

KCM (ナレッジ・チェーン・マネジメント)・ e-KCM による COSO 改訂版内部統制と ERM の構築

上 原 衛

1. はじめに

近年、組織を取り巻く環境が大きくかつ急激に変化しており、リスクの複雑さ不透明さが増している。組織は、日々の業務をこなしたうえで、このようなリスクを回避しつつ、新しい機会を逃さず捉え、新たな戦略を立案・実行していく必要がある。絶えず変化している事業環境の要請に則して、組織がリスクを管理するためのアプローチとしての全社的リスクマネジメント (Enterprise Risk Management: 以下 ERM という) の重要性が増している。

このような経営環境の変化に対応するために、米国トレッドウェイ委員会支援組織委員会 (Committee of Sponsoring Organization of the Treadway Commission: 以下 COSO という) は、2004年に公表されて以来、リスク管理の手法として広く受け入れられてきた「ERM—統合的フレームワーク」を2017年9月に改訂した。COSOは2017年のERM改訂に先立つ2013年に、内部統制のフレームワークも改訂しており、これによって、内部統制とERMの両者を、進化しつつある事業環境の要請に則した対応を整えた。近年のように、変化の激しい事業環境の下では、内部統制とERMの役割はより一層重要になり、有効に機能することが期待されている。しかし、内部統制とERMが相次いで改訂されたこともあり、両者の関連性や、位置づけについて分かり難いところが生じてきた。また、いかに良いフレームワークであったとしても、両者の関係性や位置づけが理解されていなければ、導入の負担が増えるだけであり、スムーズに組織内部に定着・浸透させることはできない。

本稿では、まず、COSOの内部統制とERMの改訂の経緯、両者の改訂版の関係性と位置づけを整理する。そのうえで、組織の内部に内部統制構築と、企業の戦略と整合性のある企業全体のリスクを総合的に管理するERM構築とを別々に考えず、両者を統合した概念で捉える必要性を提示する。そのために、知識を共有し組織学習を行うことによって効率的活動や創造的・革新的活動に進展させていくためのナレッジ・チェーン・マネジメント (Knowledge Chain Management: 以下 KCM という)[1]、さらに、e-KCM[2][3] の概念を導入して、組織の「統制環境」「カルチャー」という基盤・土台の上に、内部統制とERMを統合して構築する方法を提示する。

2. 内部統制・ERM 体制構築の必要性

内部統制強化の要請が高まってきている現状の認識と、内部統制を深化させたERMの必要性について、著者の先行研究[4][5]に基づき以下に概観する。

2.1 内部統制強化の要請

近年、日本のみならず世界中のビジネス社会において、新しい機会が生まれる一方で、潜在的风险も増加している。そして、そのリスクが顕在化する事例が多く報告されている。特に、企業や公的機関の不正や不祥事は後を絶たず、また、顕在化したリスクへの対応を間違えたがゆえに、さらなる膨大な対価を支払い、企業の株主価値を減少させ、企業の評判を傷つけ、ついには企業の崩壊につながった数多くの事例を目撃してきた。そのため、企業の内部統制強化が求められている。

このような状況下で、1992年に、トレッドウェイ委員会支援組織委員会(COSO)は「内部統制の統合的枠組み」(Internal Control—Integrated Framework)を発表した。そして、COSOのこの内部統制の枠組みに基づいて、米国では企業改革法(Sarbanes Oxley Act:以下SOX法という)が施行された。そして、日本でも日本版SOX法(J-SOX)といわれる「金融商品取引法」が2006年6月に成立し、経営者による内部統制評価と報告(内部統制報告書)と、監査人による内部統制監査(内部統制監査報告書)が上場企業に求められることとなった。また、2005年8月に改正された新「会社法」では、その362条5項で大会社(資本金5億円または負債200億円以上)の「取締役による内部統制整備義務」が課せられた。このように、日本企業に対して内部統制の体制整備を求め、このことを内外に示したことは、規制緩和、経営の健全性確保、グローバル化という厳しい競争環境におかれた日本企業への対応を意図したものと認識できる。

2.2 内部統制を深化させたERMの必要性

今日、企業が直面するリスクは、会計・財務の観点からのリスク管理のみならず、自然災害・テロ・戦争、コンプライアンス違反、ガバナンス体制の不備、そしてコンピュータ・ウイルスなどによるセキュリティ侵害、個人情報の漏洩など、種類も範囲も広範である。したがって、従来型の断片的かつ事後処理型の受け身のリスクマネジメントから脱し、また、さらに一歩進めてビジネス戦略と整合的なレベルで、企業全体にわたる統合的かつ継続的に実施する新しいリスクマネジメントの採用が求められている。そのためには、これらすべてのリスクを管理するためにはSOX法の立法精神をくみ取り全社的な内部統制体制を構築するとともに、内部統制をさらに深化させる必要が生じた。そこで、COSOは2004年に、「Enterprise Risk Management:ERM(全社的リスクマネジメント)—統合的フレームワーク」を公表した。

このERMを構築することにより、企業価値に対する信頼性が高まる。ERMは、まさに企業価値を最大化させる長期的戦略作成のための体制づくりといえる。リスクが統合され、戦略的かつ、組織横断的に実施するERM[6]への移行が必要となっている。その意味で、著者はこれまでERMを「戦略的総合リスクマネジメント」[4]と呼ぶことを提唱してきた。

3. COSOの内部統制とERMの改訂

3.1 2013年「改訂版COSO内部統制」

2013年5月に、COSOは「内部統制の統合的フレームワーク」の改訂版を公表した。1992年に、「内部統制の統合的枠組み」(Internal Control—Integrated Framework)を発表以来、約20年ぶりとなるこの改訂は、昨今の複雑化したビジネス環境に合わせて、フレームワークを見直したものと位置づけられている。1992年から比べると、この20年間で、ビジネスを取り巻く環境は大きく変化した。たとえば、ビジネスモデルや組織のみならず、利用するテクノロジーも大きく変わった。また、グローバリゼーションも大きく進展した。さらに、ステークホルダーのビジネスに対する見方とかかわり方も大きく変わり、内部統制に関して、組織に対する期待値が一層高まってきた。このように、組織の外部環境・内部環境とも大きく変化してきたため、内部統制に及ぼす影響も非常に大きく、COSOは内部統制のフレームワークを改訂することとなった。

2013年改訂版COSO内部統制のフレームワークの主な改訂ポイントは、以下の2点である。

①内部統制を支える「原則」と「着眼点」

内部統制の5つの構成要素(「統制環境」「リスクの評価」「統制活動」「情報と伝達」「モニタリング活動」)それぞれを支える概念が17の「原則」として明示され、それぞれの原則を満たすための実務上のポイントが「着眼点」として例示された。

②目的の「財務報告の信頼性」を「報告の信頼性」へ変更

内部統制の目的のひとつである「財務報告の信頼性」が「報告の信頼性」と変更され、その範囲が広がり、非財務情報の報告も目的に含まれることとなった。また、報告には「内部向け報告」と「外部向け報告」が含まれることが明示された。

この2013年の改訂に従い、米国で上場している日本企業は、2014年12月15日以降、新フレームワークを使用する必要がある。

そして、内部統制の5つの構成要素はどれも重要性は同じであるが、順番としては、最初に「統制環境」が確立されなければならないと考えられている。

3.2 「2013年版COSO内部統制」と「COSO ERM」との関係

2013年改訂版COSO内部統制のフレームワークは、その改訂が報告の範囲を財務以外にも拡

大するなどによって、COSO ERM のフレームワークに近づいてきた。そこで、内部統制のフレームワークと ERM の2つのフレームワークについて、これらをどのように連携して機能させるかを整理する必要が生じてきた。COSO は、2014年2月に“Improving Organizational Performance and Governance: How the COSO Frameworks Can Help”[7]を公表し、内部統制と ERM の両フレームワークの関係を示した。この文書は、ERM のフレームワークは、目的の設定と特定、目的の達成に向けたリスクの緩和または受容に基づいていると述べており、また、内部統制のフレームワークは、目標を達成するためにリスクを受容可能なレベルまで減らすことによってリスクを管理するように設計されていると述べている。そして、両フレームワークは、目的の達成を通じて事業の運営に密接に結びついているとしている。

3.3 2017年版 COSO ERM

COSO の「ERM—統合的フレームワーク」は、2004年に初めて公表されて以来、リスク管理手法のグローバル・スタンダードとして位置づけられてきた。しかし、残念ながら組織への浸透・定着は十分とはいえなかった。その理由としては様々な要因が考えられるが、世界的に経済が低迷し複雑化し、不確実性が増加し続けているなかで、リスク管理に時間とコストを費やすことができない、また、時代の流れの速さに対応するためには多少の無理もやむを得ないという、経営者の考え、そして、組織全体の雰囲気や組織風土があったのではないかと考える。

このような情勢に鑑み、COSO は2017年9月にERM フレームワークの改訂版として、「全社的リスクマネジメント：戦略およびパフォーマンスとの統合」[8][9]を公表した。2004年版ERM フレームワークは、企業、特に経営者層にあまり浸透・定着しなかったことを教訓として、2017年の改訂では経営者に理解と共感を得て、活用できることを意識させているものとする。したがって、改訂版では、戦略策定時や日常業務においてリスクを関連づけて意思決定を行うことが有意義であることや、目標となるパフォーマンスを達成するため、また、事業戦略・目標に適合した取るべきリスク（リスク選好）を決定することが有効であることなどが提示されている。すなわち、組織管理のひとつの手法としてERM の検討を促しており、「ERM の重要性と役割は、組織運営を支援し、パフォーマンスを管理し、最終的には価値を創造し、実現し、維持するという視点から示される」[10]のである。

改訂版ERM では、5つの構成要素（「ガバナンスとカルチャー」、「戦略と目標」、「パフォーマンス」、「レビューと修正」、「情報、伝達および報告」）と20の原則が提示されているが、基本的に2004年版ERM を踏襲している。しかし、用語について加筆・修正がなされ、リスクを戦略やパフォーマンスと統合し一体のものであることが強調されるなどの様々な改訂が行われている。

2017年改訂版ERM と2013年版内部統制との関係性については、内部統制はERM の基盤として、改訂版ERM に位置づけられている。そして、改訂版ERM と2013年版内部統制との間に優劣はなく、別個のものであり、互いを補完する関係にあるとしている。改訂版ERM

においては、冗長性を避けるために、両フレームワークに共通した内部統制の特徴は、改訂版 ERM では繰り返されていない。2014年2月に“Improving Organizational Performance and Governance: How the COSO Frameworks Can Help”[7]でも触れられていたが、ERM フレームワークは事業機会に関連する戦略的意思決定プロセスに係わるリスクに適用され、内部統制のフレームワークは戦略設定で特定された事業活動の遂行に係わるリスクに対応するために適用される。

また、改訂版 ERM では、「カルチャーが全社的リスクマネジメント活動に与える影響の重要性は、改訂文書に導入された最初の概念の一つである」[11]とされており、さらに重要なことは、「カルチャーは、リスクの識別と評価、これらのリスクへ対応する際の資源の配分を提供することである」[11]とも示されている。著者が実務上最も重要であると考えられるポイントは、ERM を構築するために必要とされる5つの構成要素のなかの「ガバナンスとカルチャー」の「カルチャー」である。取締役会は、戦略を監視し、ガバナンスの責任を果たすことにより、経営者が戦略と事業目的を達成できるように支援する。そして、組織のカルチャーは、リスクの識別、評価、対応に影響を及ぼすため、組織にとって望ましいカルチャーを作りあげていくことは、取締役会および経営者の責任である。カルチャーは、組織文化・組織風土と捉えても良いかもしれないが、これを適切に備えていない組織が、リスクへの対応を怠り、コンプライアンスやガバナンスへの軽視へと至るのである。カルチャーの内容や強さは、組織の内部環境や組織構成員のリスクに対する姿勢に影響を与える。しっかりとしたカルチャーを有する組織こそが、ERM を実現できるのである。

4. 知識の連鎖と共有による内部統制と ERM の構築

知識の連鎖と共有による ERM の構築に関しては、著者の先行研究[5]で述べたが、COSO の内部統制と ERM がそれぞれ改訂されたことに伴い、再度、知識の連鎖と共有によって内部統制と ERM を構築することについて、以下に再確認する。

4.1 知識の連鎖と共有による内部統制と ERM の統合と GRC 対応

3.3節でも述べたとおり、2017年改訂版 ERM と 2013年版内部統制との関係性については、両者の間に優劣はなく、互いを補完する関係にある。ERM フレームワークは事業機会に関連する戦略的意思決定プロセスに係わるリスクに適用され、内部統制のフレームワークは日常の事業活動の遂行に係わるリスクに対応するために適用される。したがって、内部統制構築と、企業の戦略と整合性のある企業全体のリスクを総合的に管理する ERM 構築とを別々に考えず、両者を統合した概念で捉えるべきである。また、日本の企業は、これまでも断片的・部分的かつ分散した GRC (ガバナンス (governance), リスクマネジメント (risk management), コンプライアンス (compliance)) は行ってきた。これらの個別の GRC について、それぞれの担当部署

が独自に行ってきたケースが多く、被監査部署である現場は同様の監査を何度も受けることとなり、負担が増大し、業務の効率性からはかけ離れた手間のかかる単なる管理プロセスとの認識に拍車をかけてきた。しかし、情報システムの進展により、組織の中に存在する個別・断片的なリスクマネジメントの知識を、組織の中で共有化することによって、GRC 実施業務の重複部分を大きく削減できる。近年、企業におけるパートナーリングやコラボレーションへの関心の高まりを背景に、組織における「情報共有」の重要性がクローズアップされている。その一方で、情報共有のみでは不十分であり、これに「知識共有」が加わってこそ意味があるという指摘がなされており、このような、「知識」に対する注目は、ナレッジ・マネジメント（知識の連鎖：Knowledge Management；以下 KM という）が契機になっているといわれている[12]。

ERM が対象とする事業機会に関連する戦略的意思決定プロセスに係わるリスクと、内部統制が対象とする日常の事業活動の遂行に係わるリスクの両方に対応するため、また、組織の中において断片的かつ分散して保有されている GRC の知識を、組織が共有し学習することによって、業務の効率化や創造的・革新的活動へと進展させていくために、KCM さらには e-KCM の利用が考えられる。

以下に、KM 並びに KM を企業間の知識共有に拡張した KCM、KCM の方法論の中核に e-Learning を位置づけた e-KCM について概説する。

4.2 KM から KCM・e-KCM へ

KM の概念の拡張について、林ら[1] は対象領域と知識活用レベルの2つの側面から研究を展開している。そのひとつが、ICT の急速な展開により、企業間の知識共有が容易になったという側面であり、もうひとつは、経営環境が大きく変化し、企業間競争が、企業対企業から企業群対企業群、あるいはサプライチェーン対サプライチェーンへと拡大しつつあるという側面である。このような流れの中で、企業間 KM の知識活用レベルは、スタティックな既存知識の活用レベルから、知識をベースにイノベーションや創発を起こさせるダイナミックな活用へと進化しつつある。最近、注目を集めているコラボレーティブ・コマース (Collaborative Commerce) を実現するためには、企業間の知識共有システムが不可欠である。そこで、互いに協力関係にある企業群の企業間で知識を共有する KCM のマネジメント・コンセプトが必要となるのである。KCM は、他の企業群に対する、自社の属する企業群の競争優位を実現するために、企業間の知識共有とコラボレーションを実現させ、バリューチェーンの構築を目指すものである。

以上のような KM と KCM の動向をふまえて、林ら[2][3] は e-KCM のマネジメント・コンセプトを提示している。e-KCM は、これまで KM において個別企業ごとに行われてきた「知識共有」を、企業横断的な、あるいはサプライチェーン全体での知識共有へと拡張するという KCM の方法論の中核に e-Learning を位置づけるものである。ここで、e-Learning を e-KCM の中核に位置づけるのは、KM から KCM への知識共有の拡張過程で、ICT の有効活用

とメンバーの能動的学習が重要な役割を果たすためである。すなわち、e-Learningの方法論をKCMに活かすことにより、KCMにおける知識共有とe-Learningにおける知識共有を統合するのである。林ら[3]はこれを「二重の知識共有」と呼んでいる。e-KCMでは、この二重の知識共有により、メンバーの自動化と環境へのアジルな対応の両立を目指すのである。

このようなKCMからe-KCMへの流れには、以下の特徴がある。

- (1) KCMからe-KCMへの流れは、バリューチェーンの源泉を人間の知的・創造的活動、とりわけメンバーの学習に求める。
- (2) 上記の知的・創造的活動や学習によって生み出される価値の高い情報・知識をネットワーク上で共有する。
- (3) メンバーの学習によるエンパワーメントや自動化、すなわちバリューチェーンの深化に主眼がおかれる。
- (4) ICT活用の主たる目的が、人間の知的・創造的活動や学習の「支援」[13]にある。

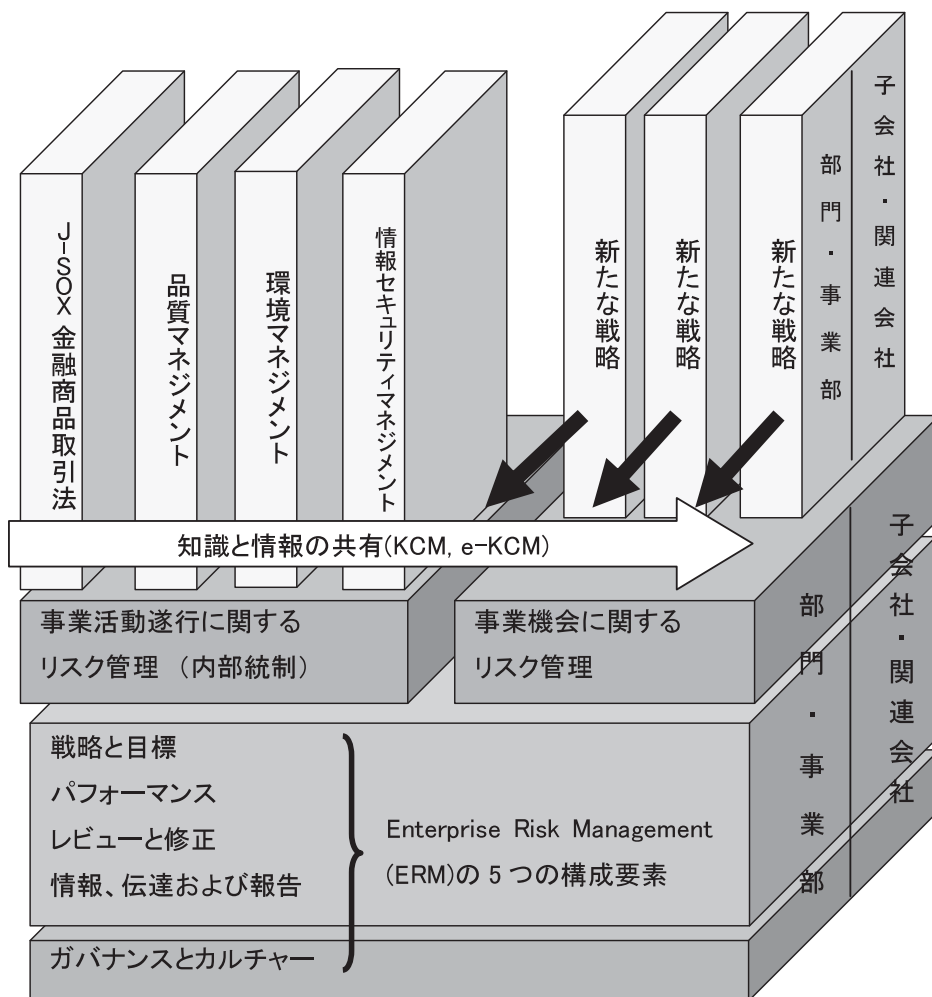


図1 KCM, e-KCMによるGRC知識共有による改訂版内部統制・ERM構築の概念図

4.3 KCM・e-KCMによる内部統制とERMの構築

ERMが対象とする事業機会に関連する戦略的意思決定プロセスに係わるリスクと、内部統制が対象とする日常の事業活動の遂行に係わるリスクの両方に対応するため、また、これまで個別・断片的に行ってきたGRCに対応し、内部統制とERMを構築するために、KCM・e-KCMの利用が考えられる。KCM、e-KCMによるGRC知識共有による改訂版内部統制・ERM構築の概念図を図1に示す。

2017年改訂版ERMと2013年版内部統制の両者の間に優劣はなく、互いを補完する関係にある。ERMは事業機会に関連する戦略的意思決定プロセスに係わるリスクに適用され、内部統制は日常の事業活動の遂行に係わるリスクに対応するために適用される。したがって、内部統制構築と、企業の戦略と整合性のある企業全体のリスクを総合的に管理するERM構築とを別々に考えず、両者を統合した概念で捉えるべき(図1の中段)であることは、4.1節で述べたとおりである。

また、我が国においては、これまでGRCをそれぞれの担当部署が断片的かつ個別に組織に対して指示を行い、またそれに伴って、被監査部署である現場はその都度同様の監査を何度も行うこととなり、監査・被監査部署双方にとって多大な業務負担が生じていた。内部統制の目的のひとつである「業務の有効性と効率性」に反する現象が生じているのが現状である。日本の企業は、日常の事業活動の遂行に係わるリスク管理として、これまでJ-SOXのみならず、品質マネジメント対策(ISO9001)、環境マネジメント対策(ISO14001)、情報セキュリティマネジメント対策(ISO27001)、ITガバナンス(COBIT)など、種々のGRC対応をこなしてきた実績がある。これらの個別・断片的なGRC知識を、KCM・e-KCMを利用して組織横断的に知識と経験を共有し、能動的な組織学習を行い、統合的に捉えるべきである(図1の上段左部分)。さらに、新たな戦略に基づく事業機会に関連する戦略的意思決定プロセスに係わるリスク管理として改訂版ERMを適用して対応することになる(図1の上段右部分)。

そして、内部統制とERMの統合した対応と、個別・断片的に存在していたGRCへの統合した対応を、全社で統一的な「統制環境」ないしは「カルチャー」という基盤・土台の上で統合していけば、内部統制とERMの体制が構築できるものとする(図1の最下段)。特に、子会社・関連会社のみならず場合によっては業務委託先の企業との知識共有が不可欠となるため、個別企業ごとに行われてきた「知識共有」を、企業横断的な企業群として知識共有へと拡張するというe-KCMの導入による内部統制とERMの構築が達成可能である(図1の上・下段右側面と中段の矢印)。e-KCMによる知識の共有と能動的な組織学習によって、内部統制とERMを組織とその日常の業務プロセスの中に深く浸透させることができ、組織の「統制環境」「カルチャー」に深く溶け込ませ、定着させることができる。

しかし、あくまでも、内部統制とERMを統合し定着させる土台は、「統制環境」ないしは「カルチャー」であり、この基盤・土台なくしては全社的に統合された内部統制とERMは構築できないことを再度強調しておきたい。

5. おわりに

本稿では、相次いで改訂された COSO の内部統制と ERM について、その改訂の経緯、両者の改訂版の関係性と位置づけを整理した。両者の関係性については、内部統制は ERM の基盤として位置づけられており、改訂版 ERM と改訂版内部統制との間に優劣はなく、別個のものであり、互いを補完する関係にある。そして、ERM は事業機会に関連する戦略的意思決定プロセスに係わるリスクに適用され、内部統制は日常の事業活動の遂行に係わるリスクに対応するために適用されている。したがって、内部統制構築と、企業の戦略と整合性のある企業全体のリスクを総合的に管理する ERM 構築とを別々に考えず、両者を統合した概念で捉えるべきであることを提示した。

そして、内部統制と ERM を統合して構築し組織に定着・浸透させるための方法として、まず、知識を共有し組織学習を行うことによって効率的活動や創造的・革新的活動に進展させていくための KCM、さらに、e-KCM の概念の導入について提示した。そのうえで、組織の「統制環境」「カルチャー」という基盤・土台の上に、内部統制と ERM を統合して構築することの重要性を示した。

COSO の改訂版内部統制と ERM の構築に際して、世界的に関心が高まっているが、本研究がその導入推進と浸透・定着の一助となれば幸いである。

参考文献

- [1] 林誠, 原田要之助, 山田啓一: ホロン型経営システムの可能性と課題, 経営情報学会 1995 年春季全国研究発表大会発表要旨, pp. 81-85, 1995
- [2] 林誠, 山下洋史, 金子勝一: e-ナレッジチェーン・マネジメント (e-KCM) に関する研究, 第 28 回日本経営システム学会全国研究発表大会講演論文集, pp. 83-86, 2002
- [3] 林誠, 山下洋史: Global e-KCM に関する研究, 第 29 回日本経営システム学会全国研究発表大会講演論文集, pp. 163-166, 2002
- [4] 上原衛: ERM 体制を構築・維持するための IT への対応とセルフアセスメント, 愛知淑徳大学論集 ビジネス学科・ビジネス研究科篇 第 3 号, pp. 1-15, 2007
- [5] 上原衛: KCM (ナレッジ・チェーン・マネジメント)・e-KCM による ERM の構築, 愛知淑徳大学論集 ビジネス学科・ビジネス研究科篇 第 4 号, pp. 1-15, 2008
- [6] Thomas L. Barton, William G. Shenkir, Paul L. Walker 著, 刈谷武昭, 佐藤勉, 藤田正幸訳: 収益を作る戦略的リスクマネジメント, 東洋経済, 2003
- [7] DeLoach, J., & Thomson, J.: Improving organizational performance and governance how the COSO frameworks can help, Research Commissioned by COSO [online], 2014, Accessed November 05, 2018, from www.coso.org/Documents/2014-2-10-COSO-Thought-Paper.pdf
- [8] 一般社団法人日本内部監査協会, 八田進二, 橋本尚, 堀江正之, 神林比洋雄 (監訳): COSO 全社的リスクマネジメント—戦略およびパフォーマンスとの統合—, 同文館, 2018

- [9] Committee of Sponsoring Organizations of the Treadway Commission (COSO): Enterprise Risk Management Integrating with Strategy and Performance, AICPA, New York, 2017
- [10] 前掲書 [8], p. 300
- [11] 前掲書 [8], p. 301
- [12] 鄭年皓, 折戸洋子, 山下洋史: KCMにおける「公共財」としての情報と知識, 第35回日本経営システム学会全国研究発表大会講演論文集, pp. 166-169, 2005
- [13] 山下洋史: 日本の組織における「支援」の役割, 支援基礎論研究編『支援学』, 東方出版, 2000