IT ガバナンスの国際標準化（ISO/IEC38500 シリーズ）の最新動向とその取組み

公益財団法人未来工学研究所　客員研究員
JTC1/SC40 専門委員会委員　WG1 メンバー
力　利則　氏

はじめに

今回ご紹介する国際標準である「IT ガバナンス」は、特に経営者・役員層に対して世界の動きを知ってもらいたい内容であり、IT 部門、監査関係の立場からも、ぜひ、経営者層に対し IT ガバナンスの重要性を紹介してもらいたい。

1.国際標準化の背景

企業経営における IT 戦略の 1 つとして、IT ガバナンスの導入と確立が重要、かつ効果的と考えられており、ISO/IEC は 2008 年に ISO/IEC38500（2015 年改訂）を、その後 38501、38502、38504、38505-1 をそれぞれ発行した。現在、諸外国でその受容性が理解され、取組みが本格化してきている。

ISO（国際標準化機構）と IEC（国際電気標準会議）の第 1 合同技術委員会（JTC1）の総会で承認された「SC40 専門委員会（IT サービスマネジメントと IT ガバナンス）」において、IT セキュリティおよびインフラの適用範囲を除外した IT ガバナンス、IT サービス管理に関する標準、ツール、枠組み、ベストプラクティスおよび関連文書の作成が検討されており、今回紹介する IT ガバナンスの検討は本委員会の WG1 が担当している。

なお、日本では 2015 年 7 月に「JIS　Q 38500：2015　情報技術　IT ガバナンス」のみが JIS 化されている。

注）ISO38500 シリーズの規格は正式には英文のみとなり、和訳版は存在しない。今回紹介する規格は NPO 法人日本システム監査人協会が和訳したものであり、公式のものではない。なお、「JIS Q 38500　情報技術　IT ガバナンス」の詳細はここでは割愛する。

2.ISO/IEC38500 の概要

（1）ISO/IEC38500（IT ガバナンス）

本規格は、組織のガバナンスを実施する経営者層に対し、①評価（Evaluate）②指示（Direct）③モニタ（Monitor）の 3 つを実践することが経営者としての役割、と定義している。

・現在と将来の IT の利用について評価する（**E**valuation）
・IT の利用が組織のビジネス目標に合致するよう、計画とポリシーを策定し、実施する（**D**irect）
・ポリシーへの準拠と計画に対する達成度をモニタする（**M**onitor）

これを EDM モデルといい、このモデルをもとに、経営者には以下の行動が求められている。

・ビジネス環境からの要求や市場に合わせて企業としての**方針を決定**する。
・企業の執行部門からの**活動をモニタして**、目標との乖離を調べる。
・その結果と執行部門からの提案を統合的に評価して、実施部門に対して**指示を行う**。

すなわち、経営者は IT の投資や利用について決定し、その結果をモニタして改善を行うことが求められているのである。

ISO/IEC38500 の適用範囲は「組織のディレクタ（経営者）のために、その組織内での IT の効果的、効率的で受容可能な使用に関するガイドとなる原則を提供すること」で、公的、私的、規模の大小に限らず、あらゆる組織が対象となる。EDM モデルを基に、経営者が 6 つの原則（責任、戦略、取得、パフォーマンス、適合、人間行動）に沿って取り組むべきことが示されている。

なお、従来のマネジメントモデルである PDCA の上位にガバナンスモデルとして EDM がある、というのが国際標準の考え方である。

ISO/IEC38500 の概要は図 1 のとおり。

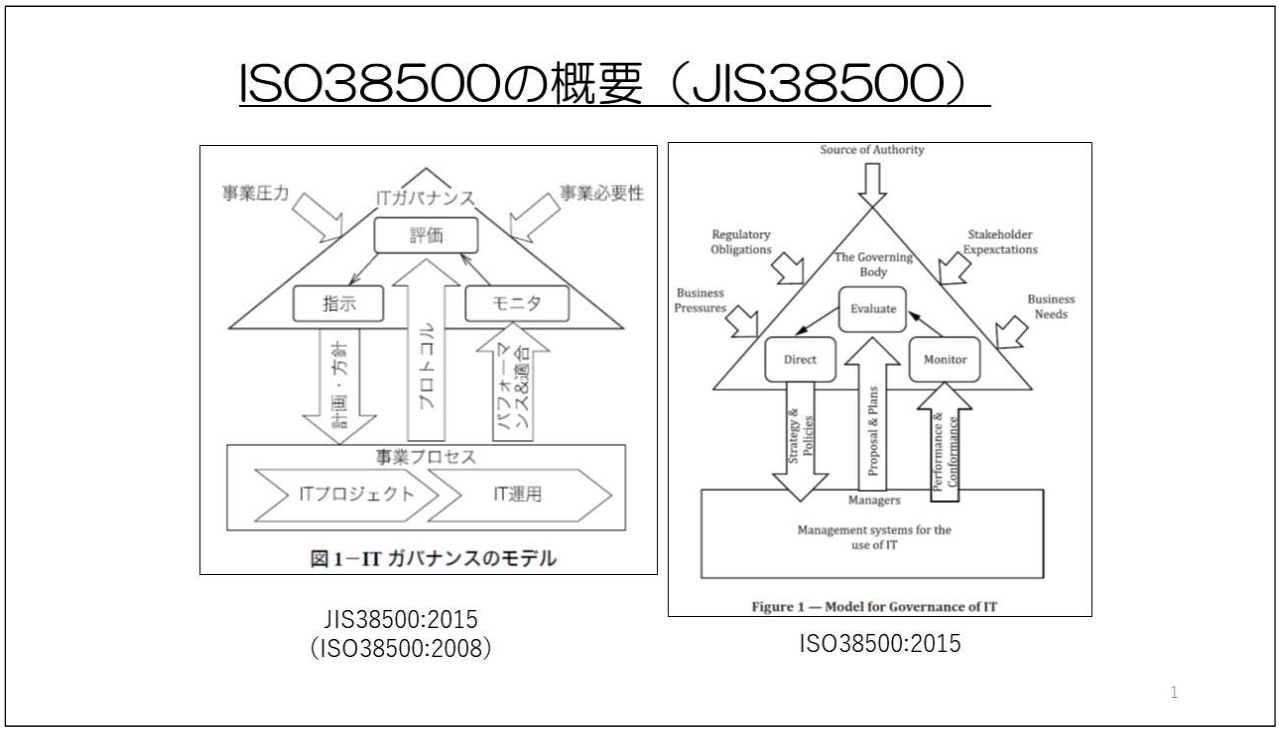

図 1.ISO38500 の概要

（2）良質な IT ガバナンス実践のための 6 原則

前述のとおり、経営者が役割を果たすべき考え方として 6 つの原則がある（図 2）。これらの原則を考慮の上、EDM モデルを実践することが重要と考えられている。

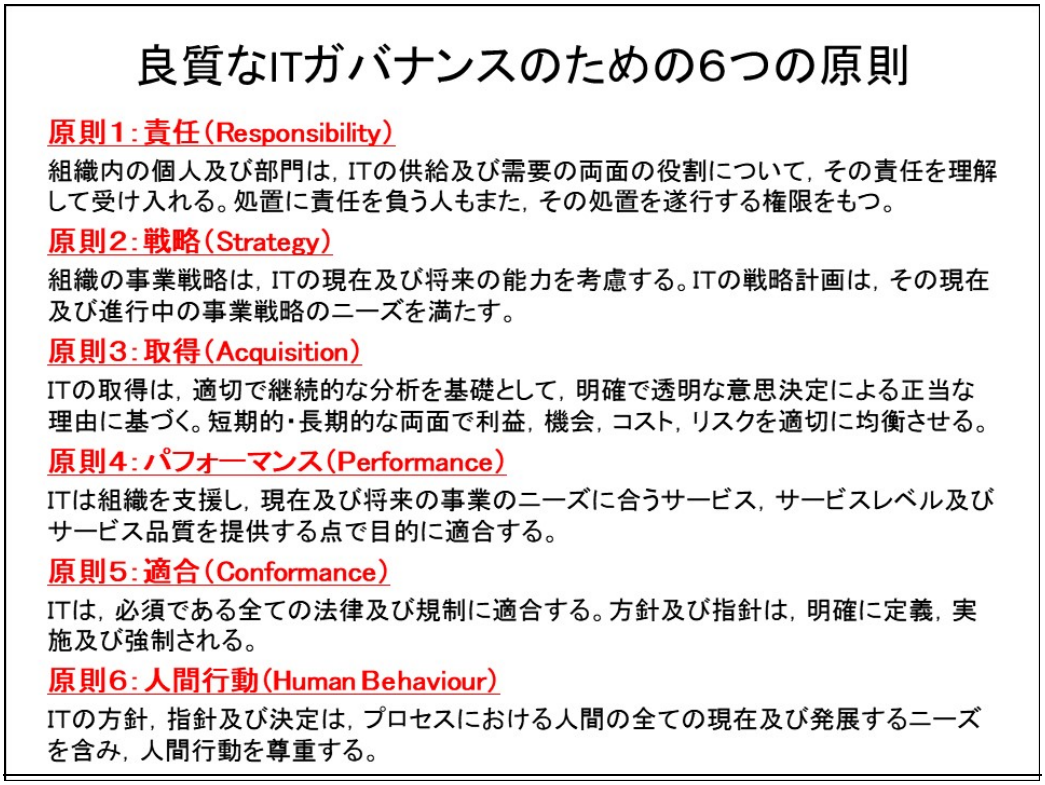

図 2.良質な IT ガバナンスのための 6 原則

3.ISO/IEC38500 シリーズの概要

（1）ISO38501（導入ガイド）

本規格は、ISO/IEC38500 の役割・原則について、JIS 化の環境をどのように作るべきか、IT ガバナンスの運用をどう回せばよいか、を示した具体的な導入ガイドである。参考として、IT ガバナンスを実施している評価のスキームが書かれており、原則どおり実践しているかを評価する。

ISO38501 は図 3 に示すとおり、IT ガバナンスの運用のまわりに継続的改善、見直しと、ステークホルダとしての役割を回していくことになる。

なお、付属書 B には、6 原則に対し経営者層がどのようなことを実践すれば評価されるか、の尺度が示されている。

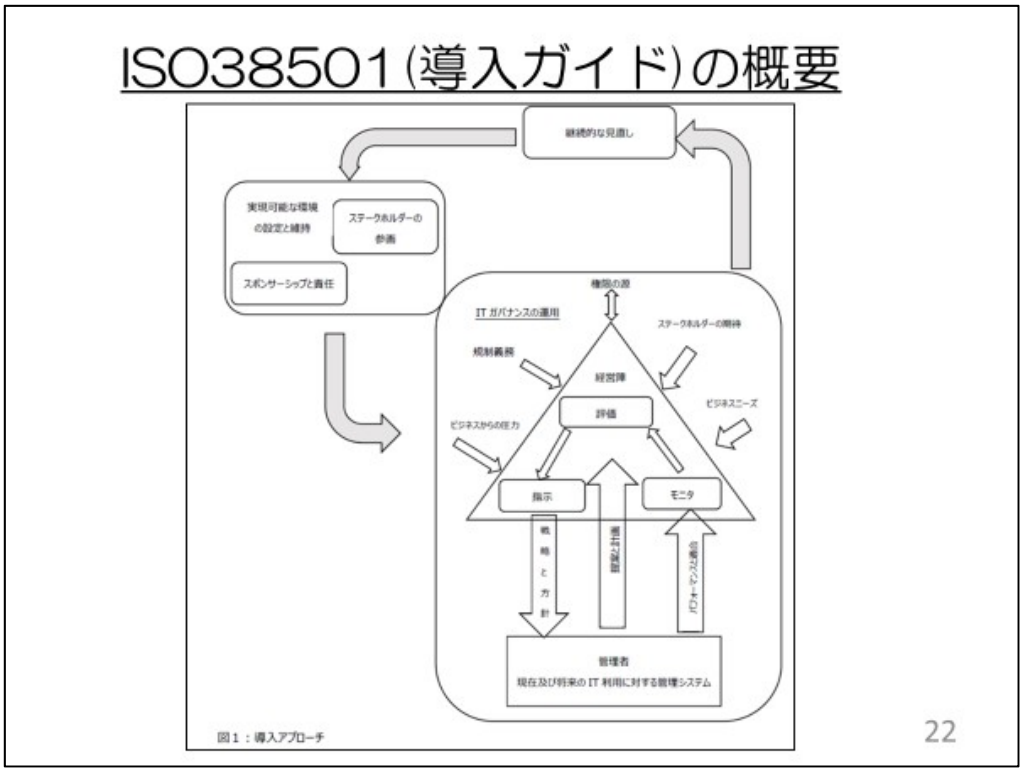

図 3.ISO38501（導入ガイド）の概要

（2）ISO38502（フレームワークとモデル）

本規格は IT ガバナンスとマネジメントの関係をフレームワークの要素として示したものである（図 4）。

図 4.ISO38502（フレームワークとモデル）の概要

2017 年 10 月 20 日開催 第 67 回 JIPDEC セミナー「IT ガバナンスの国際標準化（ISO/IEC3850 シリーズ）の最新動向とデータガバナンスについて」

（3）ISO38504（原則基盤の標準ガイド）

IT ガバナンスの原則とは何か、を追求したもので、原則をどう見ればよいかを詳細に示したもので、IT ガバナンスの標準の目的、原則基盤の指針、ガバナンスの原則を実践するために必要な情報を示したものである。

（4）ISO38503 について

本規格についてはシステム監査基準／システム管理基準（経済産業省公表、2004 年）を英語化し、日本発案で ISO 化する検討から始まった。その後、SC40 直下の WG1 にて IT ガバナンスの WG に統合され、監査ではなくアセスメントに目的が変更された。その後大幅な内容見直しが図られ、マネジメントレベルからガバナンスレベルに変更され、現在は WG1 にて検討中である。2018 年の国際会議で承認されることを目指している。

注）「ISO38505-1（データガバナンス）」の詳細は、原田氏の講演録を参照のこと。

4.ISO/IEC38500 シリーズの JIS 化に向けて

ISO/IEC38500 を除く各規格については、現段階で JIS 化されていない。グローバル的には ISO/IEC38500 シリーズの重要性が浸透しているが、日本では 38500 の JIS 化により、ようやく「EDM モデル」を含め、IT ガバナンスの重要性が認識されつつあるが、まだ具体的な導入には至っていない。日本の経営者層に浸透させるために、ぜひ日本語化するべきであると考えている。