

第10回 COBIT 5 講習会
COBIT 5 活用シミュレーション
～ I Tガバナンスの全社的な改善に向けて～

2017年 12月 7日

ISACA 東京支部 基準委員会 佐藤要太郎

当講習の目的

- ▶ ITガバナンスの全社的な改善に向けて、
GEIT (Governance of enterprise IT) を理解する
- ▶ 全社的な改善に向けた、ガイドの活用方法を理解する

本日本話する内容

- ▶ ITガバナンスとGEIT
- ▶ GEIT改善について
 - ▶ 活用できるフレームワークやガイド
 - ▶ 活用シミュレーション
 - ～ Getting Started With GEIT に沿った COBIT5 Product Familyの活用～
 - ▶ 特に考慮すべきポイント
- ▶ COBIT 5 概要

ITガバナンスとGEIT

「ガバナンス」

ガバナンスが効いてない！

...内部統制がとれていない？

...リスク管理できていない？

... ???

ITガバナンスの定義を確認



組織のITの現在及び将来の利用を指示し、管理するシステム。ITガバナンスは、組織を支援するためにITの利用を評価すること及び指示すること、並びに遂行するためにこのITの利用を確保することを含む。これには、方針を定めること、

事業体の目標を達成するために、ITの効果的・効率的な利用を確立するプロセス。IT需要・導入面のガバナンスは事業部門の経営幹部に、IT供給面のガバナンスはCIOに主な責任がある※²

Gartner

IT利活用の効果・リスク・資源配分を、組織全体で最適化する仕組みや活動

コーポレートガバナンスの原則を踏襲し、優先順位の付いたIT利活用の方向性と、組織全体としてのIT利活用の適切な推進とIT利活用をめぐるリスク対処を効果的にするための仕組みや活動をいう※⁴

出所

*1: JIS Q 38500:2015

*2: Gartner IT Glossary より抜粋・和訳

*3: COBIT5 Framework

*4: 監査役に期待されるITガバナンスの実践

GEITとは

～COBIT 5 における I Tガバナンス～

Governance of enterprise IT
(GEIT : ガイトと発音)
事業体ITガバナンス

～経営トップの全社的な視点～

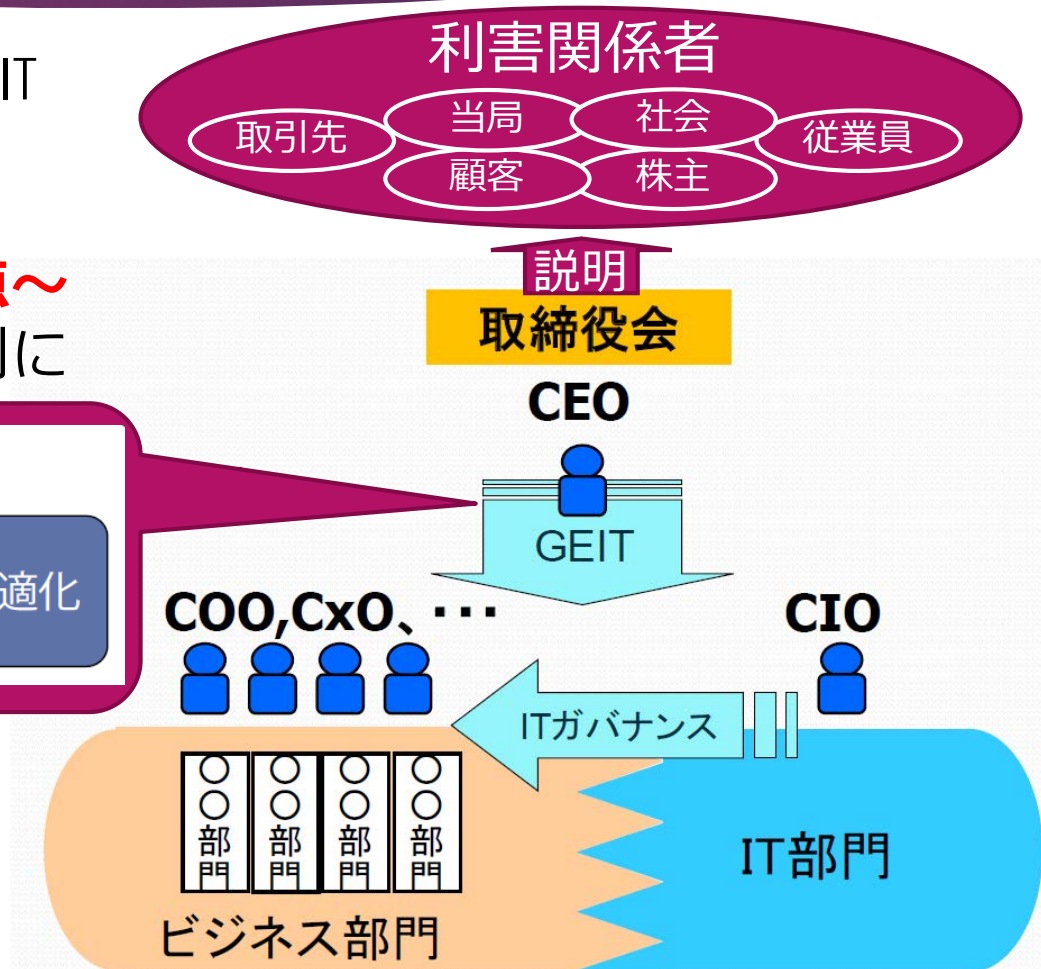
I Tが経営の中心的な役割に

ガバナンス目標:価値創出

効果の実現

リスク最適化

資源最適化



GEITとは GEITの最終的な効果

- より良いGEITの最終的な効果（ベネフィット）には、短期的にはコスト削減、長期的にはITリスク管理の改善、ビジネスとIT間の関係強化、ビジネス競争力向上がある。
- GEITはビジネス目標とITの強い整合性を確保する。
- 多くの組織は、ITリスク管理だけでなく、ビジネスとIT間の関係やコミュニケーションが改善している。



最近の流れ 攻めと守りの統合

ITと経営戦略を連携させ、企業価値の創出を実現するための仕組みである「ITガバナンス」が適切に機能することが金融機関にとって重要であると考えられる。

平成 29 事務年度
金融行政方針



平成29年11月
金融庁



攻めのITを担う「第2のIT部門」と従来のIT部門を統合する。全社の事業をデジタル化するうえで最適なIT部門の姿は「攻守統合」だ。

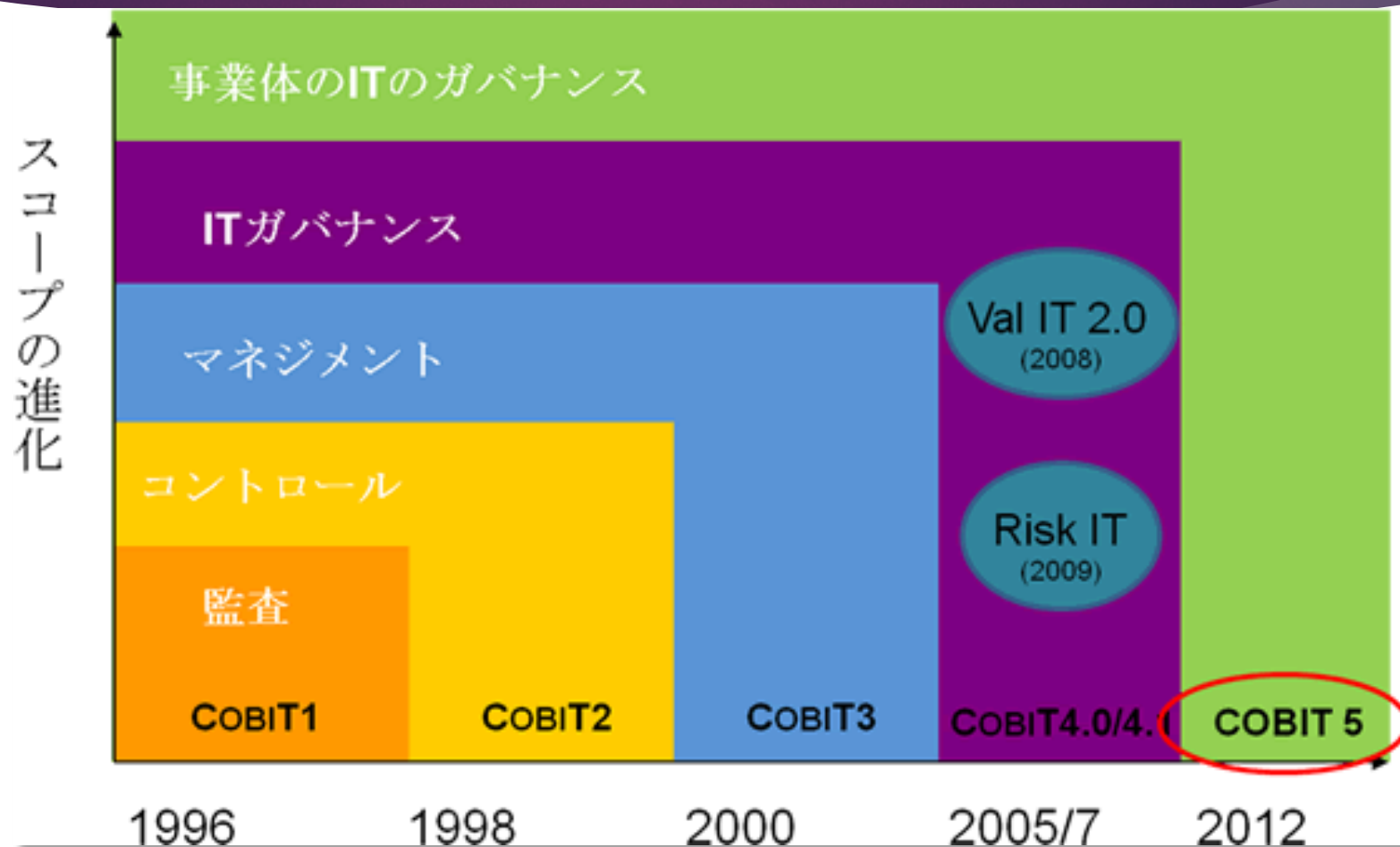
出所

* 1: 平成29事務年度金融行政方針 <http://www.fsa.go.jp/news/29/20171110.html>

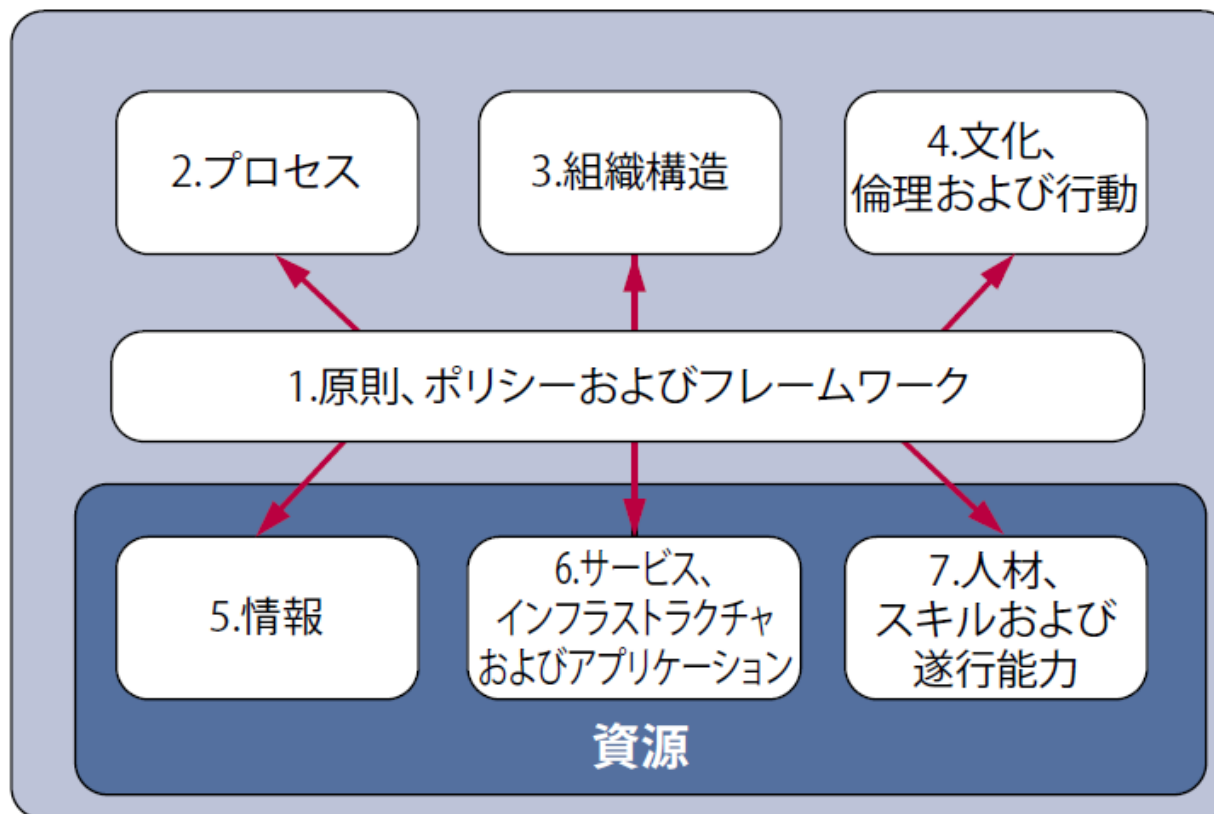
* 2: 日経コンピュータ 導火線はIoT、IT部門は攻めと守りの統合へ <http://itpro.nikkeibp.co.jp/atcl/column/17/102500442/102500001/>

COBITの変遷

監査・コントロールからガバナンスへ



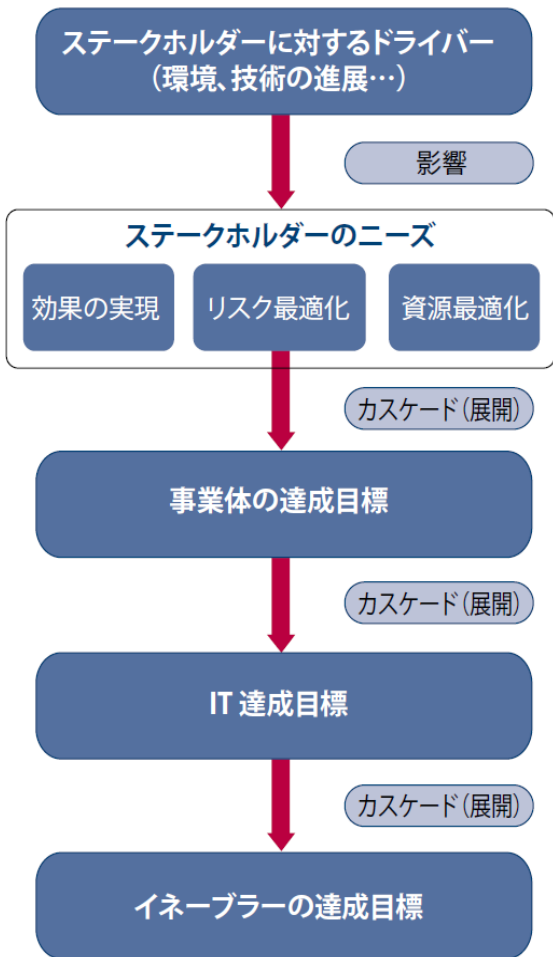
GEITとは 7つのイネーブラー（実現要因）



- GEITには7つのイネーブラー（実現要因）がある。これらイネーブラーは相互に関連している。
- プロセス以外にも様々なイネーブラーを考慮すべき。

COBIT5 Framework 達成目標カスケードとマッピング資料

ステークホルダー（利害関係者）のニーズを、GEITの実現要因（イネーブラー）へ展開（カスケード）する



図表 24 — COBIT 5 の事業体の達成目標とガバナンスおよびマネジメントの疑問のマッピング

事業体の達成目標	1	2	3
ステークホルダーのニーズ	1	2	3
IT 達成目標	1	2	3
イネーブラーの達成目標	1	2	3

図表 22 — COBIT 5 の事業体の達成目標と IT 達成目標のマッピング

事業体の達成目標	1	2	3
IT 達成目標	1	2	3
イネーブラーの達成目標	1	2	3

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	財務	顧客	内部	学習と成長
01	P	S	P	S
02	S	S	S	S
03	P	S	S	S
04	S	S	S	S
05	S	S	S	S
06	S	S	S	S
07	S	S	S	S
08	S	S	S	S
09	S	S	S	S
10	S	S	S	S
11	S	S	S	S
12	S	S	S	S
13	S	S	S	S
14	S	S	S	S
15	S	S	S	S
16	S	S	S	S
17	S	S	S	S

GEITは既にある

- ▶ ほとんどの事業体では、たとえ現状それを認識していないとしても、実現しているGEIT 構造やプロセスがないわけではない。
- ▶ すべての業界と事業体には特定のニーズ、別個の文化、異なるガバナンスレベルがある。「ここにあるGEITは何か？」を事業体自身の視点や業界・地域的背景に基づいてブレインストーミングすることが、GEIT改善のための第1歩となる。

GEIT改善に向けて

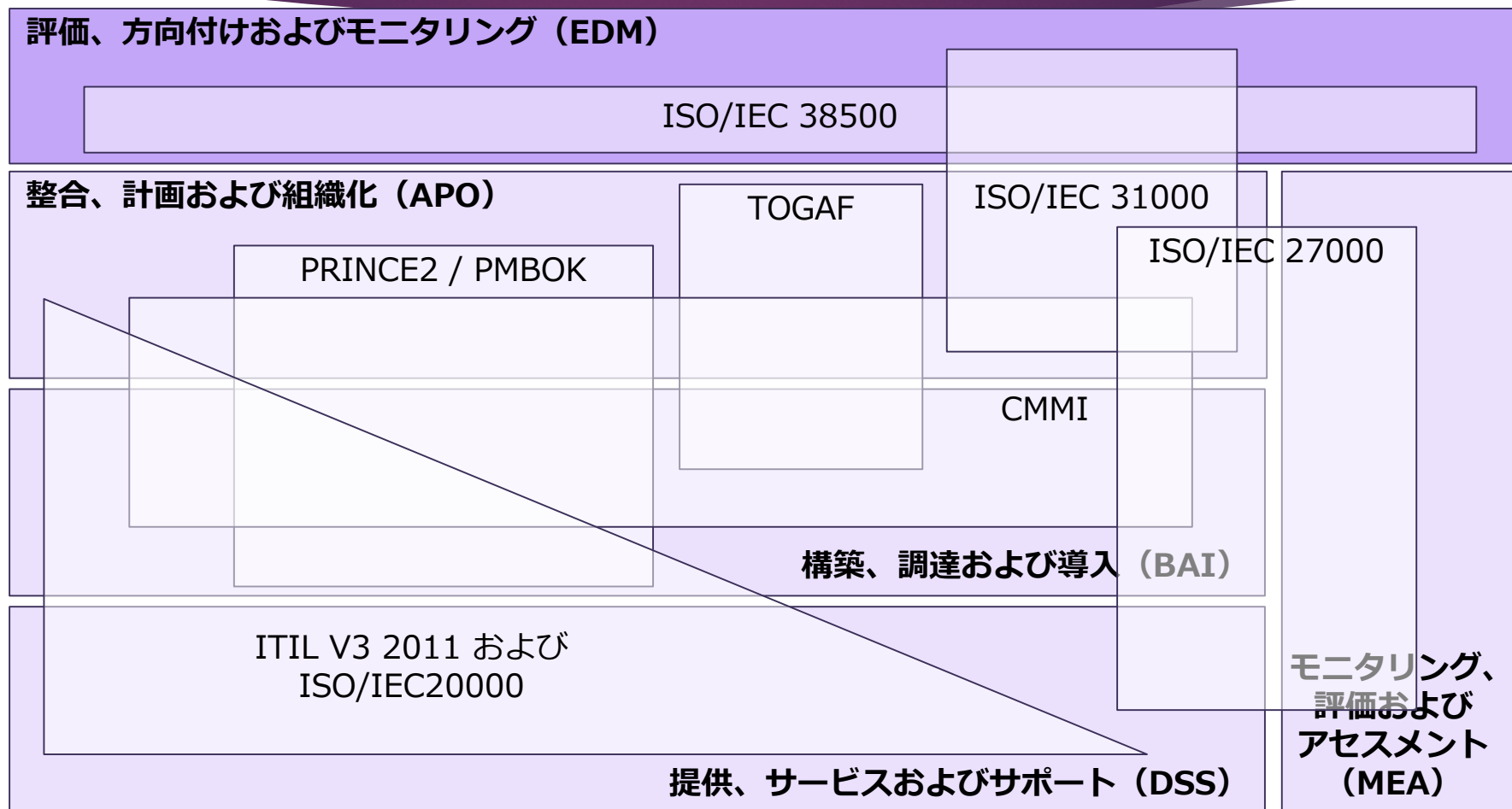
活用できるフレームワークやガイド

GEIT改善に活用できるガイド

- ▶ COBIT5 Product familyをはじめ、多くのガイドが存在する

分類	名称	発行元
実践手法	COBIT 5 Enabling Processes	ISACA
	COBIT 5 Enabling Information	ISACA
	ITIL v3 2011	TSO (OGC)
	PMBok 6 th Edition	PMI
	TOGAF 9.1	Open Group
導入方法	COBIT 5 Implementation Guide	ISACA
	Getting Started With GEIT	ISACA

各ガイドのカバー範囲



COBIT 5 Product Family

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

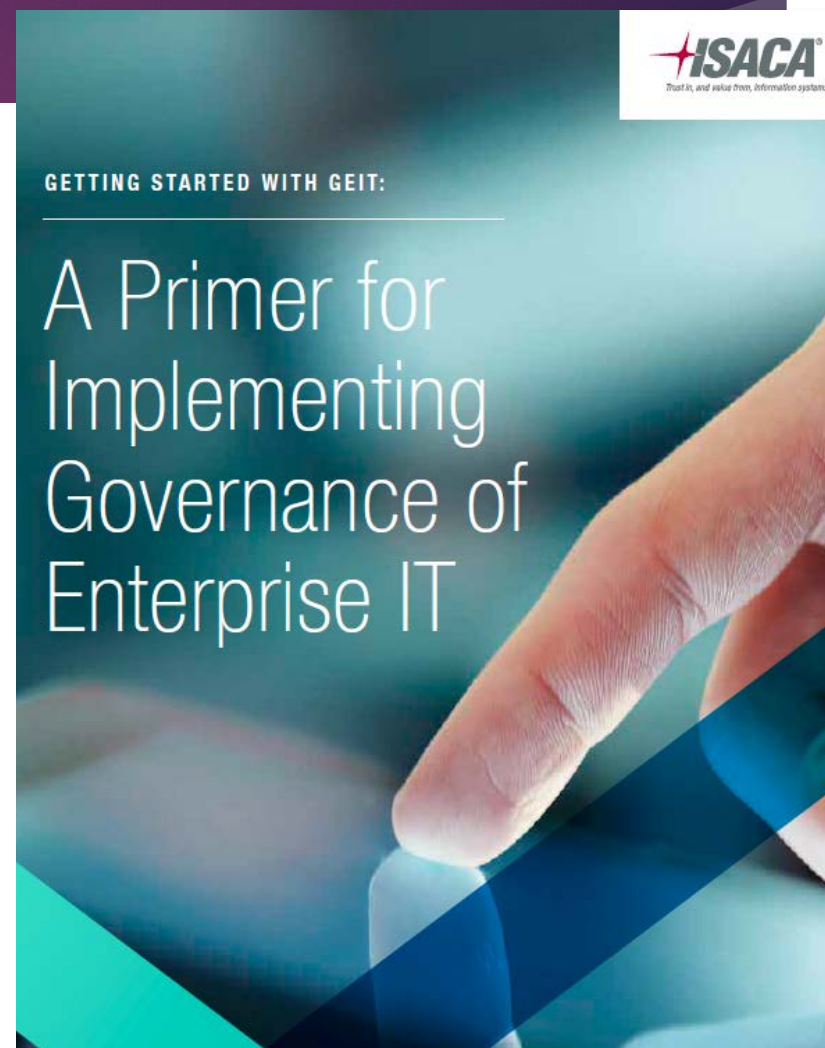
その他の
プロフェッショナルガイド

COBIT 5 オンラインコラボレーション環境

Getting Started With GEIT について

- ▶ 2016年発行。GEIT実装の入門書
- ▶ 無償（会員のみ）
- ▶ GEIT実装ステップとGEITの最終的な効果を例示し、経営陣からの同意を得ることができるようにするとともに、実現に向けた枠組みを提供する。
- ▶ COBIT 5 と関連しているものの、COBIT 5 の使用を前提条件としていない。

<http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/getting-started-with-geit.aspx>



Getting Started With GEIT アプローチ（進め方）

GEITとは
何か？

全体プログラ
ム立上げ

GEIT施策
の策定

GEIT施策
の実行

施策評価
と継続的
改善

GEIT改善に向けて

活用シミュレーション

活用シミュレーション 留意点

- ▶ Getting Started With GEIT を参考にシミュレーション
 - ▶ アプローチ詳細は、発表者の裁量で具体化／改造している
- ▶ 効果の実現、リソース最適化を中心とした価値創出のシミュレーション
- ▶ 日本語訳は正式なものではなく、参考訳

活用シミュレーション シナリオ

- ▶ あなたは旅行業を営むA社のCIOです。
- ▶ 近頃、CEO・経営企画部が「デジタルマーケティング」御旗の元で、様々なIT投資（プロジェクト）を積極的に推進しています。あなたもそこに関与しています。
- ▶ 一方で、IT部門からは「リリース後の詳細が十分に検討されていない」「効果が出ていない」との声が挙がり、あなたはそれが事実であることを認識しています。

MA、CRM導入！
BI導入、DWH構築！
モバイルアプリ開発！



運用検討が不十分！
効果が出ていない！
独り歩きしている！

活用シミュレーション GEITとは何か？

GEITとは何か？

- ✓ GEIT改善による最終的な効果（組織へアピールするもの）の検討。
- ✓ 影響を受ける領域・利害関係者の賛同を得る。

全体プログラムの立上げ

- ✓ 背景（悩み・きっかけ）、解決課題や改善機会をビジネスケース上で明確にする。
- ✓ 活用する実践手法ガイドを選択する。
- ✓ 計画フェーズの承認に向けて企画書を最終化する

GEIT施策の策定

- ✓ GEITの現状と望ましい状態を把握し、GAP分析と具体的な施策候補の洗い出しを行う。
- ✓ 効果、コスト、リスク概算から施策候補の優先順位を付ける。
- ✓ 優先度の高い施策をイネーブラー達成目標へ展開し、スコープ、コスト、スケジュール等を検討して計画を最終化する。

GEIT施策の実行

- ✓ 各施策を実行・管理する
- ✓ 抵抗に関するキーパーソンを識別し、課題を議論し、解決策を検討・実行する
- ✓ 状況に応じた計画の見直しを行う

施策評価と継続的改善

- ✓ GEIT施策の成果を、評価する。「改善した点」「次のステップ」を明確にする
- ✓ 全体レビューミーティングや、利害関係者のニーズ変化を捉えるためのインタビューを予定する
- ✓ 全体プログラムを更新する

活用シミュレーション

改善アピールポイント検討

GEITとは何か？

「IT投資が独り歩きしている」と言われているが...
 →そもそも経営陣が当社として達成したいことは何なのだろうか？
 COBIT 5 にヒントはないか？



		事業体の達成目標															
		財務					顧客					内部					
財務	01 ITと事業戦略の整合性	P	P	S				P	S	P	P	S	P	S	P		
	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				S	P											P
	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	P	S	S					S	S			S			P	
	04 ITに関連する事業リスクの管理				P	S			P	S			P			S	S
	05 ITを活用した投資とサービスサポートフォリオにより実現された利益	P	P					S		S			S	S	P		S
	06 ITコスト、効果およびリスクの透明性	S			S		P					S	P		P		

活用シミュレーション 改善効果のアピール

GEITとは何か？

- ▶ メモでCEOへGEIT改善の効果をアピールしました。

CEO向け相談メモ（全社的 I T ガバナンス改善について）

「デジタルマーケティング」投資に見られるように、弊社は新しい情報技術へ積極的に投資し、事業部門がそれを有効活用することで事業拡大を図っています。

この傾向を勘案すると、I T ガバナンス（GEIT）を全社的に改善することによる効果は大きいと考えられます。

（例）

I T ガバナンス改善目標

- ✓ マーケティング戦略と I T 投資の整合
- ✓ QCDSを遵守し、効果を出す I T プロジェクトの提供

想定効果

- ✓ 新技術を利用した事業改革・拡大の成功
- ✓ 外部からみた弊社への投資価値の向上

活用シミュレーション ビジネスケース（企画書）案を 用いた調整

GEITとは何か？

- ▶ 企画書案を挟んで他の経営陣と相談します。GEITへの期待を明確化し、アピールポイントとして盛り込むことで**賛同を得ます**。

GEIT改善プログラム 企画書（案）

- エグゼクティブサマリー
- 背景
- 事業における課題
- 効果（解決する課題と改善機会）
- 対応方針
- 進め方
- 費用対効果
- リスク
- 関係者一覧
- 成功に向けたポイント



COBIT 5 Implementation サンプルビジネスケース

付録 D ビジネスケースの例

付録 D ビジネスケースの例

注：この例は、GEIT 導入プログラムへの投資を正当化するための包括的ガイドとして提供されるビジネスケースの準備のため、重点を置いた詳細なアプローチを示している。存在するならば、既存の社内プロセスに焦点をあてることの助けとなる。Val IT™ 2.0に記載されている

シナリオ例は、伝統的な定評のあるインターネットベースのプラットフォームで政治的、文化的、経済的環境。彼らが以前から中心的に使用

ギャップ分析と達成目標

グループ全体的な GEIT の適用といった事例は、現在存在しないレベルがある。その結果、IT という点、レベルは一般的に低い

それゆえ、GEIT プログラムの目的とコントロールについての

結果は、重大なリスクが識別され報告する立場になる、となる。IT 関連の事業リスクプロファイル

究極的には、事業価値は効果的な

代替案の検討

多くの IT フレームワークが存在している。COBIT フレームワークは、と考慮されている。COBIT フレームワークは、それは GEIT のために導入されている。

ソリューションの提供

GEIT プログラムは 2 つの異なるフェーズで計画される。

フェーズ 1. 計画の事前準備 (第 3 章「GEIT に向けた最初のステップの実施」参照)

GEIT プログラムのフェーズ 1 は開発段階である。プログラムのこの段階では次の手順が行われる。

1. リスク管理サポートおよびグループ IT の間でコアチーム構成を確定
2. コアチームへ COBIT 基礎に関するトレーニングを完了
3. グループのアプローチを定義するためコアチームとワークショップを実施
4. 知識共有のためのリポジトリとして機能する Acme 社内オンラインコミュニティの整備
5. すべてのステークホルダーとそのニーズの特定
6. 現在の委員会の構成、役割と責任、意思決定ルール、報告要領を必要に応じて明確化および再構成
7. プログラムの導入を成功させるための基盤として、GEIT プログラムのビジネスケースを開発および承認
8. プログラム全体の指針となる原則、方針、期待効果のためのコミュニケーション計画
9. プログラムの有効期間中およびそれ以降使用するための評価および報告ツールの開発
10. 特定のエンティティにおけるアプローチのテスト。このアクティビティは、物流の容易さやアプローチとツールの改良を容易にするために選ばれた。
11. 外国のエンティティの一つにおける改良されたアプローチのパイロット。これは、より厳しい経営条件の下で GEIT プログラム評価フェーズを実行することの難しさを理解し、定量化するためである。
12. Acme 社経営幹部の承認得るための展開計画を含む最終的なビジネスケースやアプローチのプレゼンテーション

フェーズ 2. プログラムの導入 (第 3 章 第 2 節「継続的な改善ライフサイクルアプローチの適用」参照)

GEIT プログラムは、次の手順を実行して、良く運営されているライフサイクルの繰り返しに基づいた、継続的改善の持続的なプログラムを開始するように設計されている。

1. Acme 社グループおよび事業部門レベル両方の観点から、GEIT を向上させるためのドライバーを決定

活用シミュレーション 全体プログラムの立上げ

GEITとは何か？

- ✓ GEIT改善による最終的な効果（組織へアピールするもの）の検討。
- ✓ 影響を受ける領域・利害関係者の賛同を得る。

全体プログラムの立上げ

- ✓ 背景（悩み・きっかけ）、解決課題や改善機会を企画書上で明確にする。
- ✓ 活用する実践手法ガイドを選択する。
- ✓ 計画フェーズの承認に向けて企画書を最終化する

GEIT施策の策定

- ✓ GEITの現状と望ましい状態を把握し、GAP分析と具体的な施策候補の洗い出しを行う。
- ✓ 効果、コスト、リスク概算から施策候補の優先順位を付ける。
- ✓ 優先度の高い施策をイネーブラー達成目標へ展開し、スコープ、コスト、スケジュール等を検討して計画を最終化する。

GEIT施策の実行

- ✓ 各施策を実行・管理する
- ✓ 抵抗に関するキーパーソンを識別し、課題を議論し、解決策を検討・実行する
- ✓ 状況に応じた計画の見直しを行う

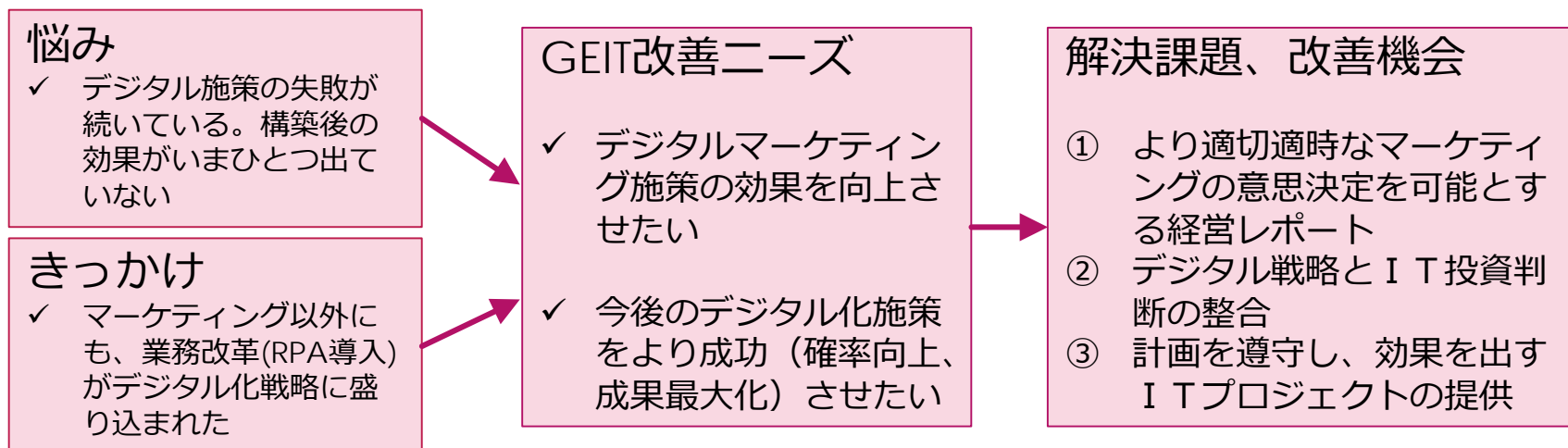
評価と継続的改善

- ✓ GEIT施策の成果を、評価する。「改善した点」「次のステップ」を明確にする
- ✓ 全体レビューミーティングや、利害関係者のニーズ変化を捉えるためのインタビューを予定する
- ✓ 全体プログラム（全体計画）を更新する

活用シミュレーション 解決する課題と改善機会の明確化

全体プログラムの
立上げ

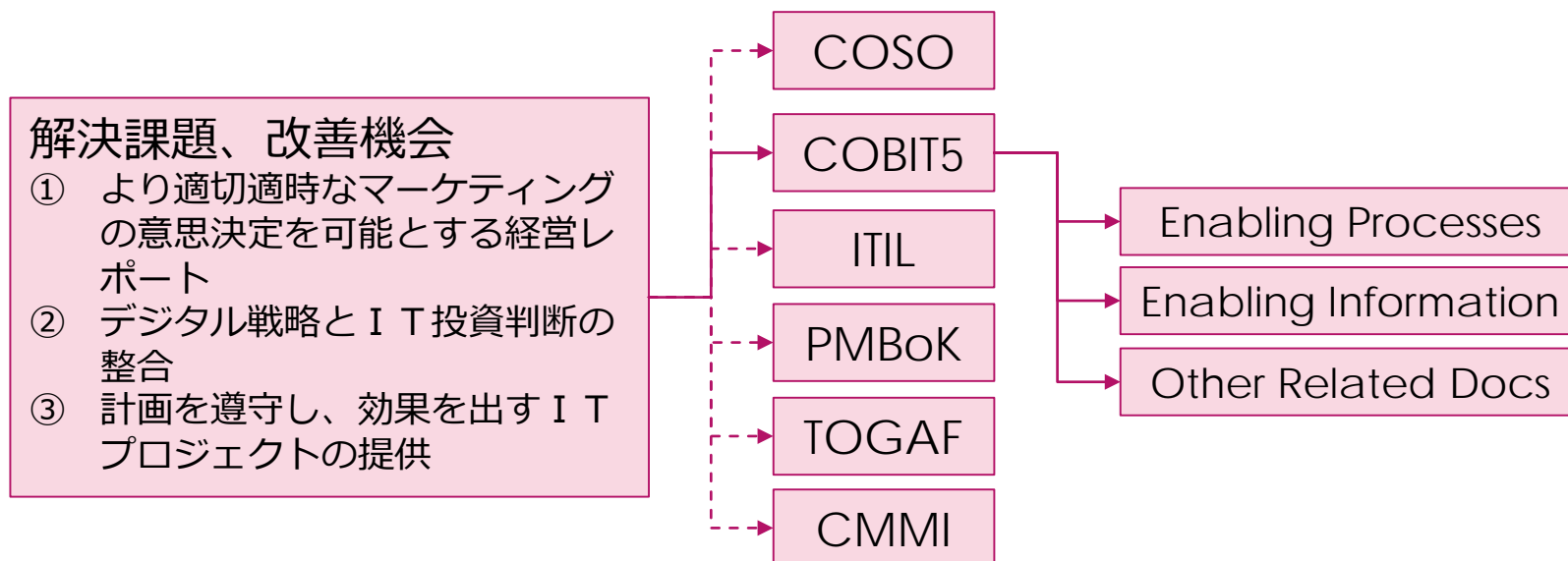
- ▶ 「悩み」「きっかけ」から「GEIT改善ニーズ」を改めて整理し、解決する課題や改善機会を明確化します。



活用シミュレーション 使用するフレームワークの選択

全体プログラムの
の立上げ

- ▶ 解決課題と改善機会を勘案し、COBIT 5 Product family をフレームワークとして使用することにしました。



活用シミュレーション 事務局編成と企画書の最終化

全体プログラムの
の立上げ

- ▶ 計画フェーズの経営承認に向けて企画書を最終化します。
- ▶ また、GEIT改善事務局を編成するため各部門と人員の調整を行います。

GEIT改善プログラム 企画書

- エグゼクティブサマリー
- 背景
- 事業における課題
- **効果** (解決する課題と改善機会)
- 対応方針
- 進め方
- **推進体制**
- 費用対効果
- リスク
- 関係者一覧
- 成功に向けたポイント

承認頂きたい内容

- 計画フェーズ
- 推進体制
 - コスト



活用シミュレーション GEIT施策の策定

GEITとは何か？

- ✓ GEIT改善による最終的な効果（組織へアピールするもの）の検討。
- ✓ 影響を受ける領域・利害関係者の賛同を得る。

全体プログラムの立上げ

- ✓ 背景（悩み・きっかけ）、解決課題や改善機会をビジネスケース上で明確にする。
- ✓ 活用する実践手法ガイドを選択する。
- ✓ 計画フェーズの承認に向けて企画書を最終化する

GEIT施策の策定

- ✓ GEITの現状と望ましい状態を把握し、GAP分析と具体的な施策候補の洗い出しを行う。
- ✓ 効果、コスト、リスク概算から施策候補の優先順位を付ける。
- ✓ 優先度の高い施策をイネーブラー達成目標へ展開し、スコープ、コスト、スケジュール等を検討して計画を最終化する。

GEIT施策の実行

- ✓ 各施策を実行・管理する
- ✓ 抵抗に関するキーパーソンを識別し、課題を議論し、解決策を検討・実行する
- ✓ 状況に応じた計画の見直しを行う

評価と継続的改善

- ✓ GEIT施策の成果を、評価する。「改善した点」「次のステップ」を明確にする
- ✓ 全体レビューミーティングや、利害関係者のニーズ変化を捉えるためのインタビューを予定する
- ✓ 全体プログラムを更新する

活用シミュレーション

GEIT改善計画の策定開始

GEIT施策の
策定

- ▶ 事務局として経営企画部やシステム部門メンバーを従え、GEIT改善計画の策定を開始します。
- ▶ 段階的に成果を得るために、全体計画とサブ計画の構成とすることを検討します。

GEIT改善全体計画（構成案）

- 目的と効果（解決課題と改善機会）
- 全体スコープ
- ロードマップ
- コスト
- 体制
- ステークホルダー
- リスク
- マネジメント全体方針

企画プロセス改善計画

- 目的
- スコープ
- スケジュール
- コスト
- 役割体制
- 要員、物的資源
- コミュニケーション
- 品質マネジメント
- 調達マネジメント
- リスク

経営レポート

改善計画構築プロセス
改善計画

活用シミュレーション 利害関係者インタビュー

GEIT施策の
策定

- ▶ 現状と望ましい状態について、利害関係者へインタビューを行います



①より適切適時なマーケティングの意思決定を可能とする経営レポート

現状認識

- ✓ DWHのデータが古い、誤っている場合がある（マーケティングチーム）
- ✓ 経営会議の度に抽出を依頼されるデータがある（IT部門）
- ✓ 他社では感情分析ソリューションを用いていると聞いた。弊社ではできていない（マーケティングチーム）
- ✓ マーケティング施策はKPIが上手く設定できていない（経営企画）

望ましい状態

- ✓ ブログやSNS、カスタマーセンターにおける会話を分析対象に含めたい（マーケティングチーム）
- ✓ AIを用いた顧客感情分析を活用できないのか（マーケティングチーム）
- ✓ BIシステム管理専従チームを立ち上げ、各データに求められる鮮度や正確性、管理レベルを適時に詳細に調整することで、マーケティングチームの分析作業がより効果的に行える（IT部門）

②デジタル戦略とIT投資判断の整合

...

...

③ITプロジェクト

...

...



活用シミュレーション SWOT分析

GEIT施策の 策定

- ▶ さらに、自社分析（SWOT：強み、弱み、機会、脅威）を行います。

良い点

内部

- ✓ 若者（～30代）シェアは国内No.1であり、デジタルマーケティングの主たる対象となる既存顧客を多く抱えている。
- ✓ 経営陣のデジタル投資への関心や意欲が高く、それが組織全体でも醸成されているため、変化に対する支持や支援を得やすい。

(強み)

悪い点

- ✓ 店頭販売の割合が高い。インターネットを介した商品の相談・販売件数が伸び悩んでおり、ネット専門の他社に劣っている。
- ✓ 長年の追加改修により基幹システムが複雑化しており、ITプロジェクトの生産性/俊敏性が低い。

(弱み)

外部

- ✓ 国内は団塊の世代が本格的に退職する段階に入ってきており、退職後の旅行需要が見込まれている。
- ✓ A社が進出しているアジア各国において、旅行市場が拡大している。

(機会)

- ✓ 大手インターネット小売業等の異業種が旅行業に参入し始めた。顧客のみならず、手数料の観点からホテルやツアー会社からも支持されている。
- ✓ 国内旅行市場は縮小傾向。

(脅威)

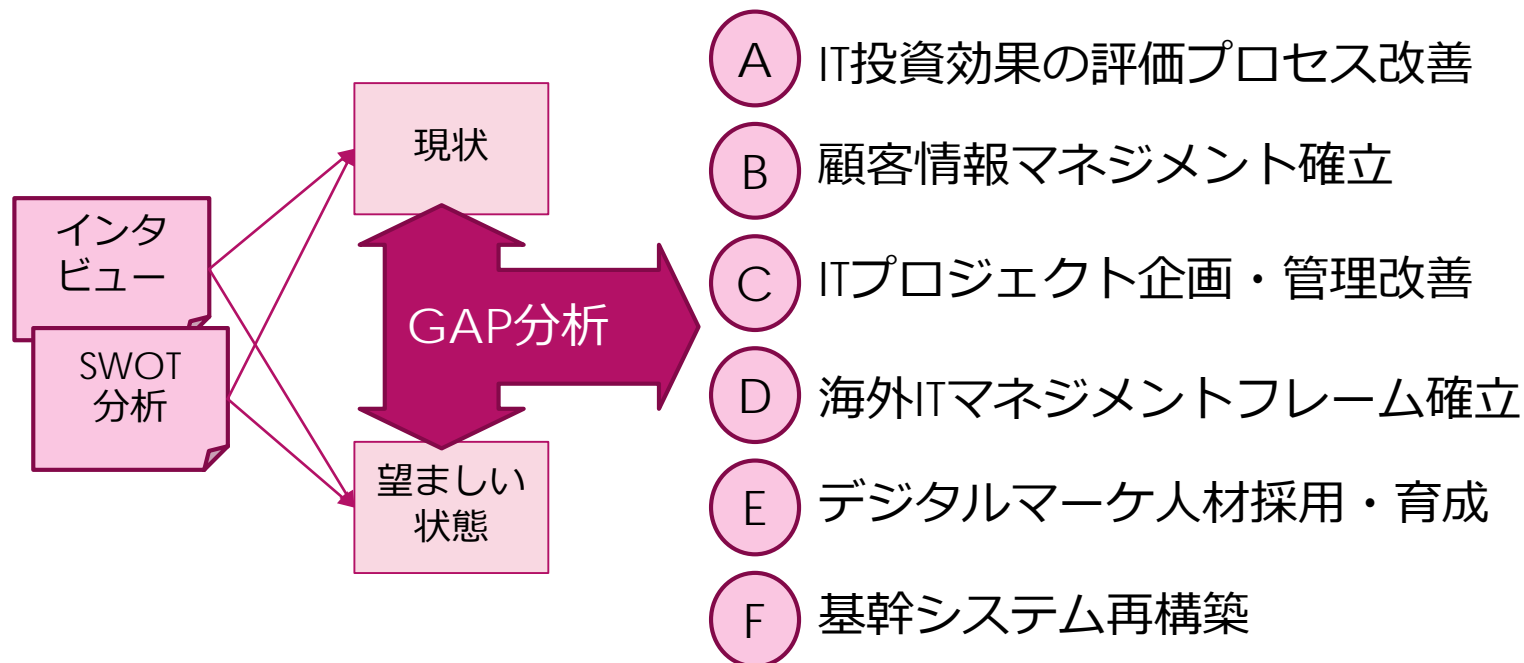


活用シミュレーション GAP分析

GEIT施策の
策定

- ▶ インタビューやSWOT分析の結果から、GAP分析を行い、具体施策の候補 A～F を抽出しました。

具体施策の候補

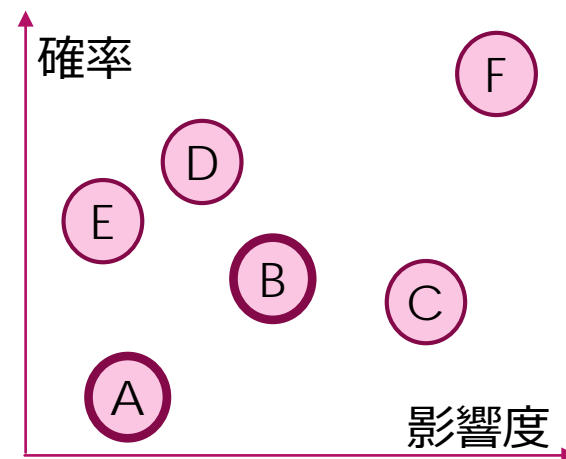


- ▶ どの施策を実行するか決定します。
- ▶ 見積りにあたっては、効果やコスト・スケジュール上のリスクも考慮します。

具体施策の候補

効果 コストリスク

具体施策の候補	効果	コスト
(A) IT投資効果の評価プロセス改善	中	小
(B) 顧客情報マネジメント確立	高	中
(C) ITプロジェクト企画・管理改善	中	小
(D) 海外ITマネジメントフレーム確立	高	中
(E) デジタルマーケ人材採用・育成	低	中
(F) 基幹システム再構築	高	極大



活用シミュレーション 全体計画書の最終化

GEIT施策の 策定

- ▶ 経営承認に向けて、全体計画とサブ計画を最終化します。
- ▶ 全体計画には、次年度以降も継続的にGEIT改善検討を行うことを記載しました。（←経営陣の期待値コントロール）

GEIT改善全体計画

- 目的と効果
- 全体スコープ
- ロードマップ
- コスト
- 体制
- ステークホルダー
- リスク
- マネジメント全体方針

IT投資効果の評価プロセス改善計画

- 目的
- スコープ
- スケジュール
- コスト
- 役割体制
- 要員、物的資源
- コミュニケーション
- 品質マネジメント
- 調達マネジメント
- リスク

顧客情報マネジメント 確立 計画

全体スコープ

- ...
- GAP分析結果
- 各施策候補の評価結果
- スコープ外施策の取扱い

ロードマップ

- ...
- 全体計画の更新方法／タイミング

活用シミュレーション
サブ計画書の最終化

IT投資効果の評価プロセス改善

GEIT施策の
策定

施策

(≒IT達成目標)

IT投資効果の
評価プロセス改善
(ITと事業戦略の整合性)

達成目標マッピング

業務ガイド

(≒プロセス)

EDM02 効果実現の確保

APO02 戦略管理

APO05 ポートフォリオ管理

BAI02 要件定義の管理

MEA01 成果と整合性のモニタリング、評価およびアセス

ツール

(≒情報項目、インフラ、プロセス)

戦略
ロード
マップ
ROI

IT関連リ
スクプ
ロファ
イル

IT予算
と効果
の一覧

DWH

会計

サービ
スポート
フォ
リオ

プロセス参
照ガイド

COBIT5 Enabling Processes

ガバナンスとマネジメントの 37プロセス

評価、方向付け、モニター (EDM)

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

EDM05 ステークホ
ルダーから見た透明
性の確保

整合、計画 および組織化 (APO)

APO01 ITマネ
ジメントフレ
ームワークの管理

APO02 戦略管
理

APO03 エン
タープライズ
アーキテクチャ
管理

APO04 イノ
ベーション管理

APO05 ポート
フォリオ管理

APO06 予算と
コストの管理

APO07 人的資
源の管理

APO08 関係管
理

APO09 サービ
スアグリーメン
トの管理

APO10 サブラ
イヤーの管理

APO11 品質管
理

APO12 リスク
管理

APO13 セキュ
リティ管理

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
変更実現性の管
理

BAI06 変更管
理

BAI07 変更受
入と移行の管理

BAI08 知識管
理

BAI09 資産管
理

BAI10 構成管
理

構築、調達および導入 (BAI)

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
プロセスコント
ロールの管理

提供、サービス、 およびサポート (DSS)

MEA01 成果と整合
性のモニタリング、
評価およびアッセ
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 外部要件へ
の準拠性のモニタ
リング、評価およびア
セスメント

モニタリング、 評価およびアセ スメント (MEA)

COBIT5 Enabling Processes プロセス参照モデル

BAI03 ソリューションの特定と構築の管理		領域：管理 ドメイン：構築、調達および導入
プロセスの概要 設計、開発、調達 / ソーシング、サプライヤー / ベンダーとの提携をカバーし事業体の要件と整合した特定済みのソリューションを構築、保守する。構成、テスト準備、テスト、要件の管理、さらにビジネスプロセス、アプリケーション、情報 / データ、クラウドチャおよびサービスの保守に関する管理を行う。		
プロセスの目的 事業体の戦略上と運用上の目標をサポートするような、タイムリーでコスト効率の高いソリューションを確立する。		
このプロセスは、以下の IT 達成目標の実現を支援する。		
IT 達成目標	関連する測定指標	
07 ビジネス要件に合致した IT サービスの提供	<ul style="list-style-type: none"> IT サービスのインシデントに起因する事業活動の中断件数 IT サービスが合意されたレベルを満たしている満足している事業部門のステークホルダーの割合 品質に満足しているユーザーの割合 	

測定指標

インプットと
アウトプット

RACIチャート
(役割表)

BAI03 RACI チャート															
マネジメントの実践手法	取締役会 (理事会)	最高経営責任者 (CEO)	最高財務責任者 (CFO)	最高執行責任者 (COO)	事業部門の幹部	ビジネスプロセスオーナー	戦略執行委員会 (プロジェクト等の)	運営委員会 プロジェクトマネジメントオフィス	プロジェクトマネジメントオフィス	バリューマネジメンントオフィス	最高リスク管理責任者 (CRO)	最高情報セキュリティ責任者 (CISO)	アーキテクチャ委員会	事業体のリスク管理委員会	人事責任者
BAI03.01 ソリューションの概要設計						R		I	R						
BAI03.02 ソリューションコンポーネントの詳細設計						R		I	R						
BAI03.03 ソリューションコンポーネントの開発						R		I	R						

BAI03 プロセス実践手法、インプット/アウトプットおよびアクティビティ				
マネジメントの実践手法		インプット		アウトプット
参照元	説明	説明	説明	送付先
BAI03.01 ソリューションの概要設計 合意された適切なウォーターフォール型開発あるいは迅速なアジャイル開発手法を用いて、概要設計の作成および文書化を行う。IT 戦略およびエンタープライズアーキテクチャとの整合性を確認する。詳細設計または構築のフェーズにおいて、また、ソリューションの進行に伴って重要な問題が発生した場合には、設計の再評価と更新を行う。ステークホルダーが積極的に設計に参加し、各バージョンを承認していることを確認する。	APO03.01 アーキテクチャの原則	アーキテクチャの原則	承認済の概要設計仕様	BAI04.03 BAI05.01
	APO03.02 ベースラインのドメインの記述とアーキテクチャの定義			
	APO04.03 イノベーションの可能性の調査分析			
	APO04.04 イノベーションのアイデアの評価			
BAI02.01		ステークホルダーから確認済の受け入れ基準		
BAI02.02		ハイレベルな取得 / 開発計画		
アクティビティ				
<ol style="list-style-type: none"> 提案されたソリューションを、ビジネス要件およびエンタープライズアーキテクチャ要件を満たすことのできるビジネスプロセス、支援サービス、アプリケーション、インフラストラクチャ、情報リポジトリに転換するための概要設計仕様を作成する。 設計プロセスにおいて適切な資格と経験を有するユーザーと IT 専門家の関与を得ることによって、ビジネスプロセス強化する IT 能力を最適に使用したソリューション設計となるようにする。 組織の設計標準に準拠し、ビジネス、事業体および IT の戦略、エンタープライズアーキテクチャ、セキュリティ計画、法規制、契約と整合した設計をソリューションと開発手法に適した詳細レベルで作成する。 品質保証の承認後、最終的な概要設計をプロジェクトのステークホルダーおよびスポンサー / ビジネスプロセスオーナーに提出し、合意された基準に基づき承認を得る。この設計は、プロジェクト全体を通して、理解が深まることでさらに発展する。 				

活用シミュレーション サブ計画書の最終化 顧客情報マネジメント確立

GEIT施策の
策定

ツールと情報資産

(≒情報項目、インフラ)

施策

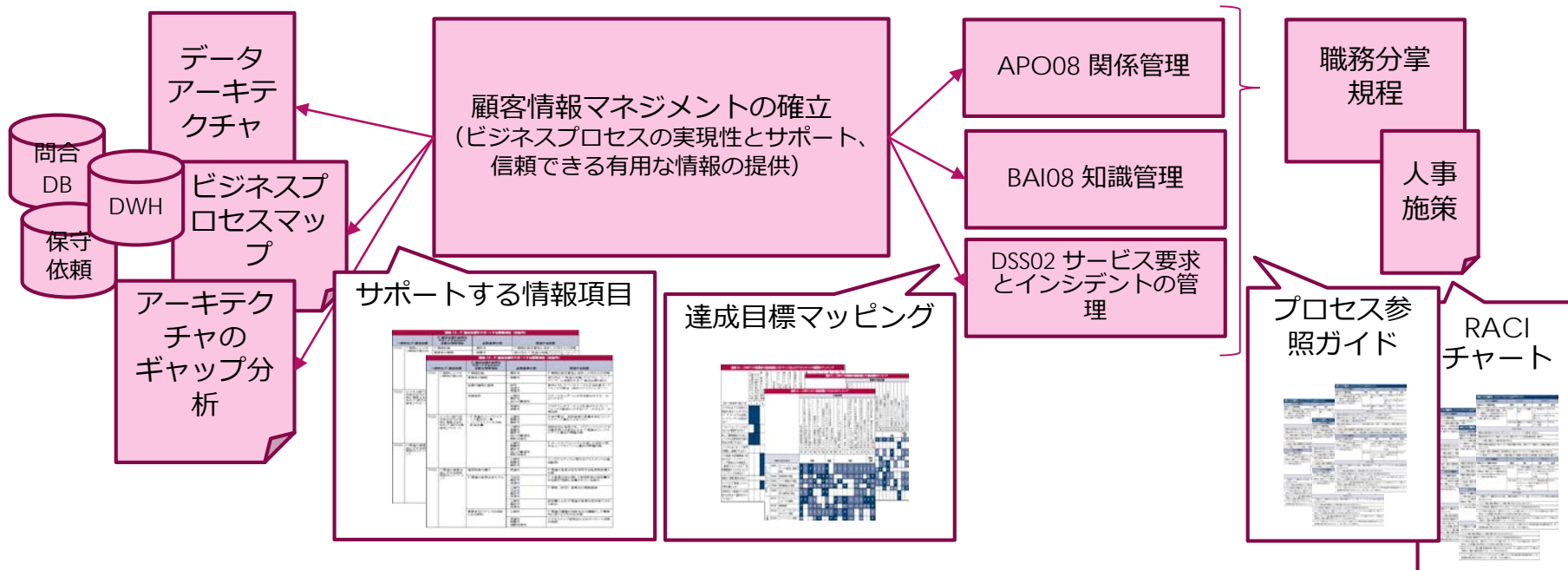
(≒IT達成目標)

業務ガイド

(≒プロセス)

組織・人材

(≒組織構造、スキル)



COBIT5 Enabling Information IT達成目標をサポートする情報項目

図表 72—IT 達成目標をサポートする情報項目 (包括的)

一般的な IT 達成目標	IT 達成目標の実現をサポートするための主要な情報項目	品質基準の例	関連する指標
ITG01 IT 戦略とビジネス戦略の整合性	IT 戦略計画	<ul style="list-style-type: none"> 最新性 	IT 戦略計画を最後に更新した時からの時間
	事業体の戦略	<ul style="list-style-type: none"> 網羅性 	潜在的な IT 関連の投資プログラム (ロードマップ) に変換される IT 達成目標の割合
	投資の種類と基準	<ul style="list-style-type: none"> 評判 信憑性 関連性 	業界に対してベンチマークとなる投資ポートフォリオの構成 (業界アナリストレポート)
	成果報告	<ul style="list-style-type: none"> 正確性 最新性 表示の簡潔性 	ステークホルダーに対する読みやすさ、わかりやすさ
<ul style="list-style-type: none"> 関連性 網羅性 		プログラムやサービスの計画されたポートフォリオの範囲に対するステークホルダーの満足度	
ITG02 ビジネス部門が外部の法令と規制に準拠するための IT 部門の準拠性とサポート	<ul style="list-style-type: none"> IT 関連のコンプライアンス要件の一覧 コンプライアンスの保証報告書 	<ul style="list-style-type: none"> 正確性 網羅性 最新性 	弁済や罰金、風評被害の影響を含むコンプライアンス違反によるコスト
		<ul style="list-style-type: none"> 正確性 網羅性 最新性 表示の簡潔性 解釈容易性 	取締役会に報告され、パブリックコメントや非難を受ける原因となる IT 関連のコンプライアンス違反の問題の数
		<ul style="list-style-type: none"> 正確性 網羅性 最新性 表示の簡潔性 解釈容易性 	IT サービスプロバイダと合意した契約に関するコンプライアンス違反の問題の数
		<ul style="list-style-type: none"> 正確性 網羅性 最新性 	コンプライアンスに関するアセスメントの適用範囲
ITG03 IT 関連の意思決定に対する経営幹部のコミットメント	報奨制度の導入	<ul style="list-style-type: none"> 関連性 	IT 関連の意思決定を参照する報奨制度導入の数
	IT 関連の意思決定モデル	<ul style="list-style-type: none"> 可用性 最新性 信憑性 	IT の意思決定に関して経営幹部の説明責任の役割が明確に定義されている割合

活用シミュレーション GEIT施策の実行

GEITとは何か？

- ✓ GEIT改善による最終的な効果（組織へアピールするもの）の検討。
- ✓ 影響を受ける領域・利害関係者の賛同を得る。

全体プログラムの立上げ

- ✓ 背景（悩み・きっかけ）、解決課題や改善機会をビジネスケース上で明確にする。
- ✓ 活用する実践手法ガイドを選択する。
- ✓ 計画フェーズの承認に向けて企画書を最終化する

GEIT施策の策定

- ✓ GEITの現状と望ましい状態を把握し、GAP分析と具体的な施策候補の洗い出しを行う。
- ✓ 効果、コスト、リスク概算から施策候補の優先順位を付ける。
- ✓ 優先度の高い施策をイネーブラー達成目標へ展開し、スコープ、コスト、スケジュール等を検討して計画を最終化する。

GEIT施策の実行

- ✓ 各施策を実行・管理する
- ✓ 抵抗に関するキーパーソンを識別し、課題を議論し、解決策を検討・実行する
- ✓ 状況に応じた計画の見直しを行う

評価と継続的改善

- ✓ GEIT施策の成果を、評価する。「改善した点」「次のステップ」を明確にする
- ✓ 全体レビューミーティングや、利害関係者のニーズ変化を捉えるためのインタビューを予定する
- ✓ 全体プログラム（全体計画）を更新する

活用シミュレーション 施策への抵抗

GEIT施策の 実行

- ▶ 承認を受けて、各施策が開始されました。
- ▶ 順調に進んでいるかに見えた矢先、「役割分担について、営業部門から強い抵抗を受けている」との相談をGEIT事務局は受けました。

役割分担を抵抗
されています...



GEIT事務局

(CEO、経営企画、IT部門混成)



施策実行部隊

(マーケ、IT、人事部門混成)

???



営業部門

活用シミュレーション 抵抗に関するキーパーソンとのコミュニ ケーション

GEIT施策の
実行

- ▶ GEIT事務局は、簡単なヒアリングを行った後、各支社の営業部門に向けたワークショップの開催を施策実行部隊に促しました。

CRMへの入力項目増加は業務負荷が高い。
営業が参照可能な情報項目を増やしたい。



【対応】

施策の目的を繰り返し説明し、短期的に見た場合には営業部門の業務が増えるものの、中長期的には組織的な成功につながることを伝えた。

各支社向けに何度もワークショップを開催して積極的に彼らの意見を聞き、評価した上でその一部を施策に反映することにした。

活用シミュレーション 計画の見直し

GEIT施策の 実行

- ▶ 営業部門からの意見を評価した結果、顧客情報マネジメント確立計画の一部が見直されました。
- ▶ また、あなた達GEIT事務局は、関連部門とのコミュニケーション不足によるリスクを再評価し、マネジメント全体方針を見直しました。

GEIT改善全体計画 ver1.1

- 目的と効果
- 全体スコープ
- ロードマップ
- コスト
- 体制
- ステップ
- **リスク**
- **マネジメント全体方針**

「関連部門とのコミュニケーション不足により、業務運営負荷が増加する」リスクを再評価。対策として、各施策のコミュニケーションマネジメント状況の事務局による月次評価を追加

営業部門とのコミュニケーション方法（資料回覧からワークショップ開催へ）と頻度を強化

顧客情報マネジメント確立計画 ver1.1

- 目的
- **スコープ**
- **スケジュール**
- **コスト**
- 役割体制
- **コミュニケーション**
- 品質マネジメント
- 調達マネジメント
- リスク

CRM改修スコープ、コスト、リリース日を見直し



活用シミュレーション 評価と継続的改善

GEITとは何か？

- ✓ GEIT改善による最終的な効果（組織へアピールするもの）の検討。
- ✓ 影響を受ける領域・利害関係者の賛同を得る。

全体プログラムの立上げ

- ✓ 背景（悩み・きっかけ）、解決課題や改善機会をビジネスケース上で明確にする。
- ✓ 活用する実践手法ガイドを選択する。
- ✓ 計画フェーズの承認に向けて企画書を最終化する

GEIT施策の策定

- ✓ GEITの現状と望ましい状態を把握し、GAP分析と具体的な施策候補の洗い出しを行う。
- ✓ 効果、コスト、リスク概算から施策候補の優先順位を付ける。
- ✓ 優先度の高い施策をイネーブラー達成目標へ展開し、スコープ、コスト、スケジュール等を検討して計画を最終化する。

GEIT施策の実行

- ✓ 各施策を実行・管理する
- ✓ 抵抗に関するキーパーソンを識別し、課題を議論し、解決策を検討・実行する
- ✓ 状況に応じた計画の見直しを行う

評価と継続的改善

- ✓ GEIT施策の成果を、評価する。「改善した点」「次のステップ」を明確にする
- ✓ 全体レビューミーティングや、利害関係者のニーズ変化を捉えるためのインタビューを予定する
- ✓ 全体プログラム（全体計画）を更新する

活用シミュレーション GEIT改善施策の評価

評価と
継続的改善

- ▶ 無事、GEIT改善施策の一つが完了しました。
- ▶ 改善施策の成果を、プロセス参照ガイドを参考に設定した測定指標に基づいてSMART※に評価します。
- ▶ 「何が改善したか？」 「何が次のステップか？」を明確にします。

顧客情報
マネジメント確立

測定指標

測定方法

改善した点

マーケティング施策案の成果測定指標、目標設定値の合理性に対する承認者の満足度	経営者向けアンケート	承認者であるCMOとCEOから「大きく改善した」と評価された。
マーケティング施策の起案時に使用された情報項目の割合	CRM、DWHへのアクセスログを分析	起案時に参照されている情報項目の種類が3倍以上となった。
マーケティング部門向けの顧客情報関連のITサービスに対する同部門の満足度	マーケティング部門向けアンケート	CRM、DWHへの問い合わせや変更対応の俊敏性が向上した。

次のステップ

- ✓ CRMやDWHの情報項目を最適化（追加、更新、廃止）するプロセスの改善
- ✓ 顧客情報に適切なセキュリティが確保されているかの評価プロセスの確立



プロセス参照ガイド



*SMART: 具体的 (Specific)、測定可能 (Measurable)、実行可能 (Actionable)、適切 (Relevant)、適時 (Timely)

活用シミュレーション GEIT全体の継続的改善に向けて

評価と
継続的改善

- ▶ GEIT改善プログラム全体について、レビューミーティングや、利害関係者のニーズ変化を捉えるためのインタビューを半年から1年後に予定します。
- ▶ 各施策の評価結果およびGEIT全体の再分析結果を踏まえて、GEIT改善全体計画の更新や新たな施策を策定します。

GEIT再分析

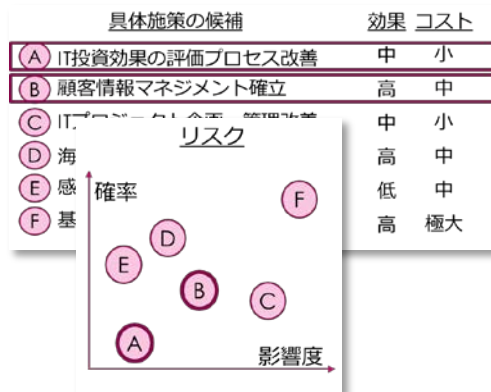
インタ
ビュー

レビュー
ミーテ
ィング

SWOT
分析

完了施策から
導出された次
のステップ

具体施策の評価



全体計画と施策の策定

GEIT改善全体計画 ver2.0

- 目的と効果
- 全体スコープ
- ロードマップ
- コスト
- 体制
- ステークホルダー
- リスク
- マネジメント全体方針

顧客情報マネジ
メント高度化
計画

基幹システム
再構築
計画



GEIT改善で 特に考慮すべきポイント

考慮すべきポイント	対応策
IT部門と事業部門のコミュニケーションギャップ	<ul style="list-style-type: none"> • 計画フェーズから全ての利害関係者を巻き込む • 各問題について、その原因がコミュニケーションギャップでないかを必ず検討する
一度に多くの/広範囲な施策を実行してしまい、難易度が高くなる	<ul style="list-style-type: none"> • 優先順位付けを20 80法則*で行う。クイックwinを考慮する。 • 今あるGEITを活かす。 • スコープマネジメント方針を予め明確にし、それに沿って運営する
GEIT改善に対するコミットメントが確保し続けられない	<ul style="list-style-type: none"> • GEIT改善効果とその体験を得やすいように、なるべく細かい施策に分ける。 • シンプルで、現実的で、実践的な計画を維持する • 適切なハウレンソウで期待値をマネジメントする

出典: Getting Started With GEITを基に作成

*20 80法則: 上位20%の要素が全体の80%を占める

COBIT 5 について

COBIT 5 Product Family

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 資料の入手方法

ISACA国際本部のWebサイトからダウンロード可能（一部無償）
<http://www.isaca.org/COBIT/Pages/COBIT-5-japanese.aspx>



The screenshot displays the ISACA website page for COBIT 5 Japanese resources. The page features the ISACA logo and navigation menu at the top. Below the navigation, there is a search bar and a list of menu items including ABOUT, MEMBERSHIP, CERTIFICATION, EDUCATION, COBIT, KNOWLEDGE & INSIGHTS, JOURNAL, and BOOKSTORE. The main content area is titled "COBIT 5 Japanese" and lists two primary sections: "COBIT 5 日本語 (Japanese)" and "COBIT 5 Enabling Processes 日本語 (Japanese)". Each section provides options for downloading (complimentary for members) or purchasing in book format (with prices for members and non-members). A "Quick Links" sidebar on the right offers links to "View COBIT 5 Home" and "View COBIT 5 Publications Directory". A book cover for "COBIT 5" is also visible on the right side of the page.

COBIT5 Framework

5つの原則

事業体はステークホルダーに向けて価値を生み出すために存在している

ステークホルダーニーズを達成目標へ展開（カスケード）する

計画・構築・実行・モニター（PBRM≒PDCA）する執行部門と、それらを評価・方向付け・モニター（EDM）する経営陣

1.ステークホルダーのニーズを充足

事業体の情報、ITガバナンス・マネジメントに関わる組織内外のあらゆる人・モノ・活動を含む

5.ガバナンスとマネジメントの分離

2.事業体全体の包含

COBIT 5 の原則

プロセスだけではない、7つのイネーブラー（実現要因）

4.包括的アプローチの実現

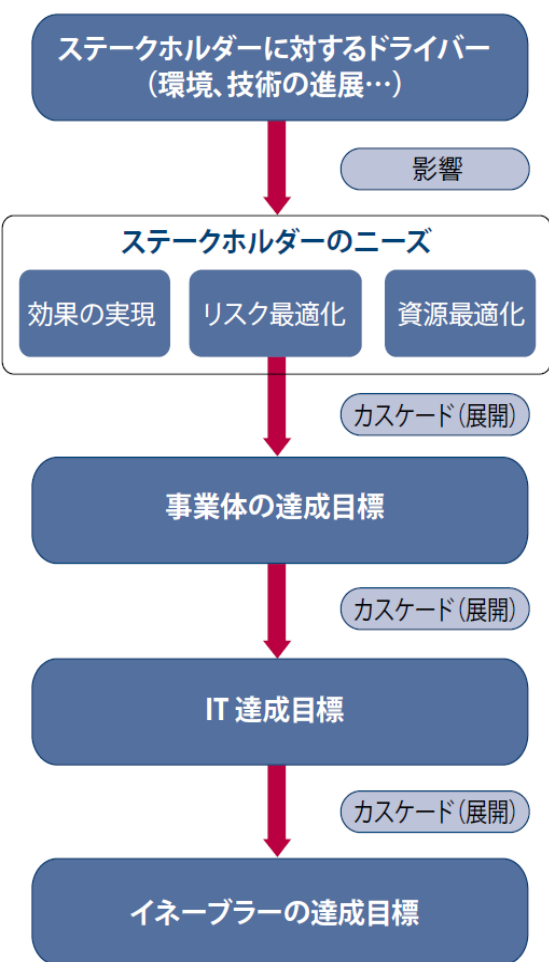
関連する最新の標準やフレームワークと整合

3.一つに統合されたフレームワークの適用

ITIL, PMBoK, ISO, ...

原則、プロセス、組織構造、文化、情報、インフラ、人材

COBIT5 Framework 達成目標カスケードとマッピング資料



ステークホルダーニーズをイネーブラーへ展開 (カスケード) する際の参考資料

図表 24 — COBIT 5 の事業体の達成目標とガバナンスおよびマネジメントの疑問のマッピング

ステークホルダーのニーズ	1.	2.	3.
1. どうすれば IT の活用から価値を得ることができるか？ IT サービスの品質にエンドユーザーは満足するか？			
2. IT のパフォーマンスをどのように管理するのか？			
3. 新しい戦略機会のために、どうすれば新技術を最も有効に利用できるか？			
4. どうすればうまく IT 部門を構築し、組織できるか？			
5. どの程度、外部事業者に依存するか？ IT アウトソーシング契約はどの程度正しく管理されているか？ 外部事業者からどのようにアシュアランスを得るか？			
6. 情報の (管理) 要件は何か？			
7. すべての IT 関連リスクへ対策を講じたか？			
8. 効率的かつ障害からの回復力がある IT 運用を行っているか？			

図表 22 — COBIT 5 の事業体の達成目標と IT 達成目標のマッピング

事業体の達成目標	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	
1. 効果の実現																		
2. リスク最適化																		
3. 資源最適化																		

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
1. IT と事業戦略の整合性	P	S	P	S	S	S	P		S	S	S	S
2. ビジネスと外部の法令と規制に準拠するための IT の適合性とサポート	P	S	S	S	S	S	S	S	S	S	S	S
3. IT に関する事業リスクの管理	P	S	S	S	S	S	S	S	S	S	S	S
4. IT を活用した投資とサービスポートフォリオにより裏付けされた利益	P	S	S	S	S	S	S	S	S	S	S	S
5. IT コスト、効率およびリスクの透明性	P	S	S	S	S	S	S	S	S	S	S	S
6. ビジネス要件に合致した IT サービスの提供	P	S	S	S	S	S	S	S	S	S	S	S
7. 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	P	S	S	S	S	S	S	S	S	S	S	S
8. IT の俊敏性	P	S	S	S	S	S	S	S	S	S	S	S
9. 情報、情報源/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	P	S	S	S	S	S	S	S	S	S	S	S
10. IT 資源、資源および能力の最適化	P	S	S	S	S	S	S	S	S	S	S	S
11. アプリケーションと技術をビジネスプロセスへ統合し、プロセスを自動化	P	S	S	S	S	S	S	S	S	S	S	S
12. アプリケーションと技術をビジネスプロセスへ統合し、プロセスを自動化	P	S	S	S	S	S	S	S	S	S	S	S

図表 25 — COBIT 5 の IT 達成目標とプロセスのマッピング (続き)

COBIT 5 のプロセス	財務	顧客	内部
EDM01 ガバナンスフレームワークの設定と維持の保証	P	S	S
EDM02 効果実現の保証	P	S	S
EDM03 リスク最適化の保証	S	S	S
EDM04 資源最適化の保証	S	S	S
EDM05 ステークホルダーから見た透明性の保証	S	S	S
APO01 IT マネジメントフレームワークの管理	P	P	S
APO02 戦略管理	P	S	S
APO03 エンタープライズアーキテクチャ管理	P	S	S
APO04 イノベーション管理	S	S	S

1. ステークホルダーのニーズを充足

COBIT5 Enabling Processes

IT達成目標とプロセスのマッピング

COBIT 5 のプロセス			IT 達成目標																																																																																			
			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	S																																																																		
	EDM02	効果実現の保証	P		S		P	P	P	S			S	S	S	S																																																																						
	EDM03	リスク最適化の保証	S	S	S	P		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																																																																						
	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																																																																					
	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	S	S	S																																																																			
			01	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				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				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				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				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			

1.ステークホルダーのニーズを充足

COBIT5 Enabling Information IT達成目標をサポートする情報項目

図表 72—IT 達成目標をサポートする情報項目 (包括的)			
一般的な IT 達成目標	IT 達成目標の実現をサポートするための主要な情報項目	品質基準の例	関連する指標
ITG01 IT 戦略とビジネス戦略の整合性	IT 戦略計画	・ 最新性	IT 戦略計画を最後に更新した時からの時間
	事業体の戦略	・ 網羅性	潜在的な IT 関連の投資プログラム (ロードマップ)
図表 72—IT 達成目標をサポートする情報項目 (包括的)			
一般的な IT 達成目標	IT 達成目標の実現をサポートするための主要な情報項目	品質基準の例	関連する指標
ITG01 IT 戦略とビジネス戦略の整合性	IT 戦略計画	・ 最新性	IT 戦略計画を最後に更新した時からの時間
	事業体の戦略	・ 網羅性	潜在的な IT 関連の投資プログラム (ロードマップ) に変換される IT 達成目標の割合
ITG02 ビジネス部門が外部の法令と規制に準拠するための IT 部門の親性とサポート	投資の種類と基準	・ 評判 ・ 信憑性 ・ 関連性	業界に対してベンチマークとなる投資ポートフォリオの構成 (業界アナリストレポート)
	成果報告	・ 正確性 ・ 最新性 ・ 表示の簡潔性	ステークホルダーに対する読みやすさ、わかりやすさ
ITG02 ビジネス部門が外部の法令と規制に準拠するための IT 部門の親性とサポート	<ul style="list-style-type: none"> IT 関連のコンプライアンス要件の一覧 コンプライアンスの保証報告書 	・ 関連性 ・ 網羅性	プログラムやサービスの計画されたポートフォリオの範囲に対するステークホルダーの満足度
		・ 最新性	弁済や罰金、風評被害の影響を含むコンプライアンス違反によるコスト
ITG03 IT 関連の意思決定に対する経営幹部のコミットメント	<ul style="list-style-type: none"> 正確性 網羅性 最新性 表示の簡潔性 解釈容易性 	・ 正確性 ・ 網羅性 ・ 最新性 ・ 表示の簡潔性 ・ 解釈容易性	IT サービスプロバイダと合意した契約に関するコンプライアンス違反の問題の数
		・ 正確性 ・ 網羅性 ・ 最新性	コンプライアンスに関するアセスメントの範囲
ITG03 IT 関連の意思決定に対する経営幹部のコミットメント	報奨制度の導入	・ 関連性	IT 関連の意思決定を参照する回数
	IT 関連の意思決定モデル	<ul style="list-style-type: none"> 可用性 最新性 信憑性 	IT の意思決定に関して経営幹部の役割が明確に定義された回数
ITG03 IT 関連の意思決定に対する経営幹部のコミットメント	<ul style="list-style-type: none"> 正確性 可用性 最新性 信憑性 	・ 正確性 ・ 可用性 ・ 最新性 ・ 信憑性	IT 戦略 (経営) 委員会の承認回数
		・ 正確性 ・ 最新性 ・ 信憑性	経営層による IT 関連の意思決定の割合
ITG03 IT 関連の意思決定に対する経営幹部のコミットメント	事業体ガバナンスの指針となる原則	・ 正確性	IT 関連の議題が取締役会の議題的に取り上げられた回数
	<ul style="list-style-type: none"> 関連性 網羅性 理解容易性 	エグゼクティブ委員会によるガバナンスの承認	

1.ステークホルダーのニーズを充足

COBIT5 Framework 事業体（組織）全体の包含

RACIチャート
(役割表)

取締役会（理事会）

責任者（CEO）

最高財務責任者（CFO）

最高執行責任者（COO）

事業部門の幹部

ビジネスプロセスオーナー

戦略執行委員会

（プロジェクト等の）運営委員会

プロジェクトマネジメントオフィス

バリューマネジメントオフィス

最高リスク管理責任者（CRO）

最高情報セキュリティ責任者（CISO）

アーキテクチャ委員会

事業体のリスク管理委員会

人事責任者

コンプライアンス

監査

最高情報責任者（CIO）

アーキテクチャ責任者

開発責任者

IT オペレーション責任者

IT 管理責任者

サービスマネージャー

情報セキュリティマネージャ

事業継続マネージャー

個人情報管理最高責任者

Processes

Enabling P

2. 事業体全体の包含

COBIT5 Enabling Processes

ガバナンスとマネジメントの 37プロセス

評価、方向付け、モニター（EDM）

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

EDM05 ステークホ
ルダーから見た透明
性の確保

整合、計画 および組織化 （APO）

APO01 ITマネ
ジメントフレ
ームワークの管理

APO02 戦略管
理

APO03 エン
タープライズ
アーキテクチャ
管理

APO04 イノ
ベーション管理

APO05 ポート
フォリオ管理

APO06 予算と
コストの管理

APO07 人的資
源の管理

APO08 関係管
理

APO09 サービ
スアグリーメン
トの管理

APO10 サブラ
イヤーの管理

APO11 品質管
理

APO12 リスク
管理

APO13 セキュ
リティ管理

MEA01 成果と整合
性のモニタリング、
評価およびアッセ
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

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
変更実現性の管
理

BAI06 変更管
理

BAI07 変更受
入と移行の管理

BAI08 知識管
理

BAI09 資産管
理

BAI10 構成管
理

構築、調達および導入（BUI）

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

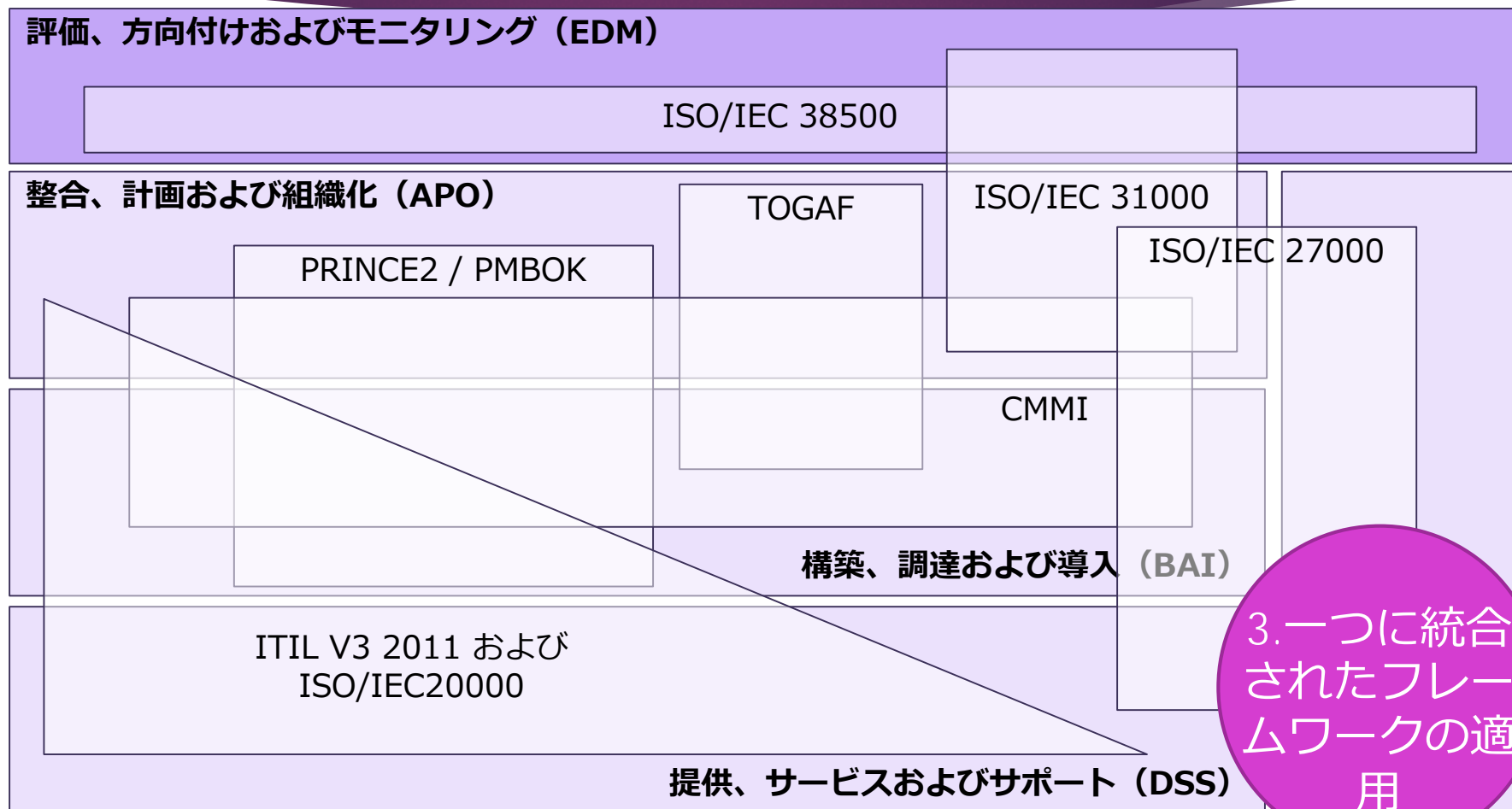
DSS05 セキュ
リティサービスの
管理

DSS06 ビジネス
プロセスコント
ロールの管理

提供、サービス およびサポート （DSS）

3.一つに統合
されたフレー
ムワークの適
用

各ガイドのカバー範囲



Information Security-specific Organisational Structures

- Chief information security officer (CISO)
- Information security steering committee (ISSC)
- Information security manager (ISM)
- Other related roles and structures

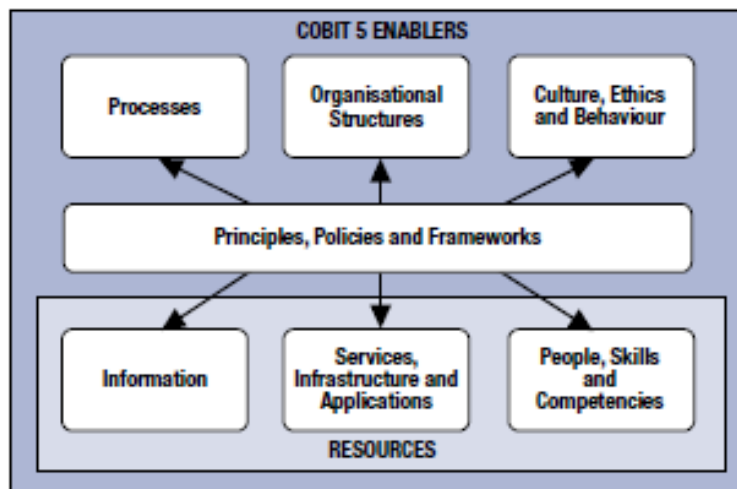
Section II, Chapter 4
Detailed Guidance: Appendix C

Desired Information Security-specific Culture, Ethics and Behaviour

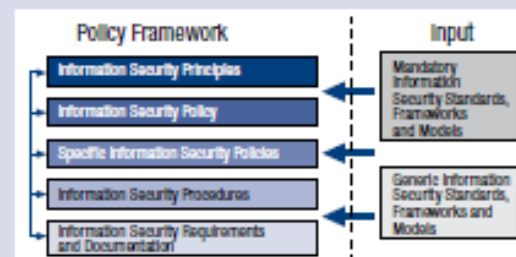
- Information security is practiced in daily operations.
- People respect the policies and principles.
- People are provided with sufficient and detailed guidance, and are encouraged to participate in and challenge the current situation.
- Everyone is accountable for protection.
- Stakeholders identify and respond to threats to the enterprise.
- Management proactively supports and anticipates innovations.
- Business management engages in continuous cross-functional collaboration.
- Executive management recognises the business value.

Section II, Chapter 5
Detailed Guidance: Appendix D

COBIT 5 ENABLERS



Information Security-specific Principles, Policies and Frameworks



Section II, Chapter 2
Detailed Guidance: Appendix A

Information Security-specific Services, Infrastructure and Applications

- Provide a security architecture.
- Provide security awareness.
- Provide secure development.
- Provide security assessments.
- Provide adequately secured and configured systems.
- Provide user access and access rights.
- Provide adequate protection against external attacks and intrusion attempts.
- Provide adequate incident response.
- Provide security testing.
- Provide monitoring and alert services.

Section II, Chapter 7
Detailed Guidance: Appendix F

Information Security-specific People, Skills and Competencies

- Information security governance
- Information security strategy formulation
- Information risk management
- Information security architecture development
- Information security operations
- Information assessment and testing and compliance

Section II, Chapter 8
Detailed Guidance: Appendix G

4. 包括的アプローチの実現

COBIT5 Enabling Processes プロセス参照モデル

BAI03 ソリューションの特定と構築の管理		領域：管理 ドメイン：構築、調達および導入
プロセスの概要 設計、開発、調達 / ソーシング、サプライヤー / ベンダーとの提携をカバーし事業体の要件と整合した特定済みのソリューションを構築、保守する。構成、テスト準備、テスト、要件の管理、さらにビジネスプロセス、アプリケーション、情報 / データ、クラウドチャおよびサービスの保守に関する管理を行う。		
プロセスの目的 事業体の戦略上と運用上の目標をサポートするような、タイムリーでコスト効率の高いソリューションを確立する。		
このプロセスは、以下の IT 達成目標の実現を支援する。		
IT 達成目標	関連する測定指標	
07 ビジネス要件に合致した IT サービスの提供	<ul style="list-style-type: none"> IT サービスのインシデントに起因する事業活動の中断件数 IT サービスが合意されたレベルを満たしていると感じている事業部門のステークホルダーの割合 品質に満足しているユーザーの割合 	

測定指標

インプットと
アウトプット

RACIチャート
(役割表)

BAI03 RACI チャート														
マネジメントの実践手法	取締役会 (理事会)	最高経営責任者 (CEO)	最高財務責任者 (CFO)	最高執行責任者 (COO)	事業部門の幹部	ビジネスプロセスオーナー	戦略執行委員会 (プロジェクト等の) 運営委員会	プロジェクトマネジメントオフィス	バリュー・マネジメントオフィス	最高リスク管理責任者 (CRO)	最高情報セキュリティ責任者 (CISO)	アーキテクチャ委員会	事業体のリスク管理委員会	人事責任者
BAI03.01 ソリューションの概要設計						R		I	R					
BAI03.02 ソリューションコンポーネントの詳細設計						R		I	R					
BAI03.03 ソリューションコンポーネントの開発						R		I	R					

BAI03 プロセス実践手法、インプット/アウトプットおよびアクティビティ				
マネジメントの実践手法		インプット		アウトプット
参照元	説明	説明	説明	送付先
BAI03.01	BAI03.01 ソリューションの概要設計 合意された適切なウォーターフォール型開発あるいは迅速なアジャイル開発手法を用いて、概要設計の作成および文書化を行う。IT 戦略およびエンタープライズアーキテクチャとの整合性を確認する。詳細設計または構築のフェーズにおいて、また、ソリューションの進行に伴って重要な問題が発生した場合には、設計の再評価と更新を行う。ステークホルダーが積極的に設計に参加し、各バージョンを承認していることを確認する。	APO03.01 アーキテクチャの原則	アーキテクチャの原則	承認済の概要設計仕様 BAI04.03 BAI05.01
APO03.02		APO03.02	ベースラインのドメインの記述とアーキテクチャの定義	
APO04.03		APO04.03	イノベーションの可能性の調査分析	
APO04.04		APO04.04	イノベーションのアイデアの評価	
BAI02.01		BAI02.01	ステークホルダーから確認済の受け入れ基準 要件定義のリポジトリ	
BAI02.02		BAI02.02	ハイレベルな取得 / 発計画	
アクティビティ				
<ol style="list-style-type: none"> 提案されたソリューションを、ビジネス要件およびエンタープライズアーキテクチャ、支援サービス、アプリケーション、インフラストラクチャ、情報リポジトリと整合性を確認する。 設計プロセスにおいて適切な資格と経験を有するユーザーと IT 専門家の関与を得る。IT 能力を最適に使用したソリューション設計となるようにする。 組織の設計標準に準拠し、ビジネス、事業体および IT の戦略、エンタープライズアーキテクチャと整合した設計をソリューションと開発手法に適した詳細レベルで作成する。 品質保証の承認後、最終的な概要設計をプロジェクトのステークホルダーおよびスポンサー / 顧客と共有し、合意された基準に基づき承認を得る。この設計は、プロジェクト全体を通して、理解が深まる。 				

4. 包括的アプローチの実現

COBIT 5 Framework

ガバナンスとマネジメントの分離

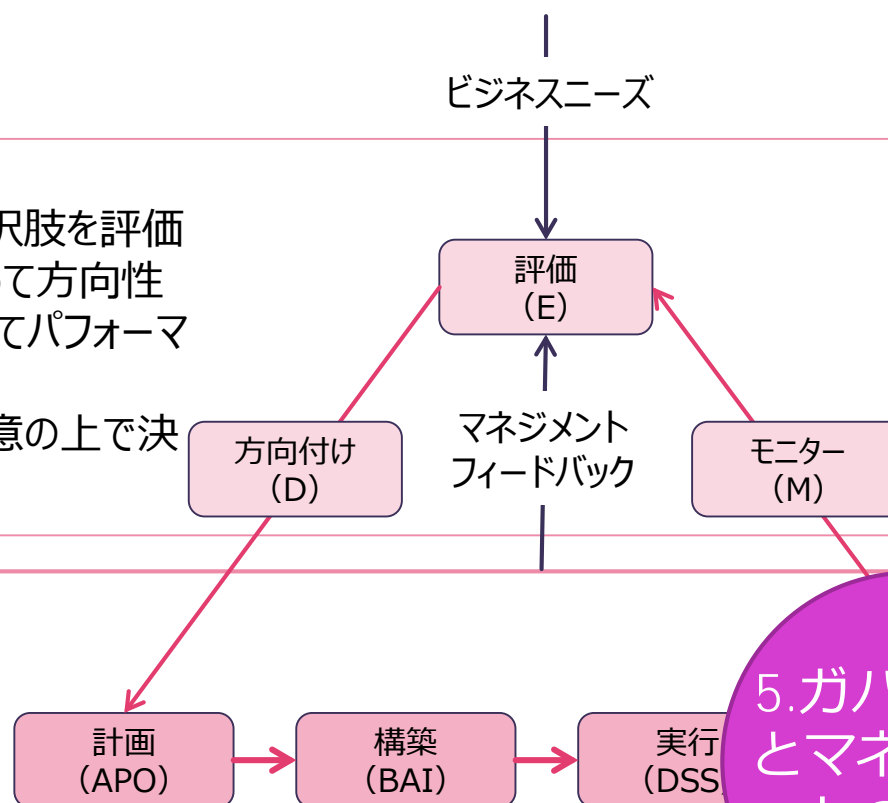
ガバナンス

ステイクホルダーのニーズや、条件、選択肢を評価し、優先順位の設定と意思決定によって方向性を定め、合意した方向性と目標に沿ってパフォーマンスや準拠性をモニターする。

事業体の目標がバランスを取って、合意の上で決定され、達成されることを確立する。

マネジメント

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アクティビティを計画、構築、実行し、評価する。



5.ガバナンス
とマネジメント
の分離

Q & A

ご清聴ありがとうございました。