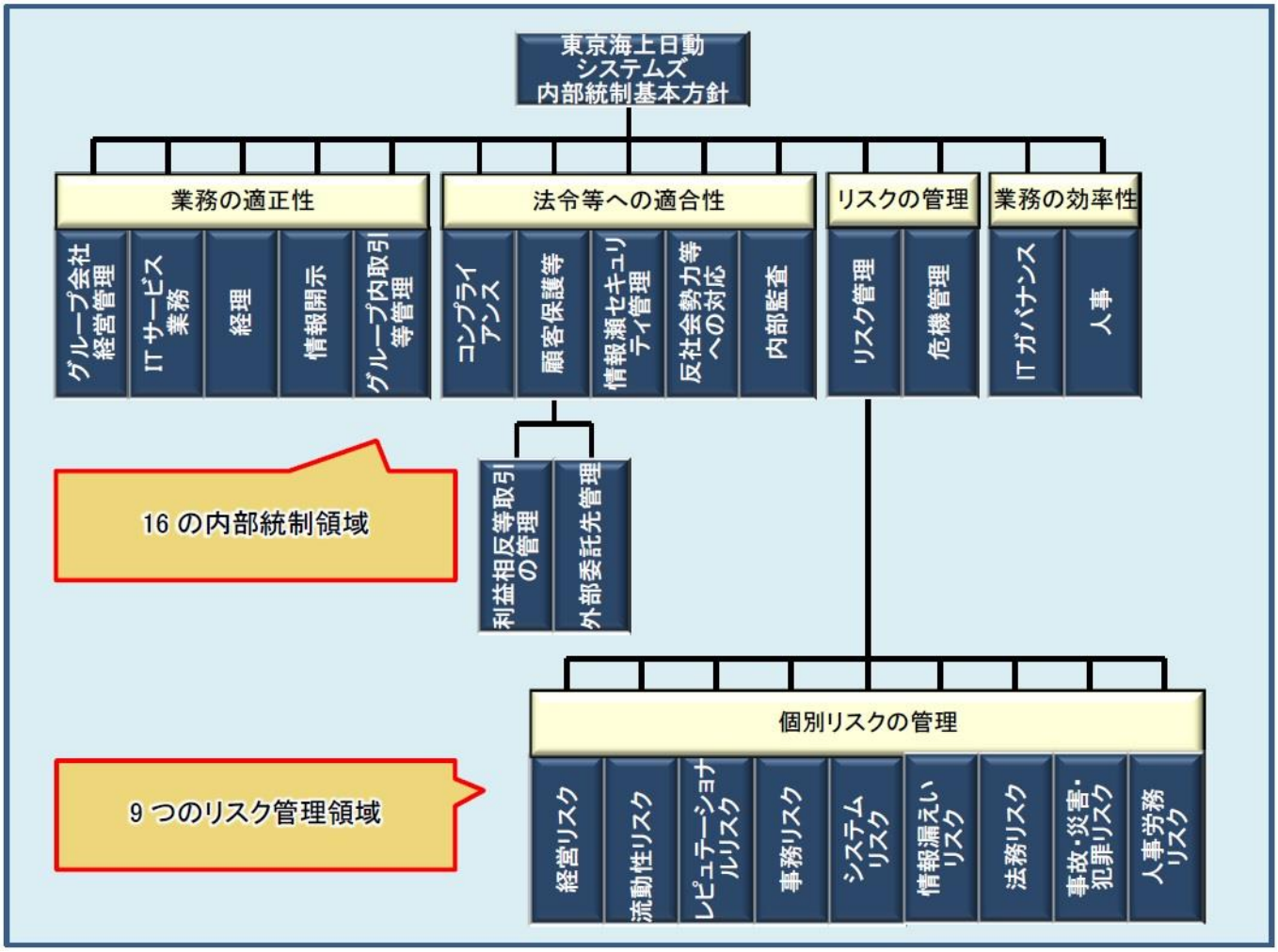
システムズの内部統制管理態勢

内部統制管理態勢を構築することはグループ会社に求められていることだが、システムズはグループコンプライアンスへの受動的な対応としてではなく、主体的に価値を創出する手段として内部統制フレームワークを活用した。言い換えれば、当社はグループ規制に準拠したが、その範囲に限定しなかった。むしろ、この機会を活用し、ガバナンスとそれによる価値創出の概念を追加して、内部統制管理態勢から GRC 態勢へと進化させた。

システムズが構築した内部統制管理態勢を図表４に示す。１６の内部統制領域が定義されている。そのうち１５の内部統制領域は東京海上グループの雛形から持ってきたものであるが、当社は意図的にシステムズ固有の内部統制領域、すなわち「IT サービス業務」を追加した。これらの統制領域のうち「IT サービス業務」と「IT ガバナンス」が IT 関連の領域であり、その他の 14 の領域は非 IT 領域である。

「リスク管理」の内部統制領域は９つのリスク管理領域にブレークダウンされている。当社は１６の内部統制領域に関する基本方針および９つのリスク領域のリスク管理方針を策定し、それらはグループの雛形を参考に作られているものの、システムズ独自に定めたものである。

図表４－システムズの内部統制領域



出典： Yuichi (Rich) Inaba、許諾による掲載

それぞれの内部統制に関する基本方針では、ルール構造、組織構造および評価・改善活動（PDCA プロセス）を構築する方針を定義し、COBIT 5 の 7 つのイネーブラー目標に該当する会社のカルチャーを定義している。

IT サービス業務はシステムズの中心的業務であり、システムズ特有の内部統制としてグループの雛形にない意図的に追加したものであり、IT サービス業務はシステムズの主要な内部統制領域である。IT サービス業務に関する基本方針の第３条は特に注目すべきものである（図表５）。そこには IT サービス業務に関する指針となる原則が記述されている。また、当社がビジネスを遂行する方法、すなわち、当社のカルチャーであり、経営トップからのメッセージでもある。

内部統制管理態勢上に築かれたGRC態勢

内部統制管理態勢の構築に加えて、システムズの GRC 態勢の継続的改善のための PDCA サイクルが導入されている。図表６に GRC システムの概要を示す。

システムズでは次の通り、COBIT 5 の原則を GRC 態勢へ明示的に適用している。

1. **ガバナンスとマネジメントの分離（原則５）** ― 明確にガバナンスとマネジメントを分離し、ガバナンス層の人々は評価、方向付け、モニタリング（EDM：Evaluate, Direct, Monitor）のサイクルを実行、マネジメント層の人々は計画、構築、実行、モニタリング（PBRM: Plan, Build, Run and Monitor）のサイクルを実行する。
2. **ステークホルダーニーズの充足（原則１）** ― 図表６の左上に示すように、ガバナンス目標を「価値創出」

図表５－ITサービス業務に関する基本方針におけるカルチャーの定義

IT サービス業務に関する基本方針

第３条（指針となる原則）

経営者は次に掲げる方針に基づき業務を遂行する。

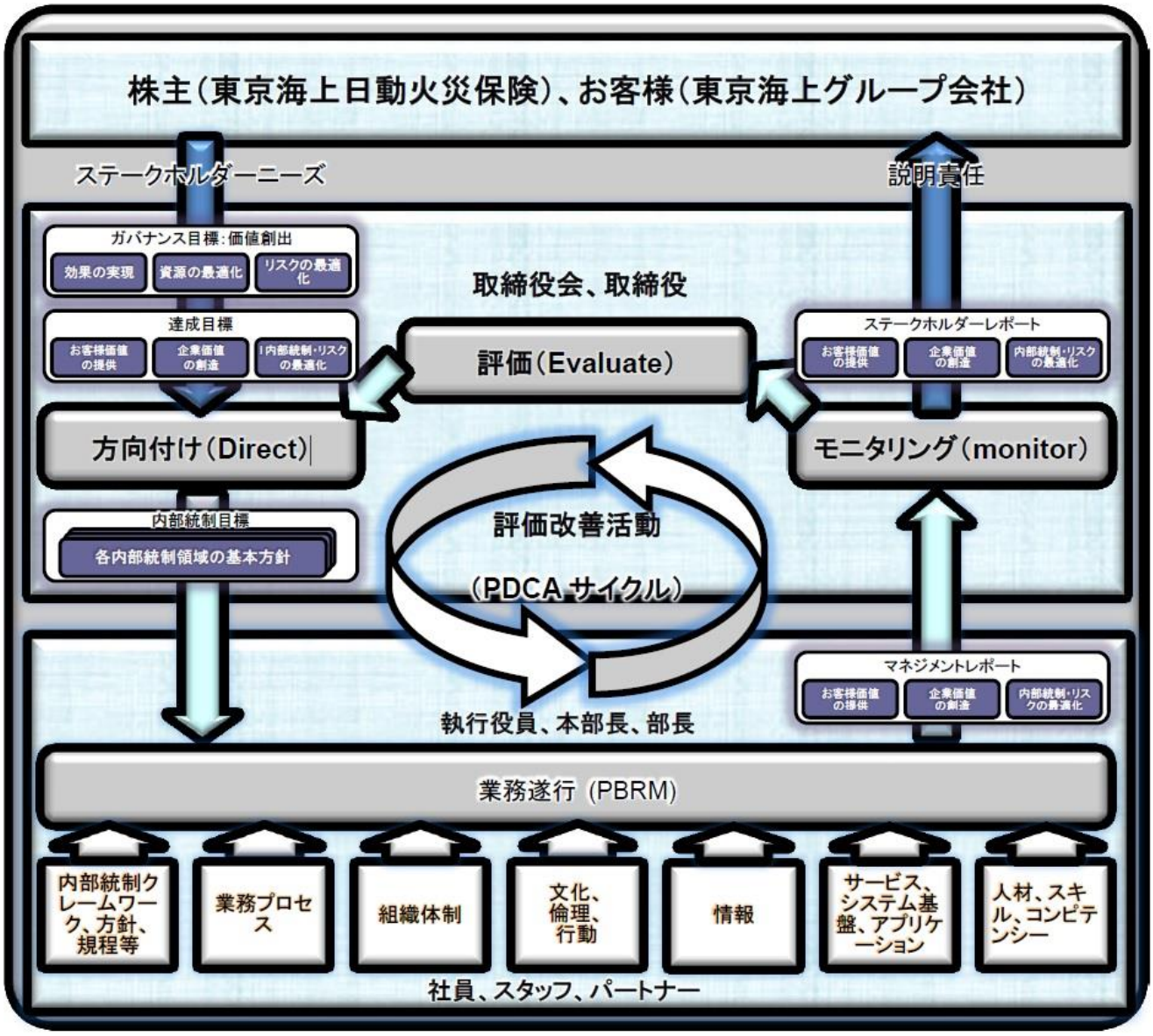
1. お客様の事業戦略を具体的なビジネスプロセスに落とし込み、お客様と同じ想いをシェアしながら業務を推進する。
2. お客様のビジネスサイドに深く踏みこんでアプリケーションオーナーと協働し、お客様の価値を共に創造する。
3. プログラムの生産量をなるべく少なく、ビジネス効果を大きく、スピードを上げることで、「システムズの品質」の極大化を共に推進する。
4. 開発と運用に関する職責を分離した上で、適切なタイミングで開発と運用の連携に基づいた業務運営を行う。

出典： 東京海上日動システムズ、許諾による掲載

と設定し、３つの部分目標である、効果の実現、資源の最適化、リスクの最適化から構成されている。この３つのガバナンスの部分目標は、次のように、会社の達成目標に１対１でカスケード（展開）されている。

- お客様価値の提供 － もっとも重要な効果は、期待どおりの QCD（品質、コスト、期間）でプロジェクトを完遂するとか、サービスレベルアグリーメント（SLA）どおりの IT サービスを提供するといったような、お客様へ価値を提供することである。
- 企業価値の創造　－ 会社にとって従業員が最も重要な資源であり、従業員のスキル開発等の育成が資源の最適化につながり、企業価値を創造することになる。
- 内部統制の最適化 － 会社はステークホルダーへの価値創出のためにはリスクを取る調整を積極的に行い、このことが内部統制の最適化につながる。

図表６－システムズのGRC態勢



出典：Yuichi (Rich) Inaba、許諾による掲載

達成目標はさらに内部統制目標、すなわちイネーブラー目標にカスケード（展開）されている。ここでは、COBIT 5 で定義されている達成目標を IT 達成目標にカスケード（展開）するプロセスは利用していない。これは、当社の内部統制領域は IT 関連領域だけではなく、非 IT 領域も含まれているためである。

3. **包括的アプローチの実現（原則４）** ー マネジメント層は PBRM サイクルに従って業務を遂行する（図表６最下部を参照）。マネジメント層は、ステークホルダーニーズを満たし達成目標を実現するために、内部統制の構成要素、すなわち、COBIT 5 の７つのイネーブラーを最大限活用するように最善を尽くす。

4. **事業体全体の包含（原則２）** ー １６の内部統制領域の基本方針および図表６に記述される PDCA プロセスは、会社全体を包含する。さらに、マネジメント層およびガバナンス層によるモニタリングプロセスは会社のすべての業務をカバーしている。マネジメント層によるモニタリングの結果について、ステークホルダーが業務成果や内部統制、コンプライアンスの状況をモニターできるように、ガバナンス層に報告される。そして、ガバナンス層はこの報告内容を評価し、マネジメント層へ推奨するアクションとして方向付けする。 このようにしてガバナンス層が EDM サイクルを実行する。さらに、ガバナンス層は外部ステークホルダーに報告し、説明責任を果たしていく。

5. **１つに統合されたフレームワークの適用（原則３）** ー 図表４に記載したとおり、１つに統合されたフレームワークとして東京海上グループの内部統制フレームワークを採用している。システムズにおいて定義された個々の内部統制領域において、ガバナンスとマネジメントの態勢のための PDCA プロセスが導入されている。これにより業務が統合された GRC 態勢によって、より効果的・効率的に遂行されている。

経営目標と達成目標の整合

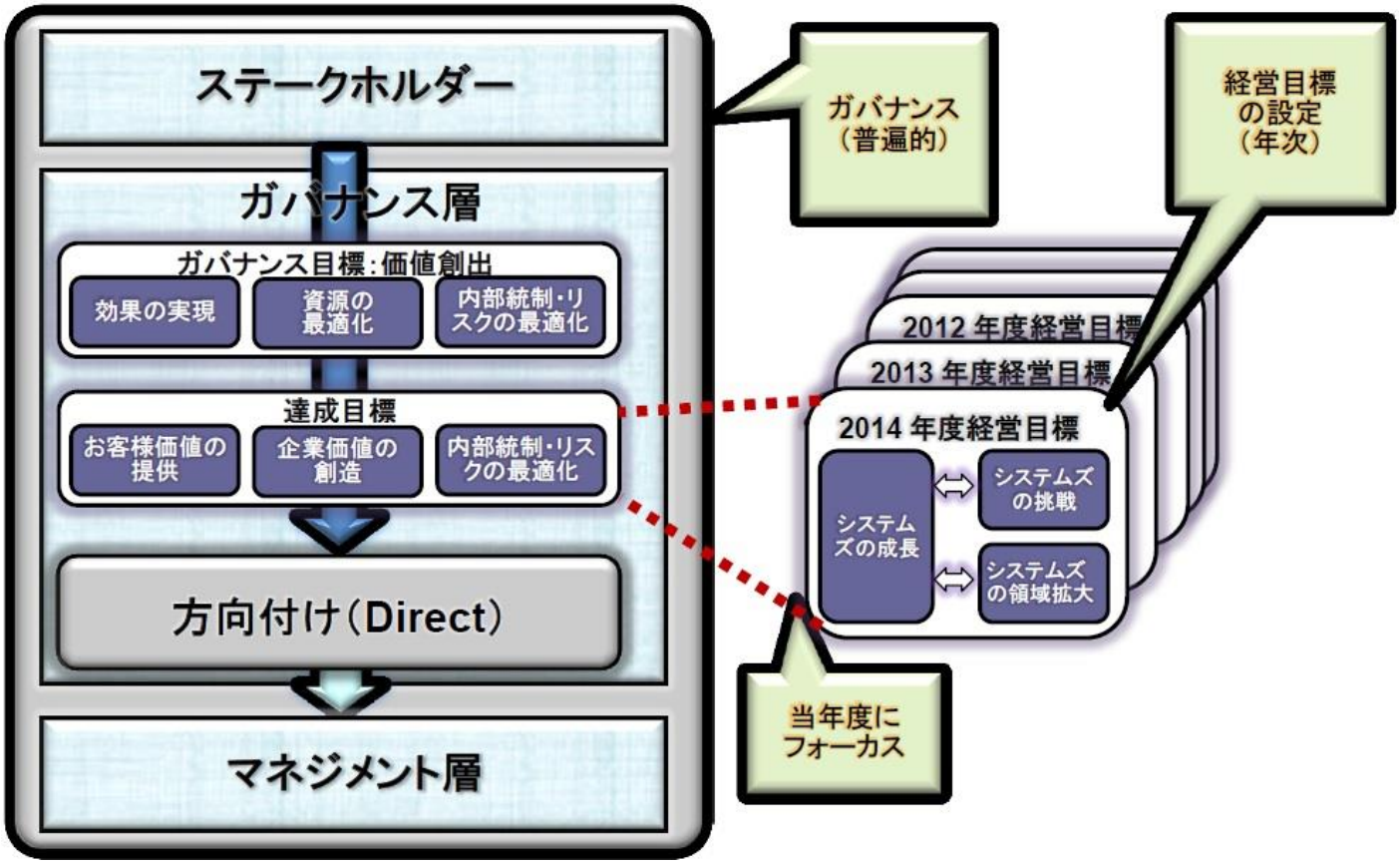
システムズでは経営者によって目標設定プロセスが実行されている認識がある。この経営目標が部門目標へとリンクされ、さらに個人目標へと連鎖させている。そして、当社はこの目標設定プロセスとGRC態勢を統合する効果的な方法にたどり着いた。

この達成目標の設定と連鎖のプロセスを明確にした結果を図表7に示す。

達成目標のカスケード（展開）プロセス（ガバナンス目標から達成目標、イネーブラー目標へ）は一般的で普遍的ものであり、一方で、経営目標を設定し組織内に連鎖させ埋め込むプロセスはその時々の経営者に依存する特定なものである。

経営目標の設定プロセスは COBIT 5 の達成目標カスケード（展開）の一部となっている。

図表７ー目標設定プロセス



出典： Yuichi (Rich) Inaba、許諾による掲載

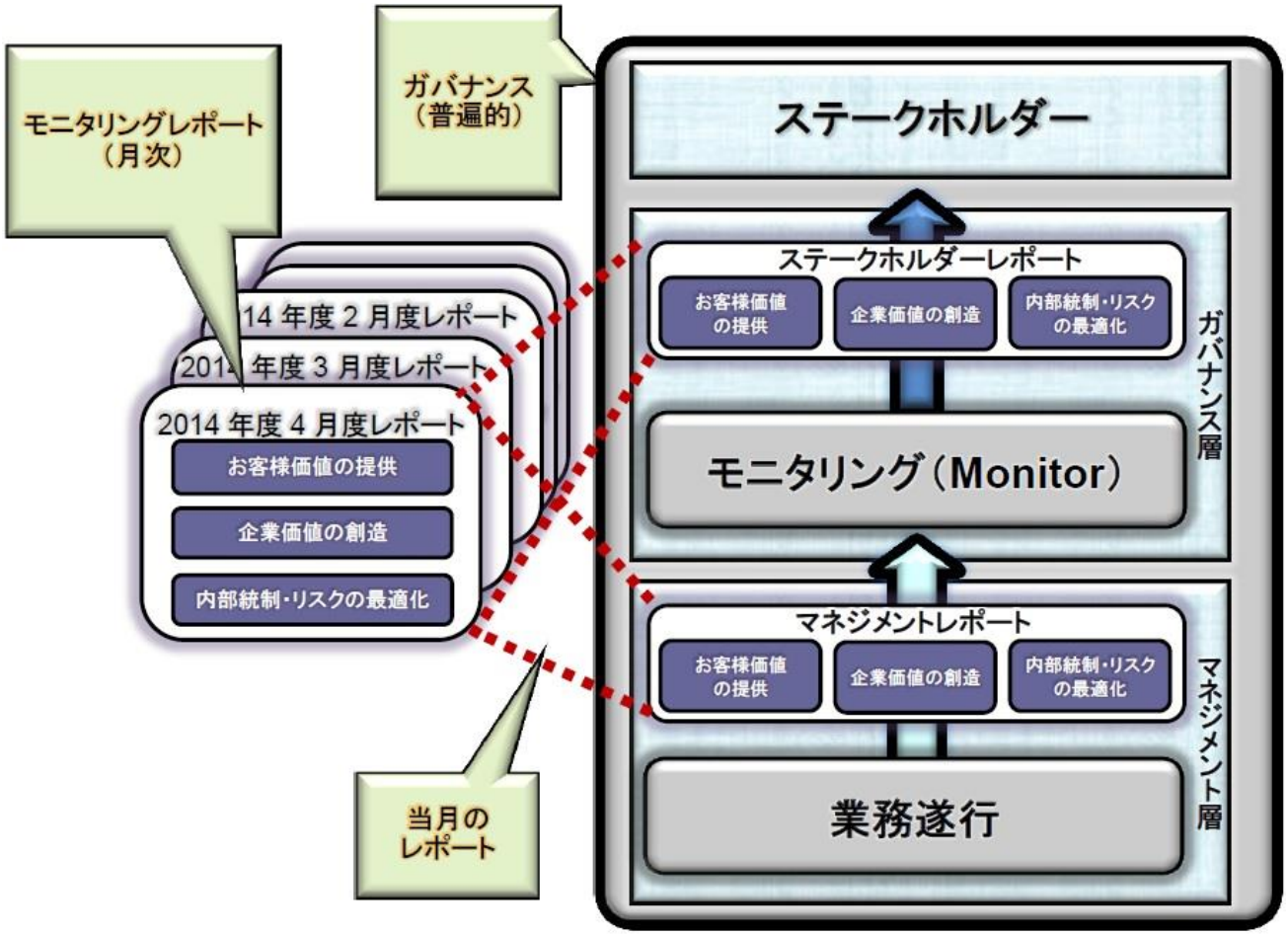
マネジメント層とガバナンス層によるモニタリング

GRC 態勢においては、COBIT 5 の MEA ドメインで定義されるプロセスに基づき、会社の業務成果や内部統制やコンプライアンスの有効性がモニタリングされる。ガバナンスチームが EDM サイクルをタイムリーに実行するために、マネジメントレポートと呼ばれるモニタリングレポートが作成され、会議体形式で取締役会に報告される。

そして、レポートはガバナンスチームにより評価され次のステップが実行される。さらに、このレポートは説明責任を果たすために会議体形式でステークホルダーと共有される。このプロセスは COBIT 5 の EDM ドメインで定義されるプロセスに従って実行されている。

図表 8 に GRC 態勢のなかでどのようにモニタリングされるかを示す。

図表 8 －マネジメントレポートとステークホルダーレポート



出典： Yuichi (Rich) Inaba、許諾による掲載

GRC態勢を業務運営基準として定義し取締役会で決議

図表６、７、８に記載したガバナンスとマネジメントサイクルはシステムズの取締役会で決議し承認されている。これは、すなわち、取締役会メンバーが GRC 態勢について自分たち自身を律する規程として定めることを決定したことを意味する。業務運営基準がシステムズの基準レベルの規定として、ガバナンスとマネジメントプロセスをルールとして定義している。

価値創出を目指した GRC 態勢を構築したことにより、会社経営はガバナンスチームを含む経営者に大きく依存することは当然である。これにより、それぞれの時代で取締役や経営者を誰が務めようとも、GRC 態勢の構築によってステークホルダーの価値を創出することが確実なものとすることができた。

ステークホルダーニーズがGRC態勢へと導く

東京海上日動システムズはステークホルダーへの価値創出を目指す GRC 態勢を構築した。受動的な内部統制管理態勢から能動的な GRC 態勢へと舵を切ったことは、ステークホルダーニーズに導かれた必然的なものであった。この GRC 態勢の導入に取り組むに際し、COBIT 5 がこの変革を強力に推進し支援してくれた。

Yuichi (Rich) Inaba, CISA

稲葉は、東京海上グループの一員である東京海上日動システムズにおける GRC 関連、IT ガバナンス、リスク管理、情報セキュリティ分野の上級エキスパート。東京海上日動システムズに異動する前は、東京海上ホールディングスの IT 企画部に出向し、COBIT 4.1 のプロセス参照モデルや成熟度モデルを活用した東京海上グループの IT ガバナンス態勢構築に従事。稲葉は、ISACA 東京支部基準委員会の副委員長を務め、ISACA 国際本部の政府・規制当局提唱アジア小委員会（GRASC1）の委員でもある。

後注

[1] 更なる学習のための参照：Inaba, Y., H. Shibuya; “**Executive Management Must Establish IT Governance**,” *COBIT Focus*, vol. 1, 2013

[2] ISACA, **COBIT 5**, USA, 2012