ITGI Japan

GOVERNANCE INSTITUTE

COBITを活用した全般統制へのアプローチ

～日立グループでの取組みを踏まえて

2007.6.20

株式会社 日立コンサルティング

高浦　孝次

要旨

COBIT for SOXはチェックリストとして活用できる

- ただし、項目内容を十分に理解し、項目数を絞り込む努力が大切

リスクアプローチで活用するには、COBITも参照すべき

- COBITも活用して、ITプロセスの内容と、財務諸表の信頼性に係るリスクを大局的に把握する

中期的な効率化にはIT管理項目の体系化が肝要

- 内部統制への対応だけでなく、IT業務で求められるさまざまな観点を整理していく上で、COBITが有用

参照資料について

COBIT for SOX

- 原題　　“IT Control Objectives for Sarbanes-Oxley”
- 日本語訳「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」
- ITGI（IT Governance Institute）が著作権を有しています
- 発表の中では、便宜上“**COBIT for SOX**”と略記

ITGI Japan

GOVERNANCE INSTITUTE

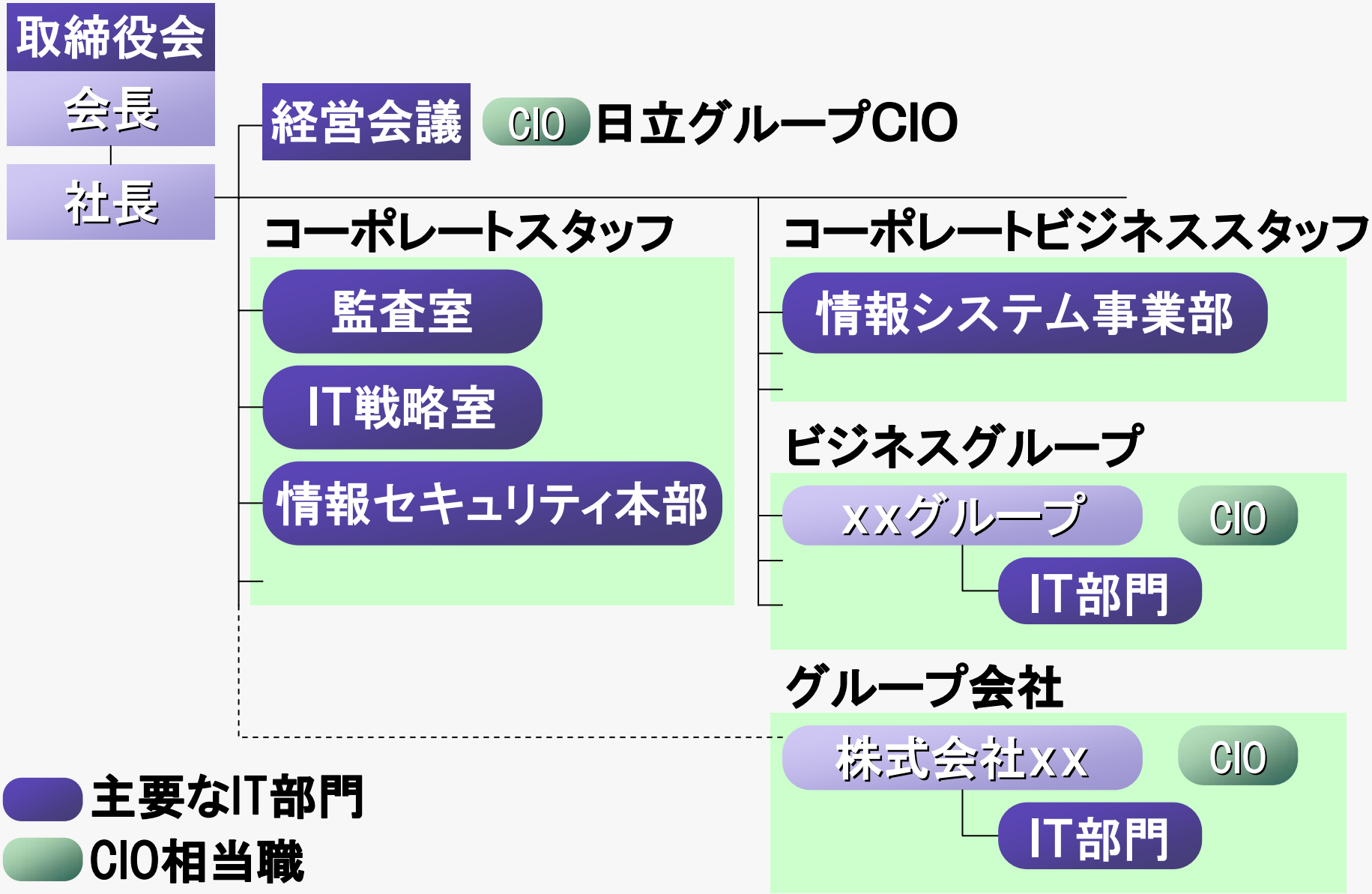
目次

日立グループの概要

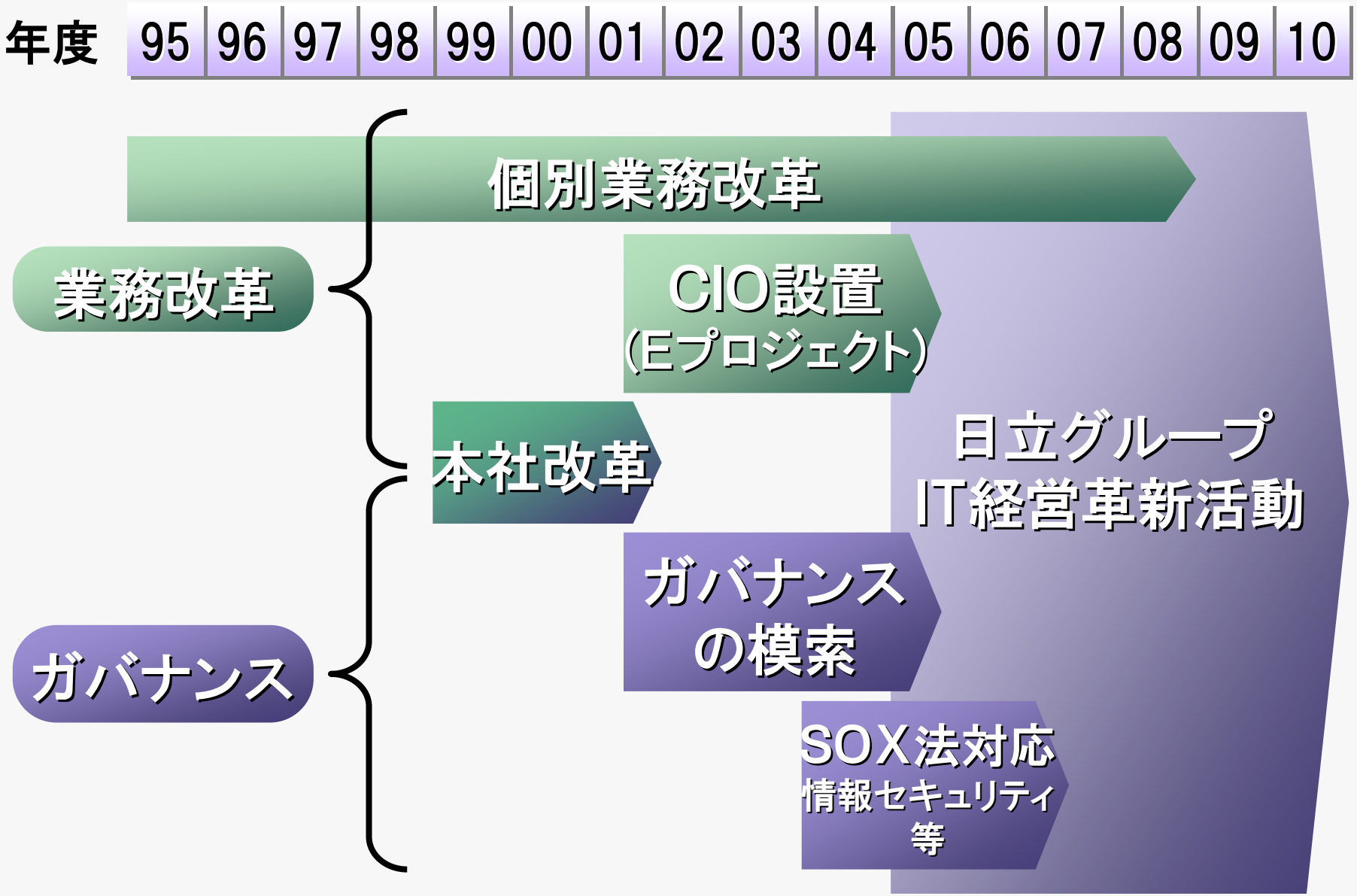
連結従業員数	35万5千人
連結子会社数	932社（日立製作所含む、国内 476社、海外456社）

（2006年3月期）

日立グループのIT組織と管理規模



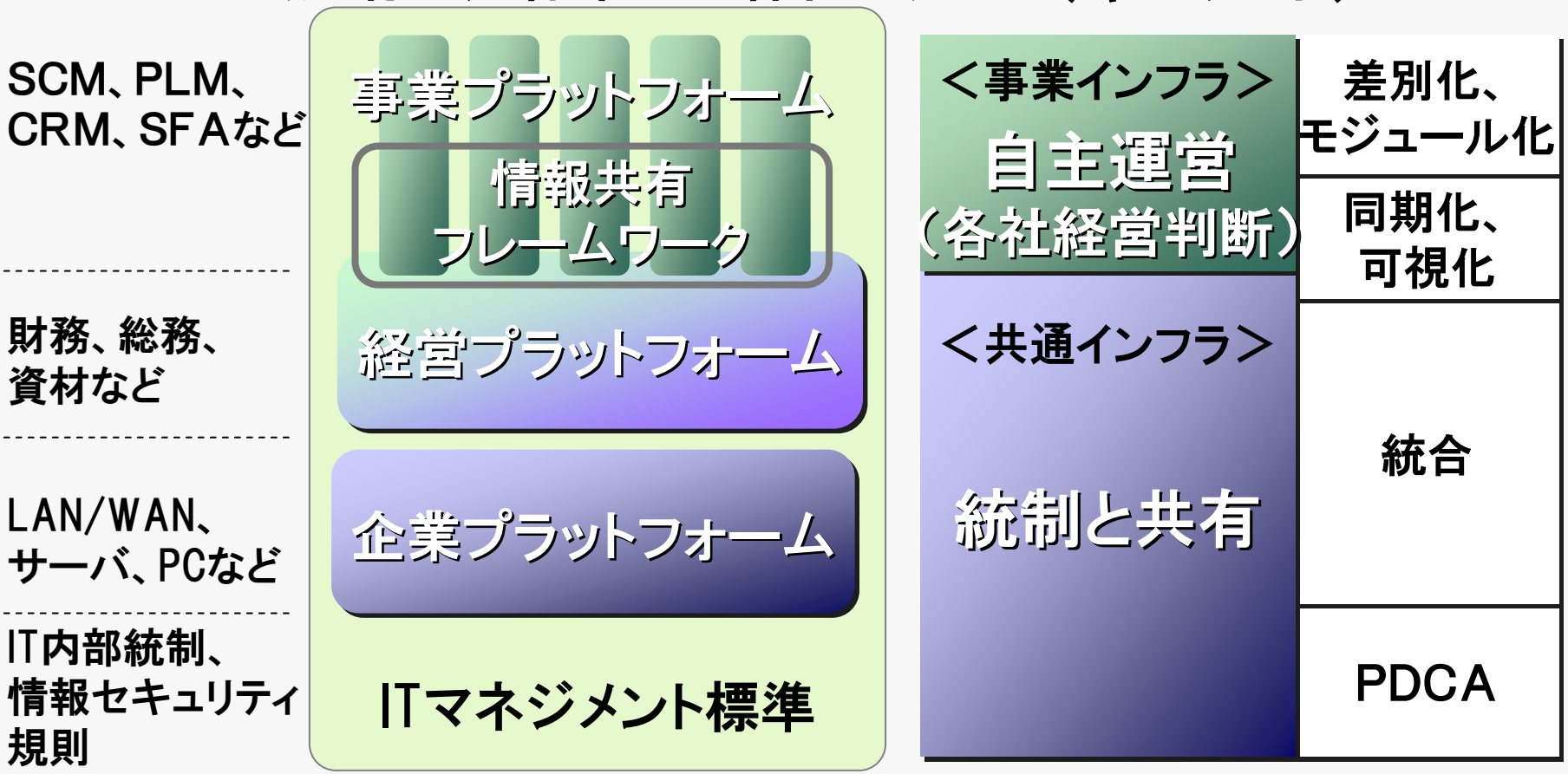
IT経営革新活動の経緯



ITガバナンスへの取組み

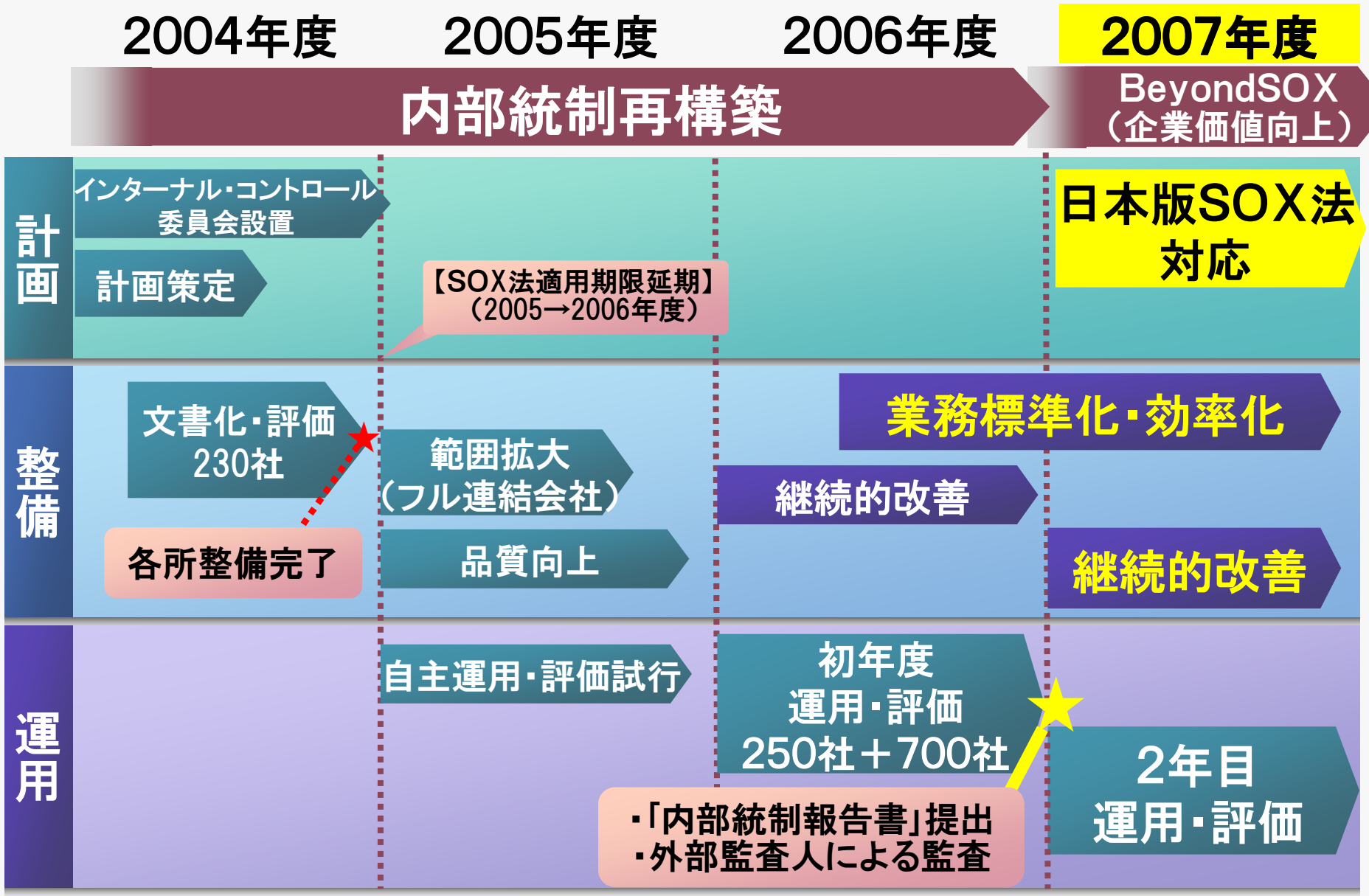
項目	主な取組み
連結企業グループとしてのITガバナンス体制	・日立グループCIO体制の確立
基本アーキテクチャ	・ガバナンスモデル確立 ・技術標準制定
IT業務標準	・関連規則制定 ・自己監査励行、支援 ・ITマネジメントの体系化
IT共通業務	・共通業務集約の加速

日立ITガバナンスモデル

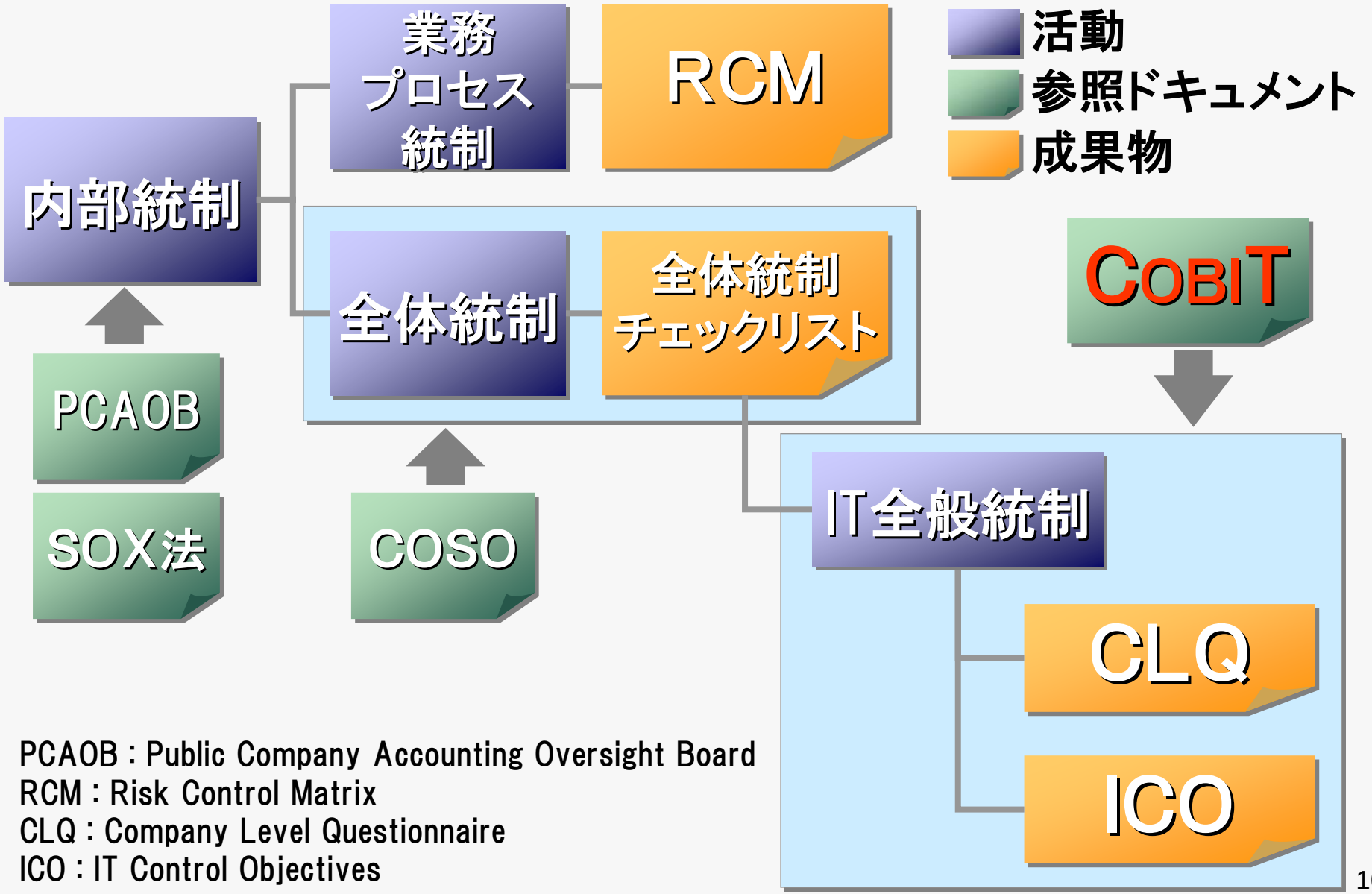


矛盾解消と成長のアーキテクチャー

SOX法対応のスケジュール



内部統制実務のフレームワーク



PCAOB : Public Company Accounting Oversight Board
RCM : Risk Control Matrix
CLQ : Company Level Questionnaire
ICO : IT Control Objectives

ITGI Japan

Make Japanese IT Governance practices

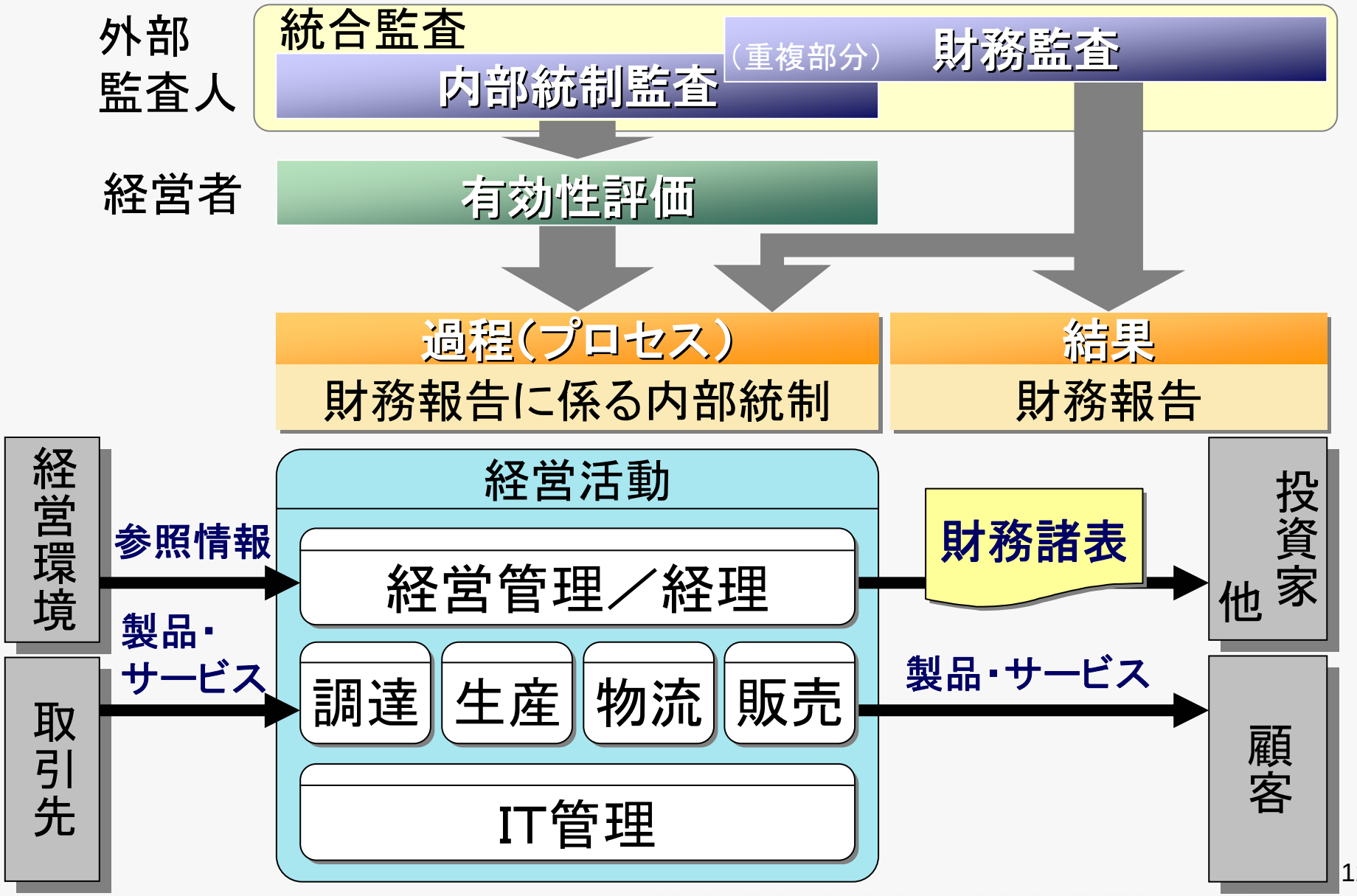
GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

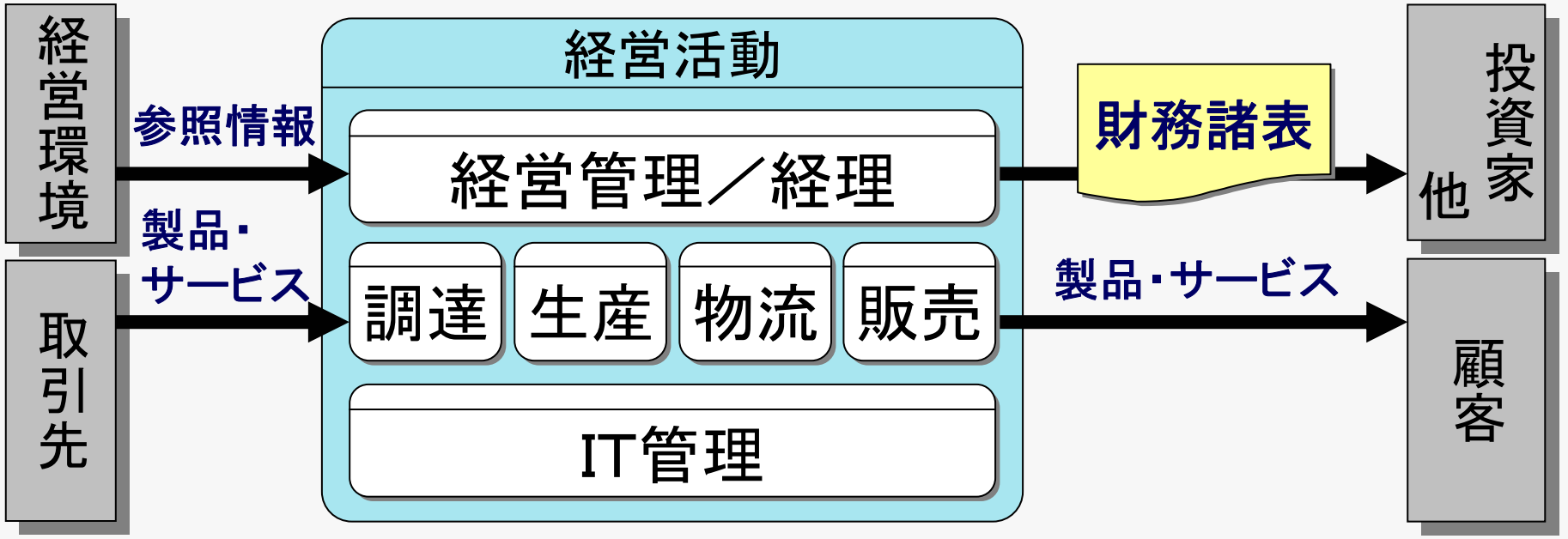
目次

1. 日立グループにおける内部統制整備
2. IT統制の枠組み
3. 全般統制への2つのアプローチ
4. COBITが提供するもの
5. 全般統制の対象となるIT業務
6. ITマネジメントの体系化

経営における内部統制評価の位置付け



経営活動全体としてのプロセス重視

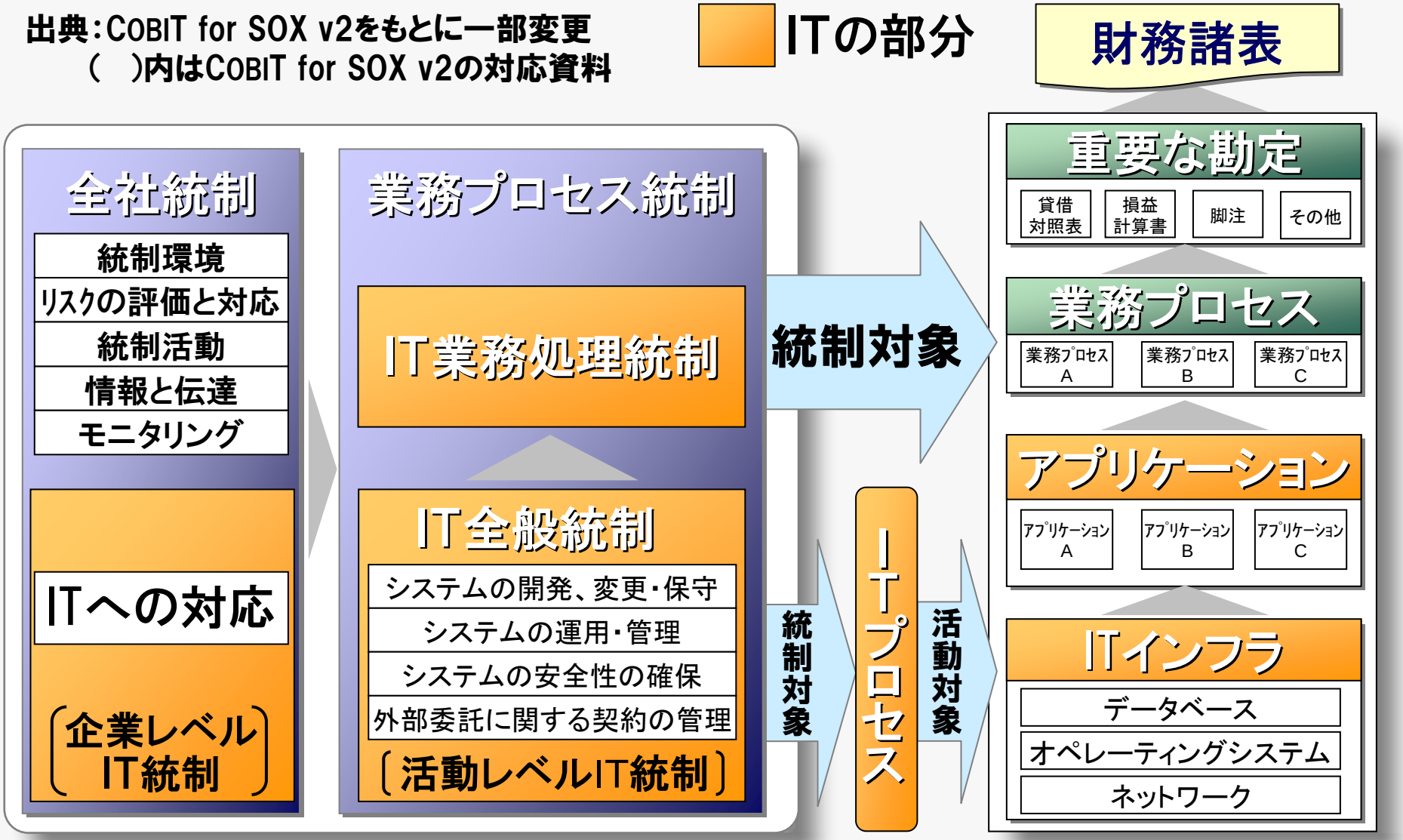


過程（プロセス）	結果
経営活動	業績／顧客満足
（今後）	（従来）
提供のためのプロセスそのものの質を高める取組みを重視	結果としての製品・サービスのQ・C・Dや業績の管理が中心

内部統制の枠組み

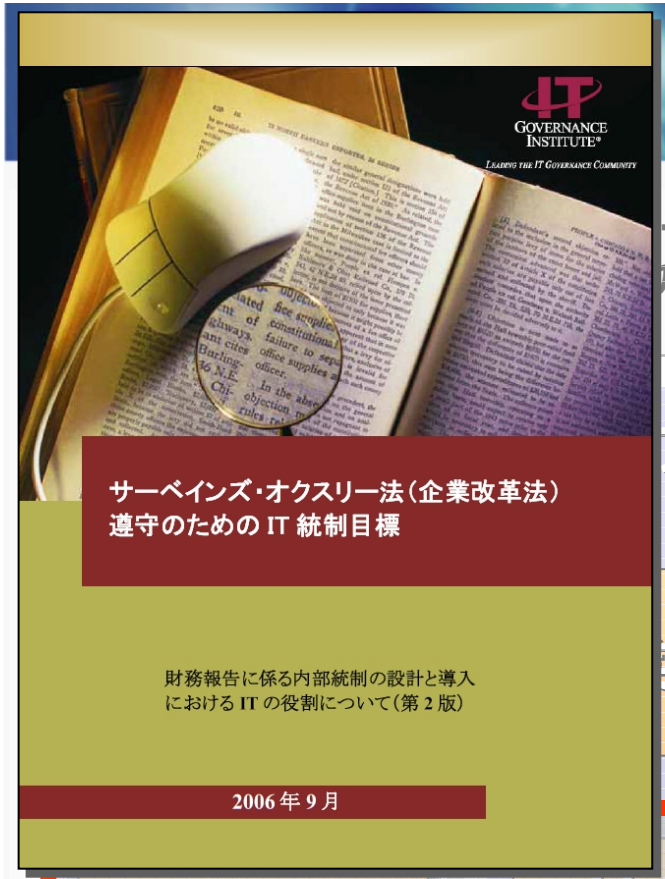
出典：COBIT for SOX v2をもとに一部変更
（　）内はCOBIT for SOX v2の対応資料

ITの部分



内部統制の枠組み　　業務とITの構造

内部統制の枠組み



一部変更
の対応資料

ITの部分

財務諸表

プロセス統制

務処理統制

統制対象

重要な勘定
- 貸借対照表
- 損益計算書
- 脚注
- その他

業務プロセス
- 業務プロセス A
- 業務プロセス B
- 業務プロセス C

アプリケーション
- アプリケーション A
- アプリケーション B
- アプリケーション C

ITインフラ
- データベース
- オペレーティングシステム
- ネットワーク

IT全般統制
システムの運用・管理
システムの安全性の確保
外部委託に関する契約の管理
〔活動レベルIT統制〕

〔企業レベル IT統制〕

プロセス統制

活動対象

ITに係わる内部統制の枠組み

COBIT for SOX

内部統制の枠組み

業務とITの構造

ITGI Japan

Make Japanese IT Governance practice

GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

目次

1．全般統制へのベースラインプローチ

ステップ	説明	成果物
(1)ITプロセスの特定	どのITプロセスを文書化すべきかを決定	―
(2)評価チェックシート作成	ベースラインとなるチェックシートや評価基準を作成	評価チェックシート
(3)各項目の評価	○×式や成熟度などの段階評価によって有効性を評価	評価チェックシート（評価実施後）

(出典)「これならできるIT統制」船城謙二郎・高浦孝次

2. 全般統制へのリスクアプローチ

ステップ	説明	成果物
(1)ITプロセスの特定	どのITプロセスを文書化すべきかを決定	―
(2)各ITプロセスの理解	特定されたITプロセスの手続を可視化	ITプロセスモデル（フローチャートなど）
(3)リスクの特定	業務処理統制との関連からITプロセスにおけるリスクを特定	リスクコントロールマトリクス
(4)統制の識別	特定されたリスクに対応するITプロセスにおける統制を識別	

(出典)「これならできるIT統制」

2つのアプローチの特徴

	ベースラインアプローチ	リスクアプローチ
前提条件	適切なチェック項目と評価基準が設定されていること	ITプロセスが理解されていること
メリット	・チェックシート形式による大量展開が可能 →子会社が多い場合に有効	・論理的で、監査人への説明が容易 ・会社に最適なスコープで実施できる
デメリット	・スコープが広くなりがち ・評価の際に、論理的な説明が難しい	・大量展開が難しい
成果物	評価チェックシート等	ITプロセスのRCM等

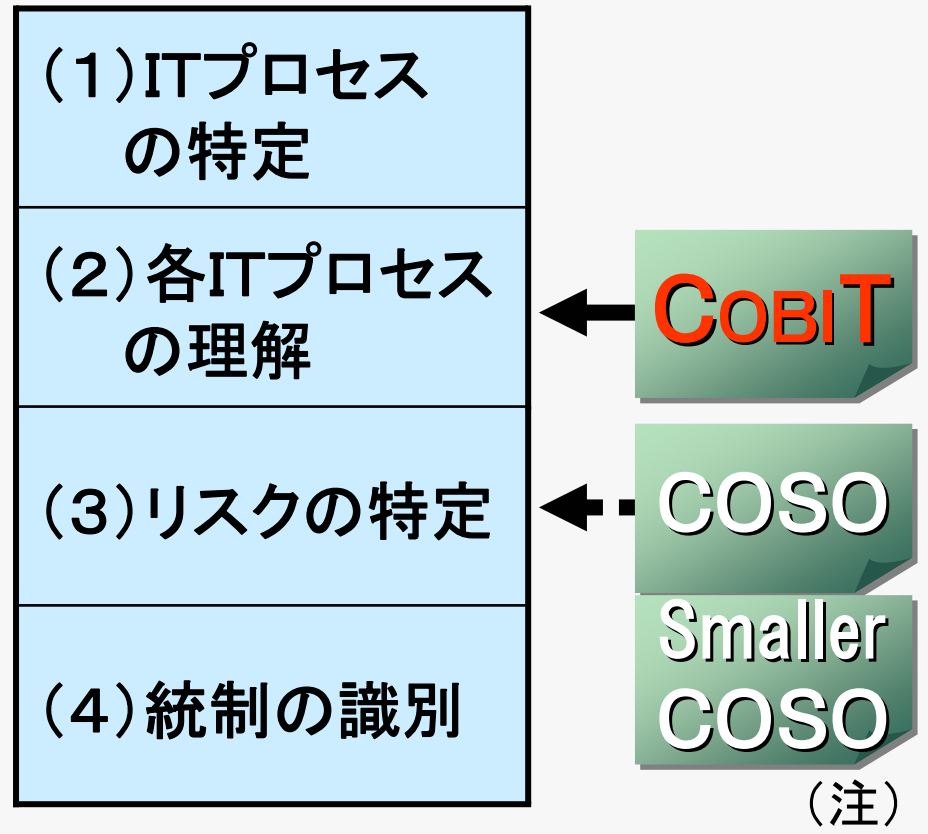
（出典）「これならできるIT統制」

CobiT for SOXをどう使うか？

CobiT for SOXの参考資料C

変更管理（AI6、AI7）	
統制目標	
根拠理由	
統制の例	統制のテストの例

リスクアプローチの作業手順



（注）「財務報告に係る内部統制
——比較的小規模な企業のための指針」
COSOが2006年7月に発行した資料

ITGI Japan

Make Japanese IT Governance practices

GOVERNANCE INSTITUTE

目次

COBITが示しているITプロセス

計画と組織

PO1　IT戦略計画の策定
PO2　情報アーキテクチャの定義
PO3　技術指針の決定
PO4　ITプロセスと組織およびそのかかわりの定義
PO5　IT投資の管理
PO6　マネジメントの意図と指針の周知
PO7　IT人材の管理
PO8　品質管理
PO9　ITリスクの評価と管理
PO10　プロジェクト管理

調達と導入

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保守
AI3　技術インフラストラクチャの調達と保守
AI4　運用と利用の促進
AI5　IT資源の調達
AI6　変更管理
AI7　ソリューションおよびその変更の導入と認定

モニタリングと評価

ME1　IT成果のモニタリングと評価
ME2　内部統制のモニタリングと評価
ME3　規制に対するコンプライアンスの保証
ME4　ITガバナンスの提供

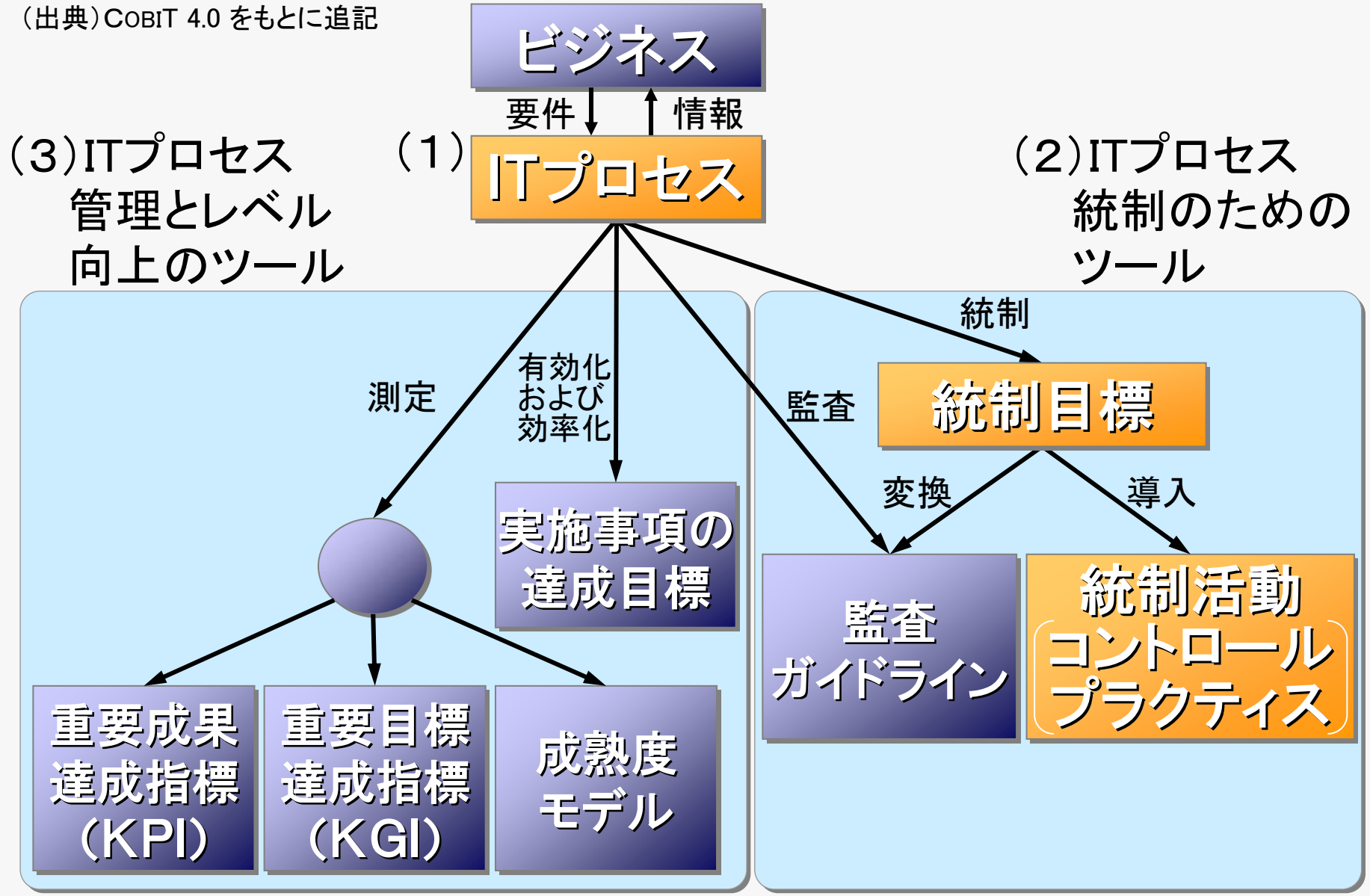
サービス提供とサポート

DS1　サービスレベルの定義と管理
DS2　サードパーティーのサービスの管理
DS3　性能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　費用の捕捉と配賦
DS7　利用者の教育と研修
DS8　サービスデスクとインシデントの管理
DS9　構成管理
DS10　問題管理
DS11　データ管理
DS12　物理的環境の管理
DS13　オペレーション管理

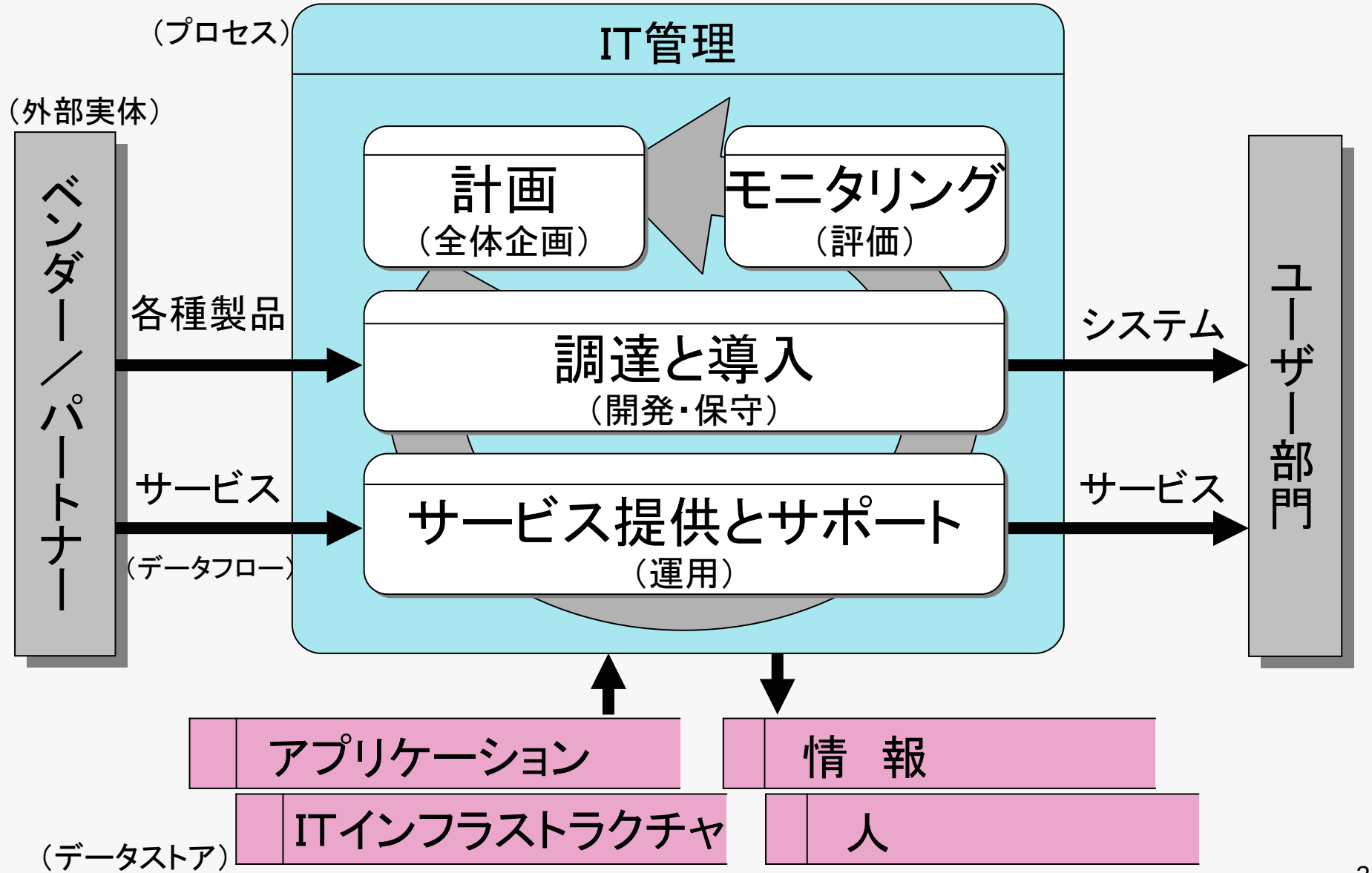
（出典）COBIT 4.0

COBIT構成要素の相互関係

（出典）COBIT 4.0 をもとに追記

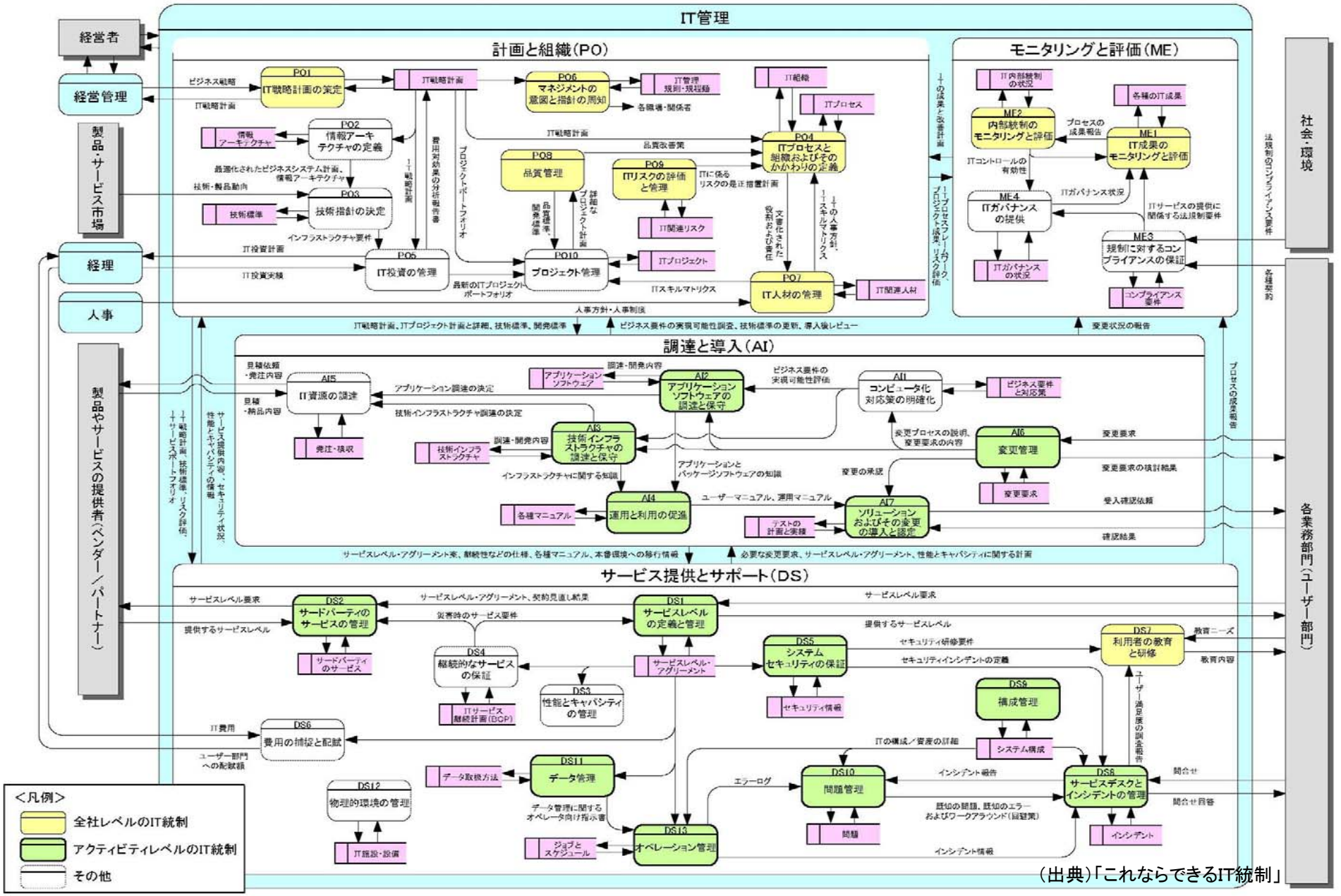


IT業務の概略モデル



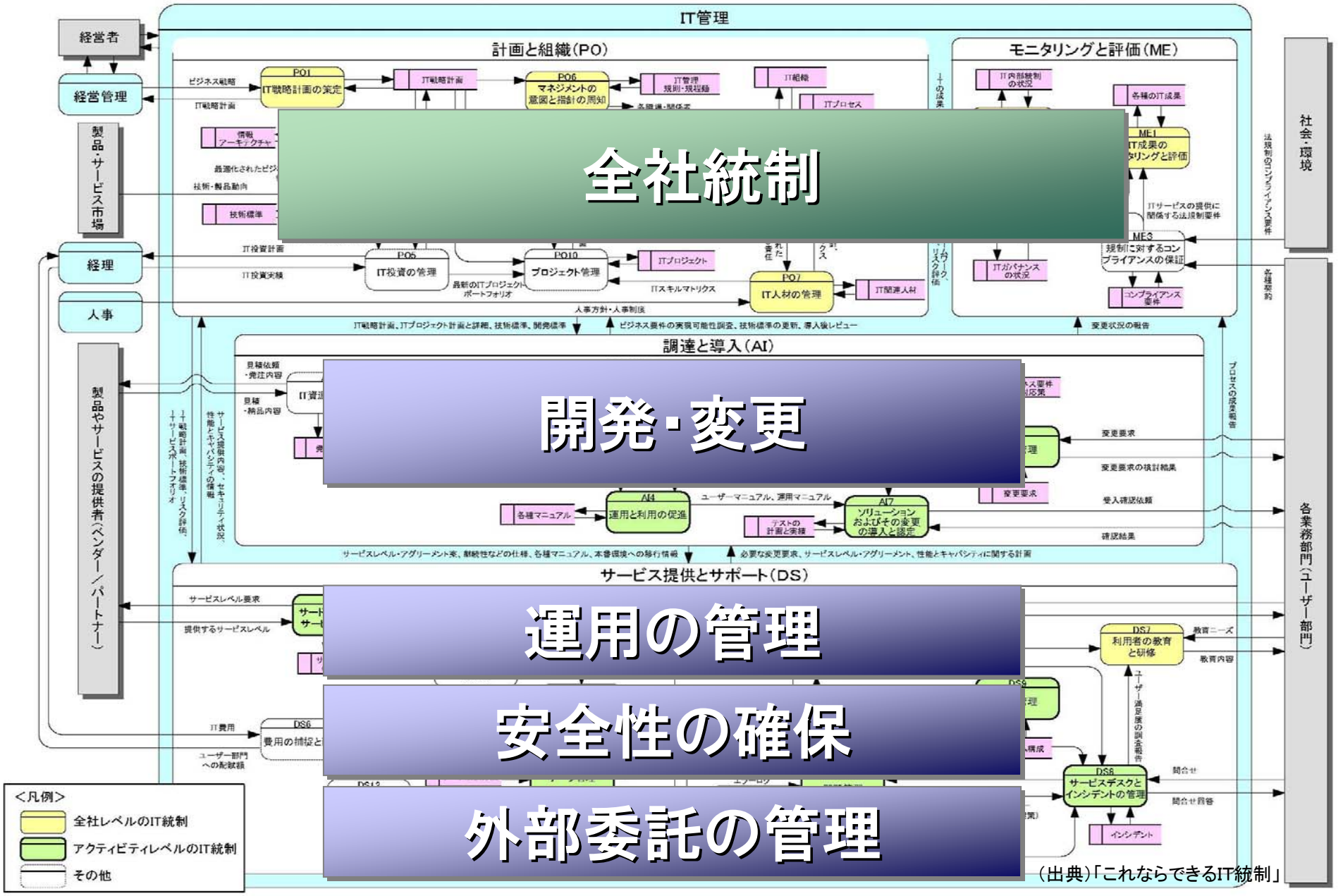
（出典）「これならできるIT統制」

CobiT4.0によるIT業務全体図



（出典）「これならできるIT統制」

CobiTドメインとIT統制の位置付け



(出典)「これならできるIT統制」

COBITを活用するメリットと難しさ

特徴

- ITプロセス（参照モデル）をベースにしている
  →コミュニケーションツールとして優れた特性

メリット

- 充実した資料を提供している（多くは無償）
- グローバルに認知されている
- 内部統制にとどまらず、IT業務のレベル向上に活用できる

難しさ

- 活用の用途が広く、何に使うかがわかりにくい
- ITプロセスの内容を理解しないと使いこなせない
  一方で、プロセス名が（翻訳のためもあり）なじみにくい
- サービス提供の考え方にもとづいている
  例：（開発）（保守＋運用）→（開発＋変更）（サービス提供）

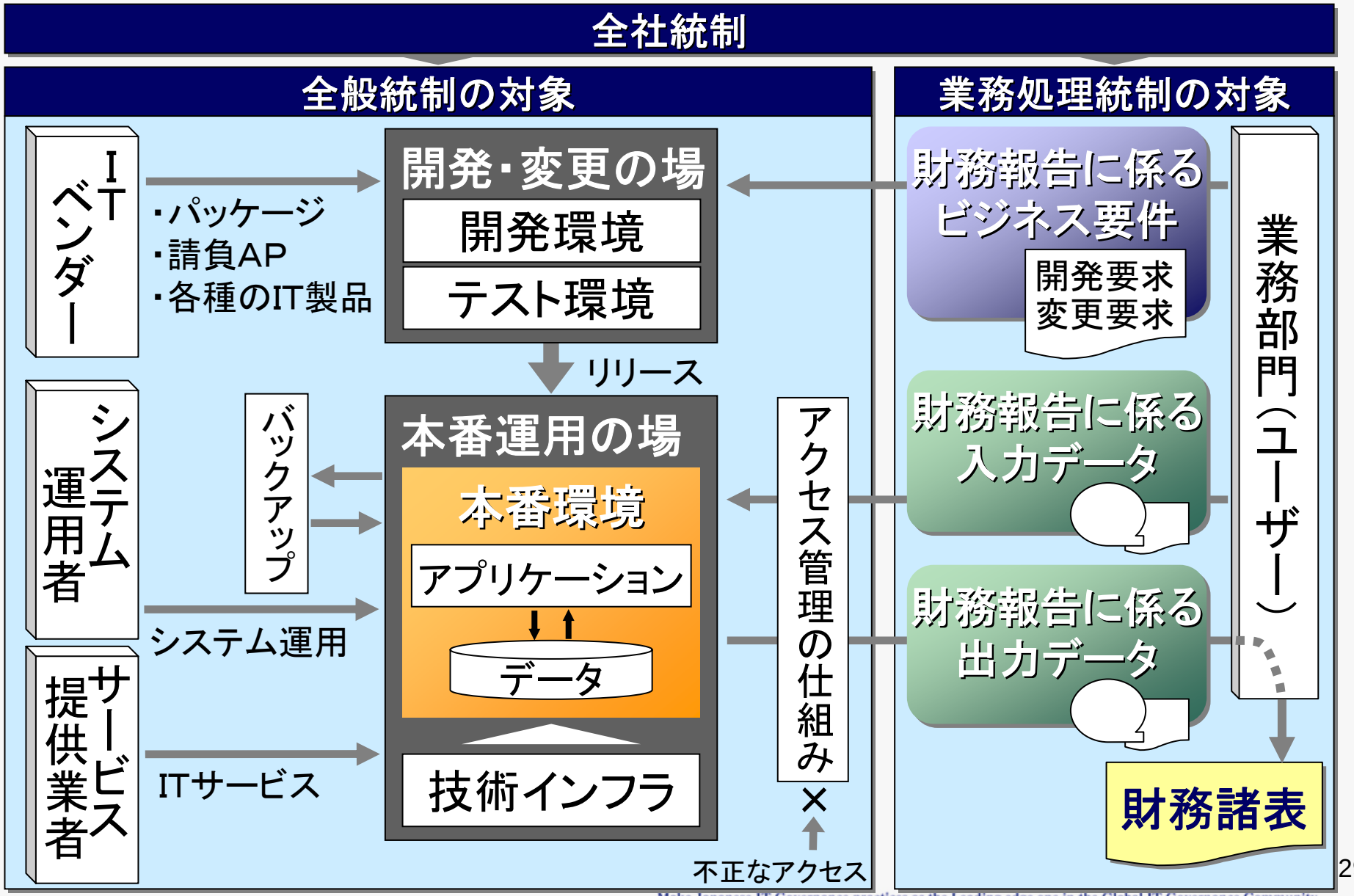
ITGI Japan

Make Japanese IT Governance practice

GOVERNANCE INSTITUTE

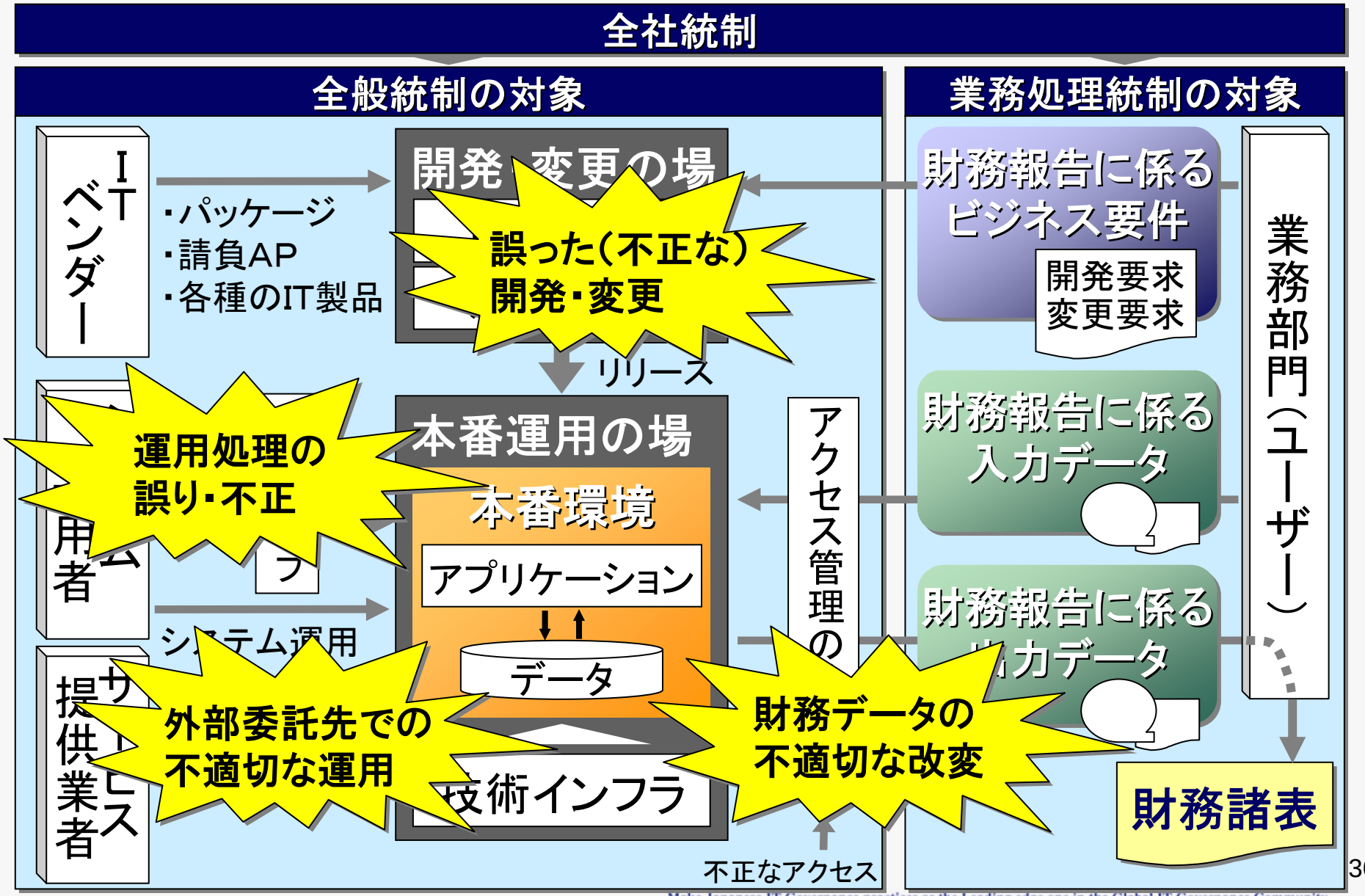
目次

全般統制の対象となるIT業務活動



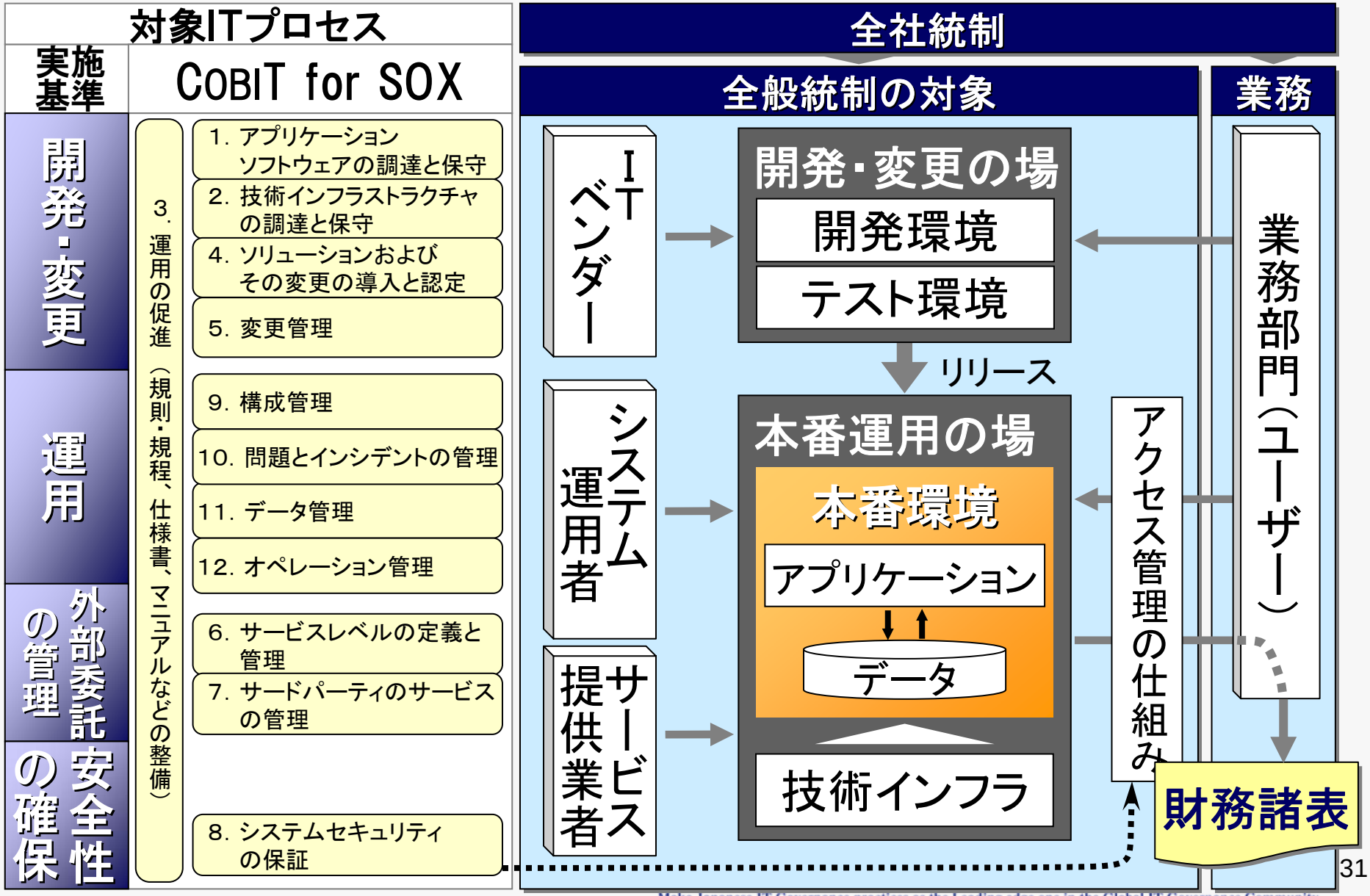
（出典）「これならできるIT統制」

財務諸表の信頼性に係るリスク



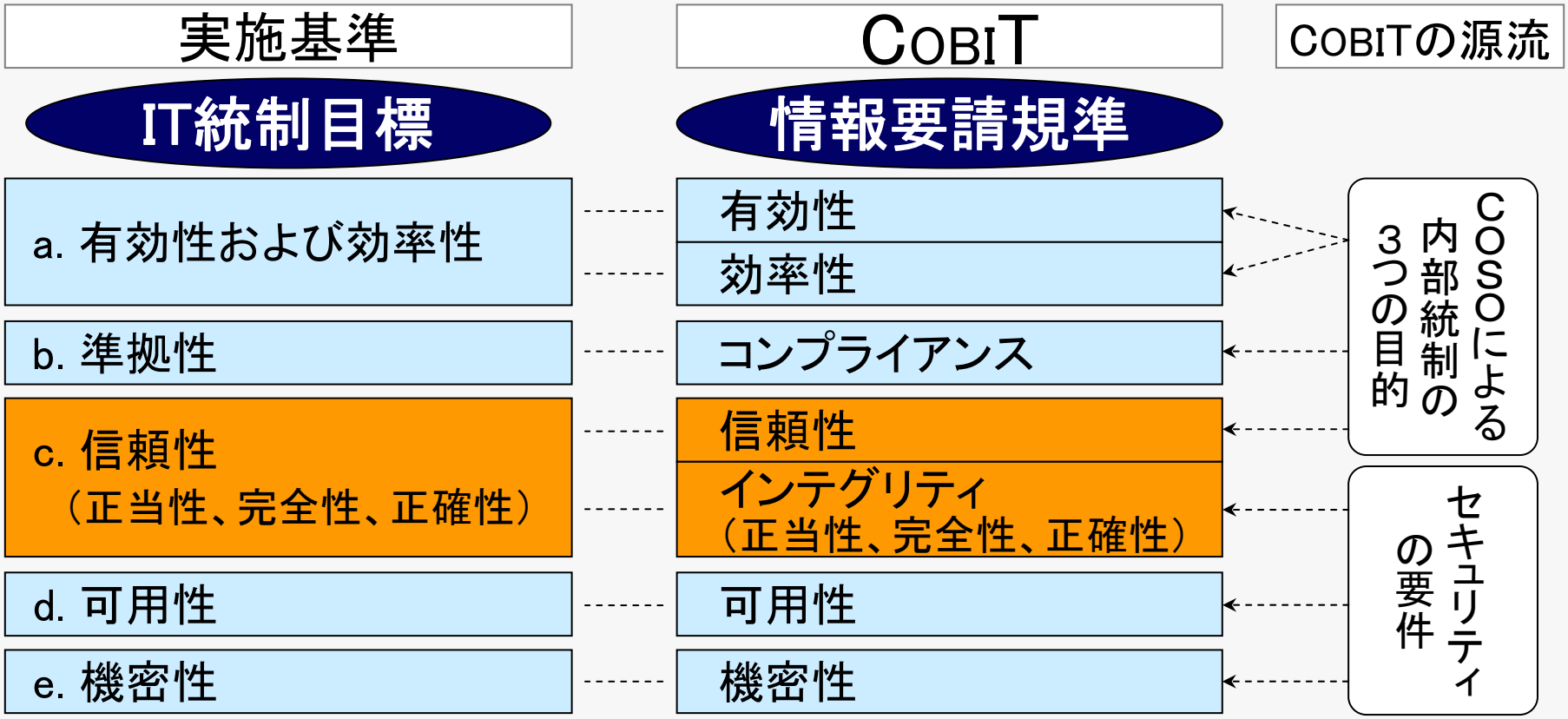
(出典)「これならできるIT統制」

全般統制の対象となるITプロセス



（出典）「これならできるIT統制」

「IT統制目標」の意味するもの



ITプロセスごとに具体化

IT統制目標

- 34のITプロセスごとの統制目標
- 更に詳細レベルの統制目標

統制目標とは

統制によって達成すべき望ましい姿・状態

（出典）「これならできるIT統制」

ITGI Japan

GOVERNANCE INSTITUTE

目次

1. 日立グループにおける内部統制整備
2. IT統制の枠組み
3. 全般統制への2つのアプローチ
4. COBITが提供するもの
5. 全般統制の対象となるIT業務
6. ITマネジメントの体系化

日立グループでの合理化と品質向上の例

- 短期的効率化
  - IT内部統制ガイドラインの整備
  - IT全般統制項目の整備、絞り込み
  - 文書管理、変更管理、ログ管理、ID管理等へのITツール適用
- 中期的効率化
  - ITマネジメントの体系化
  - ITガバナンス強化、シェアードサービス化
  - EA、BPM、SOA等を駆使した次世代情報基盤アプローチ

フレームワークの乱立

内部統制

- SOX
- J-SOX
- COBIT for SOX

経営品質全般

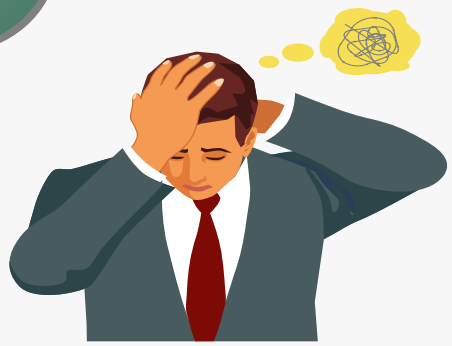
- 経済産業省 システム管理基準
- COBIT
- ITIL
- ....

個人情報保護

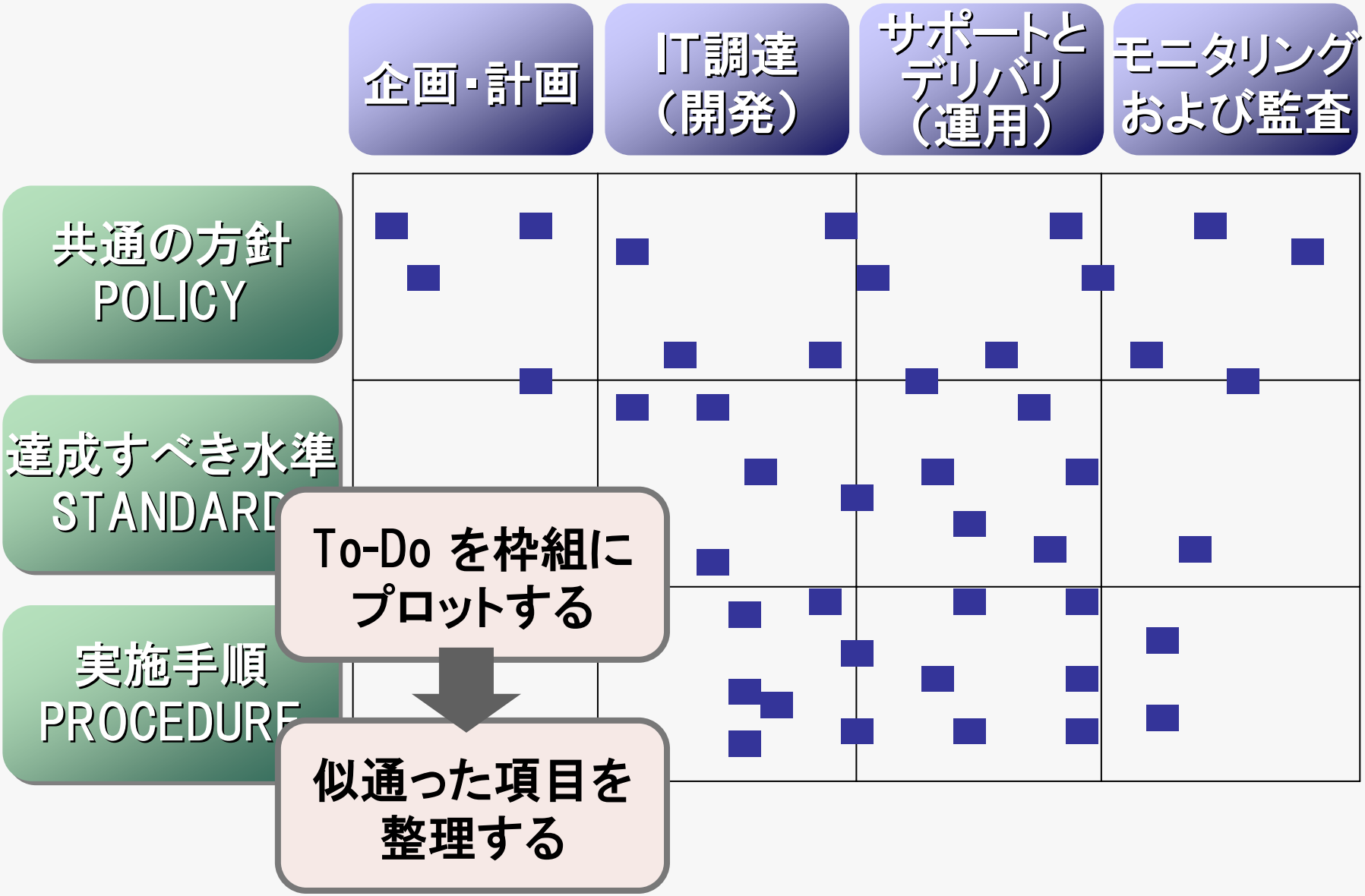
- JIS Q15001

情報セキュリティ

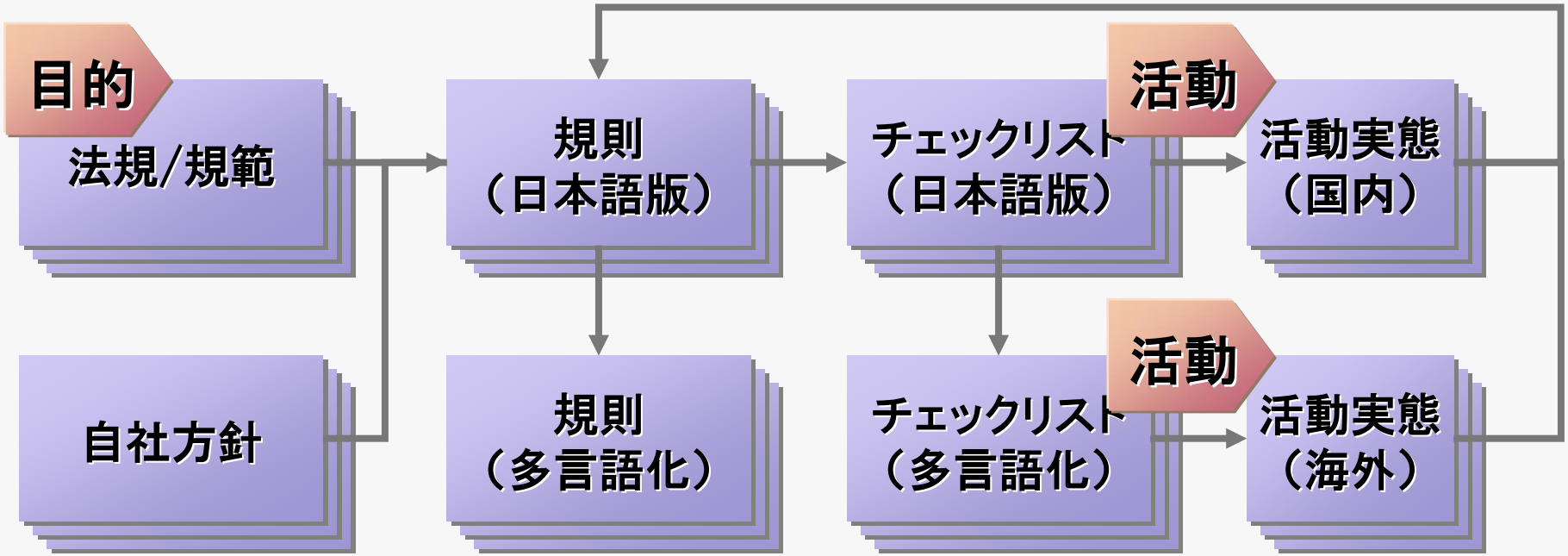
- ISO 27001
- ...



フレームワーク整理の手順



従来の規則運用の問題点

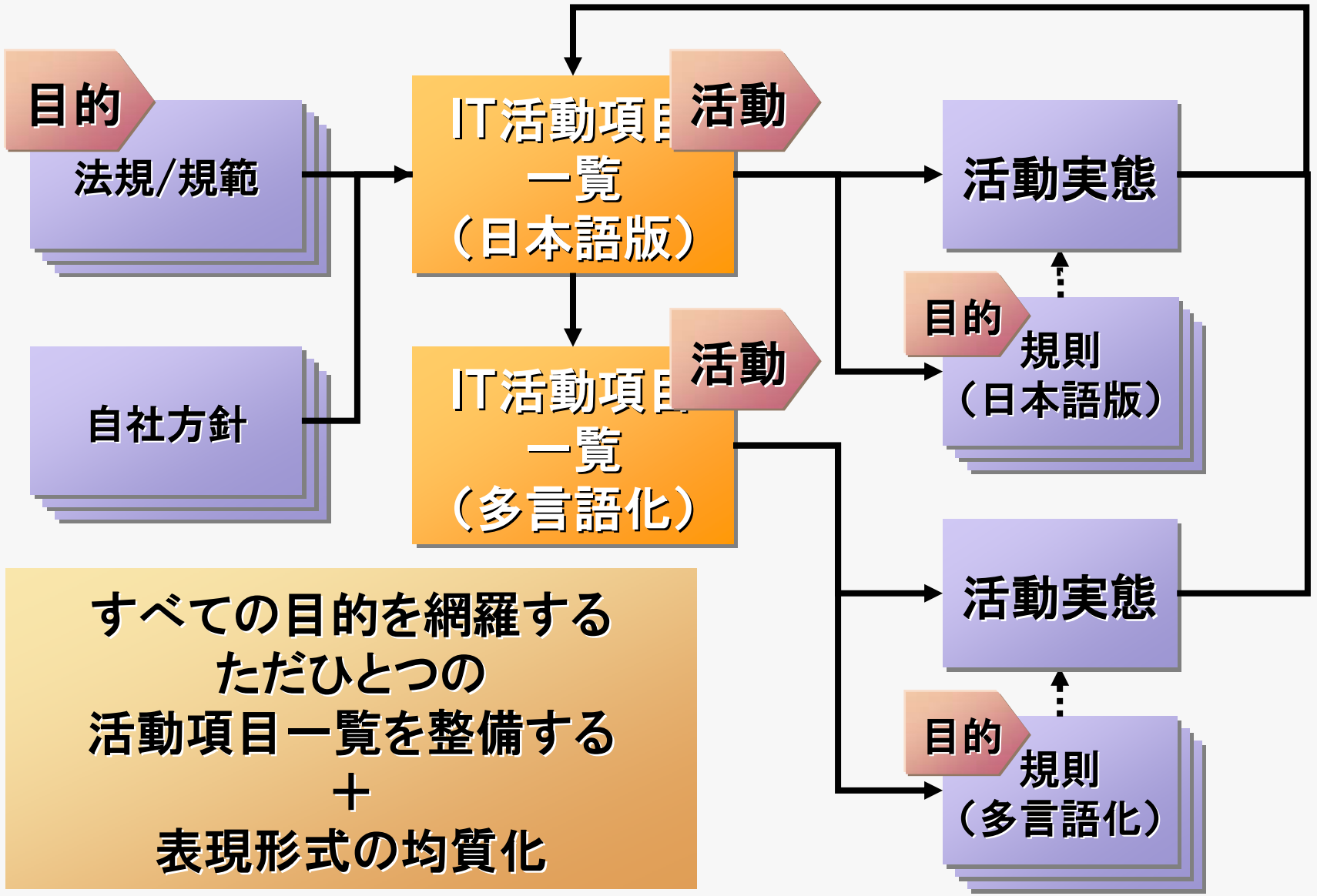


規則とは「目的から活動への変換装置」である

→目的と活動は1対1の関係にあるべき（目的中心主義）

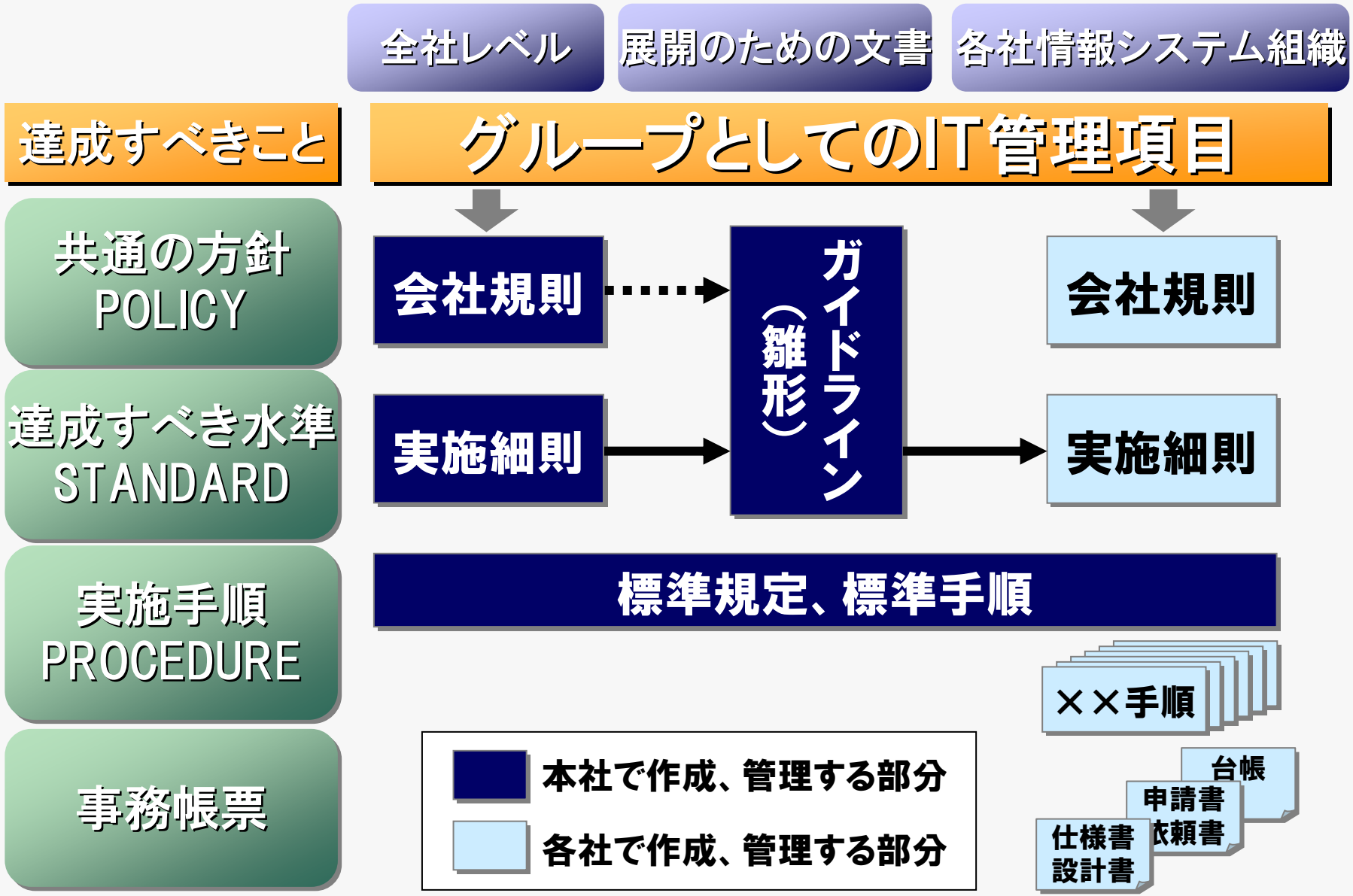
→目的の数だけ活動を規定する、規定された活動がダブッているかどうかは気にしない　＋　表現形式の混乱

IT管理への体系的アプローチ



すべての目的を網羅する
ただひとつの
活動項目一覧を整備する
＋
表現形式の均質化

各レベルで管理する領域の考え方



ITプロセスが将来のIT価値を生み出す

ITプロセス

IT管理業務

計画

モニタリング

調達と導入

サービス提供とサポート

ベンダー／パートナ

各種製品

サービス

IT資産

アプリケーション

情　報

ITインフラ

人

IT価値

システム

サービス

ユーザー部門

良質なITプロセス＋良質なIT資産 ➡ 将来のIT価値

ITプロセスは、ITガバナンスを構成する

「ITガバナンス」とは・・・

経営幹部と取締役会が責任を持つべきものであり、
組織のITが確実に組織の戦略と目標を支持し拡大するようにするための、**リーダーシップ**、**組織構造**および**プロセス**から成り立つ。

（出典）「ITガバナンスについての幹部向け概説 第2版」2003年 ITガバナンス協会

ITプロセスを通じて、IT価値を作り込む

ご静聴ありがとうございました

- ご意見・ご感想やご質問などあれば、ぜひお聞かせ下さい。

- 連絡先
  - メール

    k.takaura@hitachiconsulting.co.jp
  - オフィス

    株式会社 日立コンサルティング
    港区港南2-16-4 品川グランドセントラルタワー18階
    TEL 03-5715-5226