COBIT™
エグゼクティブサマリー

1998年4月
第2版

COBIT運営委員会および
情報システムコントロール財団

COBITの使命：
ビジネスマネジャーおよび監査人が日々利用するために
権威のある，最新の，国際的に一般に認められた
情報テクノロジーコントロール目標の体系を
調査し，開発し，公表し，推進すること

利用上の注意

情報システムコントロール財団と CobiT **のスポンサーは，「情報システムおよび関連技術のための内部統制目標**(Control Objectives for Information and Related Technology)」**製品を を主に内部統制専門家のための教育用資料として作成した。情報システムコントロール財団とそのスポンサーはこの使用による結果がすべて成功を納めることを保証するわけでない。この製品はすべての適切な手続きとテストを包んでいるわけではない。また，同じ結論を得るための合理的に指示された他の代替手続きやテストを排除するものでもない。内部統制専門家は手続きやテストが適切であるかどうかを決定する際に，特定のコントロール環境に対する特定のシステムまたは情報技術に向けられた環境についての専門家としての判断を下すべきである。**

開示

情報システムコントロール財団
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
電話: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: research@isaca.org
Web site: www.isaca.org

ISBN 0-9629440-8-4 (**エグゼクティブサマリ**)
ISBN 0-9629440-3-3 (CD-ROM **付き** 5 **分冊**)

印刷：アメリカ合衆国

経営者のための要約

情報と関連する情報技術の有効な管理は，今後の組織の成功と生き残りに極めて重要になってきている。時間，距離，スピードの制約がないサーバースペースを多くの情報が飛び交うこのグローバルな情報社会では，次のような点から有効な管理の重要性が増している。

- ･情報とこの情報を提供するシステムへの依存の増加
- ･サイバー脅威や情報戦争のような，脆弱性や広範な範囲におよぶ脅威の増大
- ･情報と情報システムへの現在および将来の投資規模とコスト
- ･組織やビジネスのやり方を劇的に変化させ，新たな機会を創造し，コストを削減する技術の可能性

組織をサポートする情報と技術は，多くの組織にとって最も価値のある資産である。さらに，今日の非常に競争的で変化の速いビジネス環境では，経営者は IT による情報配付機能に期待を高めてきた。確かに情報と情報システムは，ユーザのプラットフォームからローカルやワイドエリアネットワークへ，クライアント･サーバへ，メインフレーム･コンピュータへと浸透している。このように，経営者は，より低いコストで成し遂げられることを要求している一方で，より高い品質，機能性，容易な利用，より短い開発期間，サービルレベルの継続的な向上を要求している。***多くの組織は，技術が生み出す潜在的な利益を認識している。しかしながら，成功する組織は，新しい技術を導入することに伴うリスクを認識し，管理している。***このように，経営者は有効な方向性と適切なコントロールを実現するために，IT のリスクと制約の正しい認識と基本的な理解を持つ必要がある。COBIT は，ビジネスリスク，コントロール･ニーズ，技術的な問題の間隙を埋めるのを助ける。それは，ドメインとプロセスフレームワークをまたがる良き慣行を提供し，管理できる，論理的な構造でアクティビティを表している。COBIT の“**良き慣行**”とは，専門家のコンセンサスを意味し，それらはあなたの情報化投資も助けるが，最も重要なこととして，事態が悪化したときにあなたはこれに基づいて正しい判断ができるということである。

組織は，すべての資産に対するのと同じように，情報に対する品質，信用上の，およびセキュリティの要件を満たさなければならない。経営者はまた，データ，アプリケーションシステム，技術，設備，要員を含む利用可能な資源の利用最適化を図らなければならない。これらの目標を達成するのと同様に，経営者はこの責任を果たすために，適切な内部統制のシステムを確立しなければならない。従って，コントロールシステムあるいはフレームワークは，ビジネスプロセスを支援するためにすぐに使える状態になければならず，各々のコントロール活動がどのように情報要件を満足し，資源に影響を及ぼすかについて，明確にしなければならない。COBITフレームワークでは，IT資源への影響は，ビジネス要件としての情報の有効性，効率性，機密性，インテグリティ，可用性，準拠性，信頼性を満足することと同様に強調されている。方針，組織構造，慣行，手続を含むコントロールは，経営者の責任である。経営者は，コーポレート･ガバナンスを通して，情報システムの管理，利用，設計，開発，保守，または運用に関係するすべての個人が当然の注意を払うことを保証しなければならない。ITコントロール目標とは，特定のIT活動の内で，コントロール手続を実施することにより達成される望しい結果，あるいは目的を表明したものである。

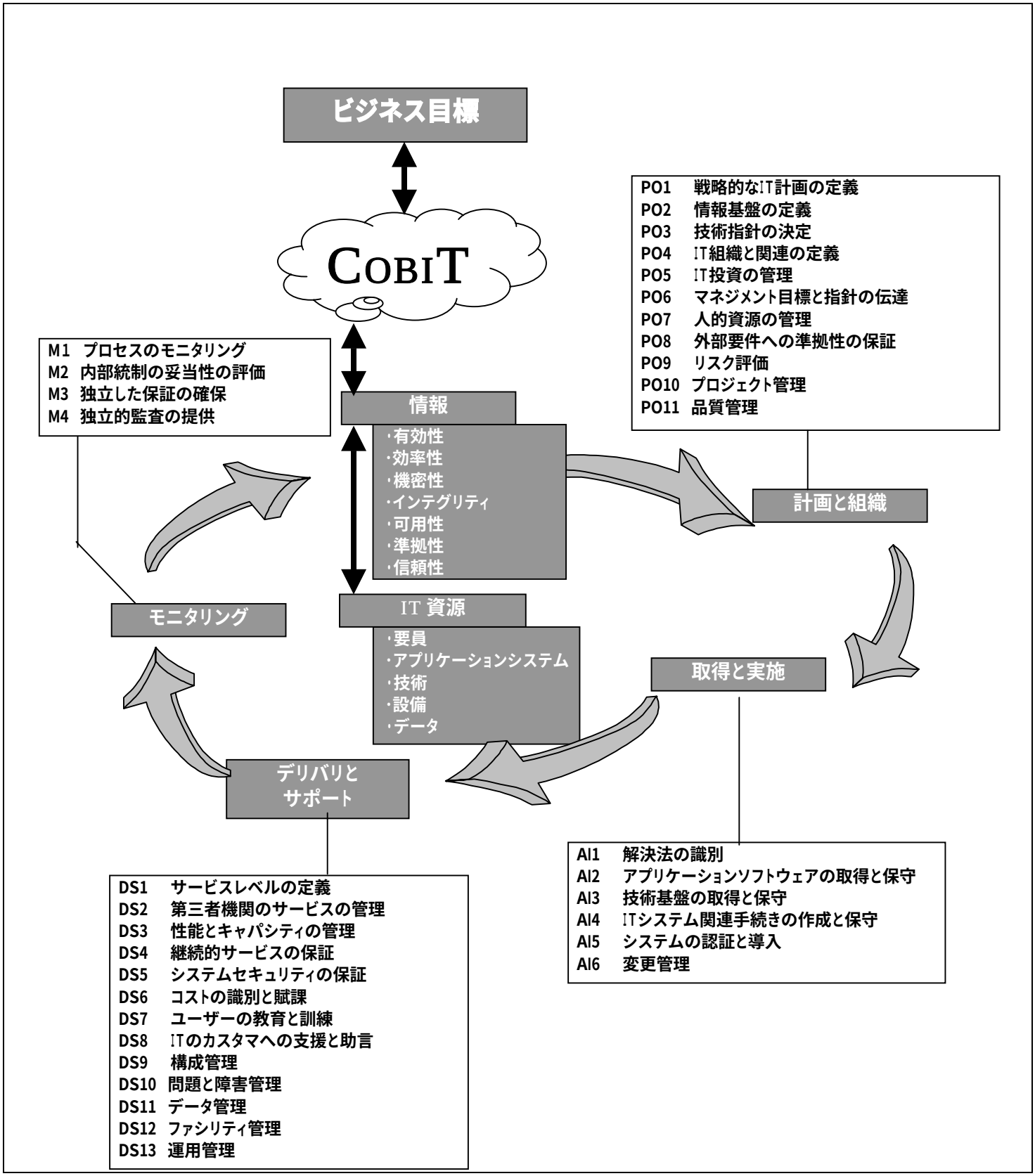
COBITの主要テーマは，ビジネス指向である。より重要なことは，ユーザや監査人だけでなく，ビジネスプロセスオーナの総合的なチェックリストとして設計されていることである。ビジネス慣行は，益々，ビジネスプロセスオーナがビジネスプロセスのすべての側面に全体的な責任を持つように，完全な権限委譲を伴うようになっている。特に，これには適切なコントロールを提供することを含んでいる。COBITフレームワークは，この責任の履行を楽にするツールを，ビジネスプロセスオーナに提供するものである。フレームワークは，次のような単純かつ実用的前提から出発している。

組織がその目標を達成するために必要とする情報を提供するために，一連の自然にグループ化されたプロセスによって，IT資源は管理される必要がある。

フレームワークは，34の高いレベルのコントール目標の体系となっており，各々のITプロセスは，計画と組織，取得と実施，デリバリとサポート，モニタリングの4つのドメインにグループ化されている。この構造は，フレームワークを支援する情報と技術のすべての側面を網羅している。これらの34の高いレベルのコントロール目標に着目し，ビジネスプロセスオーナは，情報技術の環境に対し適切なコントロールシステムが提供されていることを保証できる。加えて，34の高いレベルのコントール目標に対応する302の薦められた詳細なコントロール目標は経営者がCOBITに基づいてITプロセスをレビューする手段を与え，改善に対する保証，そして／あるいはアドバイスを提供するための，監査あるいは保証のガイドラインである。COBITには，自分達の作業環境にCOBITを早く，うまく適用した組織から学んだ教訓を提供する*導入ツールセット*が含まれている。それは，上級マネジメントのCOBITの主要なコンセプトと本質の認識とを理解するための，経営者のための要約を含んでいる。導入ガイドには，組織のITコントロール環境を分析をすることを援助するために，2つの役立つツール－経営者の認識診断とITコントロール診断－がある。

組織の経営者は，既存および計画されたIT環境の（価値）判断基準として，一般に適用可能で承認されたIT統治とコントロール慣行を必要としている。COBITはコントロール要件，技術的課題，そしてビジネスリスクの三つの側面について，経営者が会話し，ギャップを埋めるために与えられたツールである。COBITは，世界中のどんな組織に対しても，ITコントロールに関する明確な方針の作成と良き慣行を可能にすることができる。COBITの目標は，これらのコントロール目標を提供し，定義されたフレームワーク内で，世界的な民間，政府，専門家の組織からの承認を得ることである。**このように，COBITは，情報と関連するITに関するリスクを理解し，管理することを助ける画期的なIT統治（管理）ツールを目指している。**

4つのドメインに定義されたCOBITのITプロセス



背景

COBIT製品の開発

COBITは，情報技術(IT)の良きセキュリティとコントロールのための，一般的に適用可能で認められた基準として開発された。即ち，**COBITは画期的なIT統治ツールである**。COBITは，情報システムコントロール財団(ISACF)の***コントロール目標***に基づき，既存，および新しい国際的な技術標準，職業標準，規制並びに業界固有標準への対応を強化している。その結果としてのコントロール目標は，**組織全体の情報システム**へ適用されるように開発されてきている。**“一般に適用可能で認められた”**という用語は，明らかに，一般に認められた会計原則（GAAP）と同じ意味に用いられている。COBITの**“良き慣行”**とは，専門家の合意を意味し－それらはあなたの情報化投資の最適化も助けるが，最も重要なこととしては，事態が悪化したときに，あなたはこれに基づいて判断のもととなるということである。

この基準は，組織で採用された技術的ITプラットフォームによらず，比較的コンパクトで，可能な限り実用的でビジネスニーズに応えるものである。

次のような，オリジナルの***コントロール目標***の強化が決定された。

→ITコントロール目標の基礎となり，また，IT監査とコントロールにおける首尾一貫した調査研究の推進力となる，ITにおけるコントロール・フレームワークの開発

→全体のフレームワークおよび個々のコントロール目標，並びに現行の*事実上*あるいは*法律上の*国際的標準や規制との調整

→ITにおけるコントロールドメインの基礎となる色々なアクティビティやタスクに対する重点的レビュー，および，可能ならば関連するプロセスの業績ベンチマーク（基準値，ルール等）の仕様記述

→情報システム監査を遂行するための既存ガイドラインに対する重点的レビューと更新

情報システムコントロールの分野において，調査の期間中に新たに公表されたその他の認められた標準を除外するものではないが，原典として以下が利用された。

技術標準：ISO，EDIFACT等

行動綱領：ヨーロッパ会議（C.E），OECD，ISACA等の公表

ITシステムとプロセスの**認証規準**：ITSEC，TCSEC，ISO9000,SPICE，TickIT，Common Criteria等

内部統制と監査における**専門標準**：COSO報告書，IFAC，AICPA，ISACA，IIA，PCIE，GAO標準等

業界慣行と要件：業界フォーラム（ESF，I4），政府後援の標準プラットフォーム（IBAG，NIST，DTI）等

新たな業界固有の要件：銀行，電子商取引，およびIT製造業

（付録III　用語解説参照）

COBIT製品の定義

COBITの開発の結果，以下のような出版物が発行された。

- ***エグゼクティブサマリー***：この背景のセクションに加えて，経営者のための要約（上級マネジメントにCOBITの主要な概念と原理についての認識と理解を提供するもの）と*フレームワーク*（上級マネジメントにCOBITの主要な概念と原理のより詳細な理解を提供し，COBITの4つのドメインと対応する34のITプロセスを識別するもの）から構成される。
- ***フレームワーク***：COBITの34の高いレベルのITコントロール目標を詳細に記述し，それぞれのコントロール

目標によって主として影響を受ける情報とIT資源に対するビジネス要件を識別する。

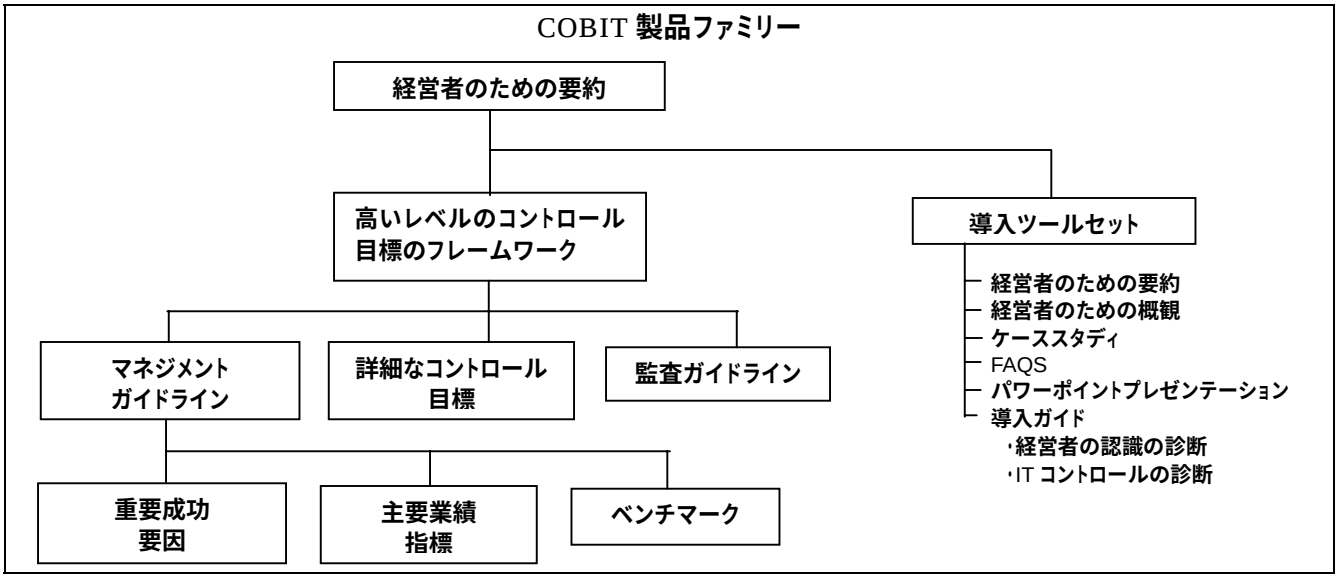
- ***コントロール目標***：34のITプロセスに関して，302の明確かつ詳細なコントロール目標を実現することで，望まれる結果あるいは達成すべき目的の記述を含む。
- ***監査ガイドライン***：マネジメントの保証や／または改善のためのアドバイスを提供するため，COBITの302の推奨された詳細なコントロール目標に対して，ITプロセスをレビューする情報システム監査人を援助するために，34の高いレベルのITコントロール目標の各々に対応した提案された監査ステップを含む。
- ***導入ツールセット***：組織の業務環境にCOBITを早く，成功裡に適用した組織から学んだ教訓を提供する。

*導入ツールセット*は，経営者のための要約を含み，上級マネジメントにCOBITの認識と理解を提供している。それはまた，組織のITコントロール環境を分析することを援助するために，2つの役立つツール―経営者の認識診断とITコントロール診断―を導入ガイドに含まれている。また，ワールドワイドの組織がどのように成功裡にCOBITを導入してきたかの多くの詳細なケーススタディを含んでいる。加えて，組織内の異なる階層レベルや読者に合うような，COBITについての25の最も頻繁に尋ねられる質問(FAQ)への回答やいくつかのスライド・プレゼンテーションが含まれている。

COBIT製品の発展

COBITは，年々発展し，今後の調査・研究における基礎となるであろう。COBIT製品ファミリーはこのように出版され，ITコントロール目標を構成するための構造を提供するITタスクとアクティビティは，今後ともさらに洗練され，ドメインとプロセス間のバランスは，業界の“日々変化する眺望”に基づいてレビューされるであろう。

製品としてのCOBITファミリーに対して近々構想されている主な追加は，マネジメント・ガイドラインの開発であり，それには，重要成功要因(KSF)，主要業績指標，およびベンチマークが含まれている。この追加は，COBITの34の高いレベルのコントロール目標に対する組織のIT環境を評価するためのツールとして経営者に提供される。重要成功要因は，ITプロセスでの良いコントロールを達成するために，経営者にとって最も重要な課題や行動を識別するものである。主要業績指標は，ITプロセスがビジネス要件をどの程度満足しているかを経営者に伝える，成功の基準となるものである。ベンチマークは，以下のような目的に経営者が利用できる，成熟レベルを定義するものである。(1) 組織の現在の成熟レベルを判断すること，(2) リスクと目標の関数として，達成したい成熟レベルを決めること，(3) 同業者や業界標準に対して，自社のITコントロール慣行を比較するための根拠を提供すること。この追加は，COBITの34の高いレベルのコントロール目標に対する組織のIT環境を評価するためのツールとして経営者に提供される。



調査と出版は，Unisys，Unitech Systems，MIS Training Institute，Zergo Ltd.，そしてCoopers &

Lybrandからの多大な寄付金によって可能となった。また，ヨーロッパ・セキュリティ・フォーラム（ESF）は，その調査資料をこのプロジェクトに快く利用可能として頂いた。さらなる寄付が，世界中のISACAの支部やメンバーから寄せられた。

COBITフレームワーク
状況設定

情報技術におけるコントロールの必要性

最近，規制者，立法者，ユーザおよびサービス提供者にとって，IT におけるセキュリティとコントロールに関する参照フレームワークの必要性が，益々，明らかになってきた。情報と関連する情報技術の有効な管理は，今後の組織の成功と生き残りに極めて重要になってきている。時間，距離，スピードの制約がないサーバースペースを多くの情報が飛び交うこのグローバルな情報社会では，次のような点から有効な管理の重要性が増している。

- 情報とこの情報を提供するシステムへの依存の増加
- サイバー脅威や情報戦争のような，脆弱性や広範な範囲におよぶ脅威の増大
- 情報と情報システムへの現在および将来の投資規模とコスト
- 組織やビジネスのやり方を劇的に変化させ，新たな機会を創造し，コストを削減する技術の可能性

組織をサポートする情報と技術は，多くの組織にとって最も価値のある資産である。確かに情報と情報システムは，ユーザのプラットフォームからローカルやワイドエリアネットワークへ，クライアント･サーバへ，メインフレーム･コンピュータへと浸透している。***多くの組織は，技術が生み出す潜在的な利益を認識している。しかしながら，成功する組織は，新しい技術を導入することに伴うリスクを認識し，管理している。***このように，経営者は有効な方向性と適切なコントロールを実現するために，ITのリスクと制約の正しい認識と基本的な理解を持つ必要がある。

経営者は，ITにおけるセキュリティとコントロールに対して，合理的に何を投資するのか，また，しばしば予想できないIT環境において，リスクとコントロールに対する投資のバランスの取り方を決定しなければならない。情報システムセキュリティとコントロールはリスクの管理を助けるとはいえ，リスクをなくしはしない。さらに，常にある程度の不確実性があるため，リスクの正確なレベルを決して知ることはできない。結局，経営者は受け入れられるリスクのレベルを決定しなければならない。許容できるレベルを判断することは，特にコストと秤にかけるとき，経営者の難しい意思決定となる。その結果，経営者は明らかに，彼らの既存および計画されたIT環境を価値判断するために，一般に認められたITのセキュリティとコントロール慣行のフレームワークを必要とする。

ITサービスの**ユーザ**にとって，内部または第三者機関によって提供されるITサービスで，適切なセキュリティとコントロールが存在することを認証と監査により保証してもらう必要性が高まっている。しかし，現状では，民間であれ，非営利または政府機関であれ，情報システムにおいて良いITコントロールを導入することが，ある種の混乱によって阻害されている。この混乱は，ITSEC，TCSEC，ISO9000による評価，最近のCOSOによる内部統制の評価等の異なった評価方法から生じている。その結果，ユーザは，先ず第一歩として確立されるべき一般的な基礎体系を必要としている。

しばしば，**監査人**がそのような国際標準化への努力に指導力を発揮してきたのは，彼らが継続して経営者に内部統制に関する監査人の意見を陳述する必要に直面していたためである。これはフレームワークなしでは，途方もなく困難なタスクである。このことは，監査人がITにおける複雑なセキュリティとコントロールの状況をどのように判断するかに関して，ほとんど同時に世界の違ったところで行われたいくつかの最近の研究によって明らかにされてきた。さらに，監査人は，経営者からITのセキュリティとコントロールに関連した問題について，前向きにコンサルティングし，益々助言することを求められつつある。

ビジネス環境：競争，変化とコスト

グローバルな競争が起こっている。組織は，業務を合理化するためにリストラクチャリングしつつあると同時に，競争上の地位を向上するためにITの進歩を活用している。ビジネス･リエンジニアリング，ライトサイジング，アウトソーシング，エンパワーメント，フラット型組織，分散処理は，すべてビジネスと政府組織の運営の方法に影響を与える変化である。これらの変化は，世界的に組織内部のマネジメントと業務コントロールの構造に対し，深い意味合いを持ちつつあり，また，持ち続けるであろう。

競争的優位と費用効率を達成することの重視は，多くの組織で主要な戦略の一要素としての技術への依存度がかつてないほど高まっていることを意味している。組織機能を自動化することは，正にその性質上，コンピュータとネットワークへハードウェアとソフトウェア双方をベースにしたより強力なコントロール機能を組み込むことを指向しつつある。さらに，これらのコントロールの基本的な構造的特徴は，基礎にあるコンピュータとネットワーク技術の進歩と同じような「蛙飛び」のような速度で展開しつつある。

加速された変化のフレームワークの内で，管理者，情報システム専門家，および監査人が実際，その役割を本当に効果的に果たすには，その技能を技術や環境の変化と同じ位，迅速に進歩しなければならない。典型的なビジネスまたは政府組織におけるコントロール慣行を評価するとき，合理的かつ慎重な判断を行うためには，そこに内在するコントロール技術およびそれが変化する性質を理解しなければならない。

必要性への対応

これらの絶え間ない変化を考慮すると，ITコントロール目標のフレームワークの開発と，このフレームワークに基づくITコントロールにおける継続的な応用研究は，情報と関連技術のコントロールにおける有効な進歩の礎石となる。

過去において，一方で米国のCOSO(Committee of Sponsoring Organisations of the Treadway Commission-Internal Control-Integrated Framework, 1992)，英国のCadbury，カナダのCoCoおよび南アフリカのKingのような全般的なビジネスコントロールモデルの開発と刊行があった。他方，より焦点を絞った重要な多数のコントロールモデルがITレベルで存在している。後者の範疇で優れた例は，DTI（英国通商産業部）のSecurity Code of ConductとNIST（米国標準技術機関）のセキュリティハンドブックである。しかしながら，ビジネスプロセスを支援するITに対して，包括的かつ利用可能なコントロールモデルを提供したものはなかった。COBITの目的は，ITに焦点をあてながら，ビジネス目標に密接に連携される基礎を提供することによって，この隔たりを埋めることである。

ITコントロールにおけるビジネス要件の重視，先端コントロールモデルの適用および関連する国際標準によって，コントロール目標は，監査人のツールからマネジメントツールとしてのCOBITへと進化したのである。**COBITは，このようにITに関連するリスクを理解し，管理することにおいて経営者を助ける画期的なIT統治ツールである。**

従って，COBITプロジェクトの主要な目標は，世界の民間，政府，専門家によって承認されたITにおけるセキュリティとコントロールに関する明確な方針と良き慣行の開発である。これらのコントロール目標を第一義的には，ビジネスの目標とニーズの展望から展開することがプロジェクトの目標である。これはCOSOの展望に沿っており，それは内部統制に対する最初のそして最も重要なマネジメントフレームワークである。その後，コントロール目標は，監査目標（財務情報の認定，内部統制対策の認定，効率性と有効性等）の視点から開発された。

利用者：経営者，ユーザ，監査人

COBITは，3つの別個の利用者区分により利用されるよう設計されている。

経 営 者：
しばしば予想できないIT環境において，リスクとコントロールへの投資の均衡を図ることを支援する。

ユ ー ザ：
内部または第三者機関によって提供されるITサービスのセキュリティとコントロールに関する保証を得る。

情報システム監査人：

内部統制に関する経営者への意見やアドバイスの根拠となる。

上級経営者，監査人，セキュリティとコントロールの専門家という直接的な利用者の必要性に応える以外，COBITは，プロセスの情報の側面へのコントロールに関する責任を持つビジネスプロセスオーナや，また，企業内でのIT活動の責任者が企業内で使うこともできる。

ビジネス目標指向

コントロール目標は，監査コミュニティの外で，意義のある利用を支援するために，ビジネス目標に明確かつ固有な繋がりを持っている。コントロール目標は，ビジネス･リエンジニアリングの原理に沿ってプロセス指向の方法で定義されている。識別されたドメインとプロセスにおいて，高いレベルのコントロール目標が識別され，ビジネス目標への繋がりを文書化するために，理論的根拠が提供される。さらに，ITコントロール目標を定義し，設定するために検討事項とガイドラインが提供される。

高いレベルのコントロール目標が適用されるドメインの分類（ドメインとプロセス），当該ドメイン内の情報に対するビジネス要件，同様にコントロール目標によって主に影響を受けるIT資源が一緒になって，COBIT *フレームワーク* を形成する。調査活動の結果，*フレームワーク*として，34の高いレベルのコントロール目標と302の詳細なコントロール目標が識別された。*フレームワーク*は，IT産業と監査の専門家のレビュー，挑戦，コメントの機会を与えるために公表された。得られた洞察は，適切に組み込まれてきた。

定　義

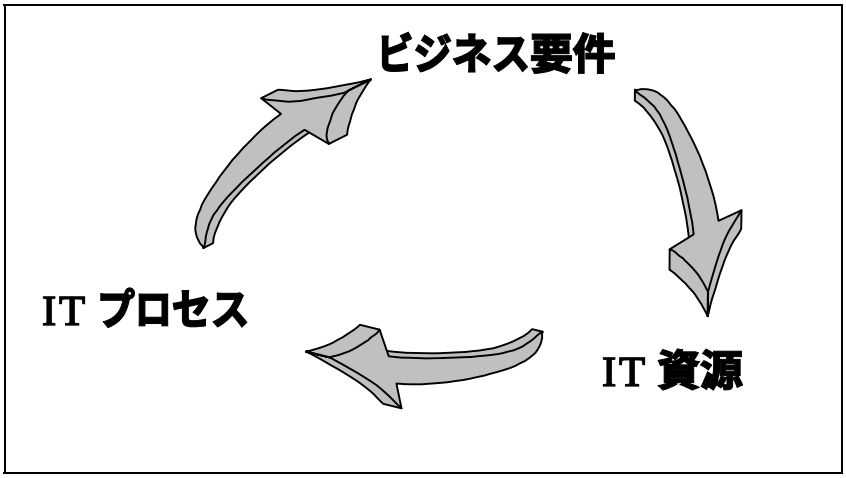
本プロジェクトの目的に関しては，以下の定義が用いられる。「コントロール」は，COSOレポート[*Internal Control-Integrated Framework,* Committee of Sponsoring Organisations of the Treadway Commission, 1992]から，「ITコントロール目標」は，SACレポート[*Systems Auditability and Control Report,* The Institute of Internal Auditors Research Foundation, 1991 and 1994]に適合させた。

コントロール	ビジネス目標が達成され，望ましくない出来事が予防され，発見され，是正されるに足る合理的な保証を提供するために設計された方針，手続，慣行および組織的構造。
IT コントロール目標	特定の IT アクティビティにおいてコントロール手続を実施することによって達成されるような，望まれる結果あるいは目的の表明。

フレームワークの原則

2つの異なった種類の現在利用できるコントロールモデル，つまり，「ビジネスコントロールモデル」(例，COSO)と「ITにより焦点をあてたコントロールモデル」(例，DTI)がある。COBITは，この2つのモデルの間にある隔たりを埋めることを狙っている。従って，COBITは，マネジメントにとってより包括的であり，情報システム管理者にとって技術標準より高いレベルで機能するものとして位置付けられる。**このように，COBITはIT統治にとってのモデルである！**

COBIT *フレームワーク*の根底に流れる概念は，ITにおけるコントロールとは，ビジネス目標や要件を支援するために必要とされる情報を検討し，次に，ITプロセスによって管理される必要があるIT関連資源の結合した適用結果の情報を検討することによってアプローチされるというものである。



ビジネス目標を満たすために，情報は，情報に対するビジネス要件としてCOBITが言及する特定の基準に準拠する必要がある。要件の一覧を作成するのに際し，COBITは，既存の周知の参照モデルに組み込まれた原則を結合している。

品 質 要 件	品質 コスト デリバリ
受託要件 (COSO レポート)	業務の有効性と効率性 情報の信頼性 法律と規制への準拠性
セキュリティ要件	機密性 インテグリティ 可用性

インテグリティ規準によっても大筋で捉えられる品質は，主にその「消極的」な側面（失敗のない，信頼性等）について考えられてきた。積極的であるが，しかし，品質のあまり定量化できない側面（スタイル，魅力，見栄えと感じ，期待以上の性能等）は，一時的にはITコントロール目標の視点から考慮されなかった。その前提は，第1のプライオリティは，機会を妨害するリスクを正確に管理するのに資するべきであることであった。品質の利用容易性の側面は，有効性の規準に含まれる。品質のデリバリ側面は，セキュリティ要件の可用性の側面，また，ある程度は，有効性と効率性とも重複していると考えられた。最後に，コストの側面も，また，効率性に含まれると考えられる。

受託要件に対して，COBITはその中枢部分を徹底的に作り直す試みはなかった－業務の有効性と効率性，情報の信頼性，法律と規制への遵守に対するCOSOの定義が使われた。しかし，情報の信頼性は，まさに財務情報

ではなく，あらゆる情報を含むように拡張された。

セキュリティ要件に関しては，COBITは主な要素として機密性，インテグリティ，可用性を識別した。そこに見られるこれらの同じ3つの要素は，ITセキュリティ要件を記述することにおいて，世界中で使われている。

より広範な品質，受託，セキュリティ要件から分析を開始すると，7つの明確で，しかしある程度は未だ幾分か重複するカテゴリーが抽出された。COBITで役立つ定義は，次に示される。

有 効 性	ビジネスプロセスに対し，目的適合性および関連性をもち，同時に適時に，正確に，一貫して利用可能な方法で伝達されるような情報を扱う。
効 率 性	資源の最適利用（最も生産的かつ経済的）による情報の提供に関連する。
機 密 性	未許可の開示からの機密情報の保護に関連する。
インテグリティ	情報の正確性と完全性，同様にビジネスの価値と期待に一致した情報の妥当性に関連する。
可 用 性	現在および将来のビジネスプロセスによって情報が要求された場合，利用できる状態にあることに関連する。また，必要な資源と関連能力の保全にも関連する。
準 拠 性	ビジネスプロセスが従わなければならない法律，規制，契約条項，つまり，外部的に課されたビジネス規準への準拠を扱う。
情報の信頼性	マネジメントが事業体を運営し，財務および準拠，報告責任を行うのに適切な情報の提供に関連する。

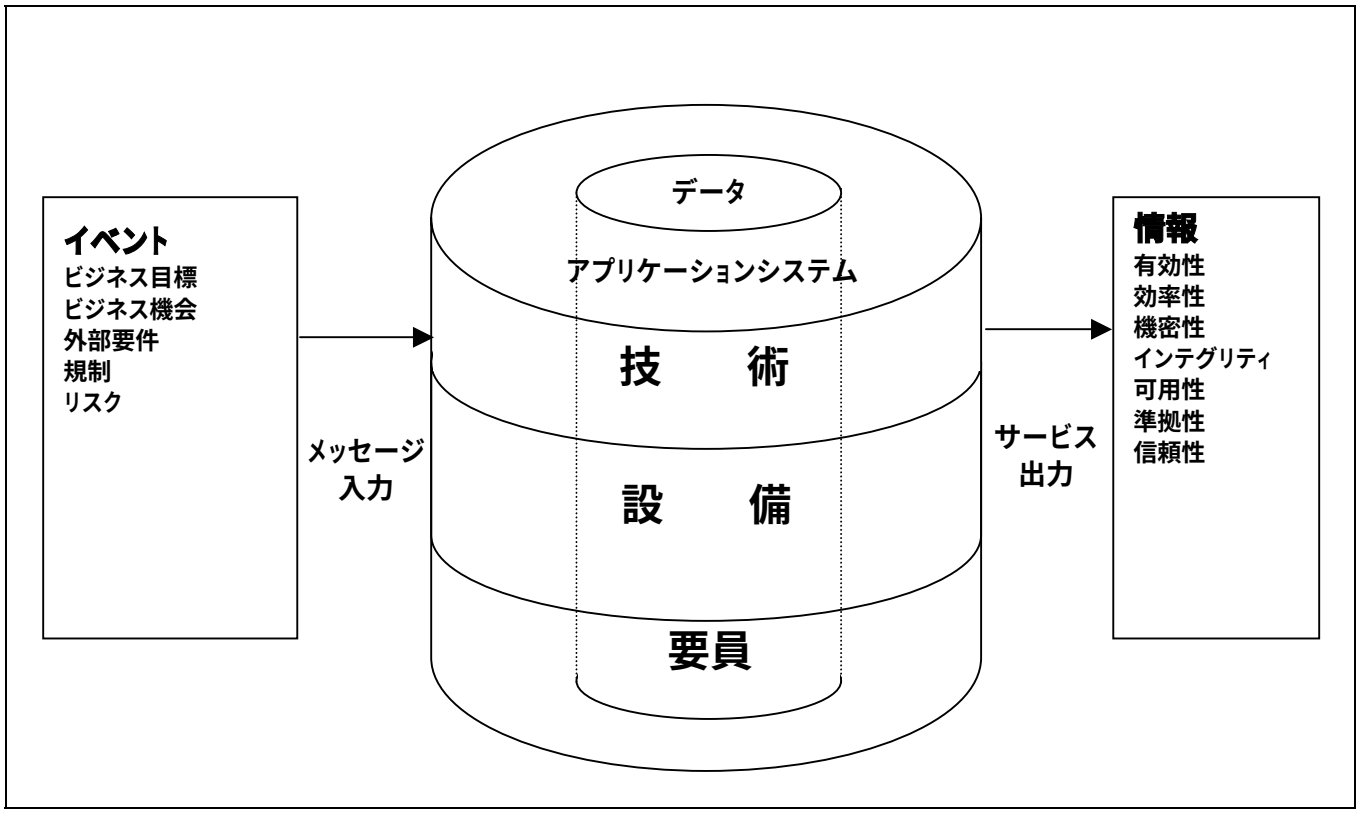
COBITで識別されるIT資源は，次のように説明･定義することができる。

データ	広義のデータオブジェクト（つまり，外部および内部），構造化された，および非構造化されたグラフィックス，音声等。
アプリケーションシステム	アプリケーションシステムは，手作業およびプログラム化された手続の総体として理解される。

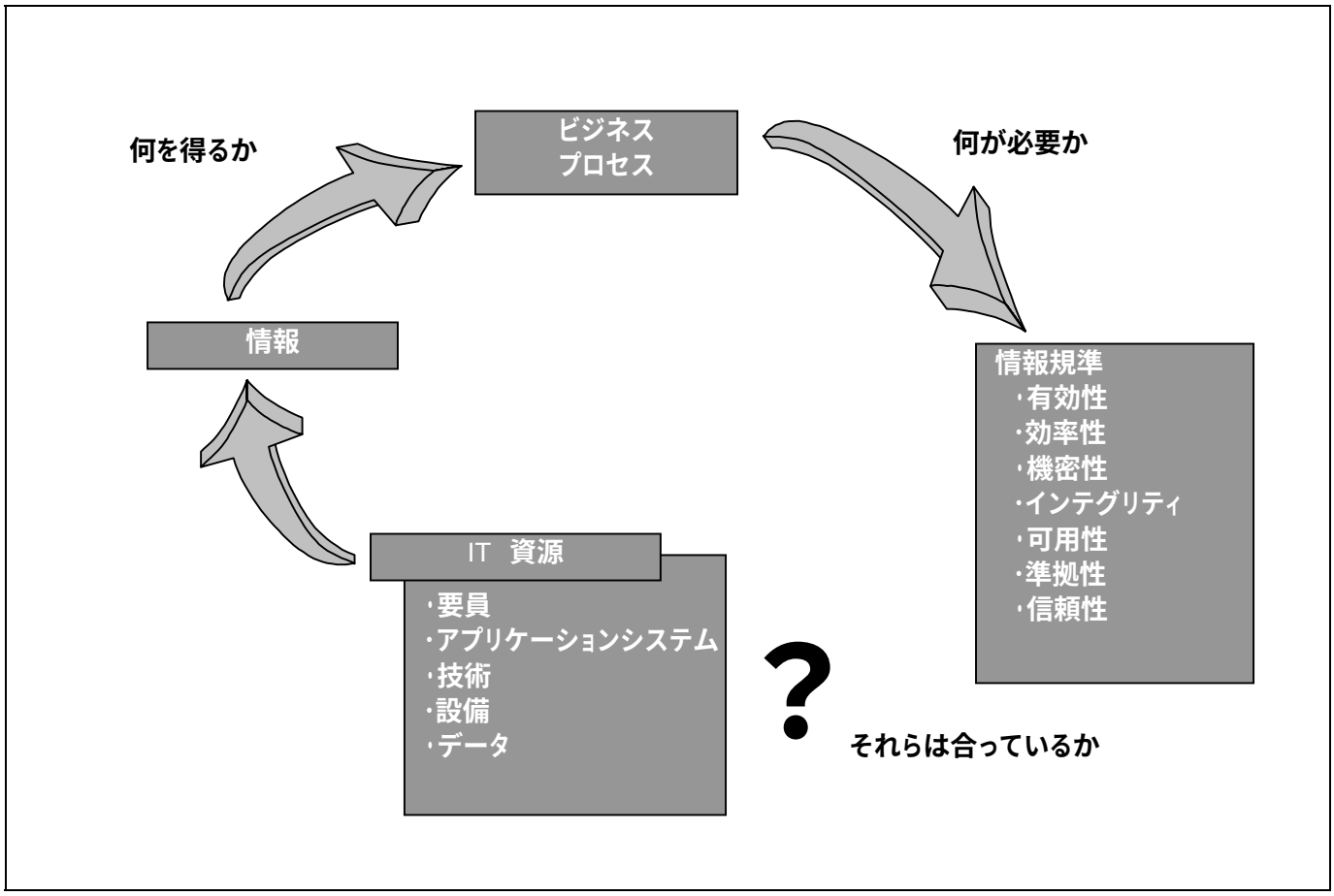
技術	技術は，ハードウェア，オペレーティングシステム，データベース管理システム，ネットワーク，マルチメディア等を網羅する。
設備	設備は，情報システムを収容し，支援する資源のすべてである。
要員	要員には，情報システムとそのサービスを計画し，組織化し，取得し，デリバリし，サポートし，モニタリングするためのスタッフ能力，意識および生産性を含む。

資金または資本は，上記の資源への投資であると考えることができるため，コントロール目標の分類ではIT資源としては認識されなかった。*フレームワーク*はまた，特定のITプロセスに関連するすべての重要文書を特に参照することはない。良き慣行では，文書化は良好なコントロールの本質であると考えられ，従って，文書化の欠如は，更なるレビューとレビュー中の何等かの特定領域における補完的なコントロールの分析を行う原因となるであろう。

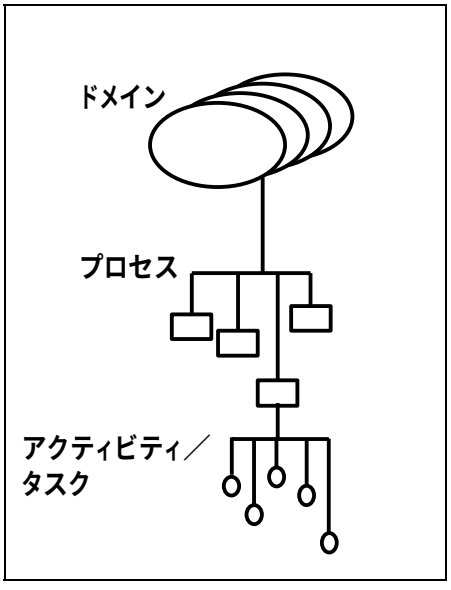
サービスのデリバリに対するIT資源の関係を眺める他の方法は，以下のように描かれる。



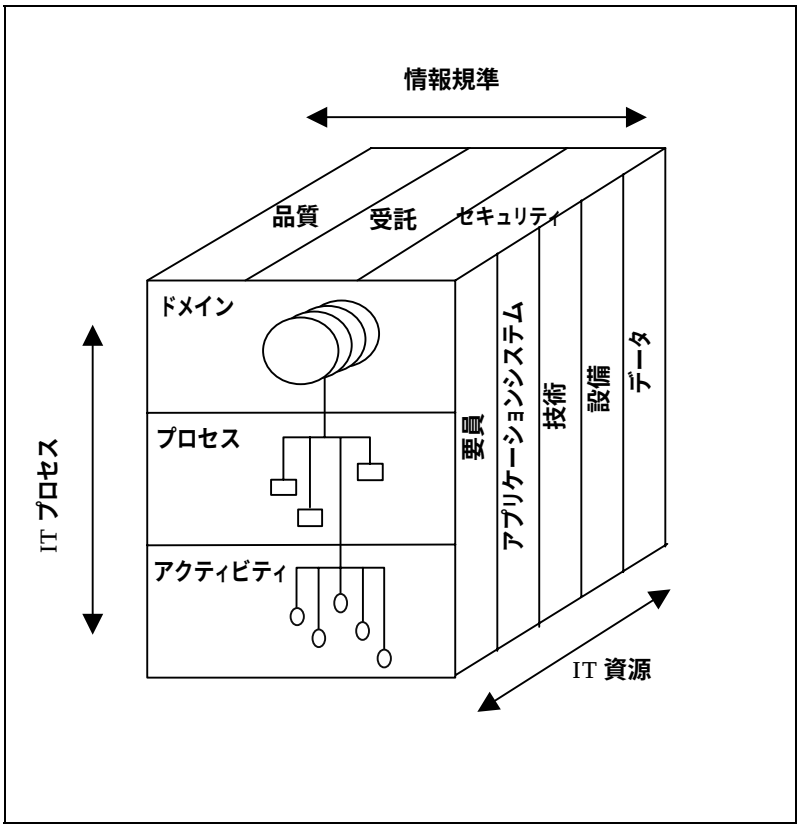
情報に対するビジネス要件が満たされていることを保証するために，これらの資源について適切なコントロール対策が明示され，実施され，モニターされる必要がある。その際，組織が入手する情報が必要とする特徴を具備していることを満足し得るであろうか。これが，ITコントロール目標の健全なフレームワークが必要とされる根拠である。次の図がこの概念を示す。



COBIT *フレームワーク*は，高いレベルのコントロール目標，およびそれらの分類に関する全般的な構造から構成される。その分類方法の基礎にある理論は，IT資源の管理を考える際，IT活動には本質的に3つのレベルがあるというものである。下のレベルから始めると，測定可能な結果を達成するのに必要なアクティビティとタスクがある。タスクがより明確に区別されているのに対し，アクティビティはライフサイクルの概念を持つ。ライフサイクル概念は，典型的なコントロール要件を有し，明確に区別されたアクティビティとは異なる。プロセスとは，自然な（コントロール）切れ目を持つ一連の結合されたアクティビティまたはタスクであり，一つ上の階層として定義される。最も高いレベルでは，プロセスは自然にドメインにグループ化される。これらの自然なグルーピングは，しばしば組織構造における責任ドメインとして確認され，マネジメントサイクルまたはITプロセスに適用できるライフサイクルに沿っている。



このように，概念的なフレームワークは 3 つの視点，つまり，(1)情報規準，(2)IT 資源，(3)IT プロセスからアプローチできる。例えば，管理者は，（7つの明確な情報規準として*フレームワーク*に含まれている）品質，受託，あるいはセキュリティの関心から見たいかもしれない。一方，,IT 管理者は，報告責任がある IT 資源を考慮したいかもしれない。プロセスオーナー，IT 専門家，ユーザは特定のプロセス，あるいはアクティビティ／タスクに特別な関心を持つかもしれない。監査人は，コントロールの適用範囲の見地から*フレームワーク*にアプローチしたいかもしれない。これらの 3 つの視点は，COBIT キューブにおいて描かれる。



フレームワークとして上に述べたこととともに，ドメインは，監査人の専門用語ではなく，組織における日々の活動の中で管理者が使う言葉を使うことで識別される。このように，4つの主要なドメインは，計画と組織，取得と実施，デリバリとサポート，モニタリングとして識別される。

高いレベルの分類のために識別された4つのドメインの定義は，次の通りである。

計画と組織

このドメインは，戦略および戦術を包含し，ITがビジネス目標の達成に最も貢献できる方法の識別に関連する。さらに，戦略的ビジョンの実現が計画され，伝達され，異なった視点から管理される必要がある。最後に，技術的基盤と同様，適切な組織が構築されなければならない。

取得と実施

IT戦略を実現するために，ITソリューションが識別され，開発または取得されると同様に実施され，ビジネスプロセスに統合化される必要がある。さらに，ライフサイクルが既存システムに対して継続されることを確かめるために，それらのシステムの変更および保守もこのドメインに入る。

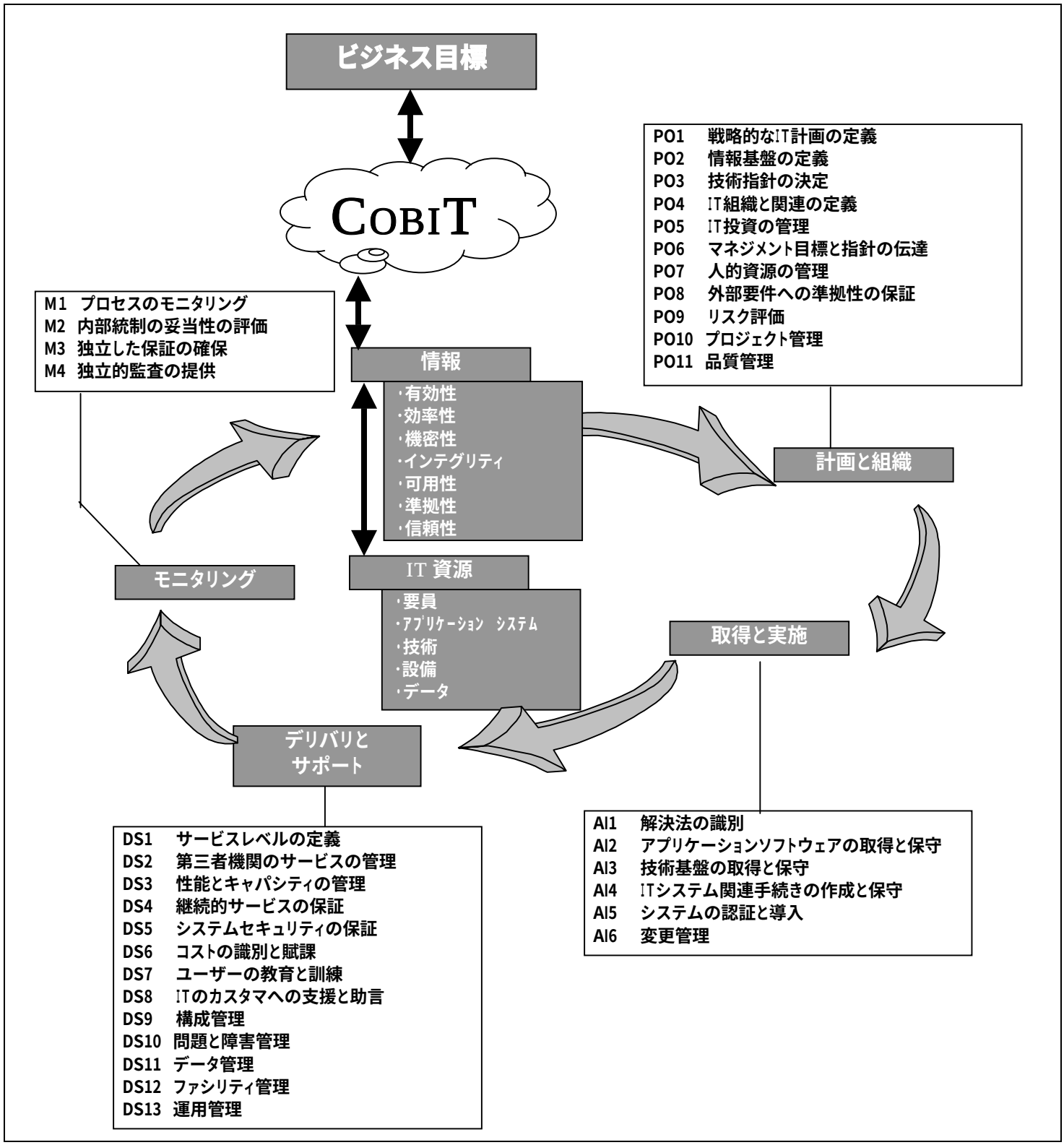
デリバリとサポート

このドメインでは，要求されたサービスの実際のデリバリに関連があり，それはセキュリティおよび継続的側面における伝統的な運用から教育までの範囲にわたる。これらのサービスを提供するために，必要なサポートプロセスが設定されなければならない。*このドメインは，しばしばアプリケーションコントロールのもとに分類され，アプリケーションシステムによるデータの実際の処理を含んでいる。*

モニタリング

すべてのITプロセスは，それらプロセスの品質とコントロール要件への準拠性について，常に定期的に評価する必要がある。このように，このドメインは組織のコントロールプロセス，内部および外部監査によって提供されるか，代替資源から得られる独立した保証に対する経営者の監視を扱う。

要約すると，組織がその目標を達成するのに必要な情報を提供するために，自然にグループ化されたプロセスによって，IT資源が管理されることが必要であるということである。
次の図がこの概念を示す。



これらのプロセスは，組織内の異なったレベルで適用することができることを注意すべきである。例えば，これらのプロセスのいくつかは，企業レベルで適用され，その他は情報サービス機能レベル，ビジネスプロセスオーナーレベルなどで適用される。

ビジネス要件に関する解決法を計画し，またはデリバリするプロセスの有効性の基準は，時々，可用性，インテグリティ，機密性の規準を網羅するであろうことにもまた，注意すべきである。実際，それらがビジネス要件となる。例えば，“解決法を識別する”というプロセスは，可用性，インテグリティおよび機密性の要件を提供する場合，効果的でなければならない。

必ずしもすべてのコントロール対策が同じ程度に情報に対する異なったビジネス要件を満足するとは限らないことは，明らかである。

- **第一次的**　定義されたコントロール目標が関心のある情報要件を完全に満たす程度。
- **第二次的**　定義されたコントロール目標が関心のある情報要件に一定の範囲だけ，または間接的に満たす程度。
- **空　白**　適用の可能性があるが，しかし，要件は，このプロセスにおける他の基準によって，または他のプロセスによって，より適切に満足される。

同様に，すべてのコントロール基準は，異なったIT資源に同じ程度の影響を与える必要はないであろう。それゆえに，COBIT *フレームワーク*は，プロセスに単に貢献しない考慮中のプロセスによって，明確に管理されるIT資源の適用性を明確に示している。この分類は，研究者，専門家，校閲者からの入力を，前述に示された厳密な定義を使って，同じ厳密なプロセスに基づくCOBIT *フレームワーク*の中でなされる。

要約表

次のチャートは，ITプロセスとドメイン，高いレベルのコントロール目標によって影響上を受ける情報規準の表示を提供し，同様に，IT資源が適用可能な表示を提供する。

			情報規準							IT 資源				
ドメイン		プロセス	効率性	有効性	機密性	インテグリティ	可用性	準拠性	信頼性	要員	アプリケーション	技術	設備	データ
計画と組織	PO1	戦略的な IT 計画の定義	P	S						✓	✓	✓	✓	✓
	PO2	情報基盤の定義	P	S	S	S					✓			✓
	PO3	技術指針の決定	P	S								✓	✓	
	PO4	IT 組織と関連の定義	P	S						✓				
	PO5	IT 投資の管理	P	P					S	✓	✓	✓	✓	
	PO6	マネジメント目標と指針の伝達	P					S		✓				
	PO7	人的資源の管理	P	P						✓				
	PO8	外部要件への準拠性の保証	P					P	S	✓	✓			✓
	PO9	リスク評価	S	S	P	P	P	S	S	✓	✓	✓	✓	✓
	PO10	プロジェクト管理	P	P						✓	✓	✓	✓	
	PO11	品質管理	P	P		P			S	✓	✓			
取得と実施	AI1	解決法の識別	P	S							✓	✓	✓	
	AI2	ｱﾌﾟﾘｹｰｼｮﾝｿﾌﾄｳｪｱの取得と保守	P	P		S		S	S		✓			
	AI3	技術基盤の取得と保守	P	P		S						✓		
	AI4	IT システム関連手続の作成と保守	P	P		S		S	S	✓	✓	✓	✓	
	AI5	システムの認証と導入	P			S	S			✓	✓	✓	✓	✓
	AI6	変更管理	P	P		P	P		S	✓	✓	✓	✓	✓
デリバリとサポート	DS1	サービスレベルの定義	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	DS2	第三者機関のサービスの管理	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	DS3	性能とキャパシティの管理	P	P			S				✓	✓	✓	
	DS4	継続的サービスの保証	P	S			P			✓	✓	✓	✓	✓
	DS5	システムセキュリティの保証			P	P	S	S	S	✓	✓	✓	✓	✓
	DS6	コストの識別と賦課		P					P	✓	✓	✓	✓	✓
	DS7	ユーザの教育と訓練	P	S						✓				
	DS8	IT のカスタマへの支援と助言	P							✓	✓			
	DS9	構成管理	P				S		S		✓	✓	✓	
	DS10	問題と障害管理	P	P			S			✓	✓	✓	✓	✓
	DS11	データ管理				P			P					✓
	DS12	ファシリティ管理				P	P						✓	
	DS13	運用管理	P	P		S	S			✓	✓		✓	✓
モニタリング	M1	プロセスのモニタリング	P	S	S	S	S	S	S	✓	✓	✓	✓	✓
	M2	内部統制の妥当性の評価	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	M3	独立した保証の確保	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	M4	独立的監査の提供	P	P	S	S	S	S	S	✓	✓	✓	✓	✓

Information Systems Audit and Control Association

A Single International Source for Information Technology Controls

The Information Systems Audit and Control Association is a leading global professional organisation representing individuals in more than 100 countries and comprising all levels of information technology; executive, senior management, middle management and practitioner. The Association is uniquely positioned to fulfill the role of a central, harmonising source of IT control practice standards for the world over. Its strategic alliances with other groups in the financial, accounting, auditing and IT professions are ensuring an unparalleled level of integration and commitment by business process owners.

Association Programmes and Services

The Association's services and programmes have earned distinction by establishing the highest levels of excellence in certification, standards, professional education and technical publishing.

- Its certification programme (the Certified Information Systems Auditor) is the only global designation throughout the IT audit and control community.
- Its standards activities establish the quality baseline by which other IT audit and control activities are measured.
- Its professional education programme offers technical and management conferences on five continents, as well as seminars worldwide to help professionals everywhere receive high-quality continuing education.
- Its technical publishing area provides references and professional development materials to augment its distinguished selection of programmes and services.

The Information Systems Audit and Control Association was formed in 1969 to meet the unique, diverse and high technology needs of the burgeoning IT field. In an industry in which progress is measured in nano-seconds, ISACA has moved with agility and speed to bridge the needs of the international business community and the IT controls profession.

For More Information

To receive additional information, you may telephone (+1.847.253.1545), send e-mail (research@isaca.org) or visit our web page (www.isaca.org).