[研究奨励賞]

IT ガバナンス向上に向けたガイドラインの活用に関する提言

Proposal of Utilizing Guidelines for Good Governance of IT

神橋　基博
Motohiro Kambashi

情報セキュリティ大学院大学
Graduate School of Information Security

概　要

企業の経営者が IT ガバナンスを強化するためには、自社の現状を判断する必要があり、良悪の具体的な尺度としてのガイドラインがあることが望ましい。一方、IT ガバナンスに関する国際標準としては ISO/IEC 38500、日本工業規格としては JIS Q 38500 があるが、具体的な尺度は含まれていない。

IT ガバナンスに関連するガイドラインの内､具体的な判断尺度を含むものとして「システム管理基準」､「情報セキュリティ管理基準」､「金融機関等のシステム監査指針」､「COBIT 5 Enabling Processes」がある。これらのガイドラインが IT ガバナンスと、どの程度関連しているかを分析するため、テキストマイニングを用いて関連性を定量的に評価した。各ガイドラインにおける IT ガバナンスとの関連性の分布に基づき、企業の経営者がこれらのガイドラインを使用して IT ガバナンスを強化する際に追加が必要となる判断尺度を提言する。

キーワード：IT ガバナンス、ISO/IEC 38500、JIS Q 38500、システム管理基準、情報セキュリティ管理基準、COBIT 5

1．はじめに

グローバル化する経済の中で、企業が競争力を獲得し､社会に有用な価値を提供し続けるために､経営者には IT を駆使した企業経営が求められる。

図 1 に示す通り、リーマンショックによる一時的な落ち込みは見られるものの、企業は IT 予算を毎年増加させており、2016 年には過去最高水準に到達している。

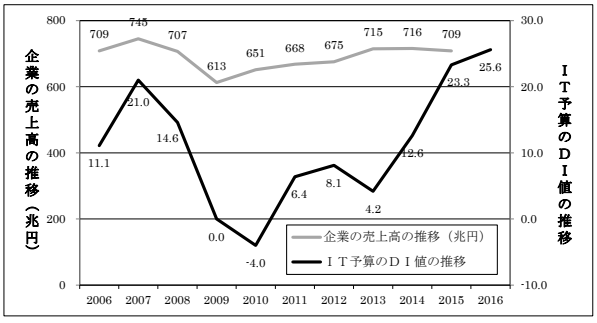

図 1　企業の売上高と IT 予算の DI 値 [a] の推移 [1]、[2]

a) 増加すると予測した企業の割合から減少すると予測した企業の割合を引いた値

投稿受理日	2016 年 9 月 30 日
再投稿受理日	2017 年 10 月 26 日

また、企業は自社のビジネスモデルにおける IT の重要性を認識しており、図 2 に示す通り、企業規模が大きくなるほど、IT の重要性が増す傾向がある。

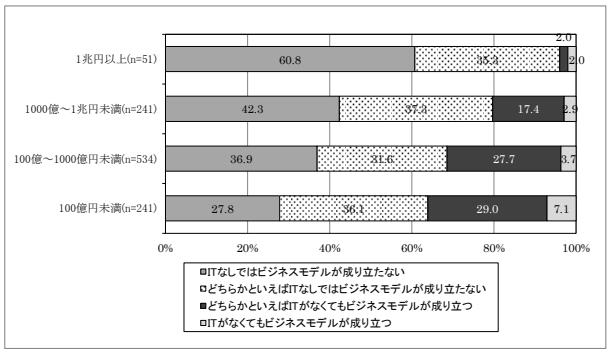

図 2　主たるビジネスモデルと IT の関係 [3]

複雑さを増す環境で企業が成長を続けるためには、ビジネスモデルの変化に対応する IT 戦略を

策定し、実現するための継続的なIT投資が不可欠であり、IT戦略を実現するための根幹となるIT関連人材の育成が経営上の重要な課題となる。

一方で、予算、人材といった経営資源は有限であることから、経営者は個々の案件について採否の判断を迫られるものの、企業規模が大きくなるにつれて、必要となるIT投資およびIT関連人材も増えることから、検討に十分な時間を割くことが難しくなる。

従って、企業規模が大きくなるほど、経営者個人の能力や努力への依存から脱し、「組織の戦略上の重要性に基づいたシステム投資、導入したシステムの効率的・安定的な運用といった組織全体の課題に取り組むためのマネジメント態勢」[4]としてのITガバナンスが必要となる。

このようなITガバナンスを強化するためには、経営者にとって自社が実践する手法の良悪を判断する尺度としてのガイドラインがあることが望ましい。

ITガバナンスに関する国際標準としてISO/IEC 38500があり、日本工業規格としてJIS Q 38500がある。しかしながら、現時点では実践手法に関する判断尺度は標準化されていない。

日本国内においてITガバナンスに関連し、実践手法に関する判断尺度を示したガイドラインとして、金融機関などでは、金融情報システムセンター(以降、FISC)の「金融機関等のシステム監査指針」(以降､FISC指針)が広く用いられている。経産省は企業、官公庁における情報システムに関するガイドラインとして「システム管理基準」、情報セキュリティに関するガイドラインとして「情報セキュリティ管理基準」を公表しており、国際的な専門団体であるISACA[b]はITガバナンスとITマネジメントの実践手法に関するガイドラインとして「COBIT 5 Enabling Processes」を公開している。

しかし、FISC指針、システム管理基準、情報セキュリティ管理基準では、どの判断尺度がITガバナンスの強化に貢献するかを明示していない。

本稿では、JIS Q 38500、FISC指針、システム管理基準、情報セキュリティ管理基準、COBIT 5 Enabling Processesについて、ITガバナンスとの関連性を分析し、企業がITガバナンスを強化する際に参考にすべき箇所、追加すべき箇所を提言する。

b) 日本では「情報システムコントロール協会」とも呼ばれる。

2. ガイドラインにおけるITガバナンス

本稿で分析対象とするガイドラインについて、ITガバナンスの定義と分析に用いる領域を以下で述べる。

なお、各ガイドラインは、判断尺度を内容に則して分類し、複数の部または章に分割することから、本稿では各ガイドラインにおける判断尺度の分類を「領域」と呼ぶ。

(1)「JIS Q 38500」

ITガバナンスの国際規格として、ISO/IEC 38500が2008年に発行され、日本では2015年にJIS Q 38500:2015(以降、JIS Q 38500)として規格化されている。

JIS Q 38500においてはITガバナンスを「組織のITの現在及び将来の利用を指示し、管理するシステム。ITガバナンスは、組織を支援するためにITの利用を評価すること及び指示すること、並びに計画を遂行するためにこのIT利用をモニタすることに関係する。」とし、図3に示す通り、「評価」、「指示」、「モニタ」を経営者の職務と定義している。

JIS Q 38500の本文は「1. 適用範囲、適用及び目的」、「2. 用語及び定義」、「3. 良好なITガバナンスのための枠組み」、「4.ITガバナンスのための手引」の4つの章で構成されており、本稿における分析ではこの4つの章を領域として取り扱う。

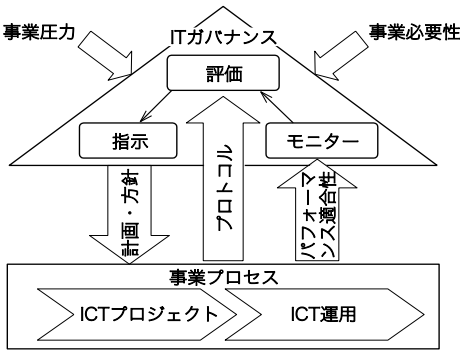

図3 JIS Q 38500におけるITガバナンスの概念[5]

また､本稿では､「経営者」に加えて「評価」､「指示」､「モニター」をISO/IES 38500における表記であるEvaluate、Direct、Monitorの頭文字を用いて、EDMモデルと呼び、ITガバナンスの関連性の分析に使用する。

(2)「金融機関等のシステム監査指針」

FISCは金融機関、保険会社、証券会社、コンピュータメーカー、情報処理会社によって出捐さ

れた公益財団法人であり、そのガイドラインは金融機関を中心に関連業界で広く用いられている。

「金融機関等のシステム監査指針」（以降、FISC 指針は、金融機関等のシステム監査導入と推進のための手引きとして 1987 年に発行された。以降、2000 年に第二版、2007 年に第三版、2014 年に改訂第三版と改訂を続け、現在は 2016 年の改訂第三版追補が最新版である。

また、本指針はシステム監査の概念およびシステム監査実施上のポイントを記載した第一部と、システム監査における具体的な点検項目をチェックポイント集として記載した第二部で構成される。また、第二部は 13 の要点項目にチェックポイントを分類している。

FISC 指針では IT ガバナンスについて「IT を経営戦略の策定と実行に生かし、同時に、IT を利用して構築した情報処理と伝達のシステムを安定的に運用するため、経営者の積極的な関与を前提とした全社的な取り組み」[6] と定義し、システム監査について、「情報システムの有効性、効率性、信頼性、安全性、及び遵守性を達成できるよう、情報システムリスクを把握し、情報システムに係るコントロール(IT ガバナンスを含む場合もある)が適切かつ効果的であることを、被監査部門から組織的に独立したシステム監査人が検証し、その結果を保証意見又は助言勧告としてとりまとめ、経営者に報告する監査」と定義している。従って、FISC 指針のチェックポイント集には IT ガバナンスに関連する判断尺度が含まれていると考えられる。しかしながら、FISC 指針には、どのチェックポイントが IT ガバナンスを含むのかについての記載は無い。

本稿では FISC 指針のチェックポイント集を分析の対象とし、13 の要点項目を領域とする。

(3)「システム管理基準」

経済産業省は、効果的な情報システム投資のための、またリスクを低減するためのコントロールを適切に整備・運用するための実践規範、およびシステム監査を行う上での判断基準[7] として、2004 年にシステム管理基準を発行している。

システム管理基準は、「本管理基準と姉妹編をなすシステム監査基準に従って監査を行う場合、原則として、監査人が監査上の判断の尺度として用いるべき基準」であり、「システム監査の実施は、組織体の IT ガバナンスの実現に寄与する」との記載[8] より、IT ガバナンスに関する判断尺度である。しかしながら、本基準のどの項目が IT ガバナンスの判断尺度となるかについての記載はない。

なお、本基準には、前文に加えて、システム管理基準の各項目が記載されている。各項目は「Ⅰ．情報戦略」、「Ⅱ．企画業務」、「Ⅲ．開発業務」、「Ⅳ．運用業務」、「Ⅴ．保守業務」、「Ⅵ．共通業務」の 6 つに分類されており、本稿ではこれらを領域として取り扱う。

(4)「情報セキュリティ管理基準」

経済産業省は、効果的な情報セキュリティマネジメント体制を構築し、適切なコントロール（管理策）を整備・運用するための実践的な規範[9] として、2003 年に情報セキュリティ管理基準を策定した。情報セキュリティについて参照する国際規格 ISO/IEC 27001（ISMS 要求事項）、及び 27002（情報セキュリティマネジメントのための実践規範）が 2005 年および 2013 年に改訂されたことを受け、2008 年および 2016 年に改訂を行っている。本稿では、「情報セキュリティ管理基準（平成 28 年改正版）」を分析の対象とする。

本基準において、IT ガバナンスという用語は使用されていないものの、システム管理基準において、情報セキュリティの確保に関する項目については「情報セキュリティ管理基準を活用して監査を実施することが望ましい。」との記載があることから、IT ガバナンスとの関連性を有すると考えられる。

本基準は「マネジメント基準」および 14 の「管理策基準」で構成される。本稿ではそれぞれを領域として項目の分類に使用する。

(5)「COBIT 5 Enabling Processes」

ISACA は情報システム監査、情報セキュリティ、リスク管理、IT ガバナンスに関する国際的専門団体として 1969 年に設立され、1996 年にシステム監査のガイドラインとして COBIT を公表、その後 2005 年に IT ガバナンスを加えた COBIT 4 を公表し、現在は 2012 年に公開した COBIT 5 が最新版である。

COBIT 5 では組織の IT に関する業務を EDM(Evaluate, Direct and Monitor)、APO(Align, Plan and Organise)、BAI(Build,Acquire and Implement)、DSS(Deliver, Service and Support)、MEA(Monitor, Evaluate and Assess) の 5 つのドメイン (領域) に分類される 37 のプロセスとし

て定義し、ITガバナンスに関してはISO/IEC 38500に則してEDMに含まれる5つのプロセスとして定義している。

COBIT 5には多数のガイドラインが含まれているが、本稿では37のプロセスを定義する「COBIT5 Enabling Processes」から、各プロセスの実践手法(Activity)を分析の対象とする。なお、COBIT5 Enabling Processesには日本語訳があるが、後述の通り、分析手法として用語の関連性を用いるにあたり、翻訳によって原文の関連性から変化していることが考えられることから、原文を分析対象とした。

3. ガイドラインの分析手法

ガイドラインとITガバナンスとの関連性を定量的に評価するため、本稿ではテキストマイニング等で用いられる計量テキスト分析を用いる。

3.1 計量テキスト分析の概要

計量テキスト分析は、樋口(2014)によると「計量的分析手法を用いてテキスト型データを整理または分析し、内容分析(content analysis)を行う方法」[10]と定義される。

計量テキスト分析では、分析者の主観による影響を極小化するため、二段階で分析を進める。
第一段階では、多変量解析を適用するために、あらかじめ形態素解析[c]を用いて、文章中の用語の出現回数を一覧表にリストアップする。

第二段階では、同義語を考慮した分析を行うためにコーディングルールを用いる。コーディングルールとは、用語の分類を明示的なルールにすることで、大量のテキストデータを漏れなく抽出する。

本稿ではEDMモデルに基づき、経営者が評価、指示、モニターする内容が含む基準項目をITガバナンスと関連があると考える。なお、ガイドラインによって用語の意味が異なるため、コーディングルールを用いて「経営者」、「評価」、「指示」、「モニター」を意味する用語を定め、文中に「経営者」を意味する用語を含み、かつ、「評価」、「指示」、「モニター」のいずれかを意味する用語を含む時に、その基準項目をITガバナンスとの関連性を持つと定義する。

3.2 コーディングルールの検討

本稿におけるコーディングルールを検討するにあたり、JIS Q 38500の定義を参照するとともに、各ガイドライン固有の用語も考慮する必要がある。

FISC指針では、経営者からの権限移譲を受け「情報システム運営委員会」や「セキュリティ委員会」といった用語で表現される各種委員会が重要事項の検討を行う。従って、これらに共通する用語「委員」は「経営者」に含める必要がある。

システム管理基準では「委員」および「組織体の長」を、情報セキュリティ管理基準では、「トップマネジメント」および「経営陣」を同じ意味[11]として用いていることから、これらを「経営者」に含める必要がある。

情報セキュリティ管理基準では「マネジメントレビュー」について、トップマネジメントが、あらかじめ定めた間隔で開催するもの[12]として定めていることから、「モニター」に含める必要がある。

一方、「戦略」という用語は、例えば「今日、組織体の情報システムは、経営戦略を実現するための組織体の重要なインフラストラクチャとなっている」[13]というように、ITガバナンス上、重要な意味があると考えられる。しかしながら、JIS Q 38500では、「戦略」は原則の一部としてEDMモデルの「評価」、「指示」、「モニター」のそれぞれに関連する概念として定義されていることから、本稿で使用するコーディングルールには含めない。

各ガイドラインにおける用語の使い方を踏まえ、本稿で使用するコーディングルールを表1で示す。

表1 本稿におけるコーディングルール

	コーディングルール
「評価」	評価、識別、分析、選定、項目、指標、基準
「指示」	指示、計画、方針、ポリシー、任命
「モニター」	モニター、状況、定期的、把握、モニタ、モニタリング、マネジメントレビュー
「経営者」	経営者、経営陣、取締役、委員、取締役会、役員、組織体の長、トップマネジメント、経営層

なお、COBIT 5 Enabling Processesについては英語版を分析対象とし、文中に経営者を表す用語が出現しないことから、表1は適用できない。COBIT 5 Enabling ProcessesにおいてITガバナンスに関するEDM領域には、項目名称として「Evaluate the governance system」、「Direct

c) 自然言語のテキストデータから，言語で意味を持つ最小単位（形態素）に分割し，それぞれの形態素の品詞等を判別する処理

the governance system」、「Monitor the governance system」という記載が見られ、それぞれが EDM モデルに該当する。従って、各項目の説明文から共通する用語を抽出し、表 2 をコーディングルールとする。

表 2　COBIT 5 におけるコーディングルール

	コーディングルール
Evaluate（評価）	Evaluate、current、make、future、judgement、evaluate、examine、asset、consider、continually、need
Direct（指示）	Direct、information、practice、 enable、plan、criterion、line、potential、responsibility
Monitor（モニター）	Monitor、assess、performance、action、deviation、target、cause、relevant、 obtain、periodically、progress、review

なお、COBIT 5 Enabling Processes では実践手法について、RACI チャートと呼ばれる表を用いて、社内の役職に実行責任者 (Responsible)、説明責任者 (Accountable)、協議先 (Consulted)、報告先 (Informed) の役割を割り当てている。従って、他のガイドラインのようにコーディングルールを用いて「経営者」を抽出できない。

本稿では、COBIT 5 Enabling Processes の分析にあたって、Chief Executive Officer (CEO)、Chief Information Officer (CIO) 等 の CxO、Steering Projects Committee 等の Committee(委員会) 及び Board (取締役会) が RACI チャートにおいて実行責任 (Responsible) の役割を持つ実践手法を「経営者」と関連する実践手法として取り扱う。

3.3　計量テキスト分析における関連性と信頼水準

本稿における計量テキスト分析には、樋口 (2014) に基づき、用語の関連性を表すために Jaccard 指数 [d] を用いる。

関連性を Jaccard 指数で示すにあたり、Jaccard 指数がどの程度であれば有意な関連であるといえるだろうか。

Jaccard 指数の有意性を調べるためには、ガイドラインにおいて用語がどのように分布しているかを調べる必要がある。

FISC 指針における、用語の出現回数と出現する文章の数をプロットしたものを図 4 に示す。

図 4 がほぼ直線上にプロットされることから、FISC 指針において、各用語が一様に分布していると仮定すると、FISC 指針に含まれる文の数を x、用語 A の出現回数を a、用語 B の出現回数を b とした時の、用語 A および B が n 個の文で同時に出現する確率 P は式 1 で、Jaccard 指数 J は式 2 で表すことができる。

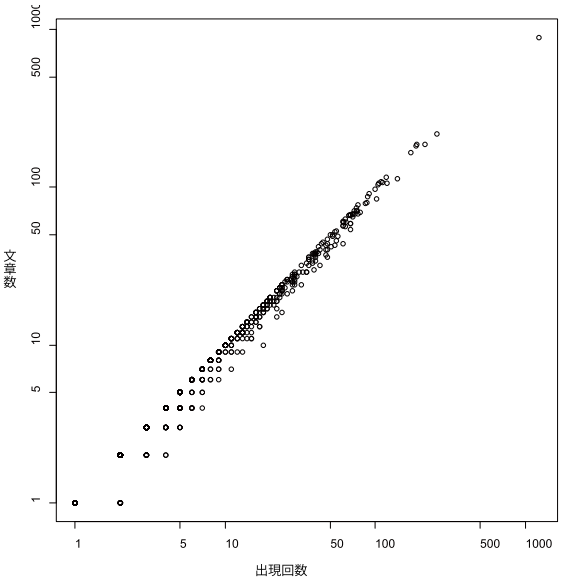

図 4　FISC 指針における用語の出現回数と出現する文章数

$$P(x,a,b,n)=\frac{{}_aC_n\times{}_{(x-a)}C_{(b-n)}}{{}_xC_b} \qquad \text{式 1}$$

$$J(a,b,n)=\frac{n}{a+b-n} \qquad \text{式 2}$$

FISC 指針では x=2643 であり、A を EDM モデルで「評価」を表す用語の集合とした時、用語 B との Jaccard 指数における信頼水準を 95% および 99% となる b および J の関係を図 5 で示す。

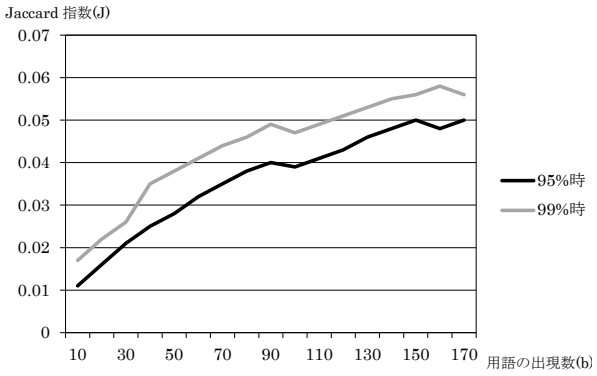

図 5　FISC 指針における Jaccard 指数

図 5 より、FISC 指針において、ある用語 B の出現数が 170 回の時、「評価」の Jaccard 指数が 0.06 を上回っていれば用語 B と「評価」には 99% の信頼水準で有意な関連性があると言える。

d) 2 つの集合の類似度を表す指数.
A, B を集合。#(A) を集合の個数とすると，A と B の Jaccard 指数 J(A, B) は以下の式で定義される。

$$J(A,B)=\frac{\#(A\cap B)}{\#(A\cup B)}$$

4. 分析結果および考察

4.1 ガイドラインの比較

(1) 出現率による比較

FISC 指針、システム管理基準、情報セキュリティ管理基準、JIS Q 38500、COBIT 5 Enabling Processes について、用語の出現率を図 6 に示す。なお、COBIT 5 Enabling Processes においては「経営者」に関連する実践手法の出現率を示す。

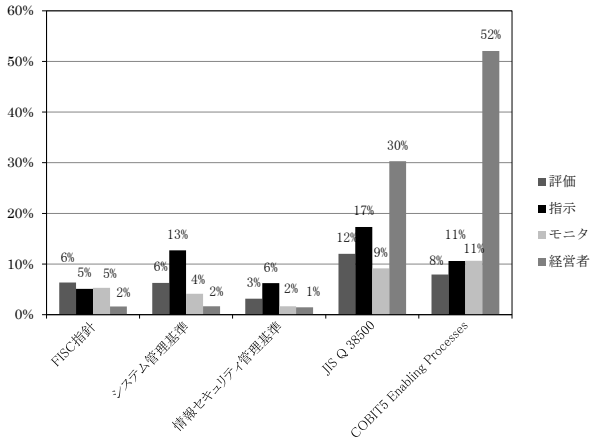

図 6 EDM モデルの出現率

図 6 より、JIS Q 38500、COBIT 5 Enabling Processes において「経営者」の出現率が高い。また、FISC 指針、システム管理基準、情報セキュリティ管理基準ではシステム管理基準および情報セキュリティ管理基準において、「指示」の出現率が高い。

(2)「経営者」と EDM モデルの関連性による比較

出現率の比較では、「指示」の出現率が高くても、それが経営者の職務ではなく、担当者や管理者の職務を表している可能性がある。そこで、各ガイドラインにおける、「経営者」と EDM モデルの関連性を図 7 で示す。

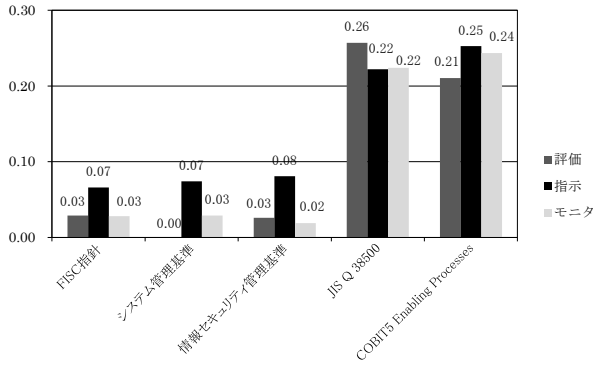

図 7 「経営者」と EDM モデルの関連性

図 7 において各 EDM モデルは「経営者」と 99% の信頼水準で有意な関連性がある。

JIS Q 38500 および COBIT 5 Enabling Processes は「評価」、「指示」、「モニター」ともに「経営者」との関連性が高い。

一方、FISC 指針、システム管理基準、情報セキュリティ管理基準では「指示」の関連性が「評価」や「モニター」よりも高い傾向を示している。なお、システム管理基準では「経営者」と「評価」に関連性が見られない。

(3) 考察

図 6 および図 7 より、FISC 指針、システム管理基準、情報セキュリティ管理基準において、JIS Q 38500 および COBIT 5 Enabling Processes よりも低いものの、EDM モデルは「経営者」と関連性があり、IT ガバナンスに関連する判断尺度が含まれていることがわかる。

また、FISC 指針、システム管理基準、情報セキュリティ管理基準を比べると、システム管理基準において EDM モデルが高い出現率を示すものの、「経営者」との関連性は高くなく、FISC 指針や情報セキュリティ管理基準と比べて IT ガバナンスに係る判断尺度が少ないと考えられる。一方、情報セキュリティ管理基準において、EDM モデルの出現率は低いものの、「経営者」との関連性は高く、FISC 指針やシステム管理基準と比べて、IT ガバナンスに係る判断尺度が多いと考えられる。

なお、システム管理基準において「経営者」と「評価」の関連性が見られない点について、当該基準の本文を見ると、「全体最適化計画は、定期的及び経営環境等の変化に対応して見直すこと」(1.4 全体最適化計画の運用) や、「情報システムの全体的な業績及び個別のプロジェクトの業績を財務的な観点から評価し、問題点に対して対策を講じること」(3. 情報化投資) という記述があり、IT 戦略や IT 投資といった評価において、役割を明示していないことが原因となっている。

4.2 用語との関連性

(1)「経営者」と関連性が高い用語

各ガイドラインにおいて、「経営者」はどのような用語と関連性を持つのだろうか。FISC 指針、システム管理基準、情報セキュリティ管理基準、JIS Q 38500 において、「経営者」との関連性が高い順から上位 10 位の用語を表 3 ～ 6 で示す。

COBIT 5 Enabling Processes については、「経営者」に関連する実践手法において、出現数の高い用語を表 7 で示す。

表 3　FISC 指針において「経営者」と関連性の高い用語（上位 10 位）

順位	用語	出現数	Jaccard 指数	有効水準 * 95% ** 99%
1	運営	11	0.200	**
2	報告	60	0.198	**
3	情報システム	69	0.192	**
4	得る	66	0.172	**
5	承認	107	0.136	**
6	担当	25	0.115	**
7	リスク	42	0.104	**
8	策定	28	0.076	**
9	関係	19	0.069	**
10	重大	4	0.068	**

表 4　システム監査基準において「経営者」と関連性の高い用語（上位 10 位）

順位	用語	出現数	Jacccard 指数	有効水準 * 95% ** 99%
1	活動	3	0.182	**
2	立案	3	0.182	**
3	得る	5	0.154	**
4	承認	32	0.135	**
5	最適化	16	0.130	**
6	全体	18	0.120	**
7	意思	1	0.100	**
8	全般	1	0.100	**
9	含む	1	0.100	**
10	是正	1	0.100	**

表 5　情報セキュリティ管理基準において「経営者」と関連性の高い用語（上位 10 位）

順位	用語	出現数	Jaccard 指数	有効水準 * 95% ** 99%
1	マネジメント	73	0.159	**
2	発揮	6	0.118	**
3	リーダーシップ	6	0.118	**
4	責任	112	0.116	**
5	権限	20	0.109	**
6	整備	26	0.100	**
7	仕組み	28	0.097	**
8	コミットメント	7	0.094	**
9	相手	32	0.092	**
10	従業員	44	0.092	**

表 6　JIS Q 38500 において「経営者」と関連性の高い用語（上位 10 位）

順位	用語	出現数	Jaccard 指数	有効水準 * 95% ** 99%
1	望ましい	66	0.720	**
2	IT	85	0.480	**
3	評価	23	0.265	**
4	確実	20	0.258	**
5	モニタ	19	0.224	**
6	指示	21	0.200	**
7	利用	28	0.197	**
8	組織	43	0.191	**
9	責任	15	0.164	**
10	適切	15	0.147	**

表 7　COBIT 5 Enabling Processes において「経営者」に関連性する実践手法で出現数の高い用語（上位 10 位）

順位	用語	出現数	Jacccard 指数	有効水準 * 95% ** 99%
1	identify	125	0.153	**
2	ensure	99	0.122	**
3	enterprise	85	0.112	**
4	include	81	0.107	**
5	define	74	0.096	**
6	program	70	0.098	**
7	change	63	0.085	**
8	consider	58	0.079	**
9	maintain	55	0.073	**
10	plan	55	0.075	**

なお、表 3 ～ 7 で、抽出された全ての用語について、Jaccard 指数は 99% の信頼水準を上回っている。

以降では、表 3 ～ 7 における特徴的な用語について考察する。

(2)「承認を得る」

表 3 および表 4 において「承認」および「得る」が共通して出現する。例えば、「全体最適化計画の立案体制は、組織体の長の承認を得ること」（システム管理基準　Ⅰ .1.2）といった IT ガバナンスに係わるチェックポイントで用いられることもあれば、「プログラムの変更は、保守手順に基づき、保守の責任者の承認を得て実施すること」（システム管理基準　Ⅴ .3）といった業務に係わるチェックポイントで用いられることもある。

従って、ある用語について「経営者」との関連性が高くとも、IT ガバナンスとの関連性について

は、文章全体での用法から判断する必要がある。

(3)「リーダーシップ及びコミットメントの発揮」

表5において出現する「リーダーシップ」、「コミットメント」、「発揮」は情報セキュリティ管理基準において一組で用いられることが多い。

例えば、「トップマネジメントは、以下によって、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する」として、組織のプロセスへ情報セキュリティマネジメント要求事項を統合すること、情報セキュリティマネジメントが成果を達成することを確実にする、情報セキュリティマネジメントの有効性に寄与するよう人々を指揮し、支援すること（情報セキュリティ管理基準 4.4.1.1）を定めており、「指示」に関連するチェックポイントに出現する。

但し、「トップマネジメントは、管理層がその責任の領域においてリーダーシップを発揮できるよう、管理層の役割を支援する。」（情報セキュリティ基準 4.4.1.3）とあるように、「リーダーシップの発揮」は一般の管理職にも使用され、「情報セキュリティの教育及び訓練には、組織全体にわたる情報セキュリティに対する経営陣のコミットメントの提示を含める」（情報セキュリティ管理基準 7.2.2.8）とあるように「コミットメント」は「経営者」にのみ使用される。これは、JIS Q 38500 における「原則 1: 責任（Responsibility）」に該当するものと考えられる。

（4）「責任」

表5および表6において「責任」の出現回数が多い。情報セキュリティ管理基準においては、「組織の役割、責任及び権限」(情報セキュリティ管理基準 4.4.1) において、「トップマネジメントは、組織の役割について、以下の責任及び権限を割り当て、伝達する。」(情報セキュリティ基準 4.4.1.2) と記載され、JIS Q 38500 においては、「組織内の個人及び部門は、IT の供給及び需要の両面の役割について、その責任を理解して受け入れる。処置に責任を負う人もまた、その処置を遂行する権限をもつ。」(JIS Q 38500 3.1.1 原則 1 責任 (Responsibility) と記載され、いずれも「責任」は「役割」および「権限」と一組の概念として出現する。

COBIT 5 Enabling Processes では実践手法に「責任」を意味する用語は出現しないが、RACI チャートの説明において、「A suggested assignment of level of responsibility for process practices to different roles and structures.」(COBIT 5 Enabling Processes Chapter 5) とあるように、RACI チャートによって「責任」と「役割」が対応付けられている。

（5）「確実にする /ensure」

表6において出現する「確実にする」は、表7において出現する「ensure」の訳語である。

JIS Q 38500 においては、「経営者は、プロジェクトの運用状態への移行が適切に計画され、管理されていることを確実にすることが望ましい。」(JIS Q 38500 3.2.3)、COBIT 5 Enabling Processes においては、「Ensure governance framework setting and maintenance.」(COBIT 5 Enabling Processes EDM01) というように組織体制の整備を意味する用語として用いられる。なお、表5には出現しないものの情報セキュリティ管理基準においても、「トップマネジメントは、情報セキュリティマネジメントに必要な資源が利用可能であることを確実にするため、以下のような資源を割り当てる。」(情報セキュリティ基準 4.5.1.2) というように、同様の意味で用いられる。また、FISC 指針およびシステム管理基準の判断尺度には同様の表現は見られない。

4.3 EDM モデルの出現率

同一文中に用語が出現しなくとも、前後の文に出現する用語には文脈的な関連があると考えられる。

各ガイドラインは独自の観点に従って、チェックポイントまたは基準項目を複数の領域に分類する。例えば FISC 指針ではチェックポイントを 13 の要点項目に分類している。

本稿では各ガイドラインの文脈を分析するため、各ガイドラインの領域毎に EDM モデルの出現率を求め、対応分析 [e] によって二次元にマッピングする。

（1）FISC 指針

FISC 指針の 13 の領域における EDM モデルの出現率を図8に示す。

なお、図8において、円は「経営者」および EDM モデル、四角は FISC 指針の領域を示し、円および四角の大きさは出現数を示している。また、対応分析によって円および四角は出現率が高い程、近くになるようにマッピングされている。このことから、x 軸（成分1）および y 軸（成分2）は特別の意味を持たない。（以降、図9から図12においても同様）

e) 多次元データ解析手法の一つであり，表形式のデータについて，行要素同士，列要素同士の距離関係を図示する。

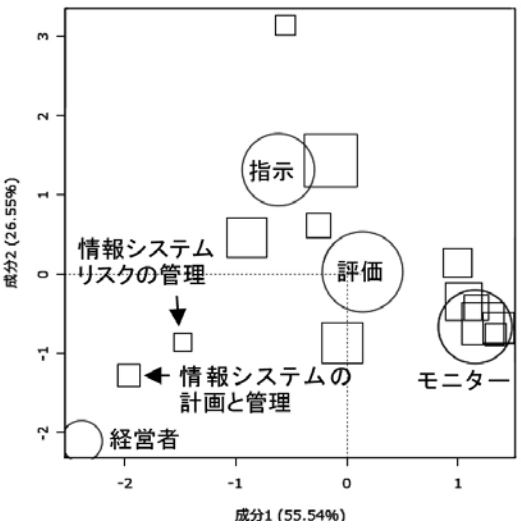

図８　FISC 指針と EDM モデルの関連性

図８より、本指針では要点項目「情報システムの計画と管理」および「情報システムリスクの管理」が、「経営者」および EDM モデルとの出現率が高い。

例えば、要点項目「情報システムの計画と管理」では、情報システム運営委員会が情報システム戦略、情報システム中長期 / 短期計画を策定することを定めており（FISC 指針 1.1.B. 情報システム運営委員会、下線部はコーディングルールの該当箇所であり、以降も同様とする)、「経営者」による「指示」に関するチェックポイントとして利用可能である。

また、要点項目「情報システムリスクの管理」では、「情報システムリスク管理部門が全社的な観点からリスクの評価と識別を行った結果を情報システムリスク委員会に報告することを定めており（FISC 指針 2.1. B . 情報システムリスクの識別と評価)、「経営者」による「評価」に関するチェックポイントとして利用可能である。

(2) システム管理基準

システム管理基準の６つの領域における EDM モデルの出現率を図９に示す。

図９より、本基準では「情報戦略」において「経営者」および「指示」の出現率が高い。

例えば、「情報戦略」では、全体最適化計画について、組織体の長の承認を得ること（システム管理基準　Ⅰ .1.2)、情報システム化委員会が、組織体における情報システムに関する活動全般について、モニタリングを実施し、必要に応じて是正措置を講じること（システム管理基準　Ⅰ .2.1) 等を定めており、「経営者」による「指示」および「モニター」に関する基準項目として利用可能である。

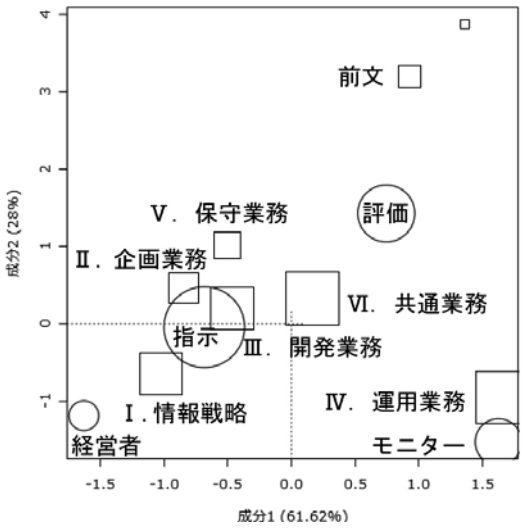

図９　システム管理基準と EDM モデルの関連性

その他の「企画業務」、「開発業務」、「運用業務」、「保守業務」、「共通業務」は「指示」の出現率は高いものの、「経営者」の出現率は低い。

また、「評価」は「前文」における出現率が高く、「モニター」は、「運用業務」における出現率が高い。

(3) 情報セキュリティ管理基準

情報セキュリティ管理基準の 15 の領域における EDM モデルの出現率を図 10 で示す。

図 10 より、本基準では「マネジメント基準」および管理策基準「人的資源のセキュリティ」において「経営者」の出現率が高い。

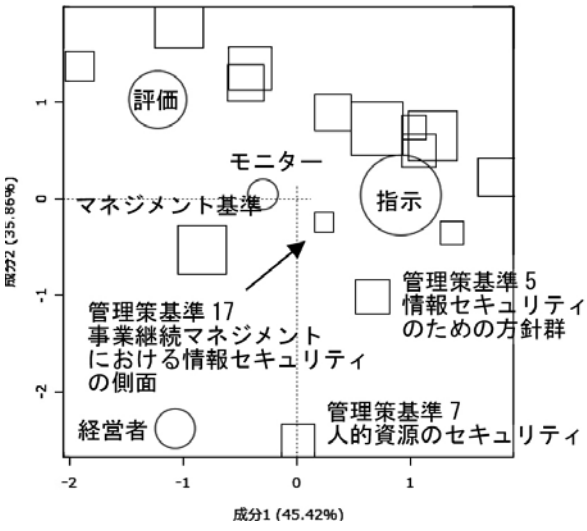

図 10　情報セキュリティ管理基準と EDM モデルの関連性

特に、「マネジメント基準」は「評価」、「指示」、「モニター」の出現率も高く、例えば、情報セキュリティ方針を達成する計画について、トップマネジメントの指示が含まれていること（情報セキュリティ管理基準 4.4.1.1）、情報セキュリティマネジメントのパフォーマンス評価をトップマネジメントに報告すること（情報セキュリティ管理基準 4.4.1.2）等を定めており、「経営者」による「指示」および「評価」に関する基準項目として利用可能である。

一方で、マネジメント基準以外の管理策基準では「経営者」の出現率は低い。これは、マネジメント基準が参照するのが、ISO/IEC 27001 であり、管理策基準が参照するのか ISO/IEC 27002 であることに起因すると考えられる。

なお、「指示」は管理策基準「情報セキュリティのための方針群」における出現率が最も高く、「モニター」は管理策基準「事業継続マネジメントにおける情報セキュリティの側面」における出現率が高い。

(4) JIS Q 38500

JIS Q 38500 の各章における EDM モデルの出現率を図 11 で示す。

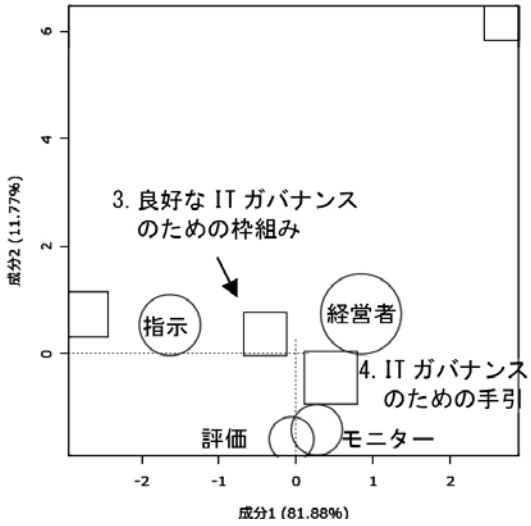

図 11　JIS Q 38500 と EDM モデルの関連性

「1. 適用範囲、適用及び目的」は JIS Q 38500 の定義に関する記述であり、IT ガバナンスに関連する記載はほとんど見られない。また、「2. 用語および定義」についても、IT ガバナンスや EDM モデルそのものに関する定義を除けば、IT ガバナンスに関する記載は見られない。

逆に、「3. 良好な IT ガバナンスのための枠組み」および「4.IT ガバナンスのための手引」では EDM モデルおよび「経営者」が、ほぼ均等に出現している。

(5) COBIT 5 Enabling Processes

COBIT 5 Enabling Processes の各領域における EDM モデルの出現率を図 12 で示す。

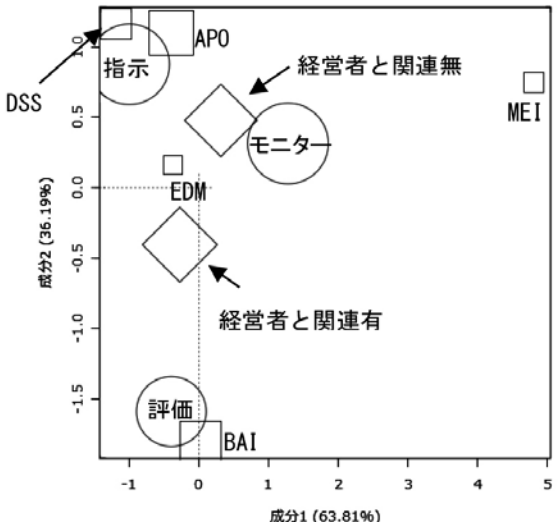

図 12　COBIT 5 Enabling Processes と EDM モデルの関連性

COBIT 5 Enabling Processes では RACI チャートを用いて実践手法単位で経営者の関与の有無を判定するため、「経営者との関連が有る実践手法」と「経営者の関連が無い実践手法」に分かれる。

経営者との関連がある実践手法及び EDM 領域では EDM モデルが均等に出現するのに対し、経営者との関連が無い実践手法では「評価」の出現頻度が低い。このことから、COBIT 5 Enabling Processes では経営者の職務として「評価」を重視しているということができる。

(6) 考察

図 8 ～ 12 より、領域単位で EDM モデルの出現率を図式化することで、文単位の分析では判別できなかった「経営者」と EDM モデルの関連性を明らかにした。各ガイドラインにおいて、計画またはマネジメントに係る領域は EDM モデルとの関連が高い傾向を示している。ISO/IEC 38500 を参照する JIS Q 38500 及び COBIT 5 Enabling Processes だけでなく、FISC 指針およびシステム管理基準、情報セキュリティ管理基準においても「経営者」と EDM モデルの関連性が見られることから、IT ガバナンスは、既存のガイドラインであっても一定の効果が期待できると考えられる。

その一方で、FISC 指針においては、インターネットサービスに関する領域「ネットワーク」において「経営者」のの出現率が低いことから、インターネットバンキングやサイバーセキュリティに関する IT ガバナンスのガイドラインとしては不十分であると考えられる。同様にシステム管理基準においては、システム開発の上流工程である領域「企画業務」において「経営者」の出現率が低いことから、プロジェクト管理に対する IT ガバナンスについては判断尺度の追加を検討する必要がある。また、情報セキュリティについては、ISO/IEC 27014:2013(日本規格では JIS Q 27014:2015) として「情報セキュリティガバナンス」が策定されていることから、「情報セキュリティ管理基準」との適切な使い分けが必要となる。

5. おわりに

本稿では、FISC 指針、システム管理基準、および情報セキュリティ管理基準、JIS Q 38500、COBIT 5 Enabling Process と IT ガバナンスとの関連性を分析した。具体的には各ガイドラインに計量テキスト分析を適用し、ISO/IEC 38500 の EDM モデルに該当する用語と、「経営者」に該当する用語の関連性を比較した。

各ガイドラインは目的、経緯が異なるものの、「経営者」および EDM モデルとの関連性を求めることで、IT ガバナンスに関する判断尺度が存在することを示した。本稿で用いた手法は、今回取り上げた以外のガイドラインにも、適用可能であり、IT ガバナンスの以外の切り口で比較することも可能となる。サイバーセキュリティ、IoT、アジャイル等を、今後の研究テーマとして取り組みたい。

また、各ガイドラインを図式化することで、「経営者」および EDM モデルとの関連性から、IT ガバナンスの観点が不足する領域を指摘した。多くの企業にとって IT ガバナンスの重要性が増していることから、本稿における分析結果を踏まえ、既存のガイドラインに IT ガバナンスに関する判断尺度を追加することは有益である。

ただし、各企業の経営上、重要な領域は異なることから、見直しに際しては、経営者の観点に立って、重要な領域を特定し、経営に求められる要件を洗い出すことが望ましい。

本稿で用いた計量テキスト分析は本来、アンケート調査やインタビューといった社会調査において開発された手法であり、定量的に分析することが難しい経営者の関心、ニーズの分析に適している。IT ガバナンスに求められる社会的要件、経営からの要請への適用についても今後の研究テーマとして取り組みたい。

参考文献

[1] 日本情報システムユーザー協会 . “第 22 回企業 IT 動向調査 2016（15 年度調査）～データで探るユーザー企業の IT 動向～” . http://www.juas.or.jp/servey/it16/it16_ppt.pdf、(参照 2017-01-17)、p. 19.

[2] 経済産業省。” 企業活動基本調査” . http://www.meti.go.jp/statistics/tyo/kikatu/index.html、(参照 2018-01-05)

[3] 日本情報システムユーザー協会 . “第 22 回企業 IT 動向調査 2016（15 年度調査）～データで探るユーザー企業の IT 動向～” . http://www.juas.or.jp/servey/it16/it16_ppt.pdf、(参照 2017-01-17)、p. 12.

[4] 金融庁 . 金融モニタリングレポート . 2015、p. 109.

[5]JIS Q 38500:2015 情報技術 -IT ガバナンス . 2015、図 1.

[6] 金融情報システムセンター . 金融機関等のシステム監査指針改訂第 3 版追補). 2016、p. 3.

[7] 経済産業省 . システム管理基準 . 2004、p. 1.

[8] 経済産業省 . システム管理基準 . 2004、p. 1.

[9] 経済産業省 . 情報セキュリティ管理基準 . 2016、p. 1.

[10] 樋口耕一 . 社会調査のための計量テキスト分析　内容分析の継承と発展を目指して . ナカニシヤ出版、2014、p. 15.

[11] 経済産業省 . 情報セキュリティ管理基準 . 2016、p. 5、脚注 2.

[12] 経済産業省 . 情報セキュリティ管理基準 . 2016、p. 18.

[13] 経済産業省 . システム管理基準 . 2004、p. 1.