

COBIT 5 講習会資料

価値創出のための事業体ITガバナンス

～ ITサービス会社の実践事例による解説 ～

Presented by

東京海上日動システムズ(株) GRC支援部 上級エキスパート
ISACA東京支部基準委員会 委員

稲葉 裕一

本日の内容

【はじめに】

【第1部】 COBIT 5概説

1-1. フレームワーク

1-2. 5つの原則

1-3. プロセス参照モデル

1-4. 導入ガイダンス

1-5. プロセスアセスメントモデル

【第2部】 実践事例による解説

2-1. ITサービス会社のGRC態勢

2-2. COBIT 5の適用方法

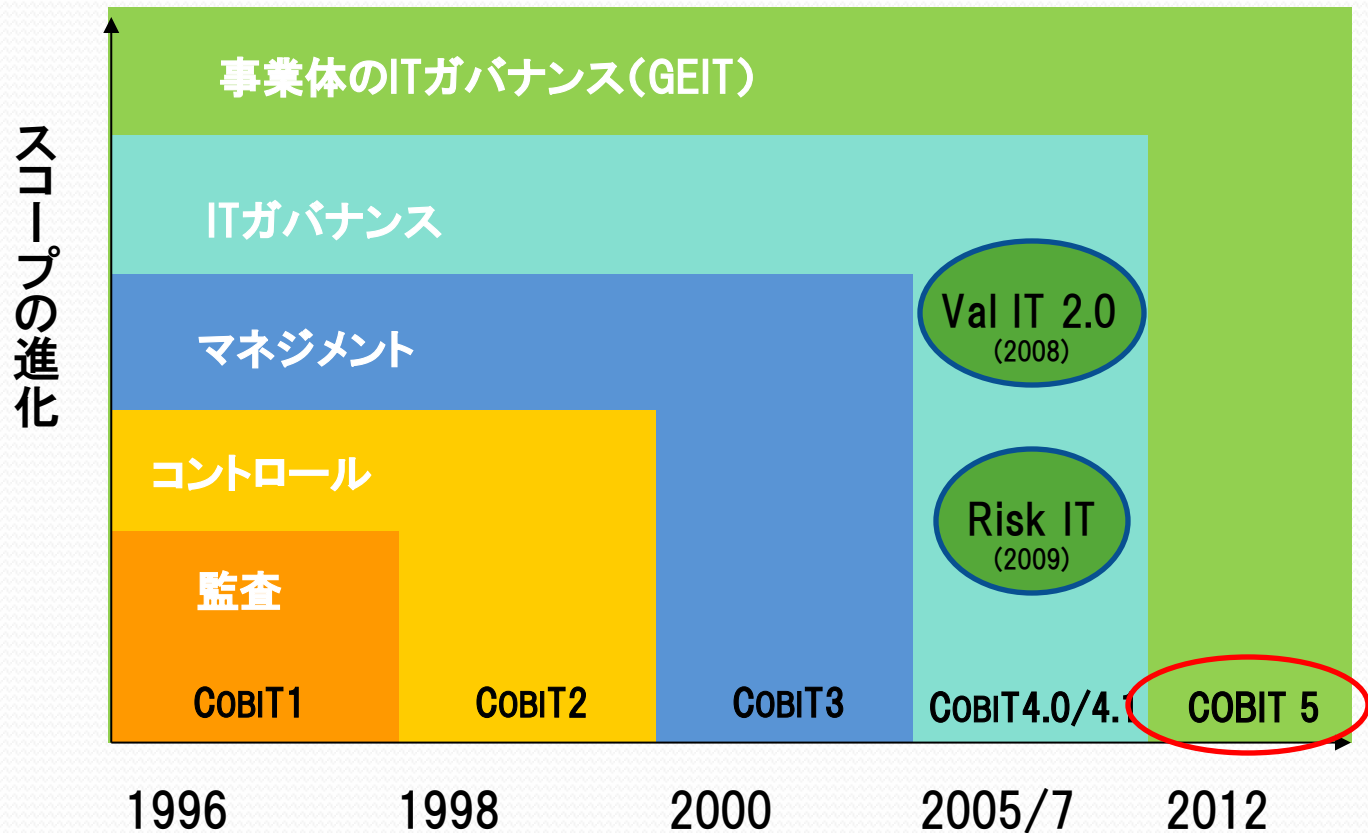
【おわりに】

【はじめに】

COBIT 5 とは

- 事業体の IT ガバナンスと IT マネジメントのためのビジネスフレームワーク
- 効果の実現、リスクの最適化、資源の最適化とのバランスを維持し、ITにより最適な価値を創り出すことを支援
- 営利、非営利、公的機関等、すべての規模の事業体に適用でき、有効なもの

COBIT 5 に至るまで



ISACAが提供するビジネスフレームワーク www.isaca.org/cobit

© 2012 ISACA® All rights reserved.

事業体ITガバナンス(GEIT)

- 「ガバナンス」は「舵取り」
 - ➡ギリシャ語の動詞kubernáo(舵を取る)に由来
 - ➡日本では「統治」が一般的(押さえつけるような語感)
- ITガバナンス
 - IT部門(CIO)の視点、IT部門中心のガバナンス
- 事業体ITガバナンス(GEIT:ガイト/ゲイトと発音)
 - 経営トップ(CEO)の視点、ビジネスガバナンス
 - ～ITが経営の中心的な役割になってきているので

GEIT vs. ITガバナンス

取締役会

CEO

GEIT

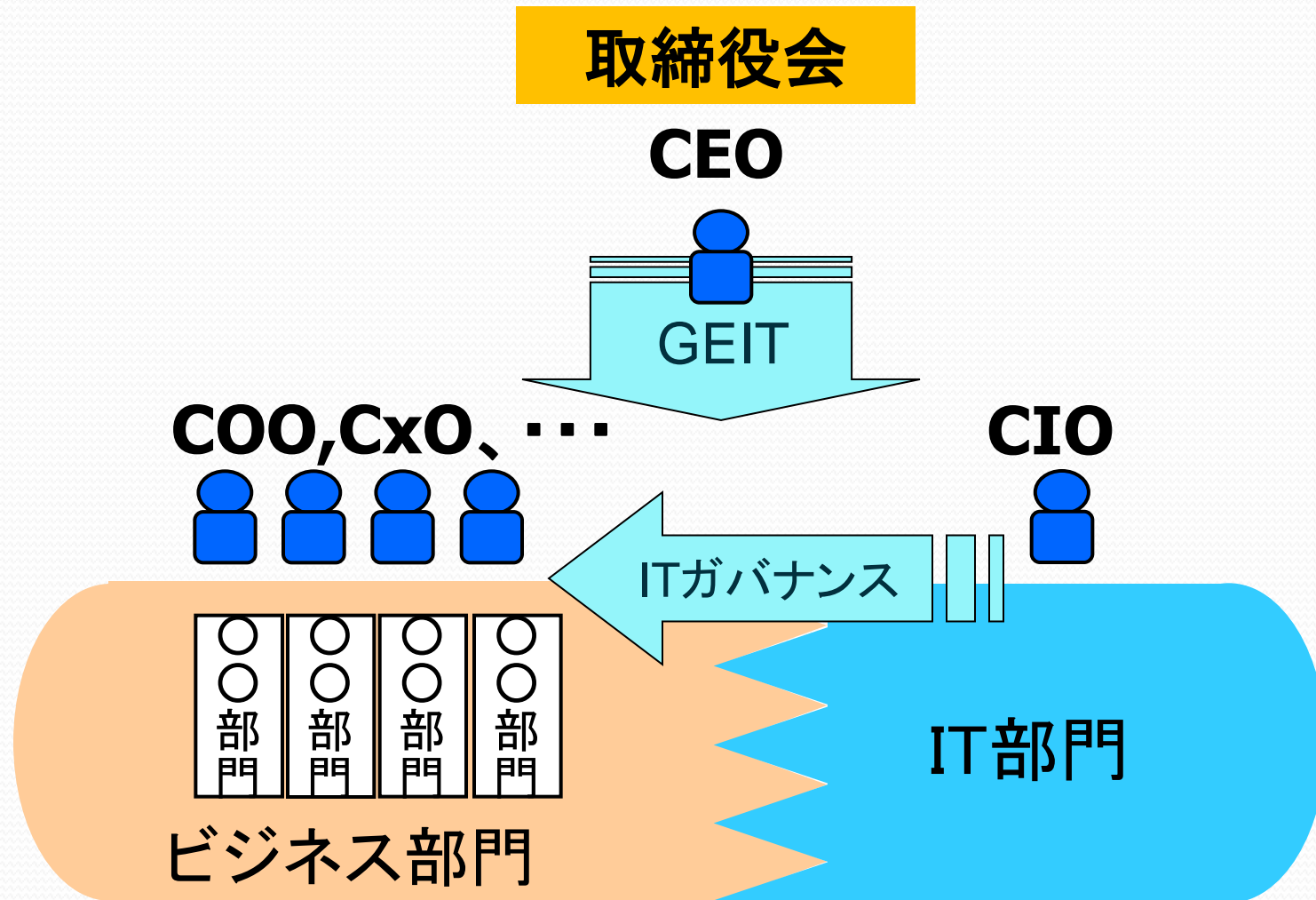
COO, CxO, ...

CIO

ITガバナンス

IT部門

ビジネス部門



COBIT 5 プロダクトファミリー

COBIT 5 プロダクトファミリー

COBIT® 5

COBIT 5イネーブラーガイド

COBIT® 5: Enabling Processes

COBIT® 5: Enabling Information

その他のイネーブラーガイド

COBIT 5プロフェッショナルガイド

COBIT® 5 Implementation

COBIT® 5 for Information Security

COBIT® 5 for Assurance

COBIT® 5 for Risk

その他のプロフェッショナルガイド

COBIT 5 オンライン コラボレーション環境

COBIT 5 プロダクトファミリー日本語版

COBIT 5 プロダクトファミリー

COBIT® 5

済

COBIT 5 イネーブラーガイド

COBIT® 5: Enabling Processes

済

COBIT® 5: Enabling Information

その他のイネーブラーガイド

COBIT 5 プロフェッショナルガイド

COBIT® 5 Implementation

済

COBIT® 5 for Information Security

COBIT® 5 for Assurance

着手

COBIT® 5 for Risk

その他のプロフェッショナルガイド

COBIT 5 オンライン コラボレーション環境

出典: COBIT® 5 日本語版, 図表11. © 2012 ISACA® All rights reserved.

COBIT Assessment Programme

COBIT® Process Assessment Model (PAM): Using COBIT 5

着手

COBIT® Assessor Guide: Using COBIT 5

COBIT® Self-Assessment Guide: Using COBIT 5

【第1部】

COBIT 5概説

1-1. フレームワーク

COBIT 5 プロダクトファミリー日本語版

COBIT 5 プロダクトファミリー

COBIT® 5

済

COBIT 5イネーブラーガイド

COBIT® 5: Enabling Processes

済

COBIT® 5: Enabling Information

その他のイネーブラーガイド

COBIT 5プロフェッショナルガイド

COBIT® 5 Implementation

済

COBIT® 5 for Information Security

COBIT® 5 for Assurance

着手

COBIT® 5 for Risk

その他のプロフェッショナルガイド

COBIT 5 オンライン コラボレーション環境

出典: COBIT® 5 日本語版, 図表11. © 2012 ISACA® All rights reserved.

COBIT Assessment Programme

COBIT® Process Assessment Model (PAM): Using COBIT 5

着手

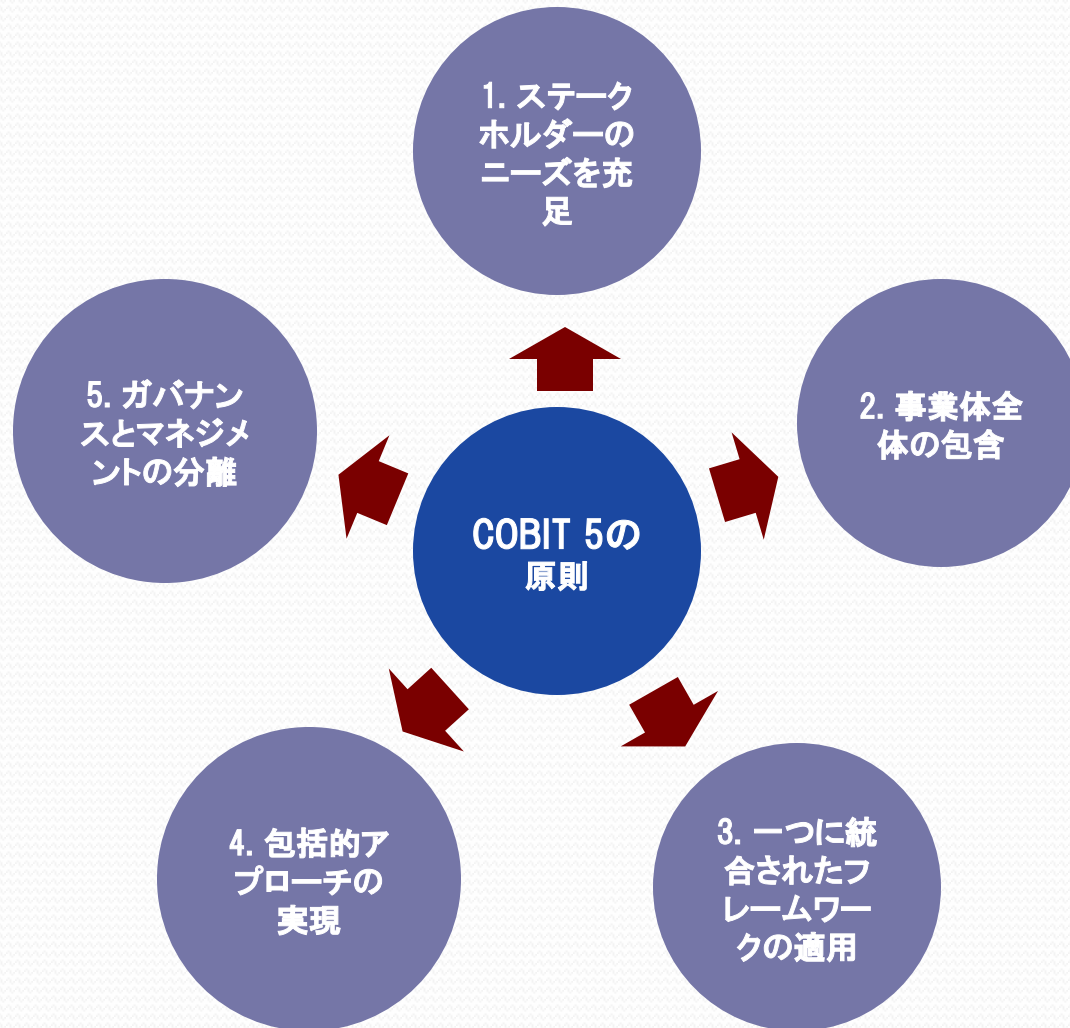
COBIT® Assessor Guide: Using COBIT 5

COBIT® Self-Assessment Guide: Using COBIT 5

COBIT 5 フレームワーク

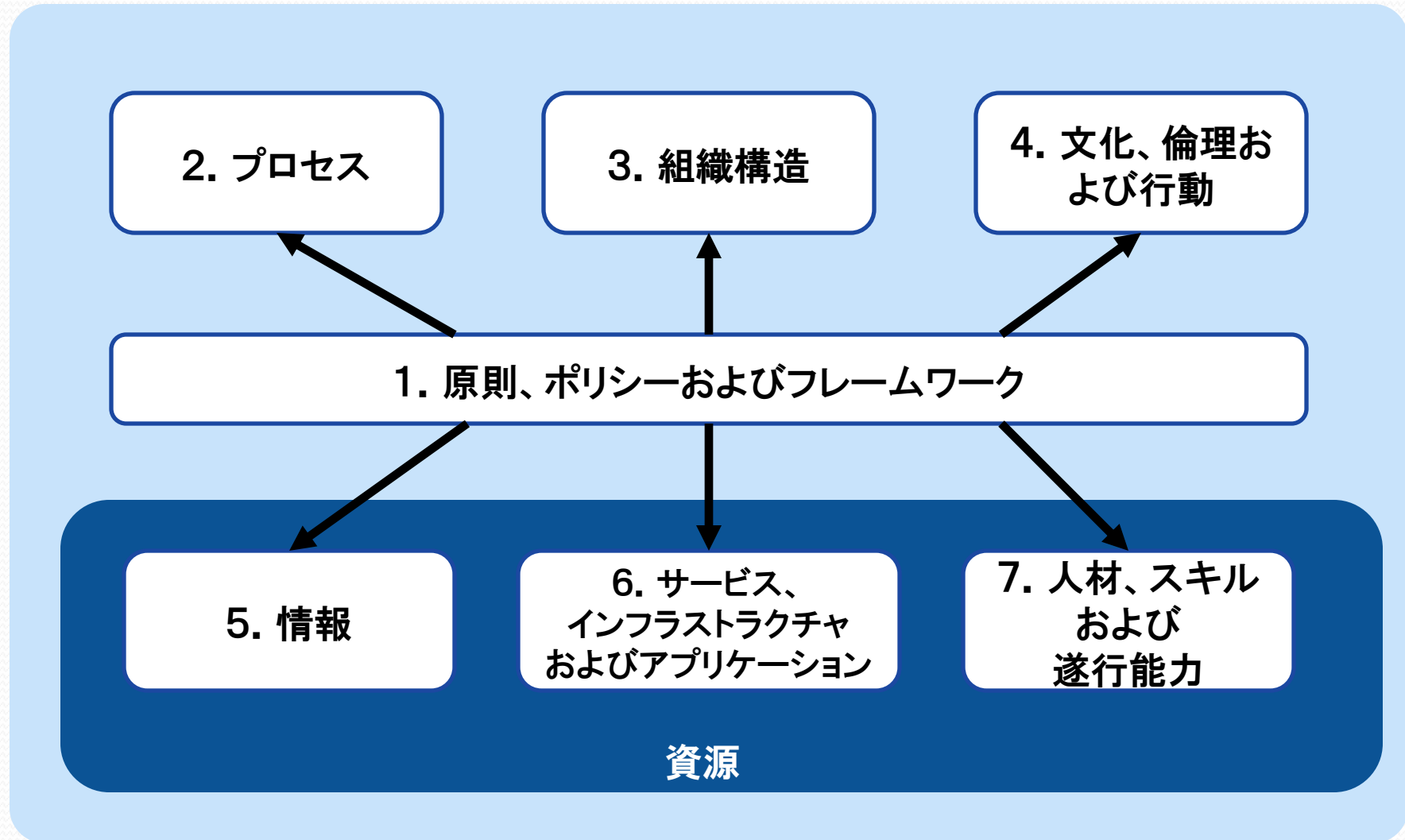
- 正式名称:「COBIT 5 : *A Business Framework for the Governance and Management of Enterprise IT*」
- COBIT 5 プロダクトの中心であり、全体を包括
- 構成
 - COBIT5の5つの原則
 - COBIT5の7つのイネーブラー
 - COBIT5 プロセス参照モデル
 - COBIT5の導入ガイダンスの紹介
(*COBIT 5 Implementation*)
 - COBITアセスメントモデルの紹介
(*COBIT Process Assessment Model : PAM*)

COBIT 5の原則



出典: COBIT® 5 日本語版, 図表2. © 2012 ISACA® All rights reserved.

COBIT 5のイネーブラー



COBIT 5 プロセス参照モデル

事業体ITガバナンスのためのプロセス 評価、方向付けおよびモニタリング

EDM01 ガバナンス
フレームワークの設
定と維持の確保

EDM02
効果提供の確保

EDM03
リスク最適化の確保

EDM04
資源最適化の確保

EDM01
ステークホルダーへ
の透明性の確保

整合、計画および組織化

AP001
ITマネジメント
フレームワークの
管理

AP002
戦略管理

AP003
エンタープライズ
アーキテクチャ管
理

AP004
イノベーション
管理

AP005
ポートフォリオ
管理

AP006
予算と費用の管
理

AP007
人材の管理

AP008
関係管理

AP009
サービス契約の管
理

AP010
サプライヤーの
管理

AP011
品質管理

AP012
リスク
管理

AP013
セキュリティ管
理

モニタリング、評価 およびアセスメント

MEA01
成果と整合性の
モニタリング、評価
およびアセスメント

MEA02
内部統制システムの
モニタリング、評価
およびアセスメント

MEA03
外部要求への
コンプライアンスの
モニタリング、評価
およびアセスメント

構築、調達および導入

BAI01
プログラムと
プロジェクトの
管理

BAI02
要件定義の
管理

BAI03
ソリューションの
特定と構築の
管理

BAI04
可用性とキャパ
シティの管理

BAI05
組織の変革実現の
管理

BAI06
変更管理

BAI07
変更受入と
移行の管理

BAI08
知識の管理

BAI09
資産の管理

BAI10
構成の管理

提供、サービスおよびサポート

DSS01
オペレーション
管理

DSS02
サービス要求と
インシデントの
管理

DSS03
問題管理

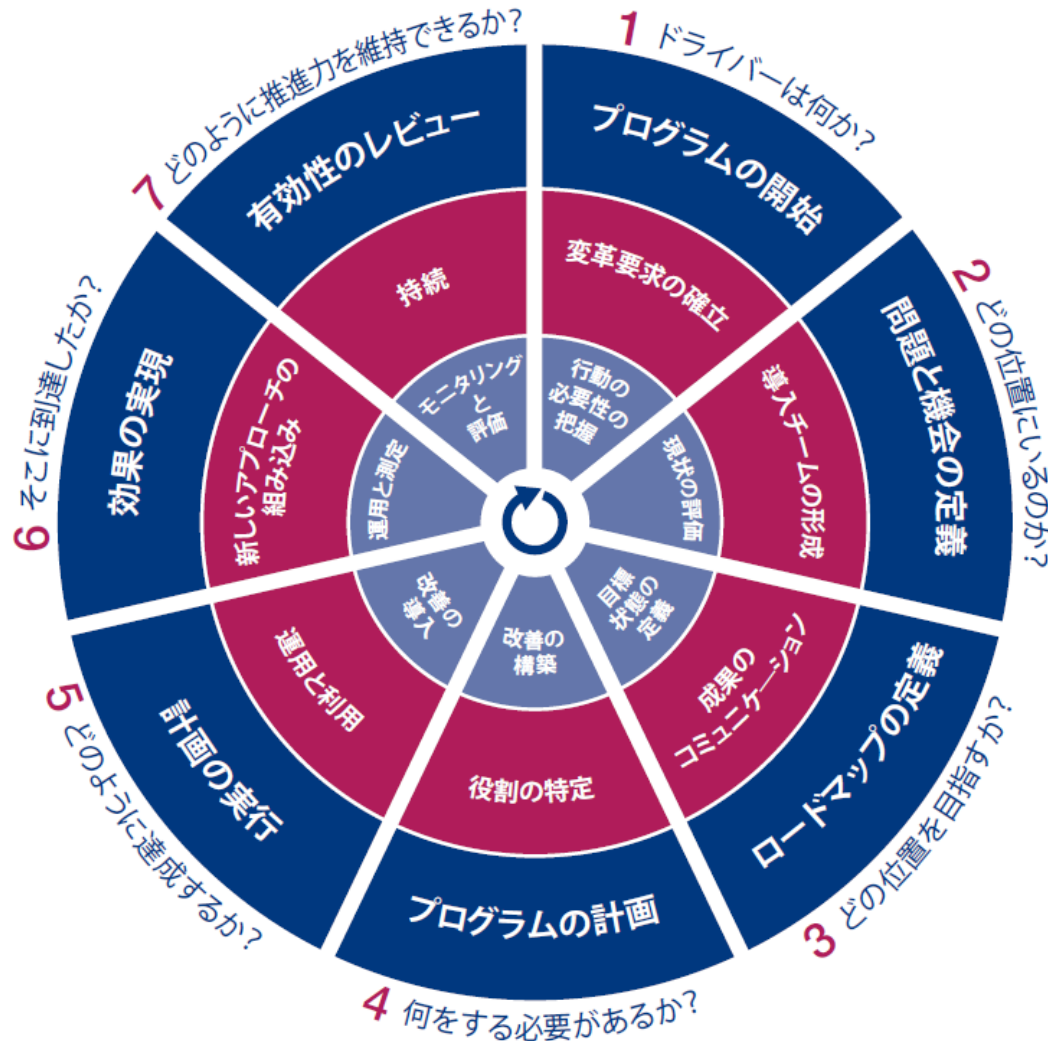
DSS04
継続性
管理

DSS05
セキュリティ
サービスの管理

DSS06
ビジネスプロセス
のコントロールの
管理

事業体のITマネジメントのためのプロセス

COBIT 5 Implementation

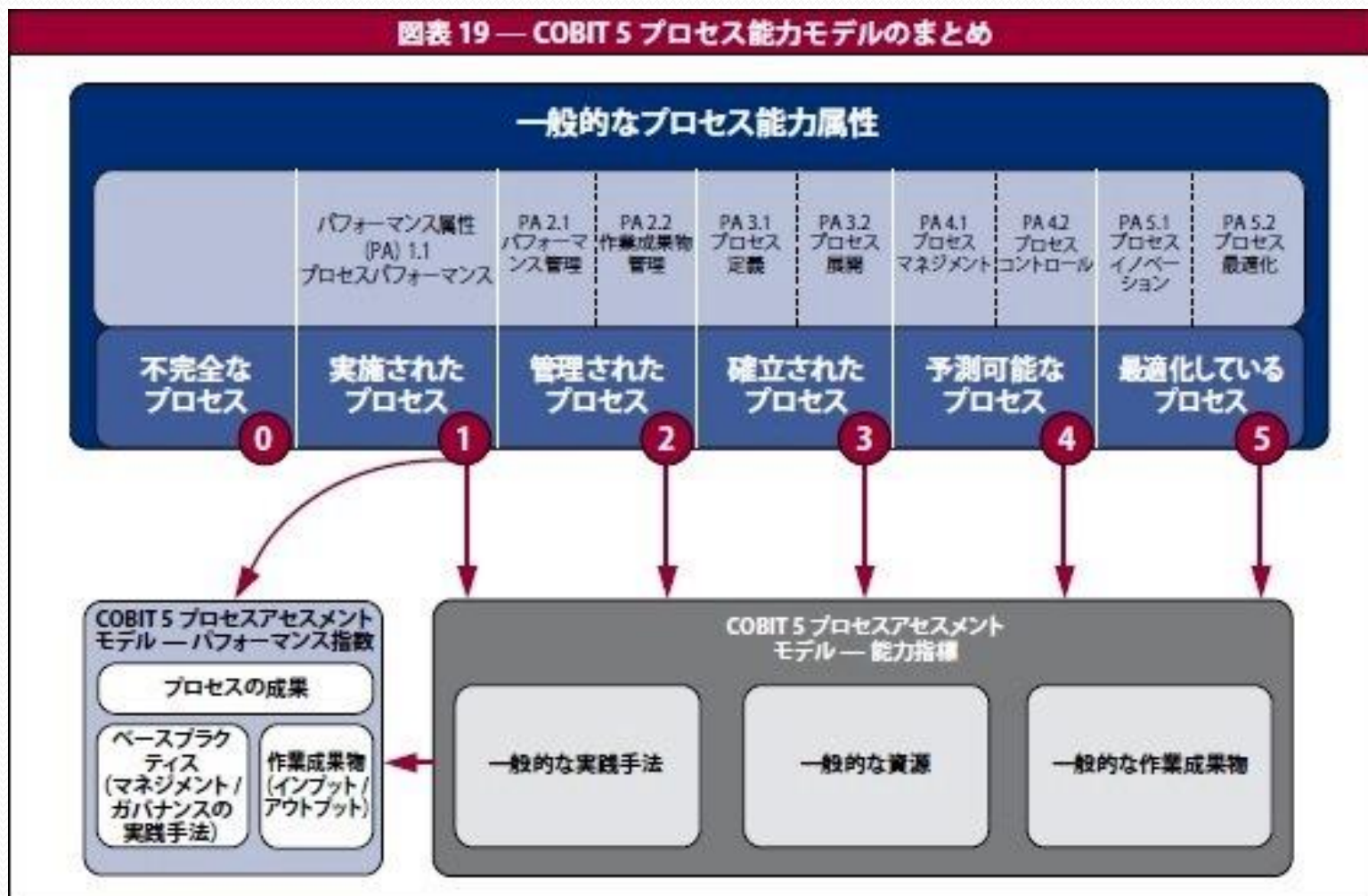


- プログラム管理 (外部リング)
- 変革の実現 (中間リング)
- 継続的改善ライフサイクル (内部リング)

Source: COBIT® 5日本語版 図表17. © 2012 ISACA® All rights reserved.

COBIT 5 プロセスアセスメントモデル (プロセス能力モデル)

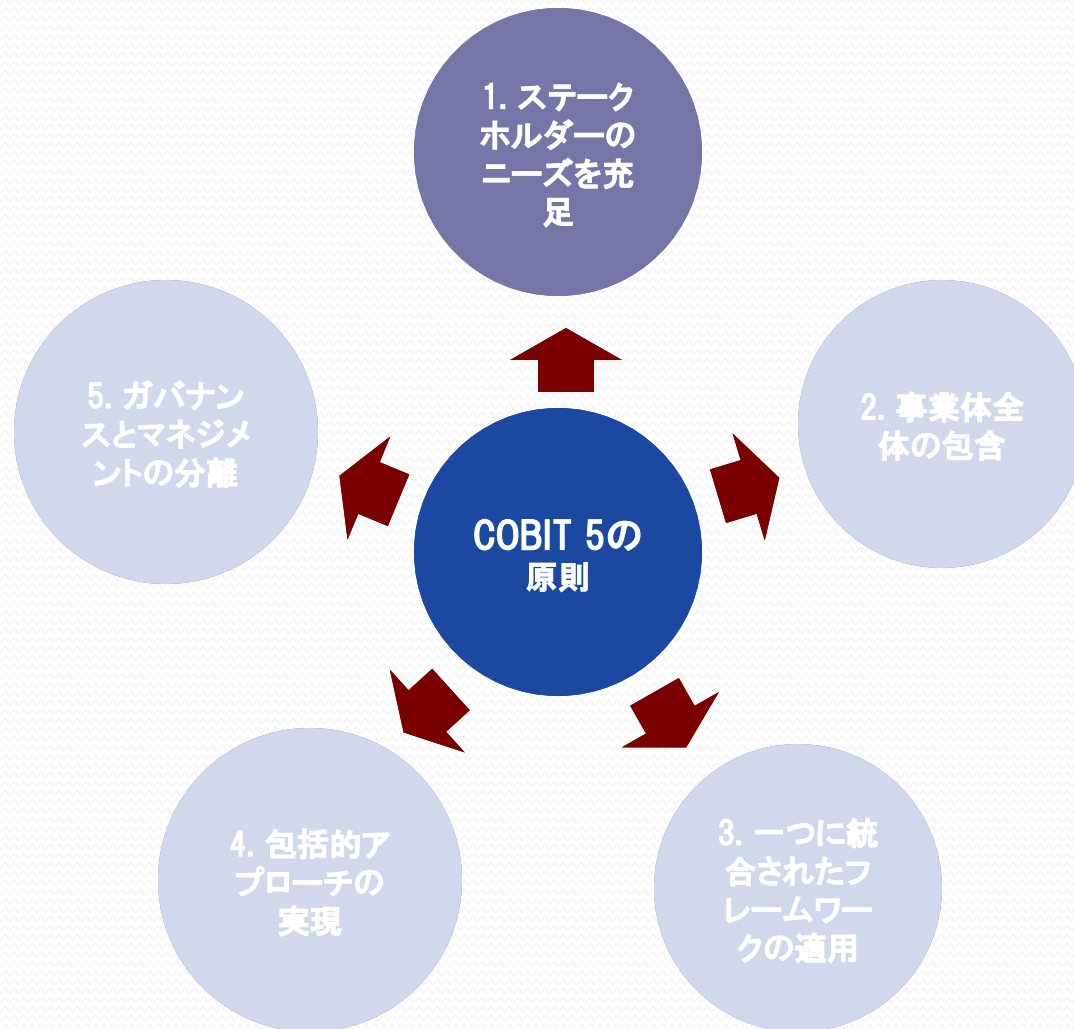
図表 19 — COBIT 5 プロセス能力モデルのまとめ



Source: COBIT® 5日本語版 図表19. © 2012 ISACA® All rights reserved.

1-2. 5つの原則

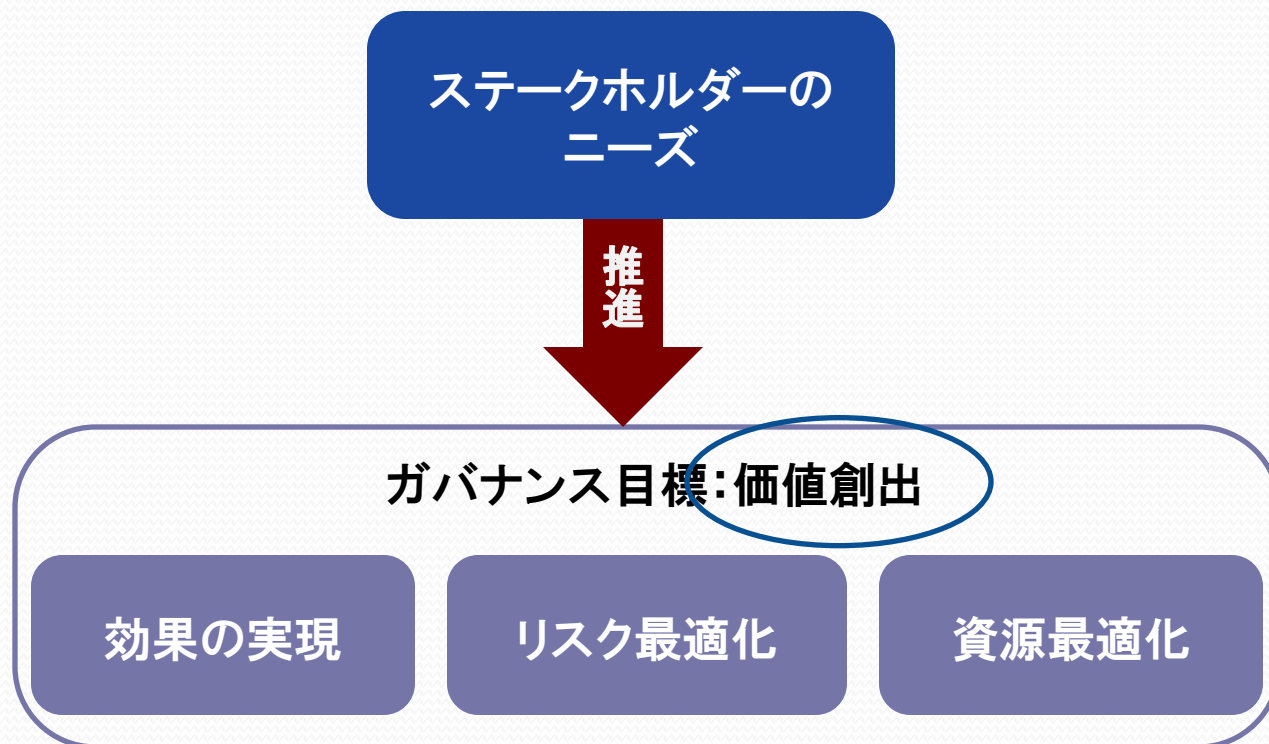
COBIT 5の原則



出典: COBIT® 5 日本語版, 図表2. © 2012 ISACA® All rights reserved.

原則1. ステークホルダーのニーズを充足

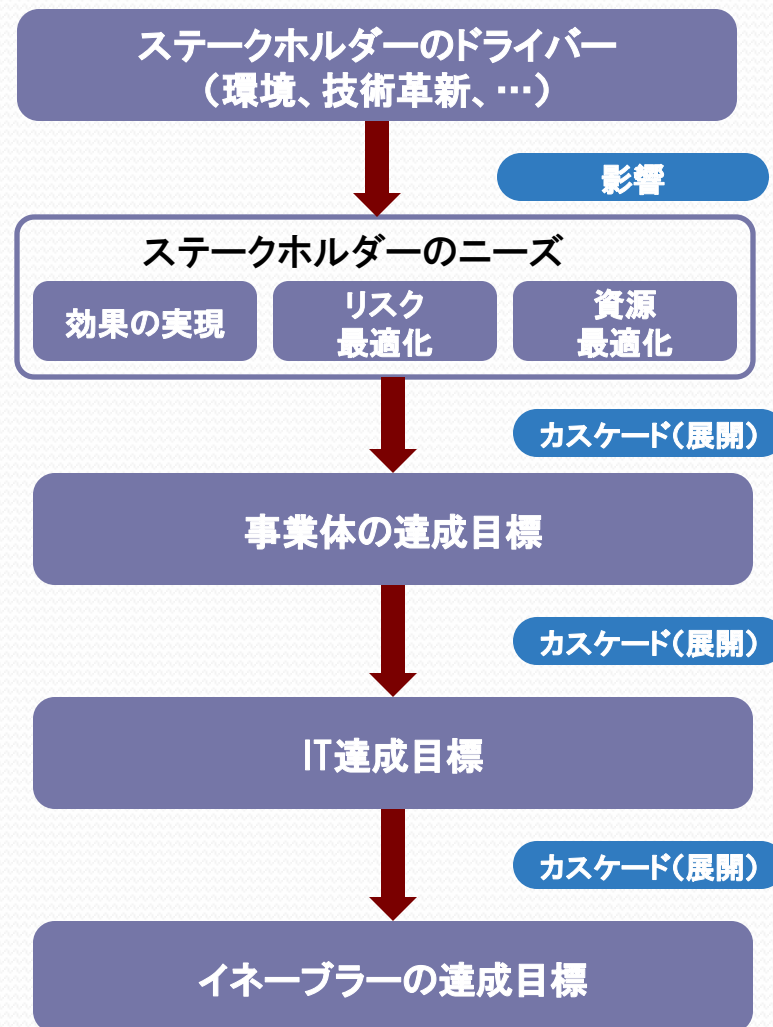
- 事業体はそのステークホルダーの価値を創出するために存在する。



原則1. ステークホルダーのニーズを充足

- ステークホルダーのニーズを事業体の戦略に変換
- COBIT 5の達成目標のカスケード(展開)

ステークホルダーのニーズから
➡ 事業体の達成目標
➡ IT達成目標
➡ イネーブラーの達成目標
へ展開する



原則1. ステークホルダーのニーズを充足

図表5 — COBIT 5 における事業体の達成目標

BSCの視点	事業体の達成目標	ガバナンス目標との関係		
		効果の実現	リスク最適化	資源最適化
財務	1. ステークホルダーから見たビジネス投資価値	P		S
	2. 競争力のある製品・サービスのポートフォリオ	P	P	S
	3. 事業リスクの管理（資産の保全）		P	S
	4. 外部の法令および規制への準拠		P	
	5. 財務上の透明性	P	S	S
顧客	6. 顧客志向のサービスを提供する文化	P		S
	7. ビジネスサービスの継続性と可用性		P	
	8. 事業環境変化への迅速な対応	P		S
	9. 情報に基づいた戦略的意思決定	P	P	P
	10. サービス提供コストの最適化	P		P
内部	11. ビジネスプロセスの機能の最適化	P		P
	12. ビジネスプロセスのコストの最適化	P		P
	13. 事業変革プログラムの管理	P	P	S
	14. 業務およびスタッフの生産性	P		P
	15. 内部のポリシーへの準拠		P	
学習と成長	16. スキルと意欲を有する人材	S	P	P
	17. 製品やビジネスを革新する文化	P		

出典: COBIT® 5 日本語版, 図表5. © 2012 ISACA® All rights reserved.

原則1. ステークホルダーのニーズを充足

図表6—IT達成目標

IT BSCの視点	情報と関連技術の目標	
財務	01	ITと事業戦略の整合性
	02	ビジネスが外部の法令と規制に準拠するためのITの準拠性とサポート
	03	IT関連の意思決定に対する経営幹部のコミットメント
	04	ITに関連する事業リスクの管理
	05	ITを活用した投資とサービスポートフォリオにより実現された利益
	06	ITコスト、効果およびリスクの透明性
顧客	07	ビジネス要件に合致したITサービスの提供
	08	アプリケーション、情報および技術ソリューションの適切な使用
内部	09	ITの俊敏性
	10	情報、情報処理インフラストラクチャ、アプリケーションのセキュリティ
	11	IT資産、資源および能力の最適化
	12	アプリケーションと技術をビジネスプロセスへ組み込むことによる、ビジネスプロセスの可能性とサポート力
	13	納期、予算、要件および品質基準を守り、効果を出すプログラムの提供
	14	意思決定のための信頼できる有用な情報の可用性
	15	内部ポリシーへのITの準拠
学習と成長	16	有能で意欲のあるビジネスおよびITの担当者
	17	ビジネス革新のための知識、専門性および取り組み事例

事業体の達成目標とのマッピング

COBIT 5ではP(主要)とS(副次)で事業体達成目標とのマッピングを示している
(COBIT® 5 日本語版 図表22参照)

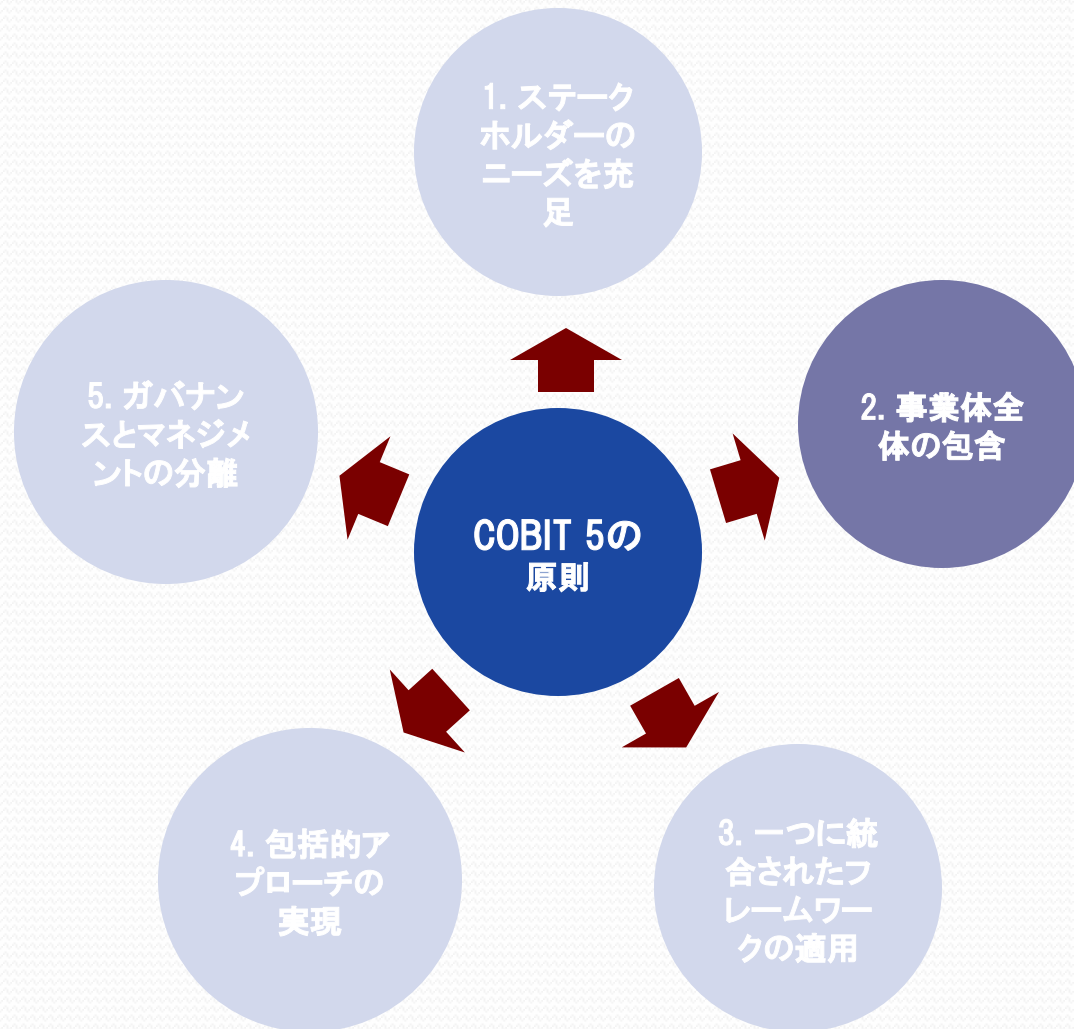
出典: COBIT® 5 日本語版, 図表6.© 2012 ISACA® All rights reserved.

原則1. ステークホルダーのニーズを充足

図表 23 — COBIT 5 の IT 達成目標とプロセスのマッピング

			IT 達成目標																
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
			ITと事業戦略の整合性	ビジネスが外部の法令と規制に準拠するためのITの準拠性とサポート	IT関連の意思決定に対する経営幹部のコミットメント	ITに関連する事業リスクの管理	ITを活用した投資とサポートフォリオにより実現された利益	ITコスト、効果およびリスクの透明性	ビジネス要件に合致したITサービスの提供	アプリケーション、情報および技術ソリューションの適切な使用	ITの俊敏性	情報、情報処理インフラストラクチャ、アプリケーションのセキュリティ	IT資産、資源および能力の最適化	アプリケーションと技術をビジネスプロセスへ組み込むことによる、ビジネスプロセスの可能性とサポート力	納期、予算、要件および品質基準を守り、効果を出すプログラムの提供	意思決定のための信頼できる有用な情報の可用性	内部ポリシーへのITの準拠	有能で意欲のあるビジネスおよびITの担当者	ビジネス革新のための知識、専門性および取り組み事例
COBIT 5 のプロセス			財務					顧客		内部							学習と成長		
評価、方向付けおよびモニタリング	EDM01	ガバナンスフレームワークの設定と維持の保証	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	効果実現の保証	P		S		P	P	S			S		S	S	S		S	P
	EDM03	リスク最適化の保証	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	資源最適化の保証	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	ステークホルダーから見た透明性の保証	S	S	P			P	P						S	S	S		S
整合、計画および組織化	APO01	IT マネジメントフレームワークの管理	P	P	S	S		S		P	S	P	S	S	S	P	P	P	P
	APO02	戦略管理	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	エンタープライズアーキテクチャ管理	P		S	S	S	S	S	P	S	P	S		S				S
	APO04	イノベーション管理	S			S	P			P	P		P	S					P
	APO05	ポートフォリオ管理	P		S	S	P	S	S	S	S		S			P			S
	APO06	予算とコストの管理	S		S	S	P	P	S	S			S			S			
	APO07	人的資源の管理	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	関係管理	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	サービス契約の管理	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	サプライヤーの管理		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	品質管理	S	S		S	P		P	S	S		S			P	S	S	S
	APO12	リスク管理		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	セキュリティ管理		P		P		P	S	S		P				P			

COBIT 5の原則



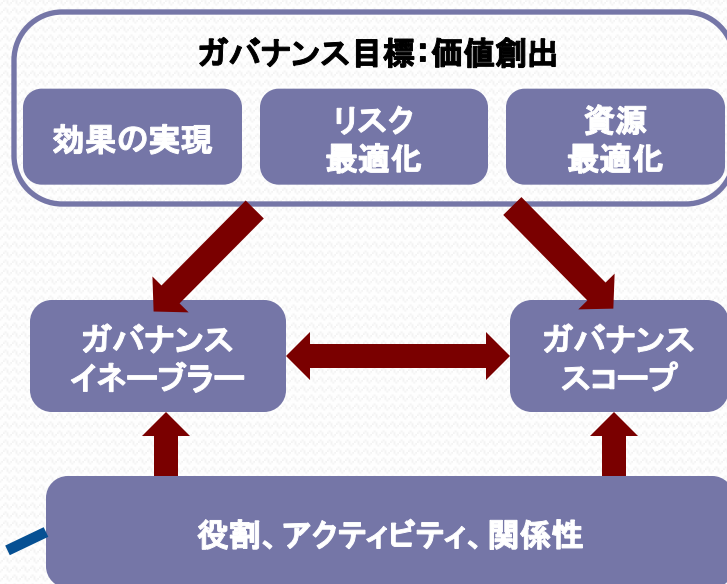
出典: COBIT® 5 日本語版, 図表2. © 2012 ISACA® All rights reserved.

原則2. 事業体全体の包含

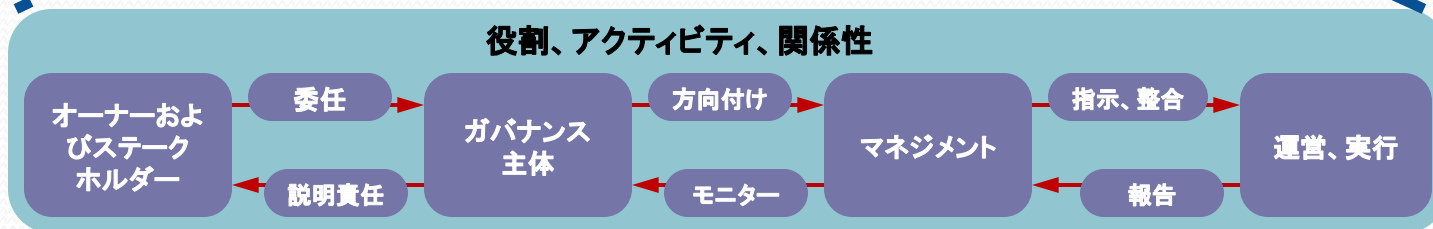
- 事業体全体にわたる**包括的な視点**から、**情報とそれに関連する技術のガバナンスとマネジメント**を取り扱う。
- 事業体の中の**全ての部門**、**全てのプロセス**をカバー。
- 事業体ITガバナンス(GEIT)はコーポレートガバナンス(ビジネスガバナンス)そのもの。

原則2. 事業体全体の包含

ガバナンスのアプローチ

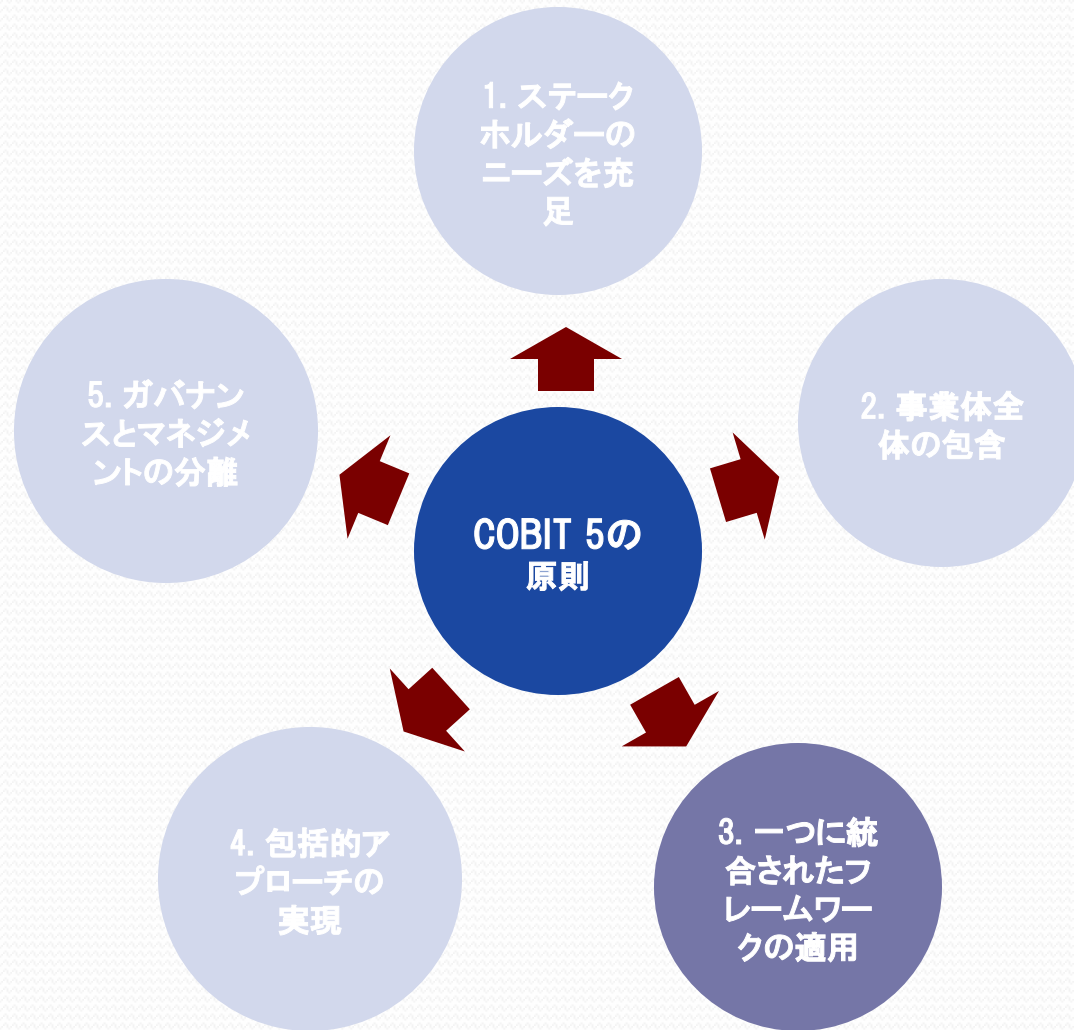


出典: COBIT® 5 日本語版, 図表8. © 2012 ISACA® All rights reserved.



出典: COBIT® 5 日本語版, 図表9. © 2012 ISACA® All rights reserved.

COBIT 5の原則

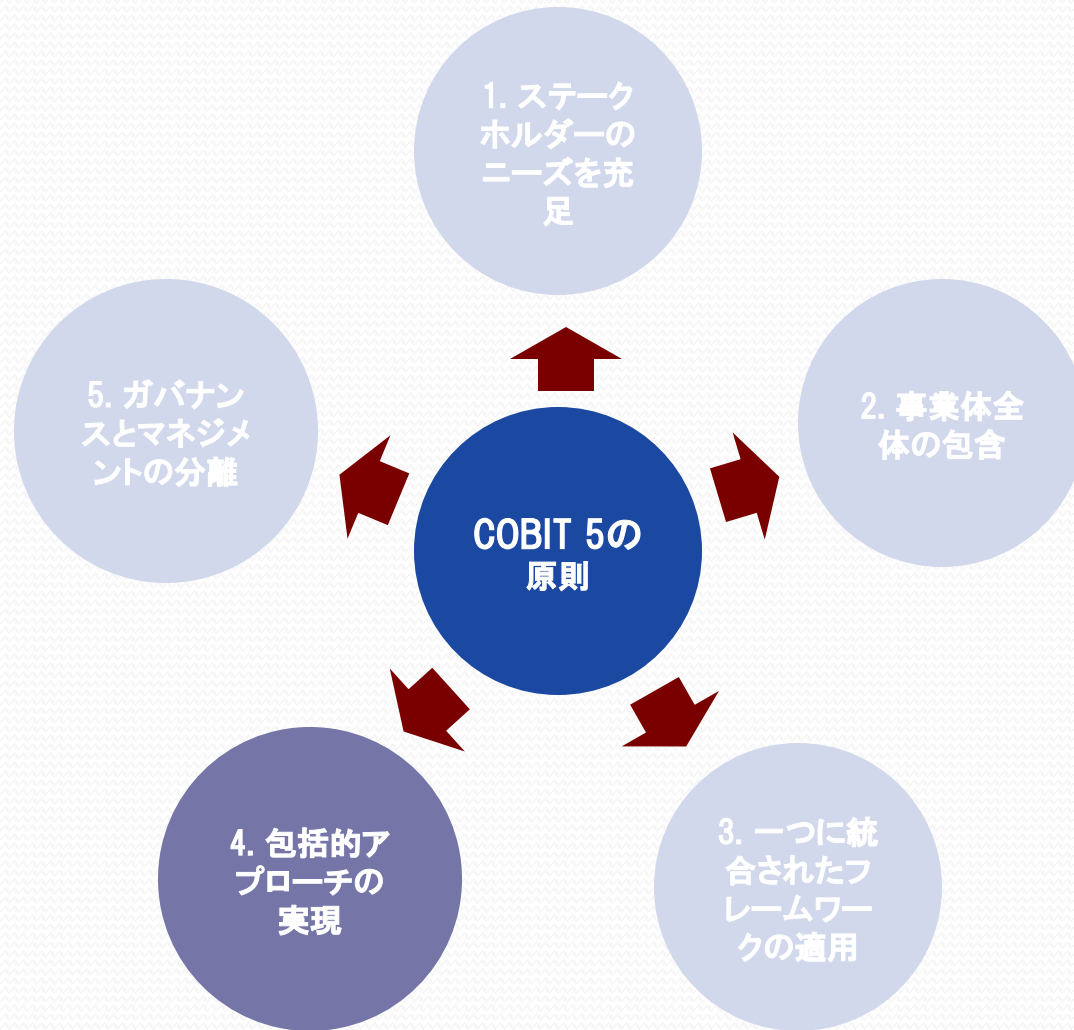


出典: COBIT® 5 日本語版, 図表2. © 2012 ISACA® All rights reserved.

原則3. 一つに統合されたフレームワークの適用

- 最新の関連する他の標準やフレームワークと整合
 - 事業体: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000
 - IT関連: ISO/IEC 38500, ITIL, ISO/IEC 27000シリーズ, TOGAF, PMBOK/PRINCE2, CMMI
- ガバナンスとマネジメントのフレームワークを統合するものとして利用可能

COBIT 5の原則



出典: COBIT® 5 日本語版, 図表2. © 2012 ISACA® All rights reserved.

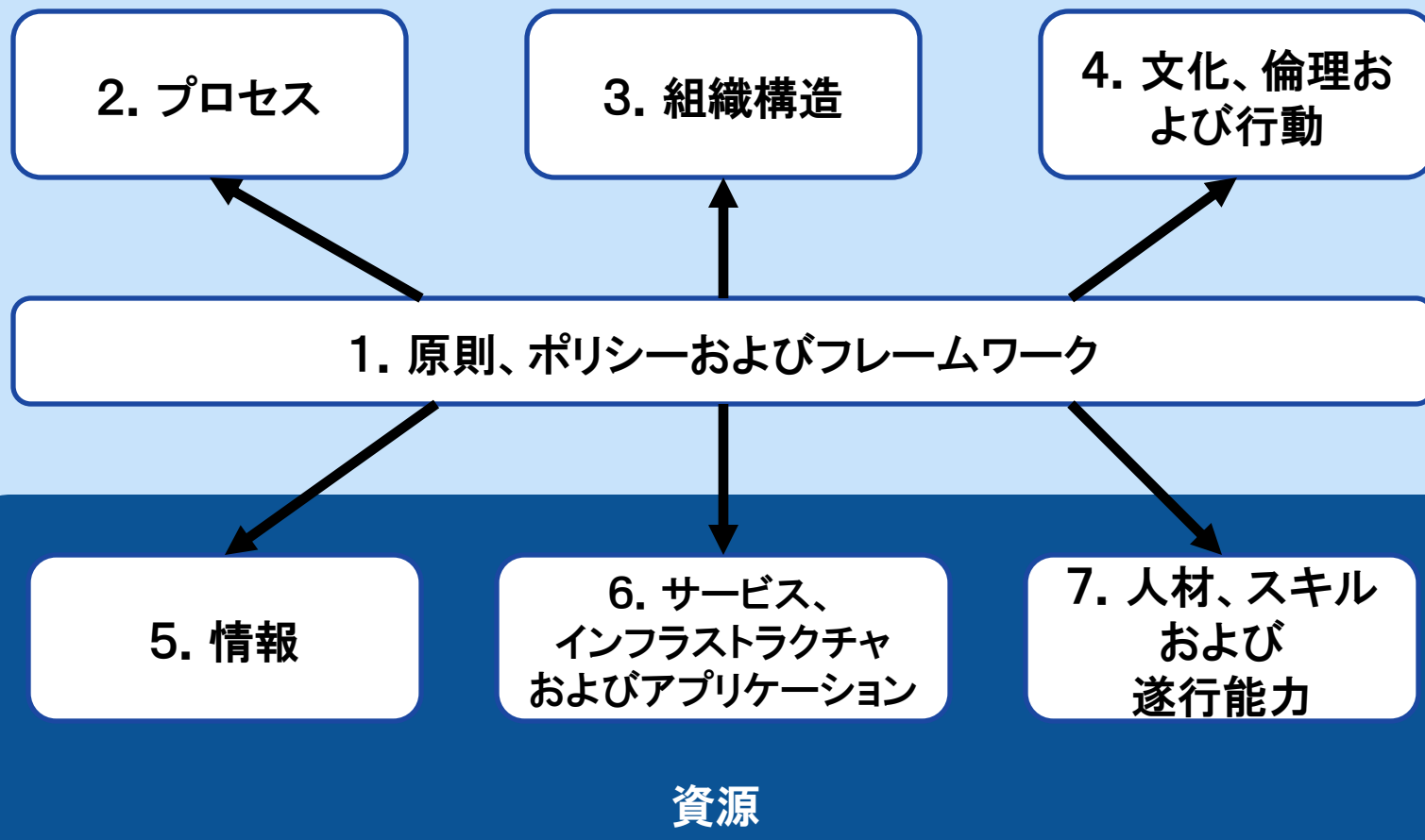
原則4. 包括的アプローチの実現

COBIT 5 のイネーブラー

- 事業体のITに関するガバナンスとマネジメントに対して、個々にかつ集合的に、影響を与える要因。
- 目標のカスケード(展開)により推進される。
- 7つのカテゴリーで記述。

原則4. 包括的アプローチの実現

COBIT 5の事業体のイネーブラー



原則4. 包括的アプローチの実現

1. **原則、ポリシーおよびフレームワーク**—要求される行動を日々のマネジメントの実践的なガイダンスに変換する手段。
2. **プロセス**—文書化され組織化された、確かな目標を達成しIT関連目標をサポートするアウトプットの集合を生み出すための実践と活動の組織化された集合を記述。
3. **組織構造**—組織における重要な意思決定の実体（エンティティ）。
4. **文化、倫理および行動**—各個人のものであり、組織のもの。多くの場合、ガバナンスとマネジメントの活動の成功要因として過小評価されている。
5. **情報**—いかなる組織でも全体に深く浸透しているもの。事業体で生み出され使用されている全情報が取り扱われる。情報はその組織の運営を維持し、うまくガバナンスされるために必要とされるが、運用レベルでは、多くの場合、情報が事業体そのものの重要な生産物。
6. **サービス、インフラストラクチャおよびアプリケーション**—情報技術処理とサービスを事業体に提供するインフラストラクチャ、技術およびアプリケーション。
7. **人、スキルおよび遂行能力**—人とリンクし、全ての活動がうまく完了し、正しい意思決定を行い、是正措置を行うために必要。

原則4. 包括的アプローチの実現

相互接続されたイネーブラー

- **インプット**

十分に効果的であるために他のイネーブラーからのインプットが必要。

例えば、プロセスは情報が必要であり、組織構造はスキルと行動が必要。

- **アウトプット**

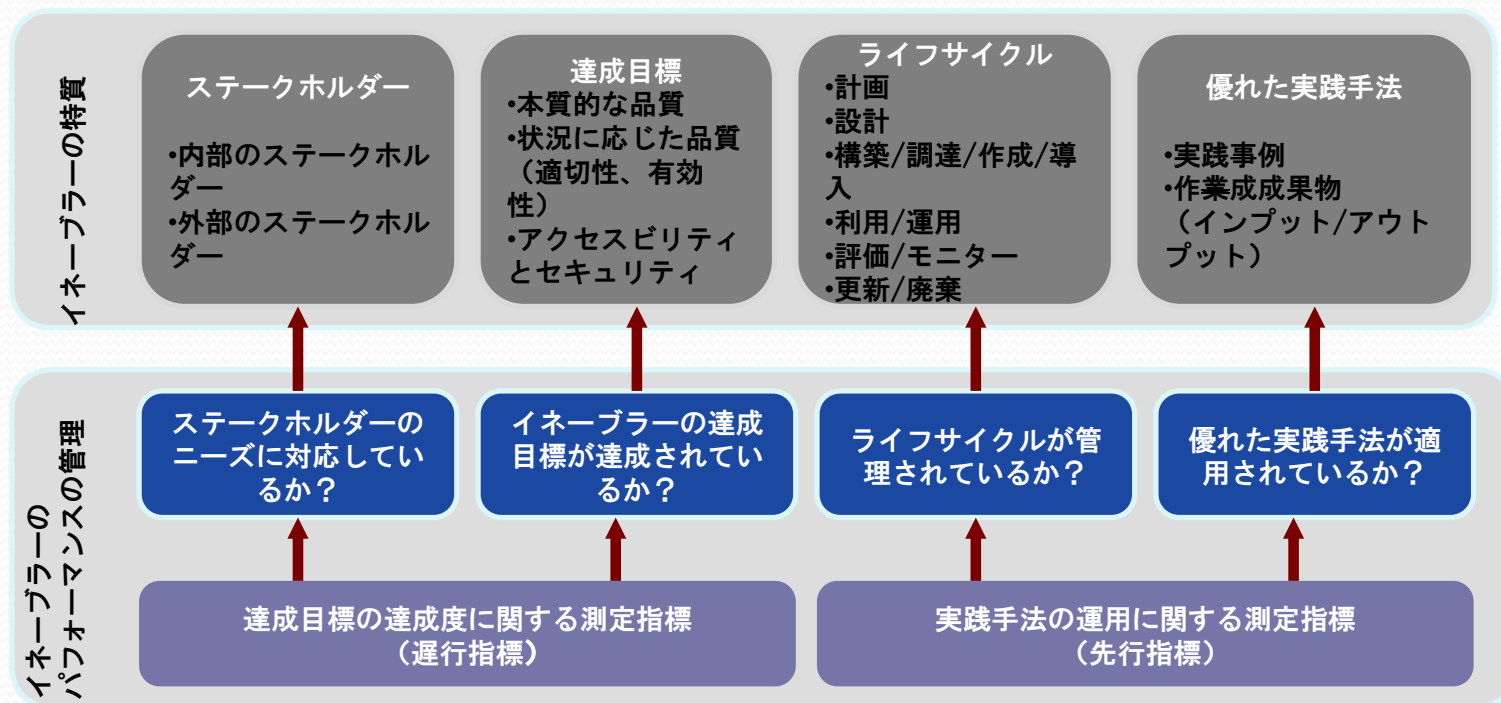
他のイネーブラーへ効果をもたらすアウトプットを提供。

例えば、プロセスは情報を提供し、スキルと行動はプロセスを効率化。

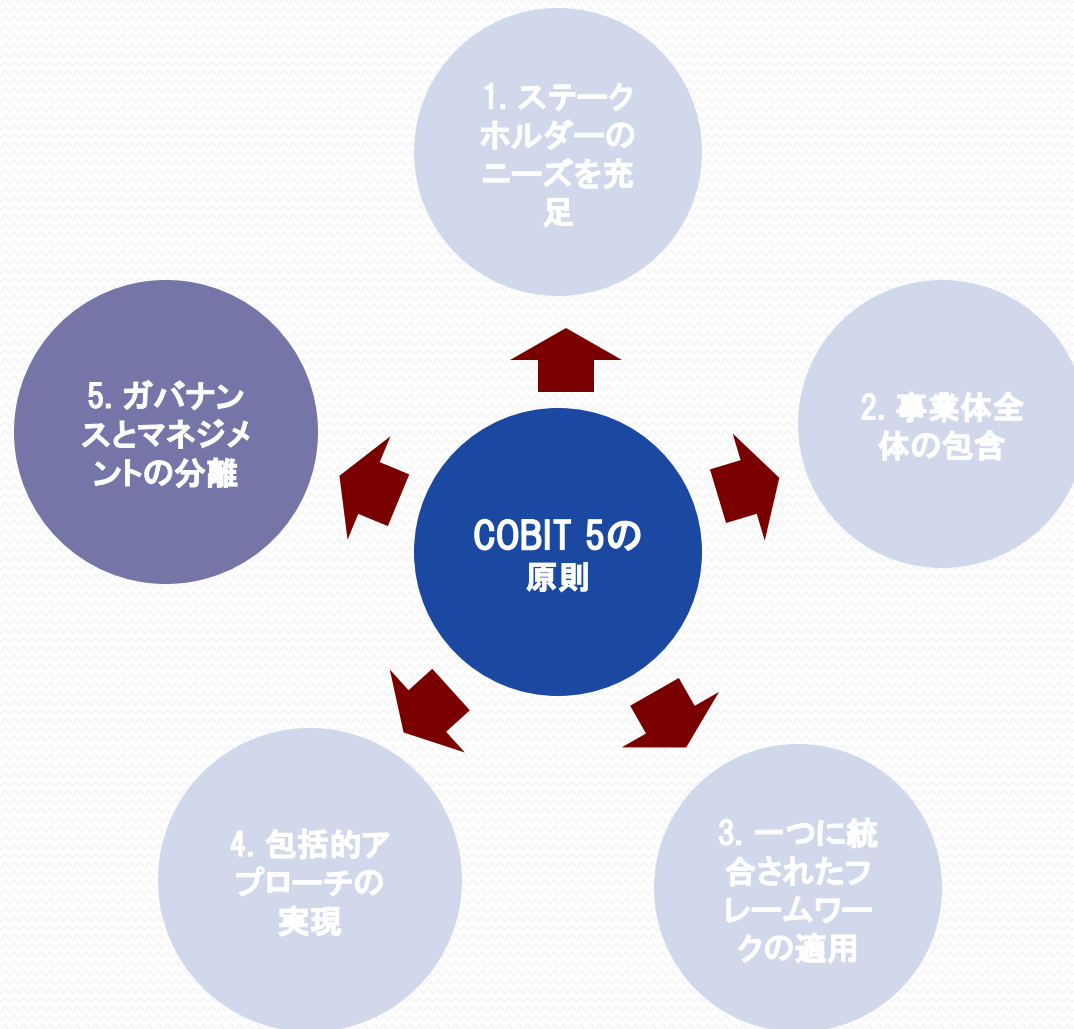
原則4. 包括的アプローチの実現

イネーブラーの特質

- 共通で、シンプルで構造化された方法を提供する
- 複雑な相互作用をマネジメントすることを可能とする
- 成果達成を手助けする。



COBIT 5の原則



出典: COBIT® 5 日本語版, 図表2. © 2012 ISACA® All rights reserved.

原則5. ガバナンスとマネジメントの分離

- **ガバナンスとマネジメントの間に明確な区別**
 - 異なるタイプの活動を包含する
 - 異なる組織構造を必要とする
 - 異なる目的を持つ
- **ガバナンス**—ほとんどの事業体において、ガバナンスは取締役会の責任であり、その取締役会議長のリーダーシップのもとにある。
- **マネジメント**—ほとんどの事業体において、マネジメントは経営幹部の責任であり、最高経営責任者（CEO）のリーダーシップのもとにある。

原則5. ガバナンスとマネジメントの分離

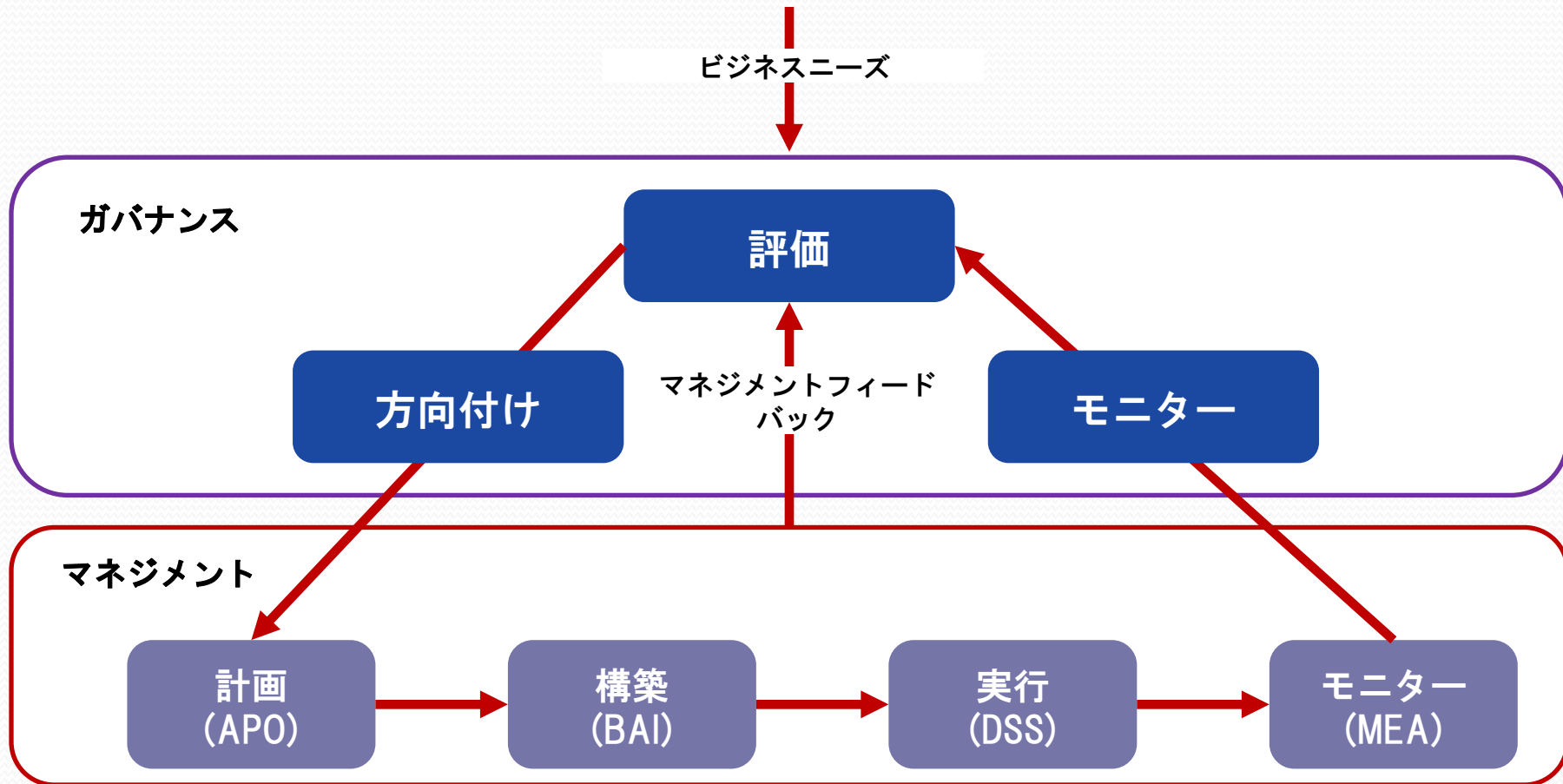
• **ガバナンスとは、バランスが取れ合意された達成すべき事業体の目標を決定するためにEDMサイクルを回すこと。**

- ステイクホルダーのニーズや、条件、選択肢を評価(Evaluate)
- 優先順位の設定と意思決定によって方向性を定め(Direct)
- 合意した方向性と目標に沿って成果や準拠性をモニター(Monitor)

• **マネジメントとは、事業体の目標の達成に向けてガバナンス主体が定めた方向性と整合するようにPBRMアクティビティを実行すること。**

- 計画(Plan)
- 構築(Build)
- 実行(Run)
- モニター(Monitor)

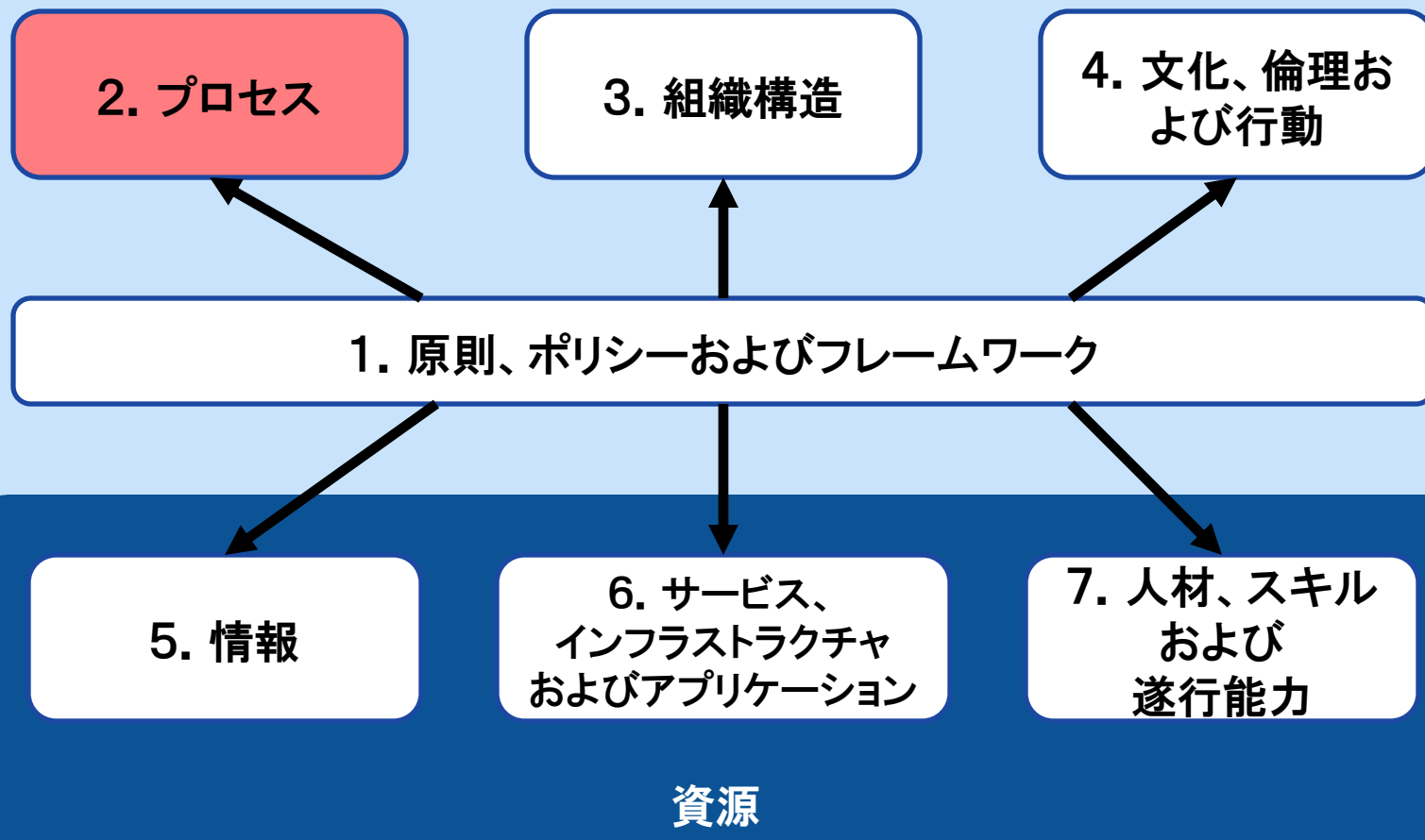
原則5. ガバナンスとマネジメントの分離



1-3. プロセス参照モデル

プロセス:イネーブラーの1つ

COBIT 5の事業体のイネーブラー



COBIT 5: Enabling Processes

COBIT 5 プロダクトファミリー

COBIT® 5

日本語化
済

COBIT 5イネーブラーガイド

COBIT® 5: Enabling Processes

日本語化
済

COBIT® 5: Enabling
Information

その他のイネーブラー
ガイド

COBIT 5プロフェッショナルガイド

COBIT® 5
Implementation
日本語化
済

COBIT® 5 for
Information Security

COBIT® 5 for
Assurance
日本語化
着手

COBIT® 5
for Risk

その他の
プロフェッショナル
ガイド

COBIT 5 オンライン コラボレーション環境

出典: COBIT® 5 日本語版, 図表11. © 2012 ISACA® All rights reserved.

COBIT Assessment Programme

COBIT® Process Assessment
Model (PAM): Using COBIT 5
日本語化
着手

COBIT® Assessor Guide:
Using COBIT 5

COBIT® Self-Assessment
Guide: Using COBIT 5

COBIT 5: Enabling Processes

- COBIT 5: Enabling Processesは、COBIT 5を補完し、COBIT 5プロセス参照モデルに定義されているプロセスに関する詳細な参照ガイドである。
 - 第1章 はじめに
 - 第2章 事業体とIT関連の達成目標のカスケード(展開)と測定指標
 - 第3章 COBIT 5 プロセスモデル
 - 第4章 COBIT 5 プロセス参照モデル
(プロセス参照モデルが図解されている)
 - 第5章 COBIT 5 プロセス参照ガイド
(COBIT 5 全37プロセスの詳細プロセス情報が記述されている)

COBIT 5: Enabling Processes

事業体のITガバナンスのためのプロセス 評価、方向付けおよびモニタリング

EDM01 ガバナンス
フレームワークの設
定と維持の確保

EDM02
効果提供の確保

EDM03
リスク最適化の確保

EDM04
資源最適化の確保

EDM01
ステークホルダーへ
の透明性の確保

整合、計画および組織化

AP001
ITマネジメント
フレームワークの
管理

AP002
戦略管理

AP003
エンタープライズ
アーキテクチャ管
理

AP004
イノベーション
管理

AP005
ポートフォリオ
管理

AP006
予算と費用の管
理

AP007
人材の管理

AP008
関係管理

AP009
サービス契約の管
理

AP010
サプライヤーの
管理

AP011
品質管理

AP012
リスク
管理

AP013
セキュリティ管
理

モニタリング、評価 およびアセスメント

MEA01
成果と整合性の
モニタリング、評価
およびアセスメント

構築、調達および導入

BAI01
プログラムと
プロジェクトの
管理

BAI02
要件定義の
管理

BAI03
ソリューションの
特定と構築の
管理

BAI04
可用性とキャパ
シティの管理

BAI05
組織の変革実現の
管理

BAI06
変更管理

BAI07
変更受入と
移行の管理

BAI08
知識の管理

BAI09
資産の管理

BAI10
構成の管理

MEA02
内部統制システムの
モニタリング、評価
およびアセスメント

提供、サービスおよびサポート

DSS01
オペレーション
管理

DSS02
サービス要求と
インシデントの
管理

DSS03
問題管理

DSS04
継続性
管理

DSS05
セキュリティ
サービスの管理

DSS06
ビジネスプロセス
のコントロールの
管理

MEA03
外部要求への
コンプライアンスの
モニタリング、評価
およびアセスメント

事業体のITマネジメントのためのプロセス

COBIT 5: Enabling Processes

- COBIT 5 プロセス参照モデルは、事業体におけるIT関連の実践と活動を2つの主要領域に分割。
 - ガバナンスドメインは5つのガバナンスプロセスで構成される。各プロセスの中に、評価、方向付け、モニタリング (EDM) の実践が定義されている。
 - 4つのマネジメントドメインは、計画、構築、実行およびモニター (PBRM) の責任領域に対応している。

1-4. 導入ガイダンス

COBIT 5 Implementation

COBIT 5 プロダクトファミリー

COBIT® 5

日本語化
済

COBIT 5イネーブラーガイド

COBIT® 5: Enabling Processes

日本語化
済

COBIT® 5: Enabling
Information

その他のイネーブラー
ガイド

COBIT 5プロフェッショナルガイド

COBIT® 5
Implementation

日本語化
済

COBIT® 5 for
Information Security

COBIT® 5 for
Assurance

日本語化
着手

COBIT® 5
for Risk

その他の
プロフェッショナル
ガイド

COBIT 5 オンライン コラボレーション環境

出典: COBIT® 5 日本語版, 図表11. © 2012 ISACA® All rights reserved.

COBIT Assessment Programme

COBIT® Process Assessment
Model (PAM): Using COBIT 5

日本語化
着手

COBIT® Assessor Guide:
Using COBIT 5

COBIT® Self-Assessment
Guide: Using COBIT 5

COBIT 5 Implementation

経営者の認識

- 事業体のITガバナンス(GEIT)の改善は、事業体ガバナンスにとって必須の部分
- 情報と情報技術(IT)は、ビジネスと社会生活の全ての局面でますます拡大
- IT投資からより多くの価値を生み出したい
- 増大するIT関連リスクをしっかりと管理したい
- 情報をビジネスで利用することにかかわる規制と法律の増大にしっかりと対応したい

COBIT 5 Implementation

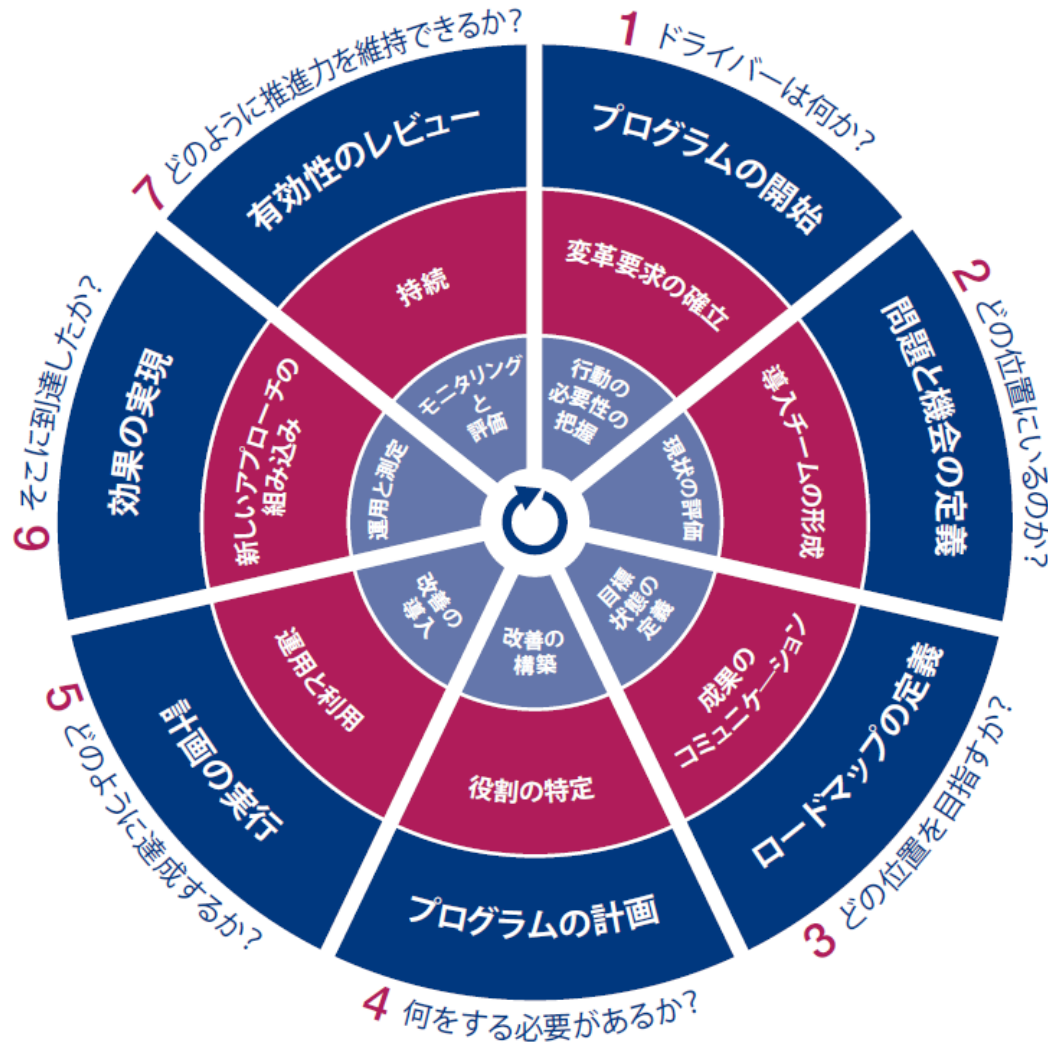
- COBIT 5は、良いGEITを導入するためのフレームワーク、ベストプラクティス、標準である。
 - フレームワーク、ベストプラクティス、標準は効果的に選択、適用されるべき
 - 成功のためには、乗り越えるべきチャレンジと課題がある
- COBIT5 Implementationは、これらを効果的に行うためのガイダンス。
- COBIT 5を活用したGEITの導入ガイダンス
～COBIT 5の導入ガイダンスではない

COBIT 5 Implementation

COBIT 5 Implementation の内容

- 事業体内におけるGEITの位置付け
- GEIT の改善に向けての第1歩を踏み出すこと
- 改善への挑戦と成功要因
- GEITに関連する組織および行動の変革の実現
- 変革実現とプログラム管理が含まれる継続的改善の導入
- COBIT 5 とその構成要素の利用

COBIT 5 Implementation



- プログラム管理 (外部リング)
- 変革の実現 (中間リング)
- 継続的改善ライフサイクル (内部リング)

1-5. プロセスアセスメントモデル

COBIT 5 プロダクトファミリー日本語版

COBIT 5 プロダクトファミリー

COBIT® 5

済

COBIT 5 イネーブラーガイド

COBIT® 5: Enabling Processes

済

COBIT® 5: Enabling Information

その他のイネーブラーガイド

COBIT 5 プロフェッショナルガイド

COBIT® 5 Implementation

済

COBIT® 5 for Information Security

COBIT® 5 for Assurance

着手

COBIT® 5 for Risk

その他のプロフェッショナルガイド

COBIT 5 オンライン コラボレーション環境

出典: COBIT® 5 日本語版, 図表11. © 2012 ISACA® All rights reserved.

COBIT Assessment Programme

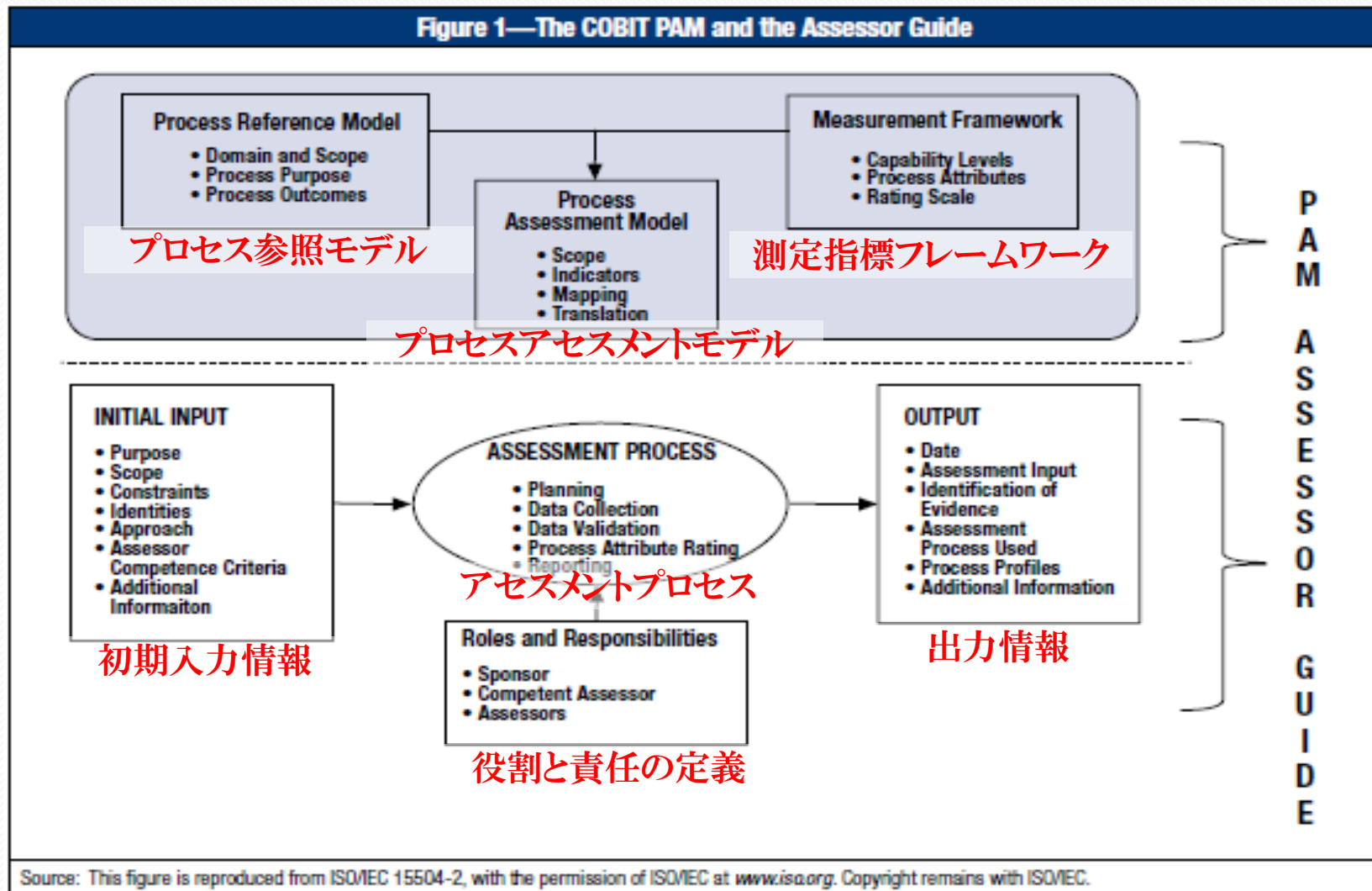
COBIT® Process Assessment Model (PAM): Using COBIT 5

着手

COBIT® Assessor Guide: Using COBIT 5

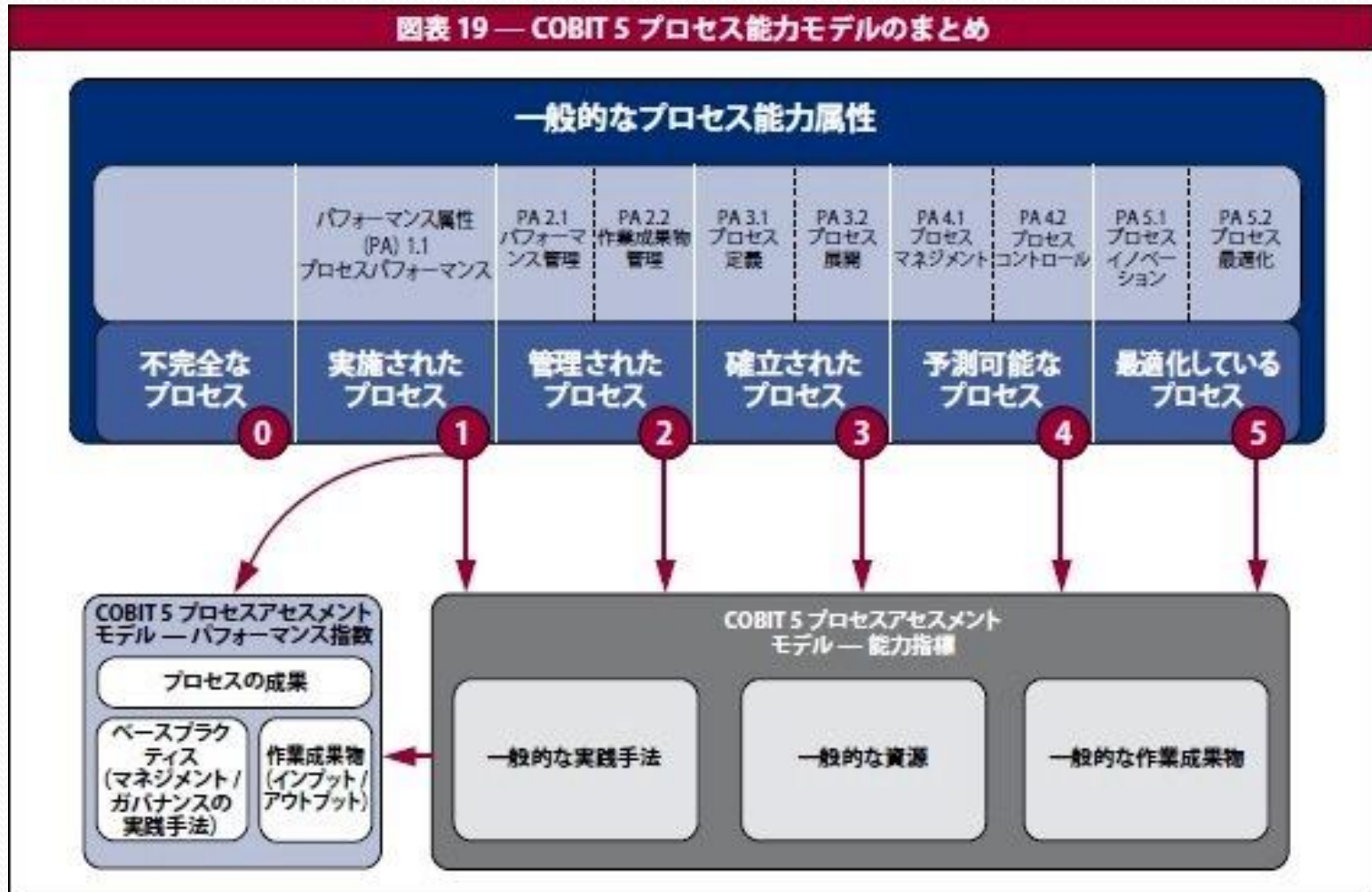
COBIT® Self-Assessment Guide: Using COBIT 5

アセスメントモデルとアセッサーガイド

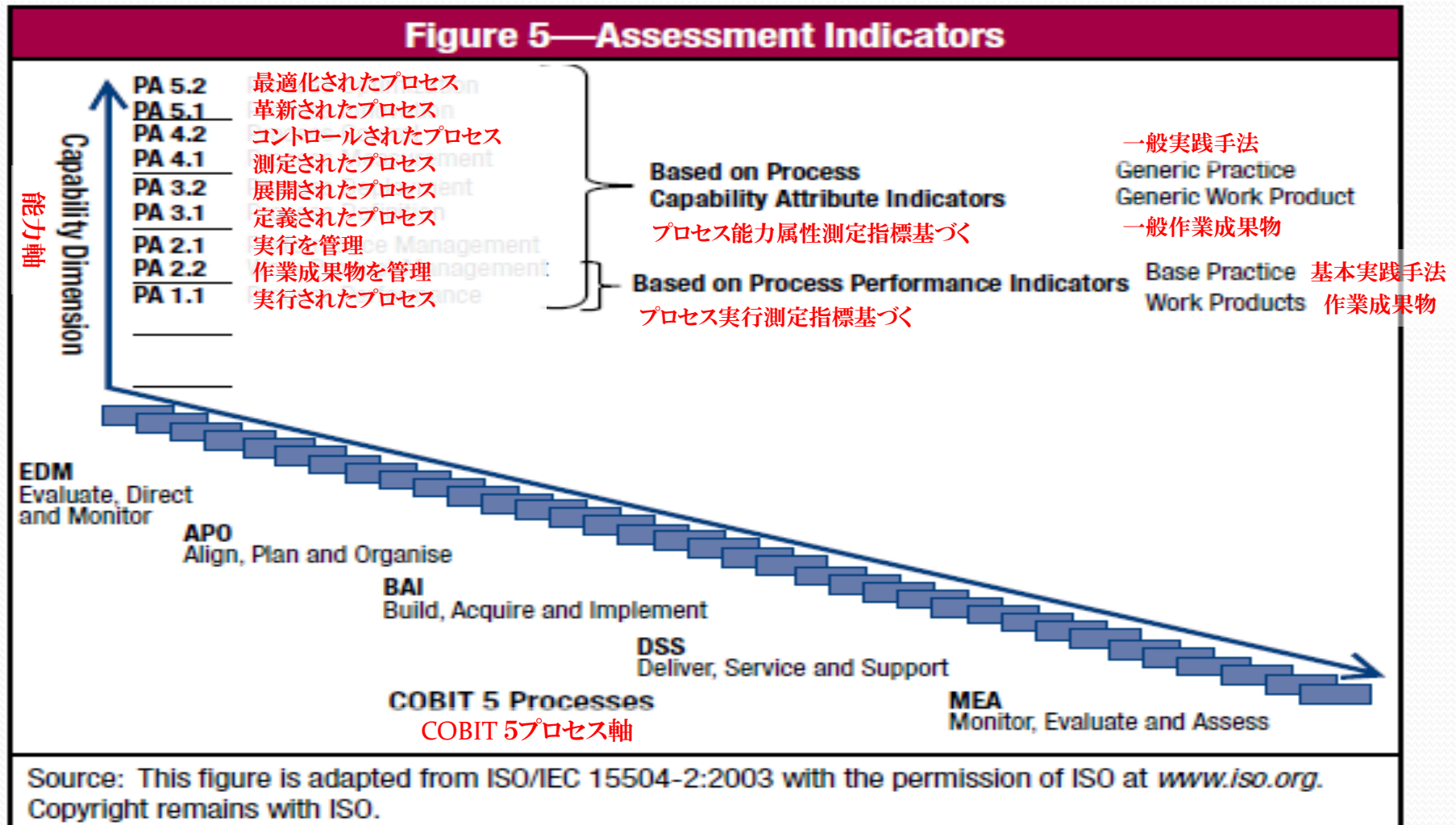


COBIT 5 プロセス能力モデル

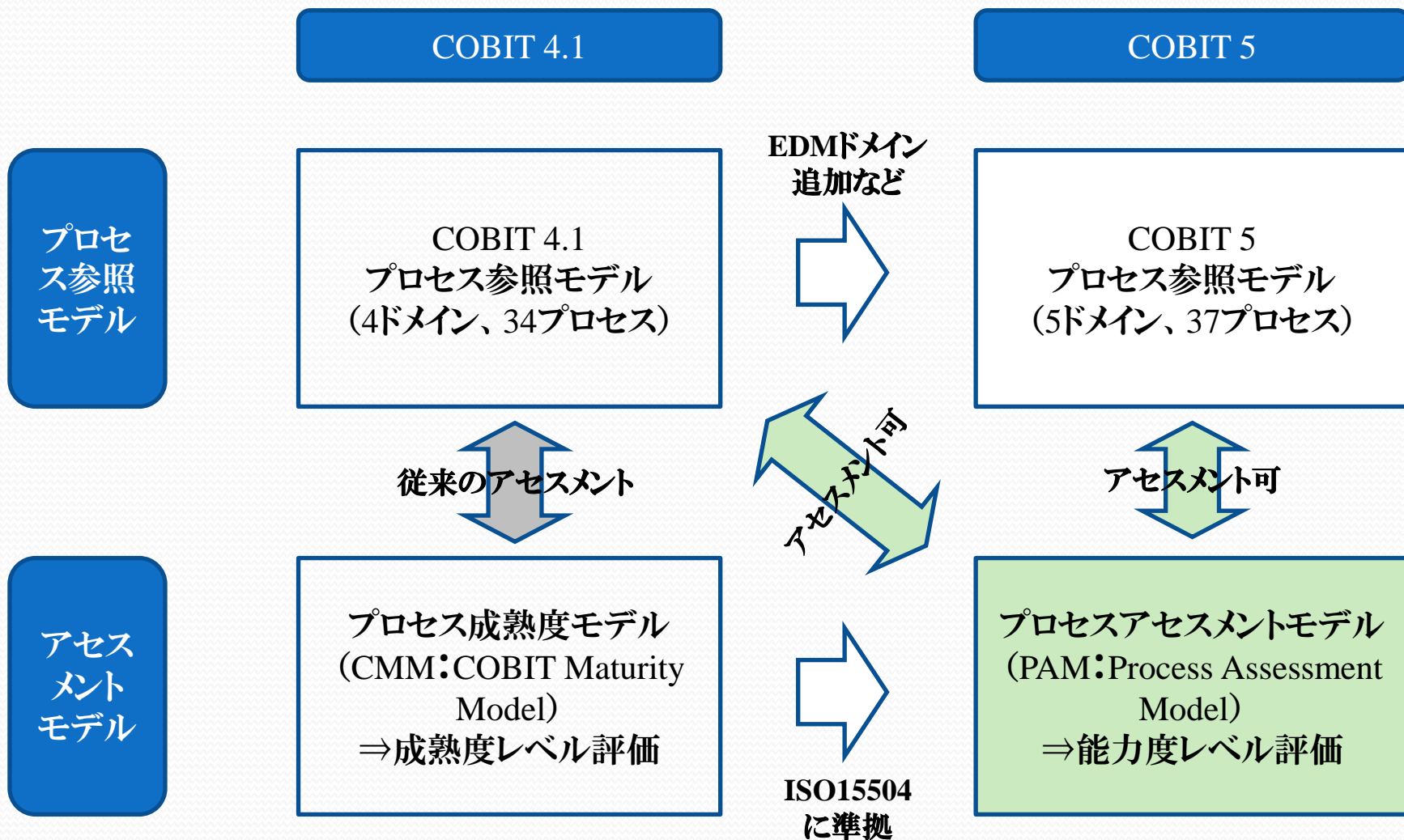
図表 19 — COBIT 5 プロセス能力モデルのまとめ



アセスメント指標



新COBITアセスメントプログラムとは



アセスメントモデル比較

COBIT 4.1 成熟度モデルレベル	COBIT 5 (ISO/IEC 15504) に基づいたプロセス能力	コンテキスト
5 最適化されている	レベル 5: 最適化しているプロセス	事業体の視点 — 企業の知識
4 管理され、測定可能である	レベル 4: 予測可能なプロセス	
3 定義されたプロセス	レベル 3: 確立されたプロセス	
	レベル 2: 管理されたプロセス	
2 繰り返し可能だが直感的	レベル 1: 実施されたプロセス	インスタンスの視点 — 個人の知識
1 初期 / アドホック		
0 存在しない	レベル 0: 不完全なプロセス	

【第2部】

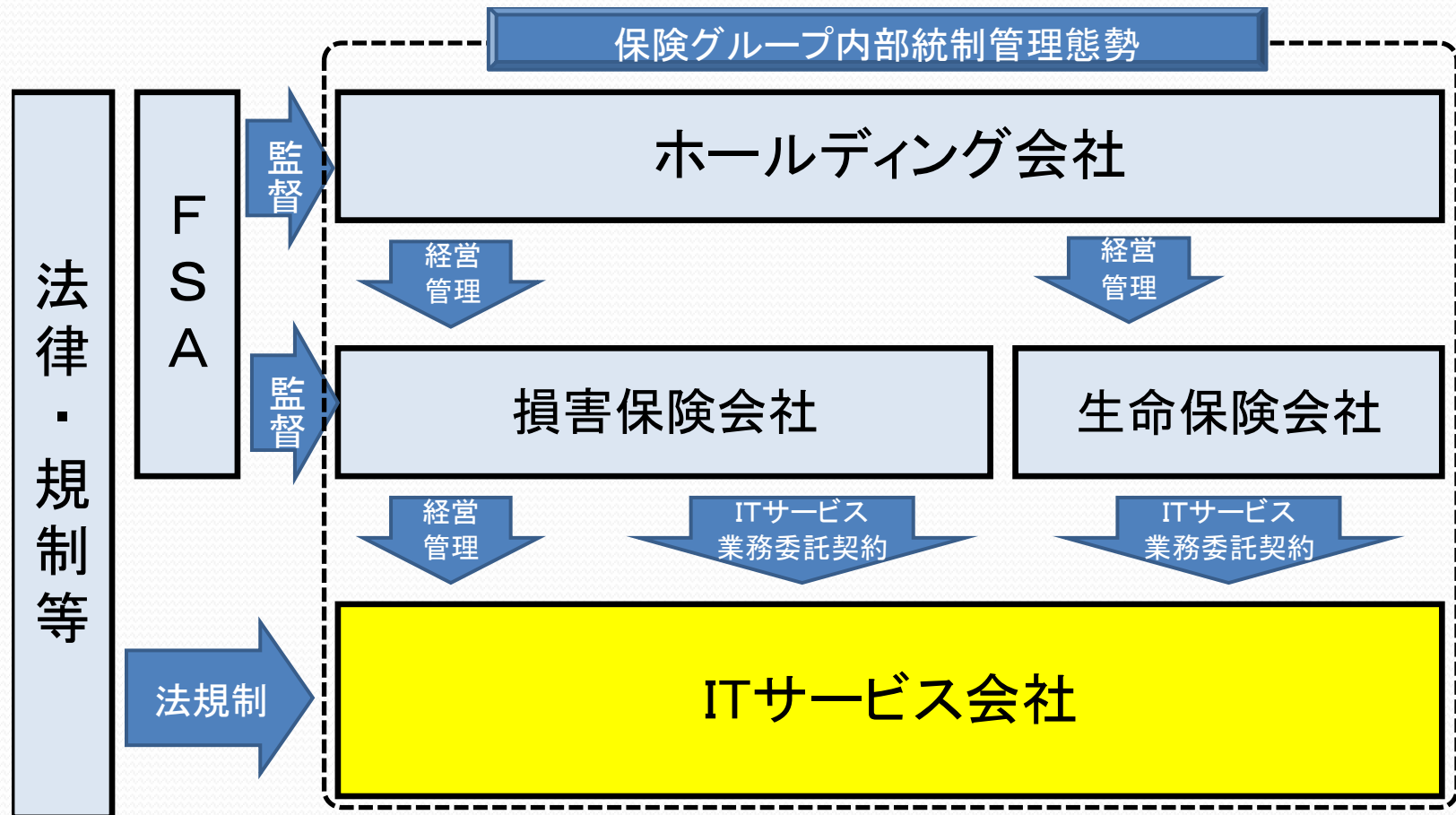
実践事例による解説

2-1. ITサービス会社のGRC態勢

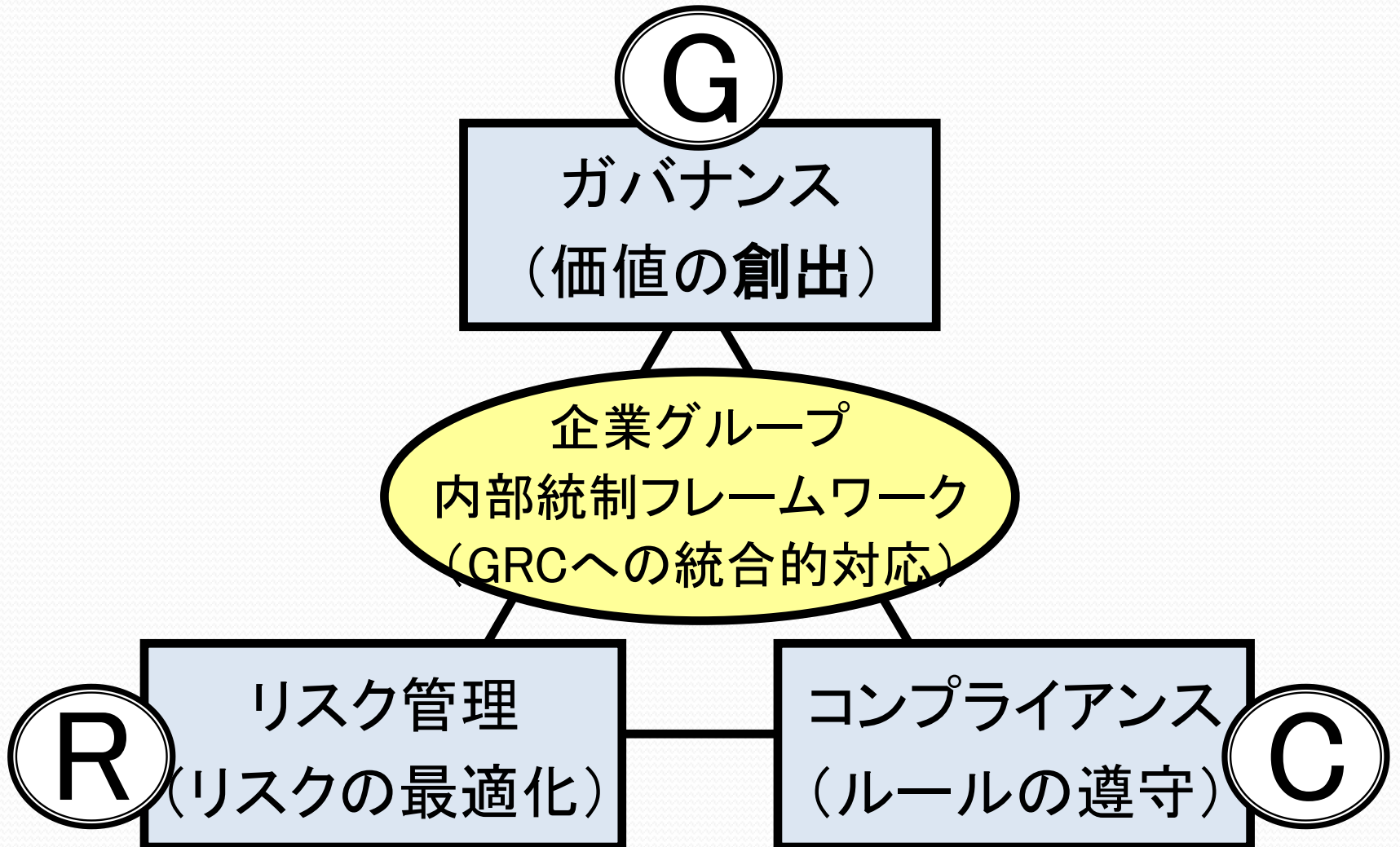
COBIT 5実践事例による解説

- ✓ COBIT 5を理解する最善の方法－それは実践事例による解説ではないか。
- ✓ 保険グループにおけるITサービス会社の事例を紹介
- ✓ COBIT 5を参考にし、部分的に適用して、GRC態勢を構築
- ✓ COBIT 5の「ひとつの使い方事例」として

保険グループのITサービス会社

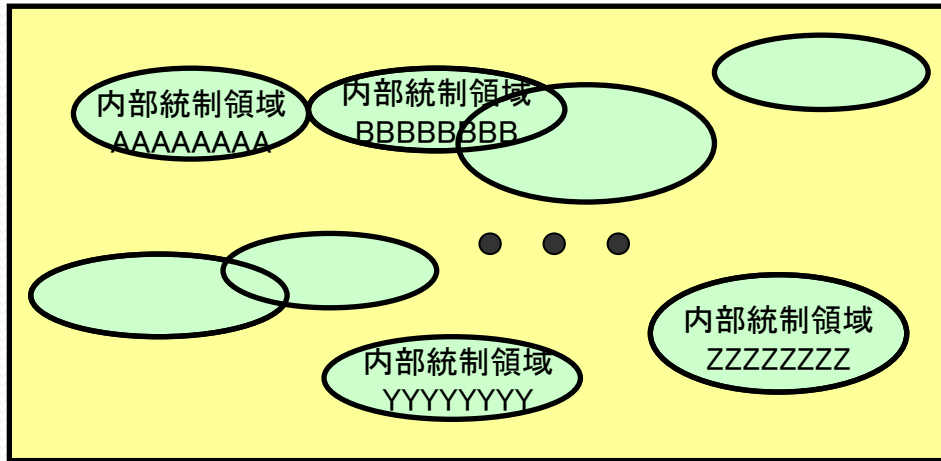


ITサービス会社のGRCの概念



保険グループの内部統制フレームワーク

グループ各社の内部統制領域



各イネーブラーの目標を設定



内部統制に関する基本方針の雛形

[グループ会社名]
□□□□□□□□に関する基本方針

- 第1条(目的)
...
- 第2条(定義等)
...
- 第3条(基本的考え方)
...
- 第4条(態勢の整備)
...
- 第5条(子会社としての役割)
...
- 第6条(改廃)
...

各内部統制領域に関する
基本方針を明確化

内部統制に関する
基本方針体系

内部統制
基本方針

AAAAAAAA
に関する
基本方針

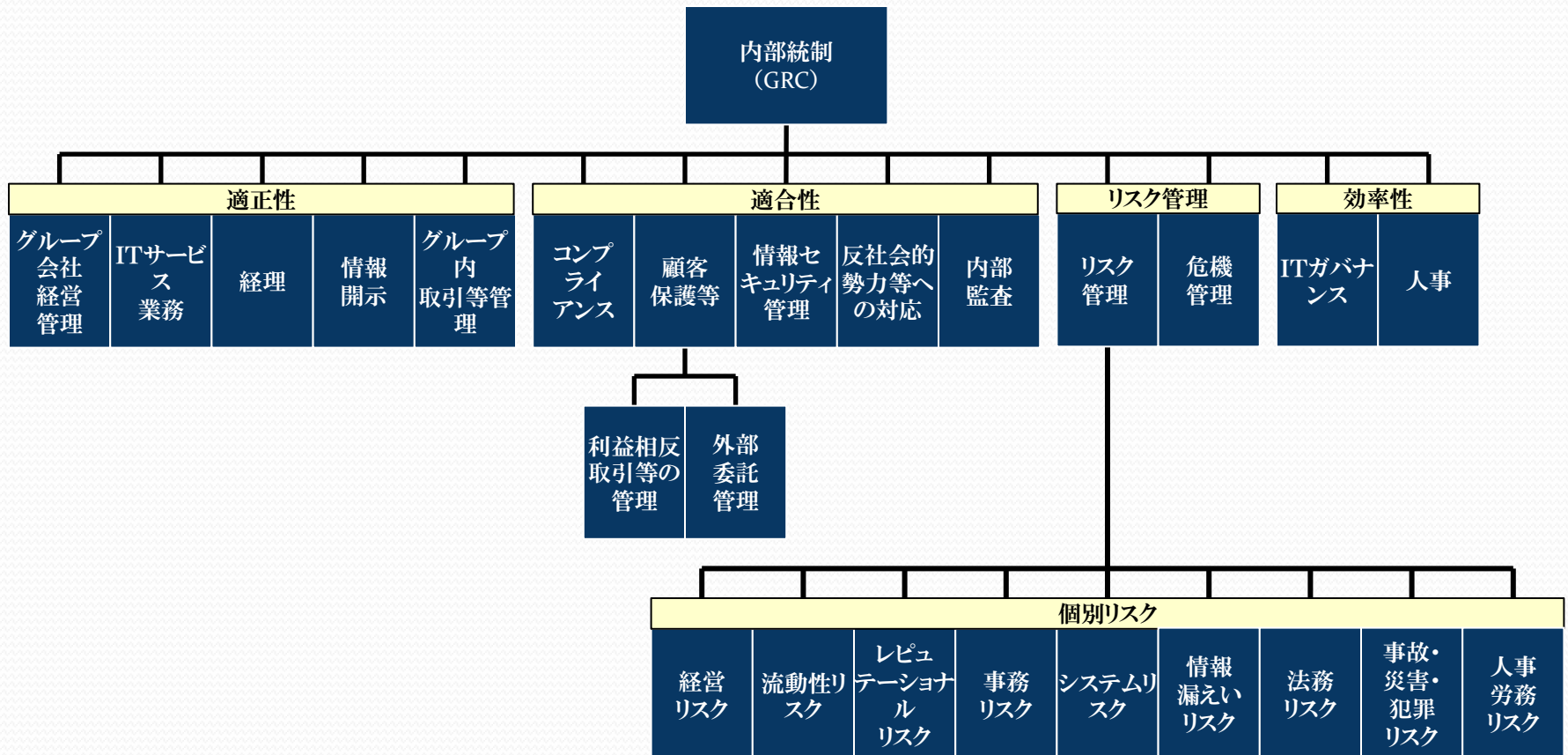
BBBBBBBB
に関する
基本方針

YYYYYYYY
に関する
基本方針

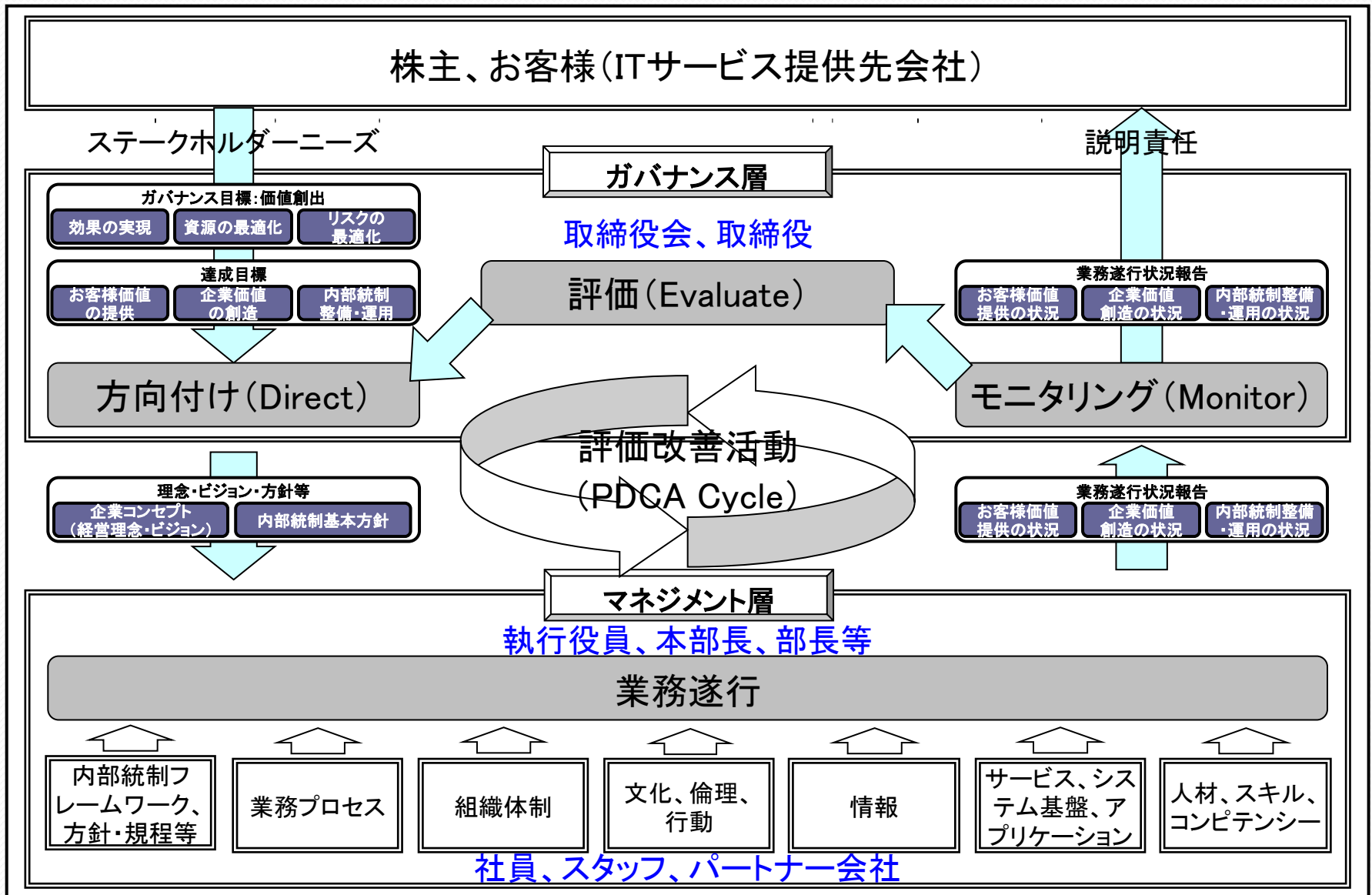
ZZZZZZZZ
に関する
基本方針

ITサービス会社のGRC領域

● 内部統制領域 (GRC領域)



ITサービス会社のGRC態勢



ステークホルダーニーズ

ガバナンス目標: 価値創出

効果の実現

資源の最適化

リスクの最適化

達成目標

お客様価値の提供

企業価値の創造

内部統制整備・運用

プロジェクトサービスイン、SLA達成など

人材育成、業務領域拡大など

内部統制・リスク管理をしっかりと

方向付け
(Direct)

理念・ビジョン・方針等

企業コンセプト
(経営理念・ビジョン)

内部統制基本方針

イネーブラー目標を具体的に表現

説明責任

業務遂行状況報告

お客様価値提供の状況

企業価値創造の状況

内部統制整備・運用の状況

プロジェクトサービスイン、SLA達成など

人材育成、業務領域拡大など

内部統制・リスク管理をしっかりと

モニタリング
(Monitor)

業務遂行状況報告

お客様価値提供の状況

企業価値創造の状況

内部統制整備・運用の状況

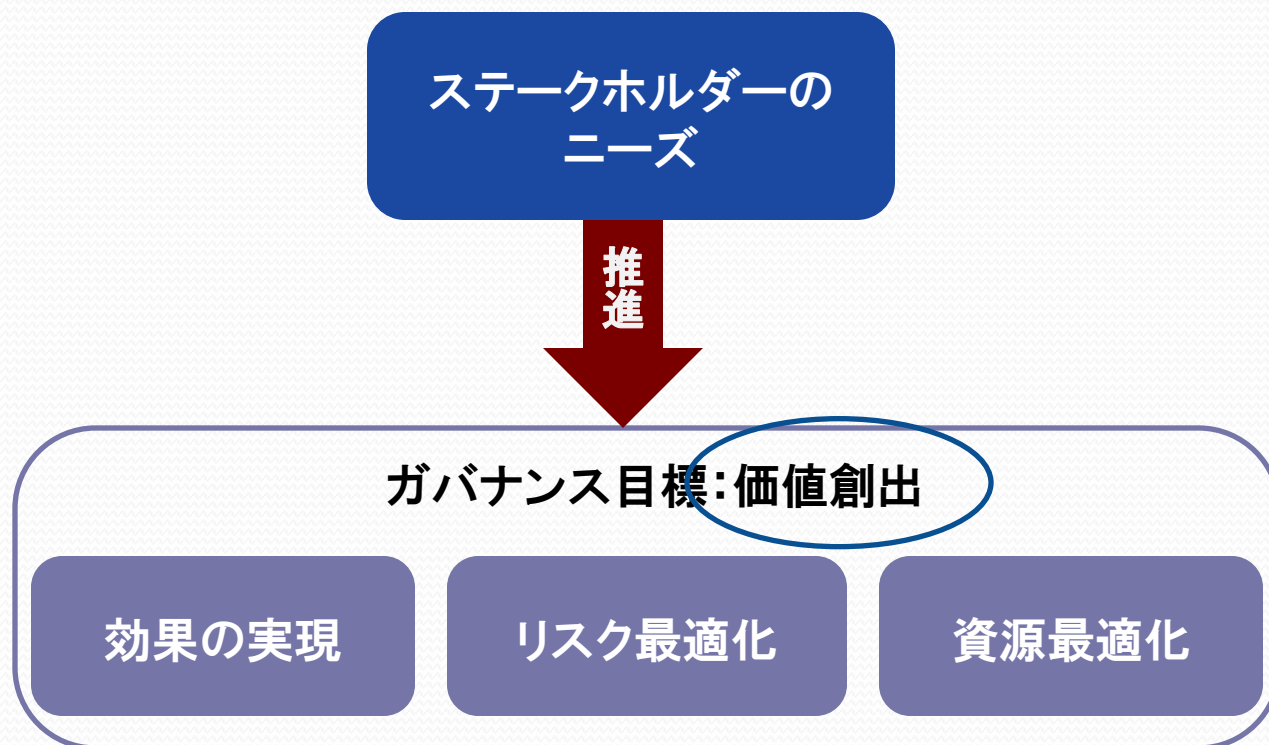
ステークホルダーニーズの充足状況
イネーブラー目標の達成状況
ライフサイクルの管理状況
優れた実践手法の適用状況

2-2. COBIT 5の適用方法

2-2-1 原則1の適用

原則1. ステークホルダーのニーズを充足

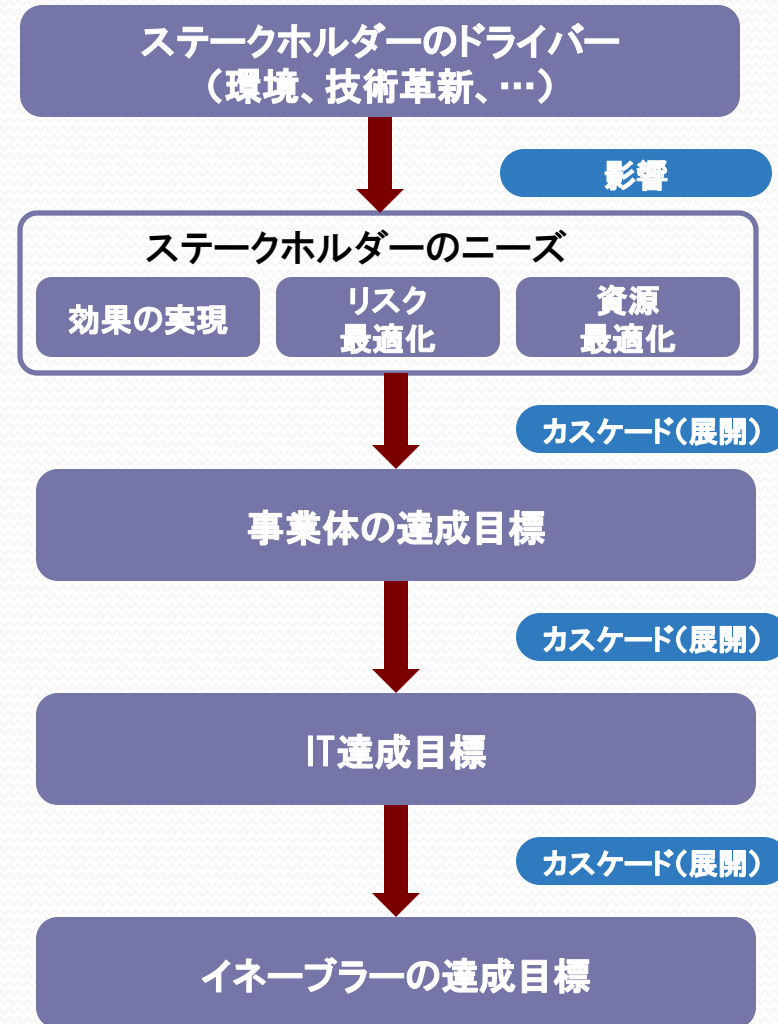
- 事業体はそのステークホルダーの価値を創出するために存在する。



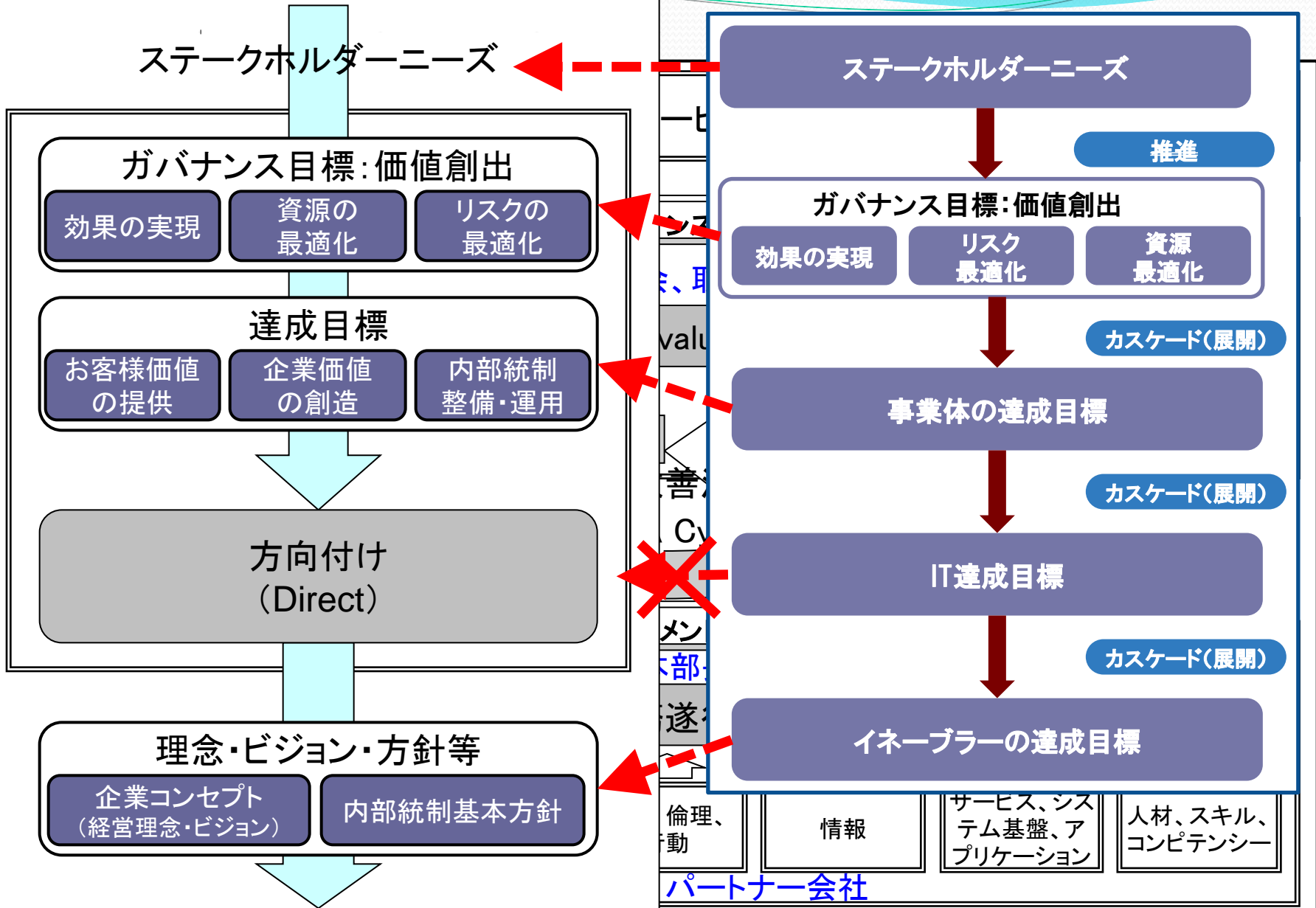
原則1. ステークホルダーのニーズを充足

- ステークホルダーのニーズを事業体の戦略に変換
- COBIT 5の達成目標のカスケード(展開)

ステークホルダーのニーズから
➡ 事業体の達成目標
➡ IT達成目標
➡ イネーブラーの達成目標
へ展開する



「原則1:ステークホルダーニーズの充足」適用



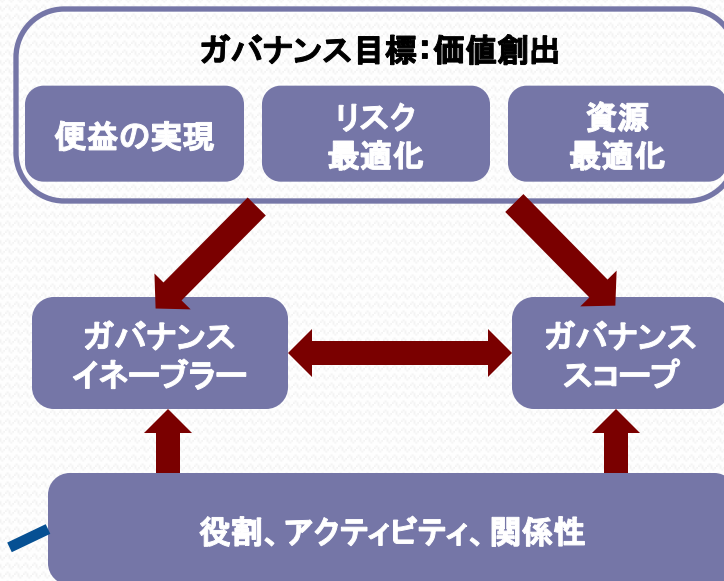
2-2-2 原則2の適用

原則2. 事業体全体の包含

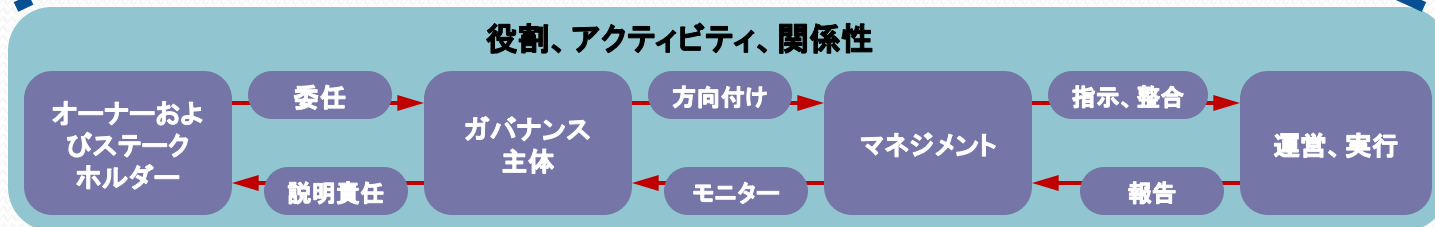
- 事業体全体にわたる**包括的な視点**から、**情報とそれに関連する技術のガバナンスとマネジメント**を取り扱う。
- 事業体の中の**全ての部門**、**全てのプロセス**をカバー。
- 事業体ITガバナンス(GEIT)はコーポレートガバナンス(ビジネスガバナンス)そのもの。

原則2. 事業体全体の包含

ガバナンスのアプローチ



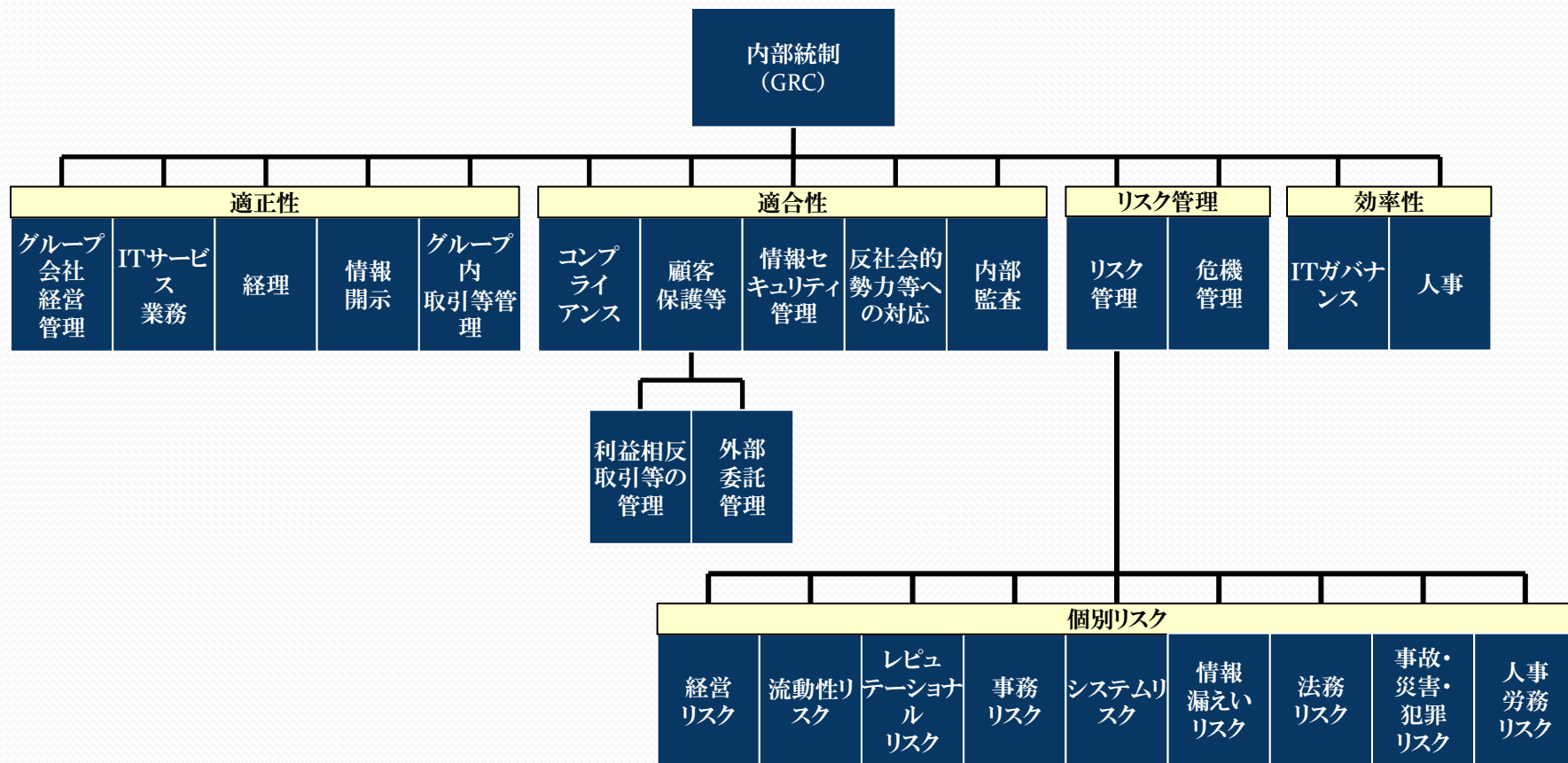
出典: COBIT® 5 日本語版, 図表8. © 2012 ISACA® All rights reserved.



出典: COBIT® 5 日本語版, 図表9. © 2012 ISACA® All rights reserved.

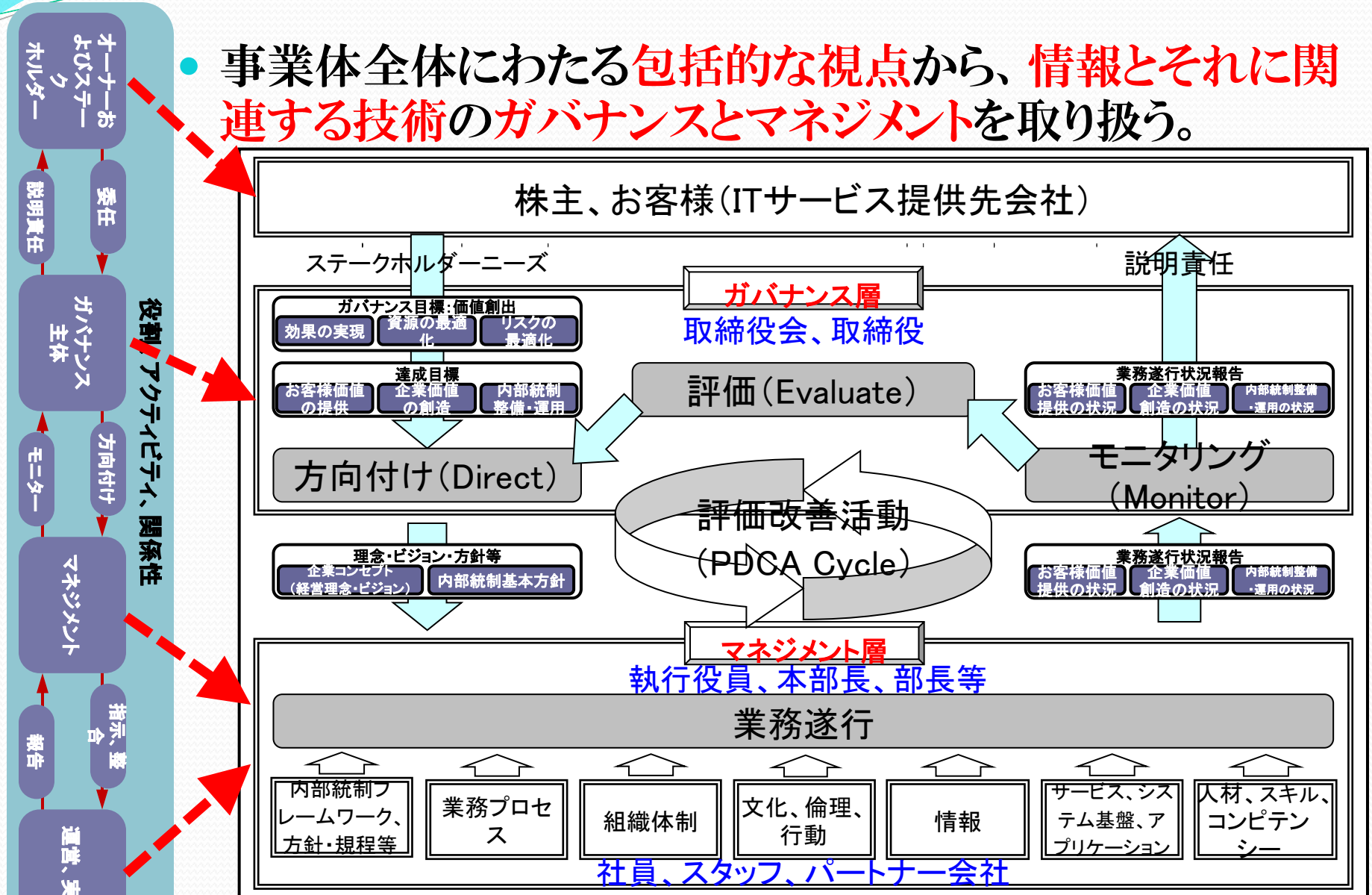
「原則2:事業体全体の包含」の適用

事業体の中の**全ての部門**、**全てのプロセス**をカバー。



「原則2: 事業体全体の包含」の適用

- 事業体全体にわたる**包括的な視点**から、**情報とそれに関連する技術のガバナンスとマネジメント**を取り扱う。



2-2-3 原則3の適用

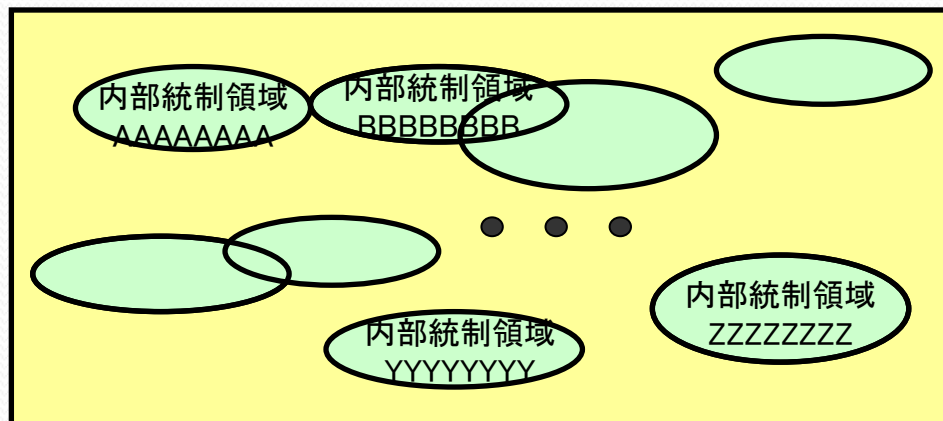
原則3. 一つに統合されたフレームワークの適用

- 最新の関連する他の標準やフレームワークと整合
 - 事業体: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000
 - IT関連: ISO/IEC 38500, ITIL, ISO/IEC 27000シリーズ, TOGAF, PMBOK/PRINCE2, CMMI
- ガバナンスとマネジメントのフレームワークを統合するものとして利用可能

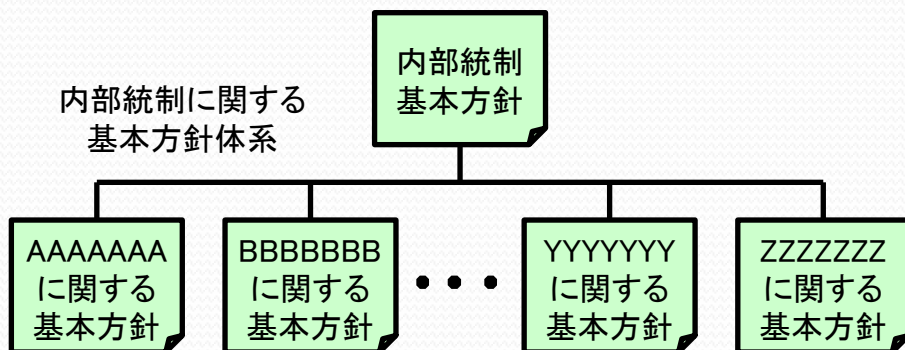
「原則3:1つに統合されたフレームワークの適用」 の適用

全てのGRC領域(=内部統制領域)に
保険グループの内部統制フレームワークを適用

グループ各社の内部統制領域



各内部統制領域に関する
基本方針を明確化



各イネーブラーの目標を設定

内部統制に関する基本方針の雛形

[グループ会社名]
□□□□□□□□に関する基本方針

第1条(目的)
…
第2条(定義等)
…
第3条(基本的考え方)
…
第4条(態勢の整備)
…
第5条(子会社としての役割)
…
第6条(改廃)
…

「原則3:1つに統合されたフレームワークの適用」の適用

- 保険グループの内部統制フレームワークを使い、各GRC領域ごとに基本方針を定義
- これら基本方針の下、配下の規程・基準にCOBIT 5等を参考として活用

保険グループ内部統制フレームワーク

COBIT 5 Framework
(GRC全体)

COBIT 5 Enabling Processes
(モニタリング)

ITIL
(ITサービス業務:運用)

CMMI
(ITサービス業務:開発)

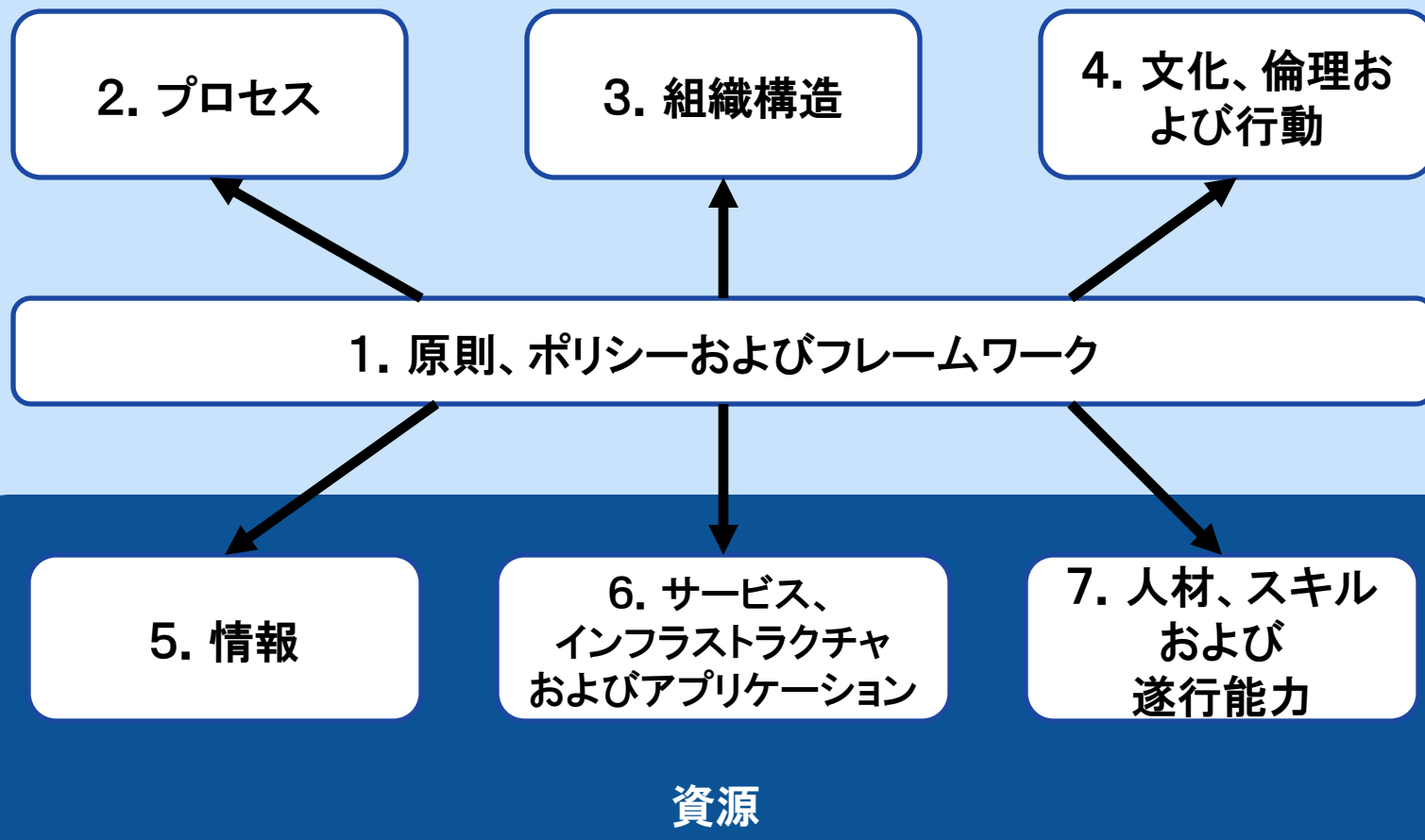
COBIT 4.1 PRM、成熟度モデル
(ITガバナンス領域)

PIMBOK
(プロジェクト管理)

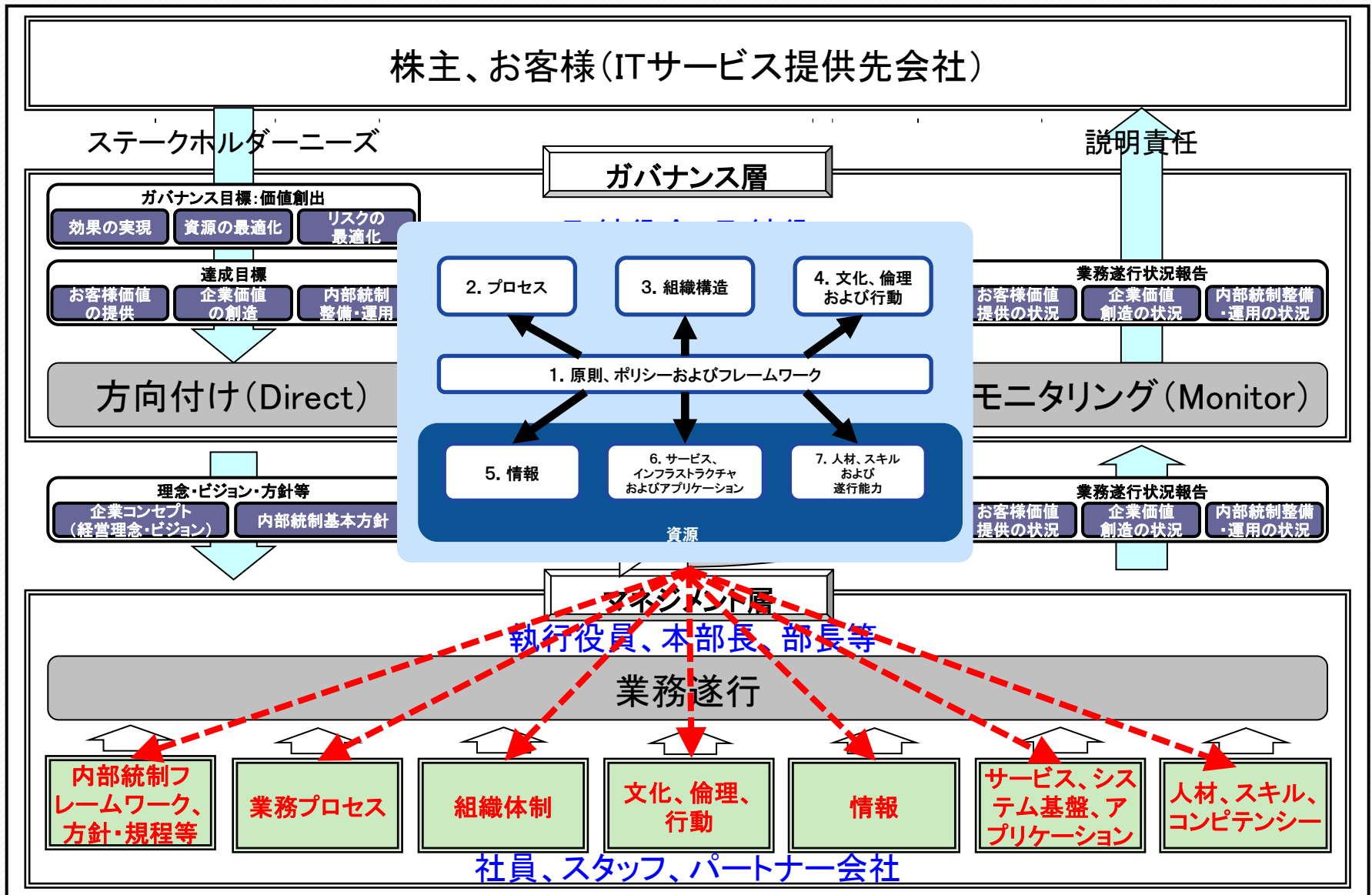
2-2-4 原則4の適用

原則4. 包括的アプローチの実現

COBIT 5の事業体のイネーブラー

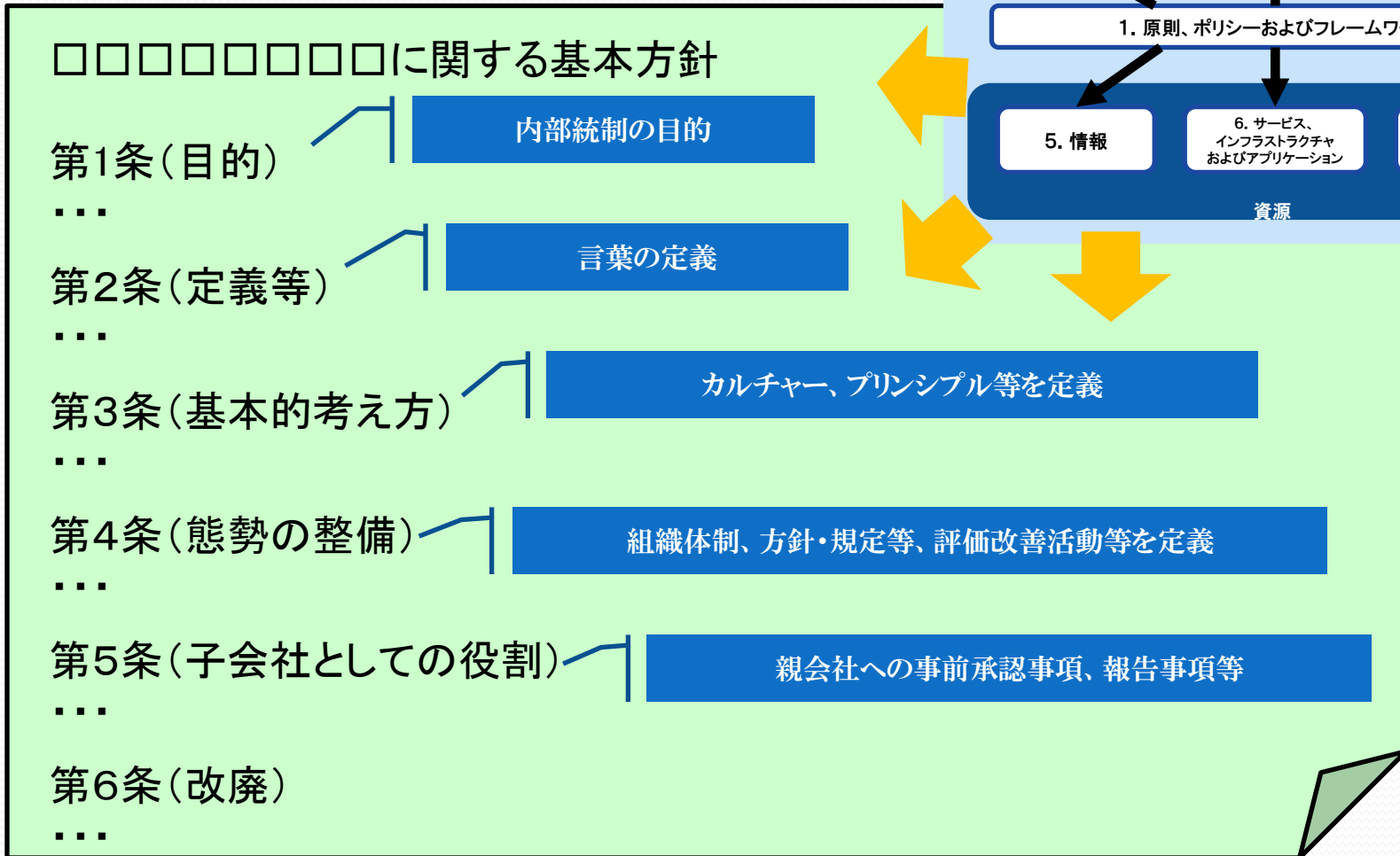


「原則4: 包括的なアプローチの実現」の適用



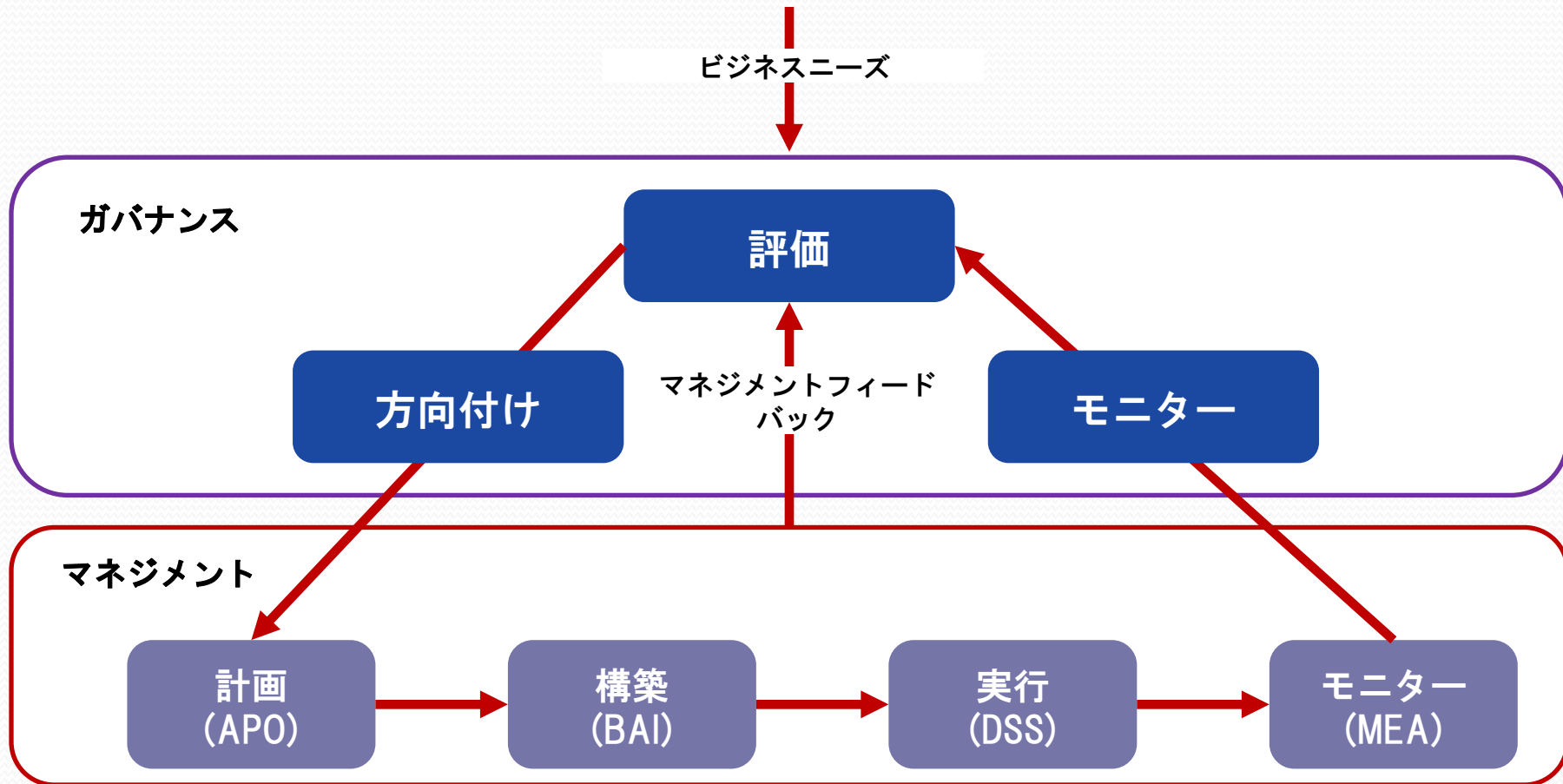
「原則4:包括的なアプローチの実現」の適用

各イネーブラー目標を内部統制
基本方針や配下規程・基準に盛り込む。

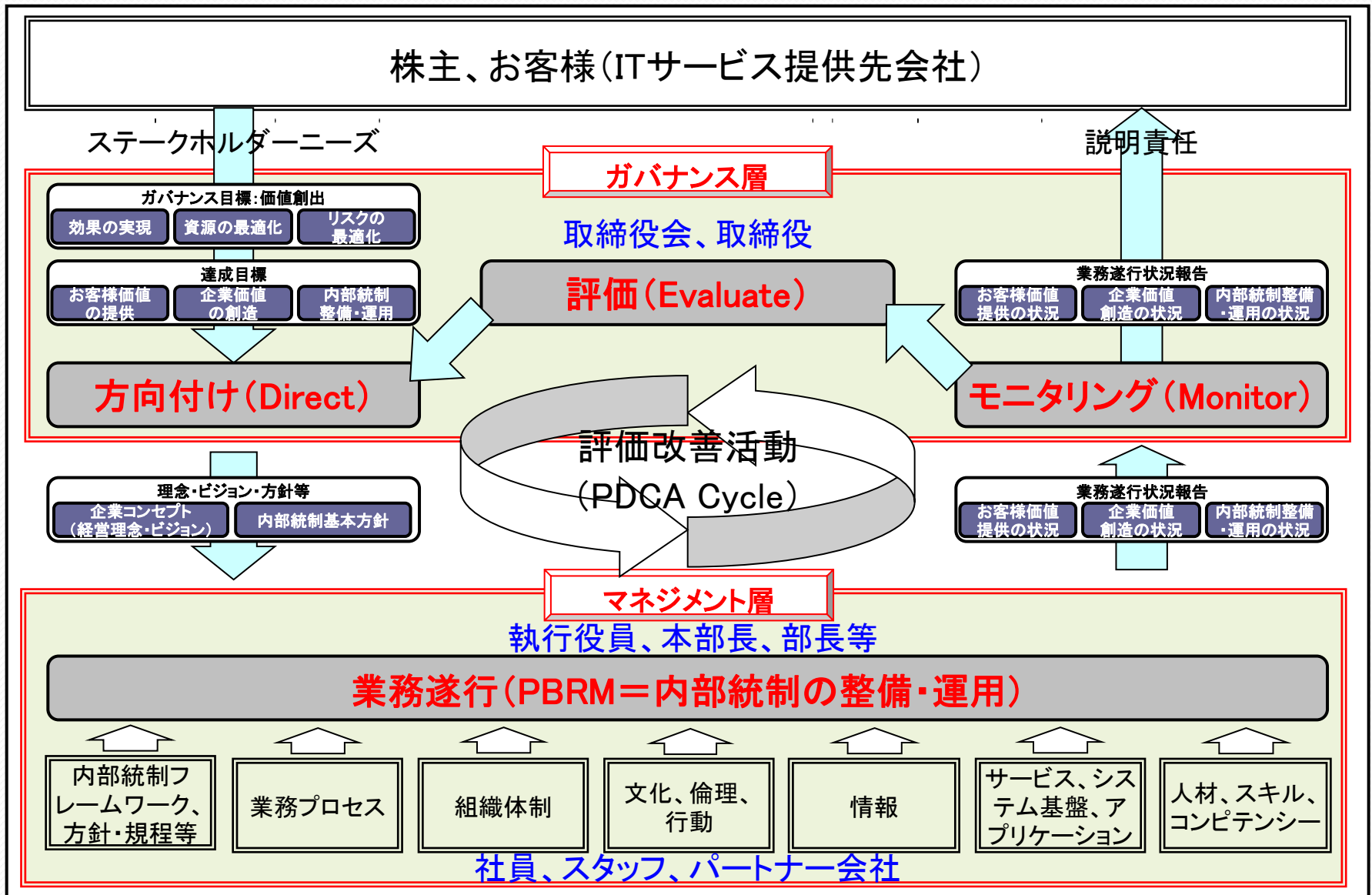


2-2-5 原則5の適用

原則5. ガバナンスとマネジメントの分離



「原則5:ガバナンスとマネジメントの分離」



2-2-6 プロセス参照モデルの適用

COBIT 5: Enabling Processes

事業体のITガバナンスのためのプロセス

評価、方向付けおよびモニタリング

EDM01 ガバナンス
フレームワークの設
定と維持の確保

EDM02
効果提供の確保

EDM03
リスク最適化の確保

EDM04
資源最適化の確保

EDM01
ステークホルダーへ
の透明性の確保

整合、計画および組織化

AP001
ITマネジメント
フレームワークの
管理

AP002
戦略管理

AP003
エンタープライズ
アーキテクチャ管
理

AP004
イノベーション
管理

AP005
ポートフォリオ
管理

AP006
予算と費用の管
理

AP007
人材の管理

AP008
関係管理

AP009
サービス契約の管
理

AP010
サプライヤーの
管理

AP011
品質管理

AP012
リスク
管理

AP013
セキュリティ管
理

モニタリング、評価 およびアセスメント

MEA01
成果と整合性の
モニタリング、評価
およびアセスメント

MEA02
内部統制システムの
モニタリング、評価
およびアセスメント

MEA03
外部要求への
コンプライアンスの
モニタリング、評価
およびアセスメント

構築、調達および導入

BAI01
プログラムと
プロジェクトの
管理

BAI02
要件定義の
管理

BAI03
ソリューションの
特定と構築の
管理

BAI04
可用性とキャパ
シティの管理

BAI05
組織の変革実現の
管理

BAI06
変更管理

BAI07
変更受入と
移行の管理

BAI08
知識の管理

BAI09
資産の管理

BAI10
構成の管理

提供、サービスおよびサポート

DSS01
オペレーション
管理

DSS02
サービス要求と
インシデントの
管理

DSS03
問題管理

DSS04
継続性
管理

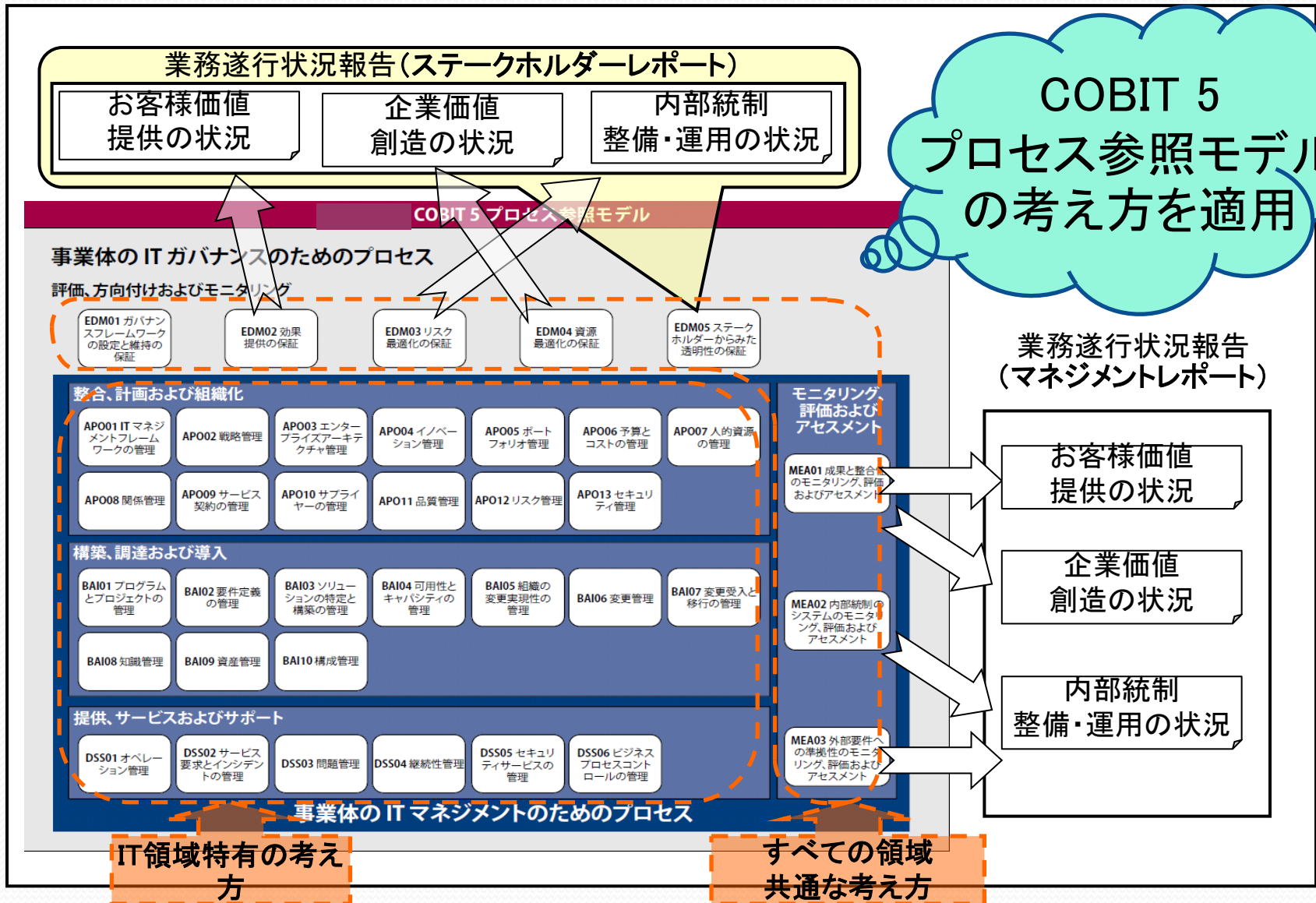
DSS05
セキュリティ
サービスの管理

DSS06
ビジネスプロセス
のコントロールの
管理

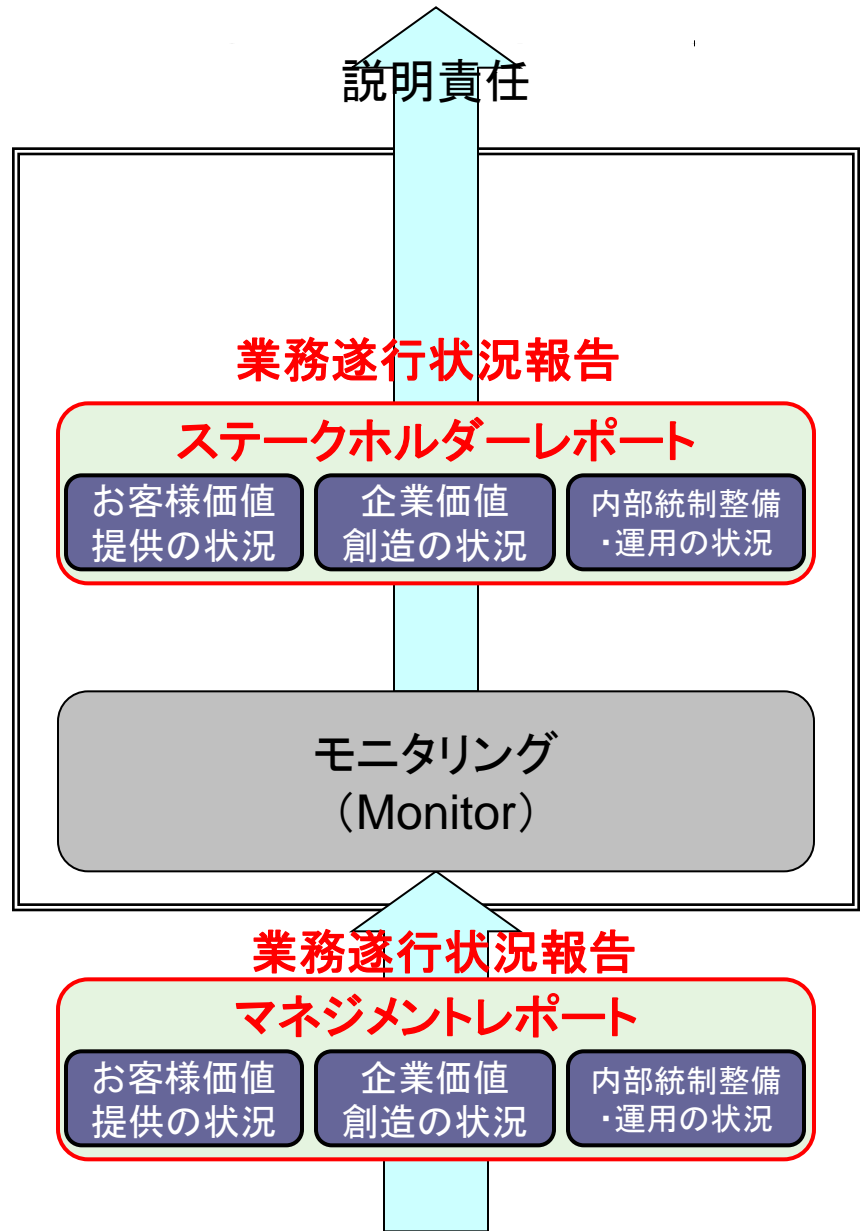
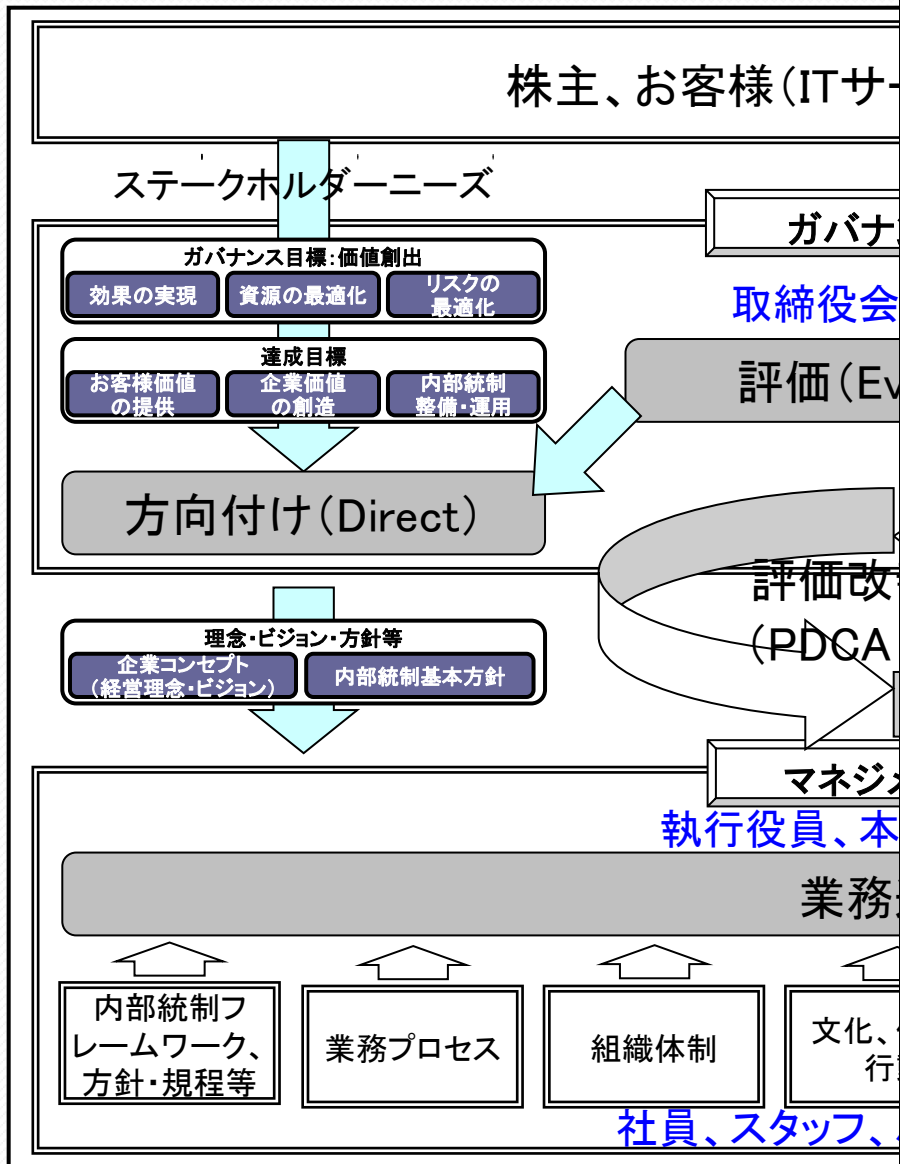
事業体のITマネジメントのためのプロセス

COBIT 5 プロセス参照モデルの適用

COBIT 5
プロセス参照モデル
の考え方を適用



プロセス参照モデルの活用



2-2-7 導入ガイダンスの適用

Implementationの適用

- GRC態勢初期導入時には適用なし(存在を知らない)
- 継続的改善サイクルの中でGRC委員会を設立
 - ➡「第3章 GEITに向けた最初のステップ」で、ITエグゼクティブ戦略委員会の設置をガイダンス。
- 振り返ってみると・・・
 - GRC態勢構築はまさにGEITの導入、変革の実現
 - 試行錯誤により構築してきた
 - 最初にImplementationを知っていれば、もっと効率的に構築できたのに・・・
 - 進め方や、直面した課題と試行錯誤でおこなってきた原因究明・解決策が、COBIT 5Implementationに書いてある！
 - ➡7つのフェーズごとの「課題」とその「根本原因」、「解決策」

2-2-8 プロセスアセスメントモデル の適用

プロセスアセスメントモデルの適用

- プロセスアセスメントモデル(プロセス能力モデル)は適用していない
(従来からIT関連内部統制領域について、グループ標準の成熟度モデルに対応～COBIT 4.1成熟度モデルに基づく)
- ガバナンスプロセス、モニタリングプロセスで適用可能性を展望(不断の改善努力の一つとして)
- 新しいプロセスアセスメントモデルは複雑で対応ロードがかかりすぎると感じられた⇒利用を躊躇した要因のひとつ
- 理解を深めるにつれて、むしろ、標準化され客観性が高くわかり易いもの



【おわりに】

COBIT 5を使ってみよう

- ガバナンス目標は価値創出～組織は何のため
- IT中心のCIO視点から、会社経営目線のCEO視点へ
(ITガバナンスからGEITへ)
- ITだけではない～Non ITにも適用可 (ビジネスガバナンス)
- つまみ食いで良い～わかるところ、使えるところから利用する
- 変革の実現、困った時のCOBIT 5 Implementation

さあ、始めよう！