運用サービスに関わる法制化／規格化の動向
～SOX法とITIL®の関連、そして運用現場に求められること～

システムビジネスユニット
AMOセンター
フロントサービス第二グループ
野 村 紀 美

1．はじめに

運用サービスに関わる法制化／規格化が急ピッチで進められている。

図1は、ITコーディネータ協会によりまとめられた『ITコーディネータプロセスガイドライン』に記載されているプロセスガイドラインのフレームに、関連する主要な法規制、規格およびガイドラインをマッピングしたものである。

もちろん、全てを網羅しているわけではない。

なかでも、金融商品取引法の一部としての日本版SOX法の制定（2006年予定）、ITガバナンスのフレームワークであるCOBITのバージョンアップ（2005年）、ITサービスマネジメントのベストプラクティスであるITILの上位規格となるISO20000の発行（2005年12月）、そして情報セキュリティ監査の規格であるISO27001の発行（2005年10月）は、我々のような運用サービス提供に従事する者にとって関わりが深く、これらの概要を理解した上で、対応を検討する必要がある。

ここで取り上げる規格あるいはガイドラインは、それぞれが様々なテーマで個別に研究されている。そこで本稿では、概念的な相互関連について整理・提示した上で、理解を深めたいと思う。そして、最後に運用の現場に求められる事項について考察することとする。

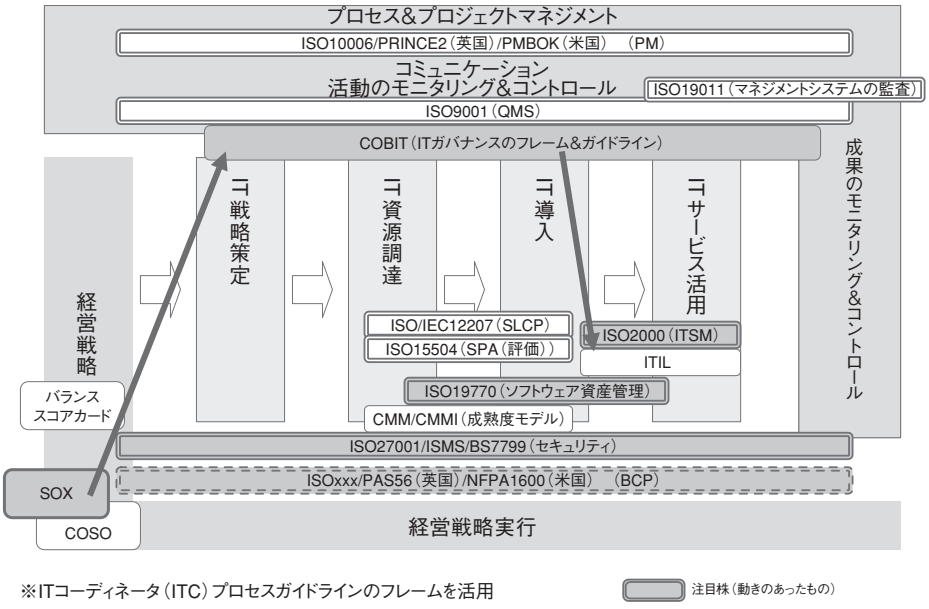


図1　ITサービスに関する規格化の動向

2．各規格およびガイドラインの概要

SOX法については、既に詳述されているので、本稿では、それ以外の関連する規格およびガイドラインについて概説する。

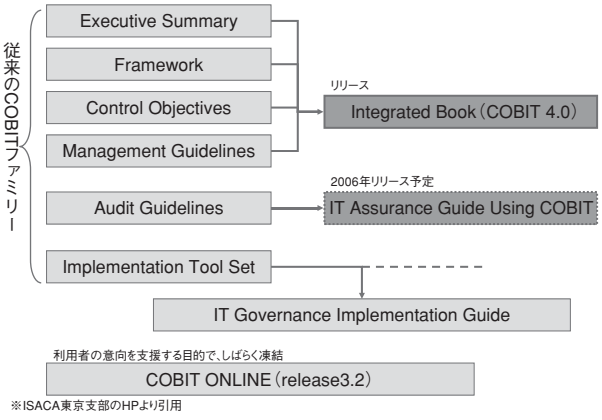
2.1　COBIT

Control Objectives for Information and related Technologyの略で、ITガバナンスのためのフレームワーク、ガイドラインや成熟度モデルなどの一連の情報から構成されているオープンスタンダード（公開標準）である。米国ISACA（Information System Audit and Control Association）の下部組織であるITガバナンス協会（ITGI：IT Governance Institute）が策定し、普及させている。

2005年には、図2に示すとおり、従来のCOBITファミリーのうち、「Executive Summary」「Framework」「control Objectives」「Management Guidelines」の4つの資料が1つにまとめられ、新たにCOBIT4.0としてリリースされた。

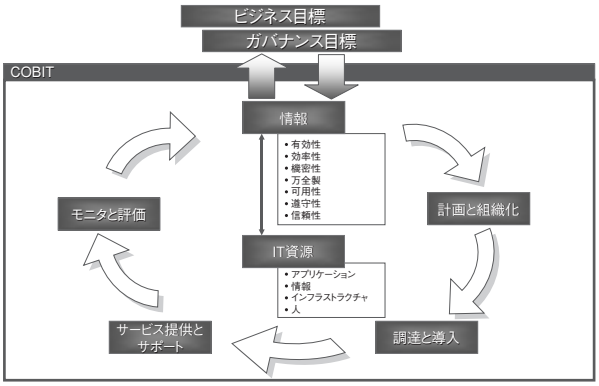
日本語版としては、「マネジメントガイドラインV3.0（Management Guidelines）」および「サーベインズ・オクスリー法（企業改革法）遵守のためのIT統制目標（IT Control Objectives for Sarbanes-Oxley）」が公開されている。

COBITには、ビジネスとガバナンスの要件に従い、図3のように、ビジネスに対して情報を提供するためのIT資源を管理するフレームワークの全体像が存在する。具体的には、図4に示す4つのドメイン、34の情報技術（IT）プロセスと、これらに加え318の詳細なコントロール目標及び監



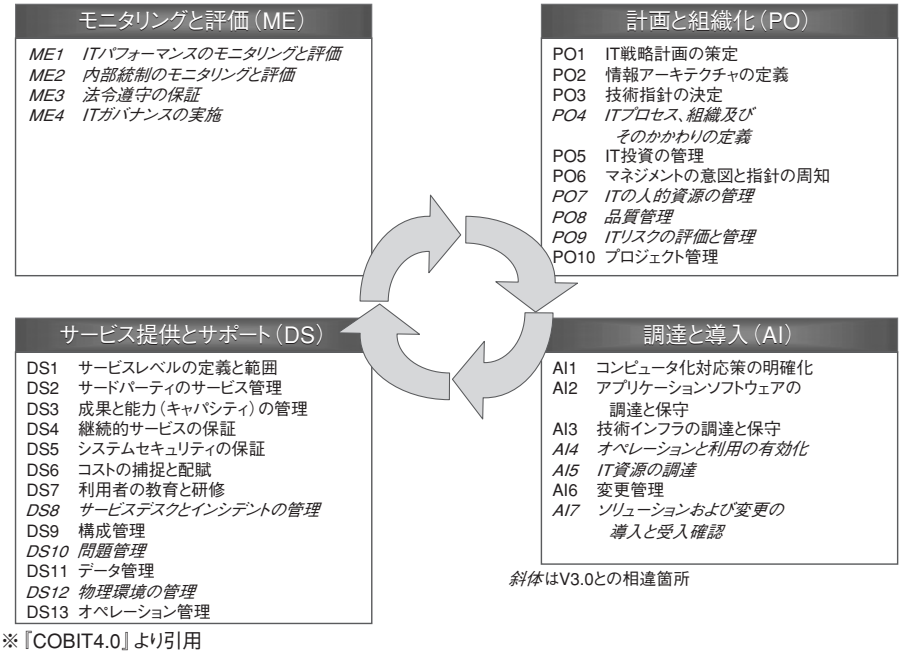
※ISACA東京支部のHPより引用

図2　COBIT4.0の構成



※『COBIT4.0』より引用

図3　COBITの全体フレームワーク



*斜体*はV3.0との相違箇所

※『COBIT4.0』より引用

図4　COBITの4ドメインと34プロセス

査ガイドラインが明示されている。

さらに、プロセスに対する成熟度モデルが定義されている。

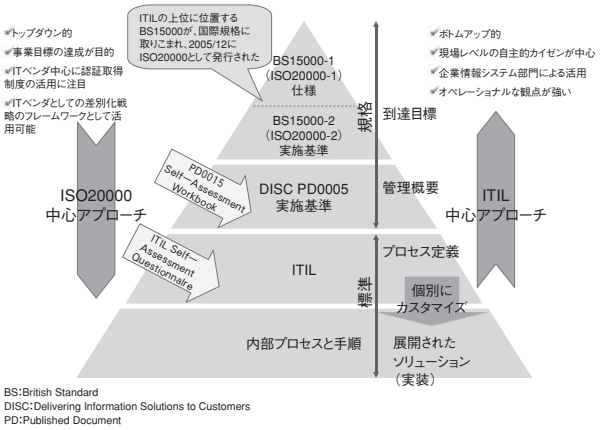
以上が、COBITの構成、フレームワークとその概要である。

COBIT4.0での主な変更点をまとめると、以下のとおりである。

・ITILやISO17799など、他の基準やガイドラインと用語や考え方を調和させた
・プロセスの定義、インプットとアウトプットを追加し、他のプロセスとの関連性を明示した
・プロセスごとの成熟度を定義した

2.2 ITILおよびISO20000

ITサービスマネジメントの体系を図5に示す。初めに、



BS:British Standard
DISC:Delivering Information Solutions to Customers
PD:Published Document

図5 ITサービスマネジメンの体系

ITサービスマネジメントのベストプラクティスであるITIL*（IT Infrastructure Library）が誕生し、その後上位規格BS15000が制定され、さらに規格が国際化されISO20000となった。

ITILとは、ITサービスマネジメントのベストプラクティス集である。ITへの投資効果に対する疑念からその品質を高めようと、英国政府機関が多様な組織におけるITサービスマネジメントの取組みに関する情報を収集・分析してまとめたものであり、補助的な冊子を含めて全8冊（2006年5月末現在）の出版物から構成される。

運用管理という旧来の枠に収まらず、ビジネス観点を持ちながらITサービス提供に関わる全体像を提示している。

図6にITILのフレームワークと、コア領域であるサービスサポートおよびサービスデリバリの10プロセスの概要を示す。

図7に示すとおり、ISO20000での要求項目とそれに対応するITILのプロセスは容易に関連付けることができる。

同じITサービスマネジメント、いわゆる“運用”を整備するにしても、ベストプラクティスであるITILを活用した現場主体の改善活動からはじめるボトムアップ的アプローチと、組織として国際標準であるISO20000取得という目標を掲げた上でその手段としてITILを活用するトップダウン的アプローチが存在する（図5）。

2.3 ISMS/ISO27001

セキュリティ関連の規格も見直された。

情報セキュリティマネジメントシステムとして体系化し、

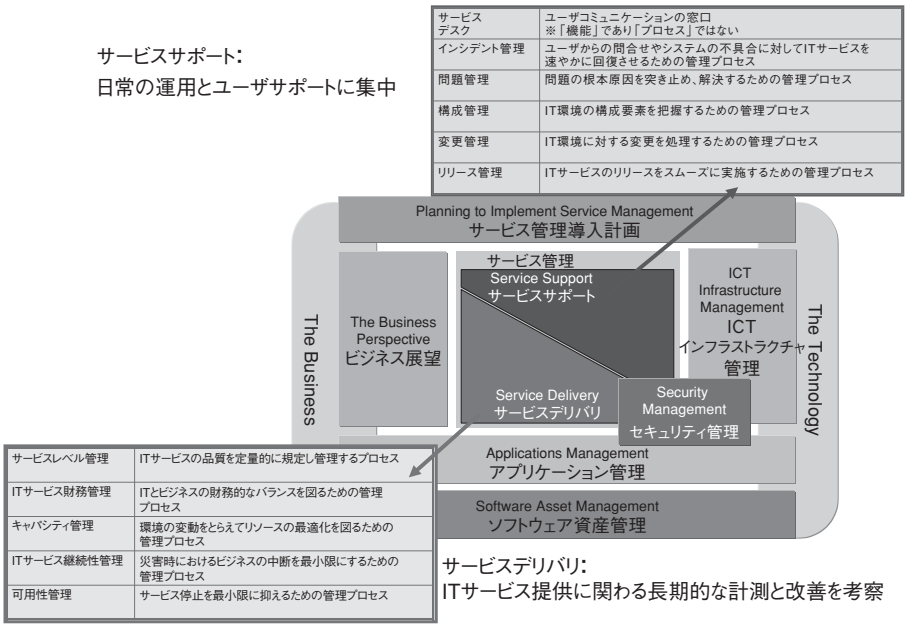


図6 ITILのフレームワーク

*ITILについては、SOFTECHS Vol.28, No.1（http://www.cac.co.jp/softechs/）で紹介しているので、参照していただきたい。

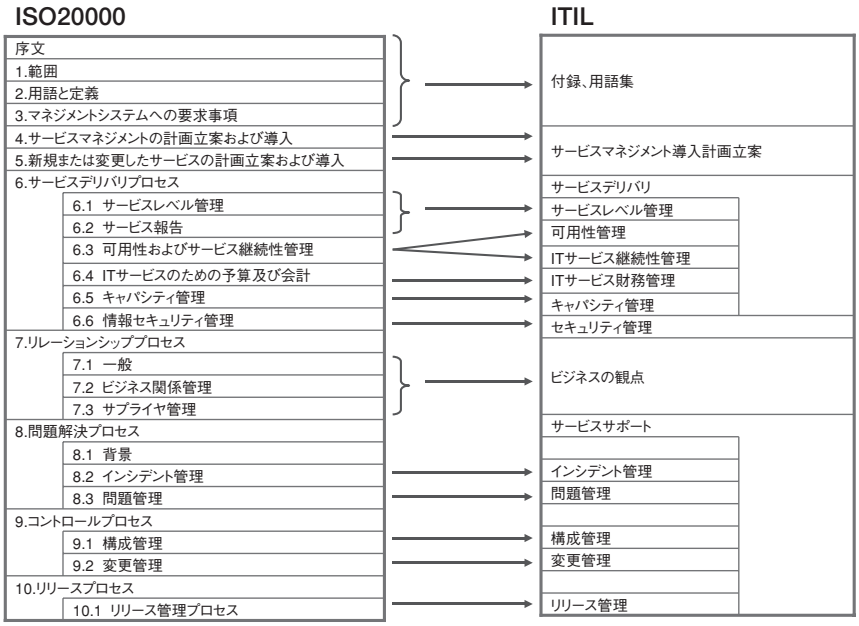
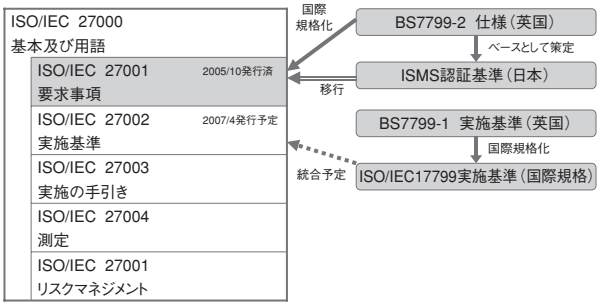


図7　ISO20000とITIL



※2006/5月末時点では、ISO/IEC27001のみ発行されている

図8　情報セキュリティマネジメントシステム（ISMS）関連規格

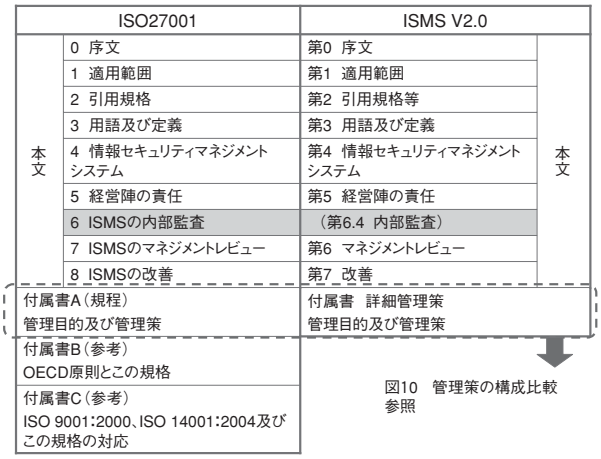


図9　ISO27001とISMSとの構成比較

ISO27001	ISMS V2.0
A.5　セキュリティ基本方針	3.　セキュリティ基本方針
A.6　情報セキュリティのための組織	4.　組織のセキュリティ
A.7　資産の管理	5.　資産の分類及び管理
A.8　人的資源のセキュリティ	6.　人的セキュリティ
A.9　物理的及び環境的セキュリティ	7.　物理的及び環境的セキュリティ
A.10 通信及び運用管理	8.　通信及び運用管理
A.11 アクセス制御	9.　アクセス制御
A.12 情報システムの取得、開発及び保守	10. システム開発及び保守
A.13 情報セキュリティインシデント管理	
A.14 事業継続管理	11. 事業継続管理
A.15 コンプライアンス	12. 適合性

図10　管理策の構成比較

ISO27000ファミリとしてまとめられた（2006年5月末時点では、ISO27001のみ発行済み）。

・ISO27000：基本及び用語

・ISO27001：要求事項

・ISO27002：実施基準

・ISO27003：実施の手引き

・ISO27004：測定

・ISO27005：リスクマネジメント

このISO27000ファミリは、図8に示すとおり、BS7799（英国規格）がもとになっている。

BS7799-2（仕様）をもとに日本ではISMS認証基準が策定されたが、英国規格の国際規格化により、日本のISMS認証組織は移行が求められることになった。

また、BS7799-1（実施基準）をもとに国際規格化されたISO17799も、将来的にはISO27000ファミリに統合される予定である。

この規格のアプローチは、リスクを評価しそれをコントロールするために、必要な管理策を特定するというものである。

図9および10に、ISMS V2.0とISO27001の記述概要を比較してみる。この二つは、章立てや詳細な部分に差異はあるものの、基本的には変わらないと考えていいだろう。

				COSO構成要素				
全社レベル	業務レベル	COBIT領域		統制環境	リスク評価	統制活動	情報と伝達	モニタリング
PO:計画と組織（IT環境）								
●		PO1	IT戦略計画の策定	●	●		●	●
●		PO2	情報アーキテクチャ			●	●	
		PO3	技術指針の決定					
●		PO4	IT組織とそのかかわり	●			●	
		PO5	IT投資の管理					
●		PO6	マネジメント意図と指針の周知	●			●	●
●		PO7	人的資源の管理	●			●	
●		PO8	外部要求事項の遵守				●	●
●		PO9	リスク評価		●			
		PO10	プロジェクト管理					
●		PO11	品質管理	●		●	●	●
AI:調達と導入（プログラムの開発と変更）								
		AI1	コンピュータ化対応策の明確化					
	●	AI2	アプリケーションソフトウェアの調達と開発			●		
	●	AI3	技術インフラの調達と保守			●		
	●	AI4	操作、運用手続きの作成と維持			●	●	
	●	AI5	アプリケーションソフトウェアと技術インフラの導入とテスト			●		
	●	AI6	変更管理			●		●
DS:サービス提供とサポート（コンピュータ・オペレーションおよびプログラムとデータへのアクセス）								
	●	DS1	サービスレベルの定義と管理	●		●		●
	●	DS2	サードパーティサービスの管理		●	●		●
●		DS3	成果とキャパシティの管理	●	●	●		●
		DS4	継続的なサービスの保証					
	●	DS5	システム・セキュリティの保証			●	●	●
		DS6	コストの捕捉と配賦					
●		DS7	利用者の教育と研修	●			●	
		DS8	利用者に対する支援と助言					
	●	DS9	構成管理			●	●	
	●	DS10	問題と事故の管理			●	●	●
	●	DS11	データ管理			●	●	
●		DS12	設備管理		●			
	●	DS13	オペレーション管理			●	●	
M:モニタリング（IT環境）								
●		M1	モニタリング				●	●
●		M2	内部統制の十分性					●
●		M3	独立した第三者の保証	●				●
●		M4	独立監査					●

※『サーベインズ・オクスリー法（企業改革法）遵守のためのIT統制目標』より引用

図11　COBIT（V3.0）とCOSO構成要素

3．SOX法対応のためのCOBIT、ITIL そしてISO27001

3.1　COBIT for SOX

図11に、2004年4月にCOBITを策定・普及しているITGIより公開された『サーベインズ・オクスリー法（企業改革法）遵守のためのIT統制目標』、通称“COBIT for SOX”に記されている、米国版COSOの構成要素とCOBIT V3.0のプロセスとのマッピングを掲載する。

このような資料が公開されていることからも、米国では、SOX法への対応に、COSOフレームワークと併せてCOBITが利用されていることがわかる。

日本でも、実施基準が公表されていない現時点では、この資料をもとに対策が進められている。

3.2　SOX対応の手段としてのITIL、そしてISO27002

ITガバナンスの視点からITILを上手く活用したいという目的で、COBITとITIL、あるいはCOBITとセキュリティ規格（ISO2700x、ISO17799、ISMS）との関連性も研究されている。

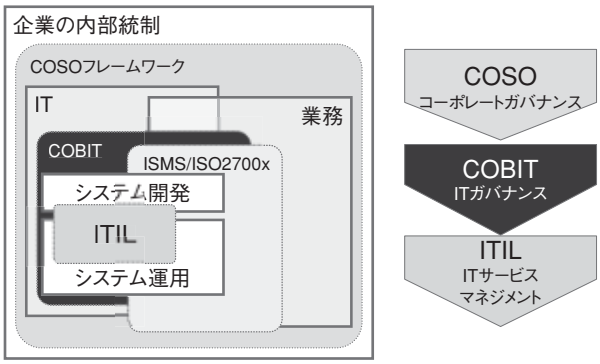


図12　内部統制とITサービス

前出のITGIとITILの作成者であるOGC（Office of Government Commerce）が『Aligning COBIT, ITIL and ISO17799 for Business Benefit』という資料を公開しているので参照していただきたい。

前述のSOX法とCOBITの関係も含めて整理すると、最終的には、図12に示すように、SOX法対応のための手段としてITILあるいはセキュリティ規格（ISO2700x、ISO17799、ISMS）が利用される、ということになる。

図13に、前述の『サーベインズ・オクスリー法（企業改

		COBITの統制目標	PCAOB IT全般統制 プログラム開発	プログラム変更	コンピュータ・オペレーション	プログラムとデータへのアクセス
1	AI2	アプリケーションソフトウェアの調達と開発	●	●	●	●
2	AI3	技術インフラの調達と保守	●	●	●	
3	AI4	方針、運用手続きの作成と維持	●	●	●	●
4	AI5	アプリケーションソフトウェアと技術インフラの導入とテスト	●	●	●	●
5	AI6	変更管理		●		●
6	DS1	サービスレベルの定義と管理	●	●	●	●
7	DS2	サードパーティサービスの管理	●	●	●	●
8	DS5	システム・セキュリティの保証			●	●
9	DS9	構成の管理			●	●
10	DS10	問題と事故の管理			●	
11	DS11	データ管理			●	●
12	DS13	オペレーション管理			●	●

※『サーベインズ・オクスリー法（企業改革法）遵守のためのIT統制目標』より引用

図13　統制のプロセス

COBITの統制目標		SOX　IT全般統制のプロセスの例	ITIL参照先	ISO27001参照先
AI2	アプリケーションソフトウェアの調達と開発	プログラム開発管理	アプリケーション管理 ICTインフラストラクチャ管理	（A.12　情報システムの取得、開発及び保守）
AI3	技術インフラの調達と保守			
AI4	方針、運用手続きの作成と維持			
AI5	アプリケーションソフトウェアと技術インフラの導入とテスト			
AI6	変更管理	システム運用管理	変更管理、リリース管理	A.7　資産の管理 A.10　通信及び運用管理 A.12　情報システムの取得、開発及び保守
DS9	構成の管理		構成管理	
DS10	問題と事故の管理		インシデント管理、問題管理	A.13　情報セキュリティインシデントの管理
DS1	サービスレベルの定義と管理		サービスレベル管理	
DS13	オペレーション管理		可用性管理、キャパシティ管理	
DS5	システム・セキュリティの保証	システムセキュリティ管理	（セキュリティ管理）	A.5　セキュリティ基本方針 A.9　物理的及び環境的セキュリティ A.11　アクセス制御
DS11	データ管理			
DS2	サードパーティサービスの管理	外部委託先管理	ビジネスの観点のサプライヤ管理	（A.6　情報セキュリティのための組織 A.10　通信及び運用管理 A.12　情報システムの取得、開発及び保守）

図14　SOX法対応のためのITIL、ISO27001の活用

革法）遵守のためのIT統制目標』に記載されているIT全般統制とCOBITの統制目標の関連を示す。

この12項目からなる統制目標をもとに、SOX法対応におけるIT全般統制のプロセス案とITILおよびISO27001の参照先をまとめた（図14）。

システム管理プロセスについてはITILを、セキュリティ管理については当然のことながらISO27001を活用して整備をすすめることができるであろう。

ただし、ISO27001は要求事項という位置づけのため、実施基準であるISO27002（2006年5月末時点では未発行なので、JIS Q 27002）を参照するべきである。

また、ITILにしてもISO27002にしても汎用的なプロセスや基準を提示しているものの、組織の現状に見合った改善策は自らが考えなければならないことを付け加えておく。

3.3　ISO20000およびISO27001両規格の活用

先にSOX法対応のために、ITILとISO27002は有効と述べた。

ここで、それぞれの上位規格であるISO20000とISO27001の2つの規格の関連性について、少し掘り下げて考えてみたい。

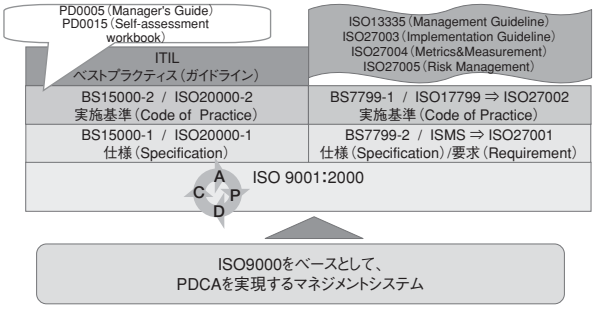


図15　マネジメントシステム

ISO20000とISO27000は、ISO14000とともにマネジメントシステムとしてくくられる。このマネジメントシステムは、図15に示すとおり、品質マネジメントの規格であるISO9001のPDCAサイクルを基本としている。

ISO20000には情報セキュリティ管理に関する要求事項が定められており、ベストプラクティスであるITILのセキュリティ管理では、ISO27001の前身であるBS7799との関連性も記述されている。

これらのことから、両者は個別の規格として別個に適用するのではなく、その共通項や相互補完のあり方を検討した上で、統合的に活用するべきものであることがわかる。

内部統制の監査にあたっても、ISO同様、プロセス設計の文書化およびその運用の記録が求められる。また、これを定期的に評価するという点では、内部統制には、継続的改善というISOに求められているものと同じ考え方がベースにある。

SOX法対応として、ISO20000やISO27001の規格の認証取得が要求されているわけではない。

しかしながら、ISO規格の認証取得を通してITサービス提供の基盤を統合的に整備することは、SOX法対応としての効果をもたらすだろう。

4．運用の現場に求められること

一見難しそうなSOX法への対応も、図14に示すとおり、個々の作業に落としてみると、変更管理やアクセス制御などの整備にたどり着くことがわかる。これらの活動は目新しいものではなく、これまでにも行ってきた品質管理や法令順守等への対応として、すでに存在しているものである。

そして今後は、ビジネス、IT企画・開発・運用、言い換えるとCOSO、COBIT、ITILという個別手段によるアプローチではなく、これらの関連性を理解したうえでベクトルを合わせることが求められるのだ。

SOX法への対応は、これまでの活動とかけ離れた、単なる法規制対応として終わらせることなく、今までの活動を統合し改善サイクルを強化する機会と捉えるべきである。

冒頭図1でも示したように、運用に関わる規格・標準の整備は急速に進んでいる。CACの運用の現場でも、それぞれの概要と関連性を理解して、継続的な提供サービスの品質改善を、日々の活動の一部として組み込まなければならない、と考えている。

〈参考文献〉

1. 『ITコーディネータプロセスガイドライン』：ITコーディネータ協会（2005年）
2. 『財務報告に係る内部統制の評価及び監査の規準のあり方について』：企業会計審議会（2005年）
3. 『COBIT　第3版　マネジメントガイドライン』：ITガバナンス協会（2003年）
4. *COBIT 4.0*：IT Governance Institute（2005年）
5. 『サーベインズ・オクスリー法（企業改革法）遵守のためのIT統制目標』：ITガバナンス協会（2004年）
6. *Aligning COBIT, ITIL and ISO17799 for Business Benefit*：IT Governance Institute他
7. 『サービスサポート』：TSO（The Stationary Office）（2003年）
8. 『サービスデリバリ』：TSO（The Stationary Office）（2004年）