システム管理基準のITガバナンスと内部統制

2019年6月7日システム監査学会研究大会
ITガバナンス研究プロジェクト　清水恵子

ガバナンスの定義

コーポレートガバナンス原則

ガバナンス原則（東証2004年3月制定：2009年改訂）

- ガバナンス：企業統治
  - 株主と経営者のエージェンシー関係
  - 会社の業務執行は株主の信任関係
- 定義：企業活動を律する仕組
  - **企業の価値向上**
    - **株主の権利・利益**が守られ平等に保証される。
    - **株主以外の利害関係者の権利・利益**の尊重
    - 情報開示による
    - コストアンドベネフィットの関係を勘案しながら具体案を模索
- 体制のモデル（2009年12月22日改訂版）

システム管理基準のITガバナンス

◆IT ガバナンス

- 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。

◆ITマネジメント

- 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 ガバナンスの定義における経営陣の行動：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（E)、指示し（D）、モニタ（M)することとする。
- JIS Q 38500のEDMモデル、評価（Evaluate）、指示（Direct）、モニタ（Monitor）

IT ガバナンス原則と管理基準記載項目

ーシステム管理基準（骨子）P3P5からP7より抜粋修正して作成ー

６つの原則（JIS)

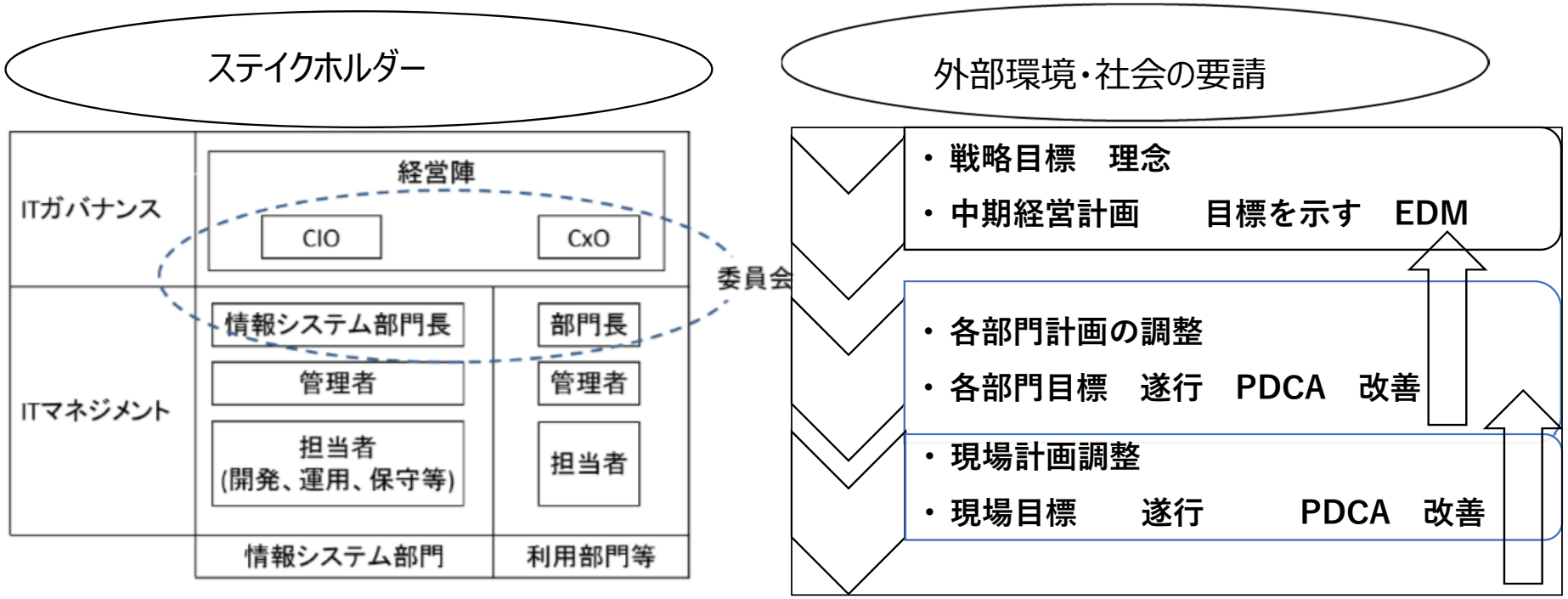
- ① 責任： 役割に責任を負う人は、その役割を遂行する権限を持つ。
- ② 戦略 ：情報システム戦略は、情報システムの現在及び将来の能力を考慮して策定し、現在 及び将来のニーズを満たす必要がある。
- ③ 取得 ：情報システムの導入は、短期・長期の両面で効果、リスク、資源のバランスが取れ た意思決定に基づく必要がある。
- ④ パフォーマンス ：情報システムは、現在及び将来のニーズを満たすサービスを提供する必要がある。
- ⑤ 適合 ：情報システムは、関連する全ての法律及び規制に適合する必要がある。
- ⑥ 人間行動： 情報システムのパフォーマンスの維持に関わる人間の行動を尊重する必要がある

管理基準ガバナンス項目

- 1. 情報システム戦略の方針及び目標設定
  - 情報システム戦略の方針及び目標の決定の手続
  - 基本計画
- 2. 情報システム戦略遂行のための組織体制
  - CIO
  - 情報システム運用委員会等
- 3. 情報システム部門の役割と体制
  - CIO配下での役割の明確化
- 4. 情報システム戦略の策定の評価・指示・モニタ
- 5. 情報システム投資の評価・指示・モニタ
- 6. 情報システムの資源管理の評価・指示・モニタ
- 7. コンプライアンスの評価・指示・モニタ
- 8. 情報セキュリティの評価・指示・モニタ

システム管理基準想定モデルとガバナンス

ーシステム管理基準より転載した想定モデルに加筆修正ー



ITガバナンスの経営陣は誰に対して説明責任を負うのか？
株主以外のステイクホルダーも尊重
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す。

コーポ―レートガバナンス：会社法の内部統制

- 会社法の機関設計（マネジメント型、モニタリング型を選択可能）
  - 監査役監査役会設置会社
  - 監査等委員会設置会社
  - 指名委員会等設置会社
- 監視監督はだれが
  - 監査役監査役会設置会社は監査役
  - 監査等委員会設置会社は監査等委員会
  - 指名委員会等設置会社は、監査委員会
  - 社外取締役の監督機能を重視
- 大会社は取締役会で内部統制整備の方針を示す義務がある。
  - 内部統制構築指示権限は委譲できない専決事項
  - 具体的な構築運用は代表取締役、執行役員

決定すべき体制：内部統制

1.取締役の職務の執行に係る情報の保存および管理に関する体制

2.損失の危険の管理に関する規程その他の体制

3.取締役の職務の執行が効率的に行われることを確保するための体制

4.使用人の職務の執行が法令および定款に適合することを確保するための体制

5.当該株式会社ならびにその親会社および子会社から成る企業集団における業務の適正を確保するための体制

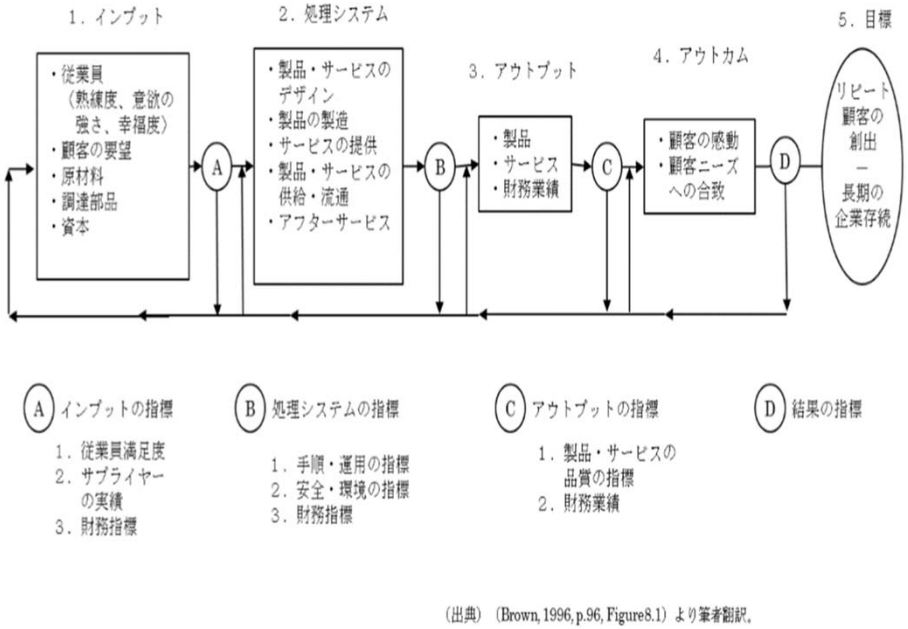
ガバナンスとマネジメント　KPIの認識

組織全体の目標を達成する指標を設け、因果関係を考慮し、構造を確立する

- 広義の内部統制はEDM（評価、指示、モニタ）とPDCAを含むプロセス
- プロセスモデルを構造として認識し組織の目標を達成するような循環があるように整備運用する。
- 参照：金融庁「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂に関する意見書」（以下「内部統制基準」）
  - 業務の有効性及び効率性財務報告の信頼性、事業活動に関わる法令等の遵守並びに資産の保全の４つの目的が達成されているとの合理的な保証を得るために、**業務に組み込まれ、組織内のすべての者によって遂行されるプロセス**をいい、
  - 統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリング（監視活動）及びＩＴ（情報技術）への対応の６つの基本的要素から構成される。

（参考）マクロプロセスモデル
公共から企業への応用

（図表７）組織体のマクロ・プロセス・モデル



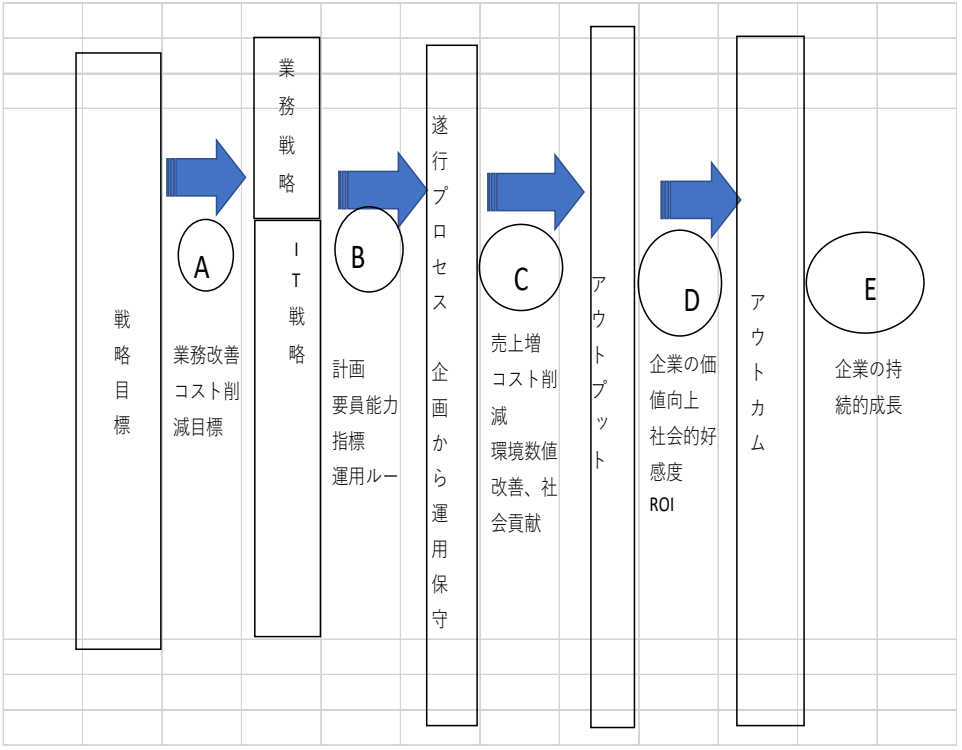
（出典）（Brown, 1996, p.96, Figure8.1）より筆者翻訳。

Bullen, Christine V. and John F. Rockart, “A Primer on Critical Success Factors”
Sloan WP , No.1220-81, June 1981の修正版を大西福本２０１６「KPIIについての論点整理」PRI Discussion Paper Series (No.16A-04)から転載

ITガバナンスのプロセスモデル
ー指標を設定し評価するー

- CEOは,組織全体の目標を明確にする。
- 組織目標を達成するための業務とその業務を遂行するためのITの構築を指示する。
- 利害関係者の要請は相反することがある。
  - 株主：利益増大による配当増
  - 従業員：雇用確保、賃金増
- ITの利用は雇用確保し、利益を増大させるか？
- CEOは異なるステイクホルダーの要請を考慮し方針を決める
- CIOは、示された方針に従って情報システムを企画開発運用保守の指揮系統を整備

- ITに関する環境を評価し（E）方針を示し指示し（D）、モニタする。
  - 方針を決め、指示する中には極端にはITを利用しない方針もありうる
  - 専任CIO必須ではなく、ITに関する方針を決め、指示する役員は必要
  - 戦略委員会も必須ではなくどの目的を達成するための手段であるかが
  - 方針を決め指示したことの実施をモニタできる仕組が必要
- ITマネジメント：管理者：PDCA：現場：PDCA
- CG白書２０１９は、CGコード実施率と株式総価に大きさに相関関係はあるとするが企業価値向上のと直接的な因果関係は立証されていない。



マクロプロセスモデル（大西福本２０１６から転載）を基に筆者作成

目標達成のプロセス過去の研究

「KPIについての論点整理」2016 年 2 月大西 淳也福元 渉
PRI Discussion Paper Series (No.16A-04) より一部を抜粋しまとめている。

・Simonsは,KPI（Key Performance Indicators：重要業績指標）活用の起源は、20 世紀初頭のデュポン社における投資利益率を展開したチャート・システムであり,KPIは,投資利益率（ROI）を財務的な要素で分解している。

・Daniel は KPI を産業別の成功決定要因と解している。

・Bullen & Rockartは組織目標としての KPI を構造化している。CSF（Critical Success Factors：主要成功要因）という指標として測定し、その測定の結果により組織行動を変える

・Kaplan と Norton のBSCの出現で,KPI を戦略の実行プロセスにおける指標と位置づける考え方である。戦略を実行していく際のプロセスそのものに着目するという特徴がある。

大西福本2016は上流で最重要項目として先行指標であるKPIを設定するほうが管理しやすいとしている。この考えに立てば上流である経営陣がITガバナンスを機能させることは重要である。

取締役会のITへの関心、関与実体調査

- JUASの調査(企業IT動向調査2019 調査結果より)
  - CIO担当役員設置状況
    - 専任3.8%兼任11.7%IT部門業務を担当する役員がいる40.1%
    - IT関連役員が不在44.4%
  - CISO設置状況
    - 設置20.4%検討中8.7%
- 東証のガバナンス白書にはCIOの調査記載は無いため数値不明。
  - CSRの記載はあるがITやセキィリティ関係ない
  - 有価証券報告書の事業のリスクにはIT関連する記載がある企業がある。
- 一 般社団法人日本サイバーセキュリティ・イノベーション委員会（JCIC）の調査「取締役会で議論するためのサイバーリスクの数値化モデル ～サイバーリスクの金額換算に関する調査～）によれば
  - 取締役レベルでサイバーセキュリティを議論すべきは海外では58%,日本では議論18%で日本では活発でないとしている。

ー

ガバナンスの課題ー組織価値は単純にはシステム投資から導けないー
経済産業省「投資評価ガイドライン」との考察ー過去の調査研究ー

- ITガバナンスの目標は組織価値向上
  - 組織によって、何が組織の価値なのかKGI
  - 企業はROIが最終目標なのか？
  - JIPDEC２０１１「18-H001 IT 投資マネジメント評価指針に関する調査研究報告書（抜粋）」は旧システム管理基準の情報戦略部分を補完するとしている
  - システム管理基準を適用する時に、CSFはなにかKPIはなにか各項目が実施できたかのチェックではなく、それが組織価値の向上に貢献できたかの視点と検証が必要
  - 単にCIOがいれば組織価値は向上するのか（JUAS２００２「ＩＴ投資の評価手法の研究 」の調査によればIT知識が十分ではないCIOが存在する）
  - 調査としてCIO専任の有無は調査されているが、CIO専任によりIT投資が企業価値向上に貢献しているかの検討が必要
    - 結果を評価するためのKPIは何か
    - システムへの投資効果の評価は、コスト削減か
    - 新システムによる新ビジネスモデルによる新規売上獲得か
- ITガバナンスの経営陣の重要な役割は説明責任を果たすこと、
- 目標達成のための評価プロセス作成の指示し、運用し改善につなげること
- IT評価につながるITマネジメントが可能なIT体制を作ること
- ガイドとして投資評価ガイドラインやプロセスモデルはあるが、実際に動く態勢にはKPIの企業にあった選定が必要ーこの認識が無いとITガバナンスの実態は動かないーこの認識の共有が課題
- 予算と評価は各企業での工夫（PDCA)が必要（JUAS２０１８ITポートフォリオ研究会分科会活動報告）
- IT投資が雇用増や賃金増との関係は業務効率化との関係で測れるか
- ガバナンスは企業の活動を律する仕組：プロセスを構築し、目標への因果関係を構造化する認識を経営陣が持つことが重要、単に形式があってもKGI、KPIが何かが認識されないと実働できない。

ITガバナンスの目指す目標はステイクホルダーの満足
ー管理基準項目から設定するKPIは結果か手段かー

ITガバナンス・ITマネジメントの構造化が必要
目標を達成する因果関係があるような態勢の構築
ーKPIは目標達成のための途中の手段か最終目標かー
ーステイクホルダーの利害対立の単純調整ではなく要望の統合を図るガバナンス

- 顧客満足増加：売上増大：企業価値増は従業員満足低下なのか
- IT導入は、関係者の対立を生むか
- 経営陣はITと業務の流れを把握し、

課題を把握する。

- 顧客、従業員、株主が満足するガバナンス,組織内のマネジメント
- 利害調整ではなく要望の統合（M.P・フォレット建設的コンフリクトと統合）
    - 情報技術は統合的システムでコンクリフトを明確に洗い出すか,コンクリフトが不明確なままグループ間の見方の相違を明らかにする。（三戸公坂井正廣１９９９第2章序説ジョン・チャイルド）

- 単に管理基準の留意点をチェックするのでなく、全体として組織目標に近づいているかを検証できるKPIを設定できるか
- 戦略委員会はどのようなCSF、KPIを提示できるか（建設的コンクリフトの解消）
- IT投資の変化（JUAS２００２「ＩＴ投資の評価手法の研究 」で既に指摘）
    - ハードウェアへの投資からAIやクラウド、IoTに移行すなど経営戦略と結びつく、もしくはビジネスそのものになっているため評価が難しい。
- IT知識と問題解決の訓練が必要
- 経営の心理的アプローチは今後も調査検証が必要
- 経営者は、企業の成長は株主、従業員,消費者,取引先の誰かの犠牲で他を発展させるのではなく、互いに成長できるように要望を統合することにより、企業の持続的発展と社会の持続性を維持できる。IT部門は経営の方針を支援する。

参考文献

- Committee of Sponsoring Organizations of the Treadway Commission〔COSO〕,Internal Control-Internal Control-Integrated Framework, AICPA, September 1992 and May1994,（鳥羽至英・八田進二・高田敏文共訳[1996]『内部統制の統合的枠組みー理論編―』白桃書房）
- Committee of Sponsoring Organizations of the Treadway Commission〔COSO〕Guidance on Monitoring Internal Control System, AICPA, 2009(八田進二監訳太陽ASG有限責任監査法人訳[2009]『COSO内部統制システムモニタリングガイダンス』日本公認会計士協会出版局)
- Committee of Sponsoring Organizations of the Treadway Commission〔COSO〕,Internal Control-Internal Control-Integrated Framework, AICPA, 2013（八田進二・箱田順哉監訳[2013]『内部統制の統合的枠組みー理論編―』『内部統制の統合的枠組みーツール編―』『内部統制の統合的枠組みー外部財務報告編』日本公認会計士協会出版局）
- Committee of Sponsoring Organizations of the Treadway Commission〔COSO〕Enterprise Risk Management Integrating with Strategy and Performance2017(一般社団法人日本内部監査協会監訳 八田進二他監訳[２０１８]『全社的リスクマネジメントー戦略およびパフォーマンスの統合―』同文館)
- Dynamic Administration －The Collected Papers of Mary Follet, edited by Henry c.Metcalf and L.Uriwick, Harper & Row,Publishers1949（米田清貴・三戸公共訳[1980]『組織の行動原理』未来社）
- IIA[2013]The Three Lines of Defense in Effective Risk Management and Control, IIA ResechFundation
- JIPDEC２０１１「18-H001 IT 投資マネジメント評価指針に関する調査研究報告書（抜粋）
- JUAS２００２「ＩＴ投資の評価手法の研究 」
- JUAS２０１８「ITポートフォリオ研究会分科会活動報告」
- JUAS２０１８「企業IT動向調査2019 」
- 大西淳也　日置瞬２０１４「ロジック・モデルについての論点の整理 」PRI Discussion Paper Series (No.16A-08)
- 大西淳也　福元渉2016年2月「 KPIについての論点整理」PRI Discussion Paper Series (No.16A-04)
- 経済産業省ＣＧＳ研究会 中間整理２０１８「実効的なコーポレートガバナンスの実現に向けた今後の検討課題 」
- 東京証券取引所２０１４改訂２０１９「上場会社コーポレート・ガバナンス原則 」
- 東京証券取引所２０１８年6月「コーポレートガバナンス・コード」
- 東京証券取引所２０１９「コーポレートガバナンス白書」
- 日本弁護士会２０１９「社外取締役ガイドライン」
- 三戸公　坂井正廣　監訳１９９９「M・P・フォレット管理の預言者」分眞堂