CISMカンファレンス
COBIT概要と基準委員会でのサイバーセキュリティ翻訳活動の紹介

2017年2月18日

ISACA東京支部
基準委員会副委員長
CISA委員会委員
ISACA　HQ
New　Technology　Identification Working Group Member
福田重遠（Shigeto　Fukuda）,CISA

基準委員会の紹介

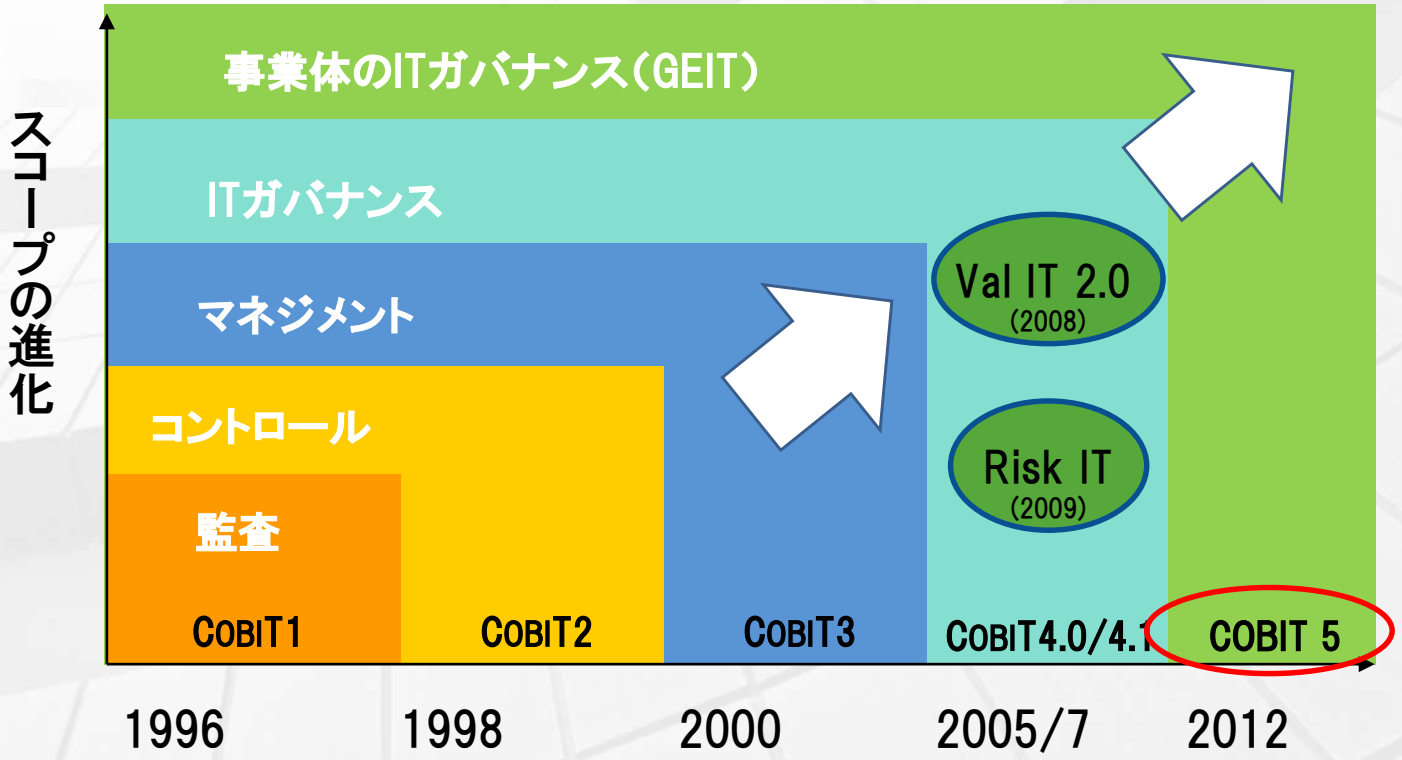
- 目標
  ISACAの基達成目標
  ISACA東京支部会員を中心とするステークホルダーへの価値創出
- ガバナンス基準・知識（知的資産）について、ISACA東京支部会員が理解を深め、知識獲得やスキルアップにつなげることを支援すると共に、支部会員を通じて日本国内にISACAの基準・知識を普及させる。
- 活動内容
  ISACAの基準・知識（知的資産）について、ISACA国際本部やITGI, Japan等の関連団体と連携して、ITAFやCOBIT5.0関連等のドキュメントの翻訳、支部会員向け講習会実施、委員会内勉強会等の活動を行う。
  （基準委員会のURL：http://www.isaca.gr.jp/standard/index.html）

COBITの紹介（COBITとの出会い）

2003年：COBIT３で、マネジメントとコントロールの違いを学ぶ

2010年：VAL　ITを読み、プログラムマネジメントの課題解決を試行

2013年：COBIT５でガバナンスとマネジメントの分離の本質を探究



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

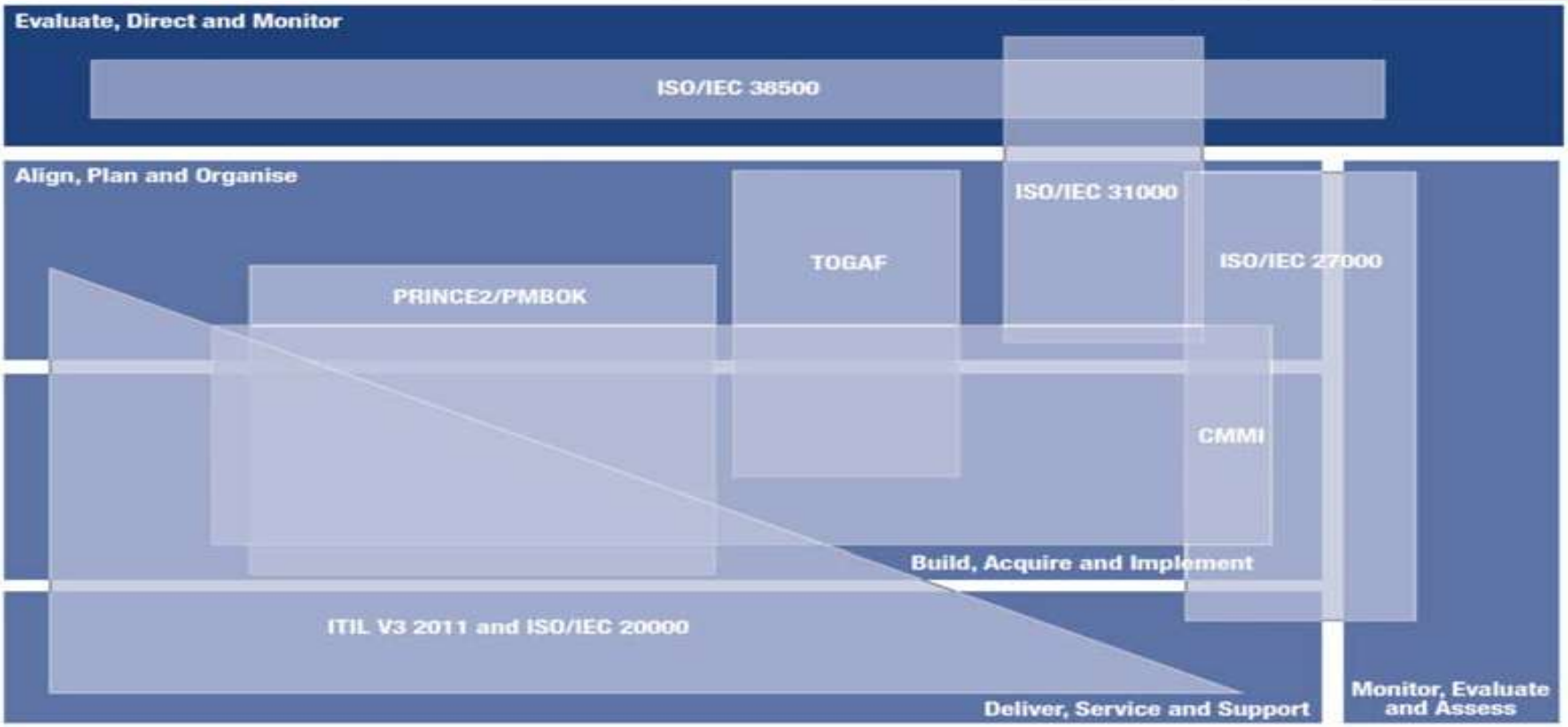
COBIT5の概要

- 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

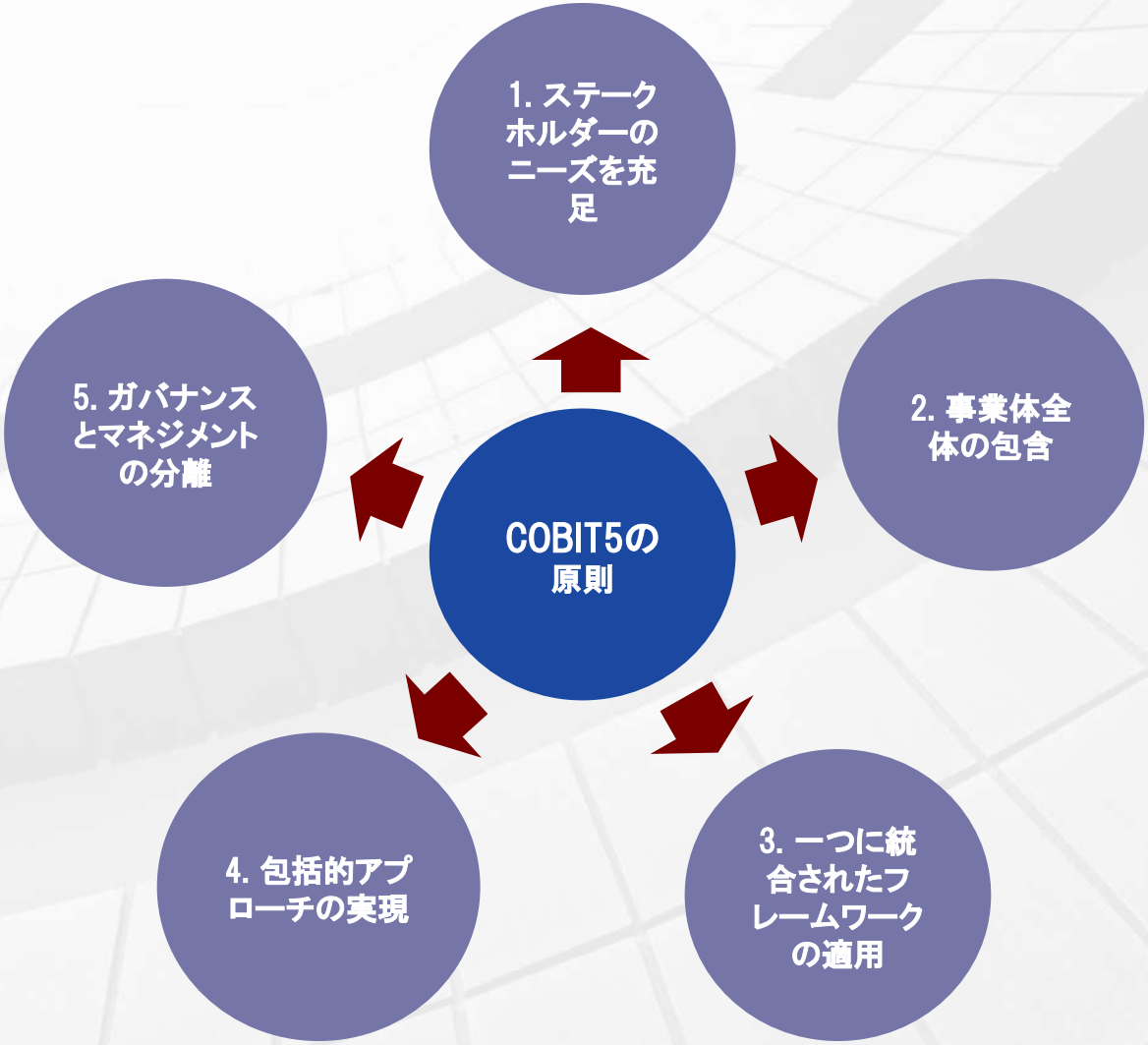
- 営利、非営利、公的機関等、すべての規模の事業体に適用でき、有効なもの

COBIT5と他フレームワークとの関係



- 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

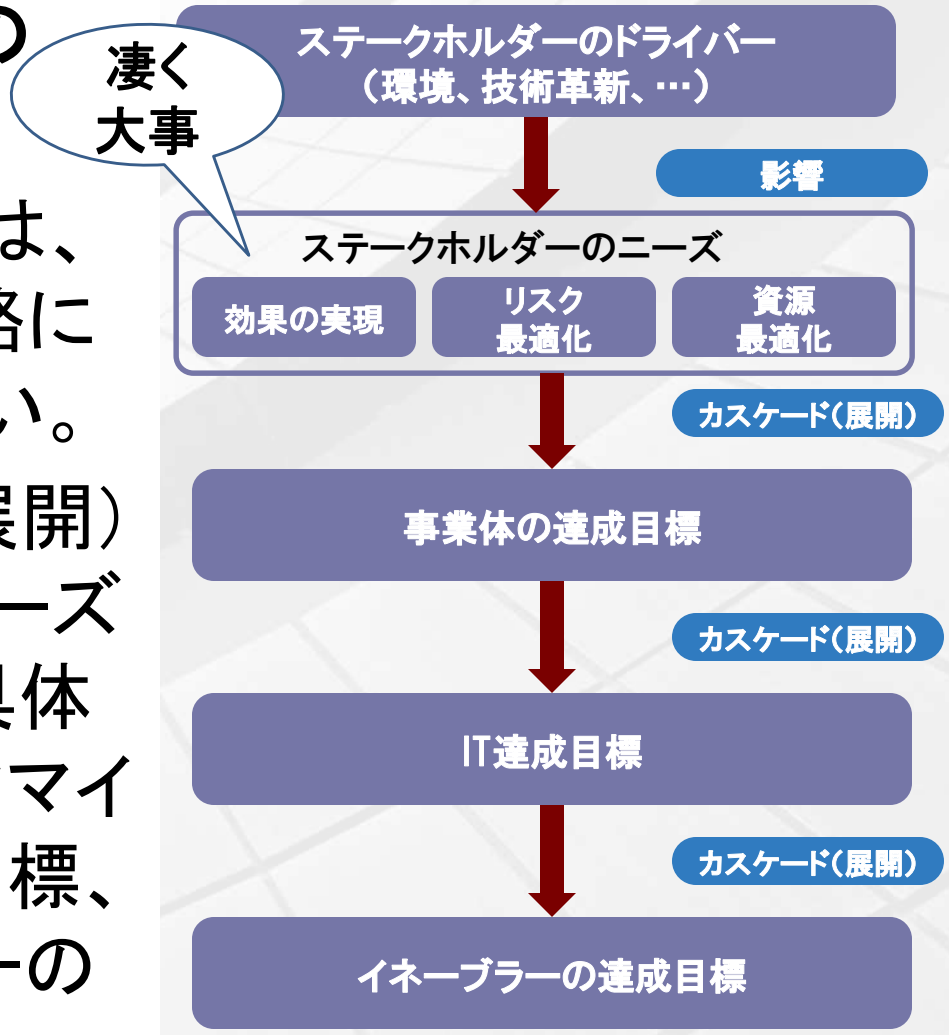
COBIT5　5つの原則



COBIT5　5つの原則（その1）

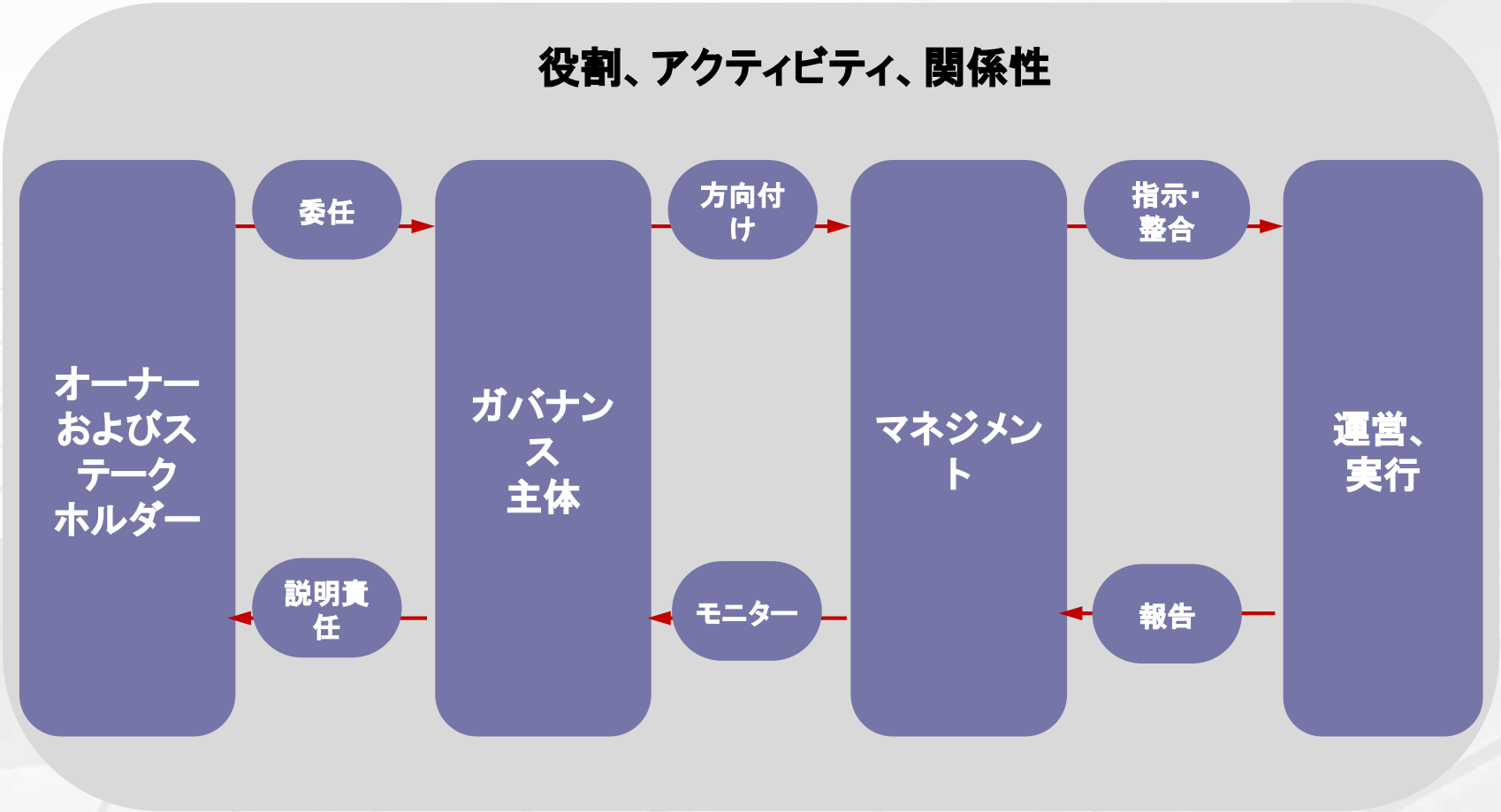
原則1．ステークホルダーのニーズを充足

- ステークホルダーニーズは、事業体の実行可能な戦略に変換されなければならない。
- 達成目標のカスケード（展開）はステークホルダーのニーズを、その状況における、具体的で、実行可能で、カスタマイズされた事業体の達成目標、IT達成目標、イネーブラーの達成目標へと変換する。



COBIT5　5つの原則（その2）

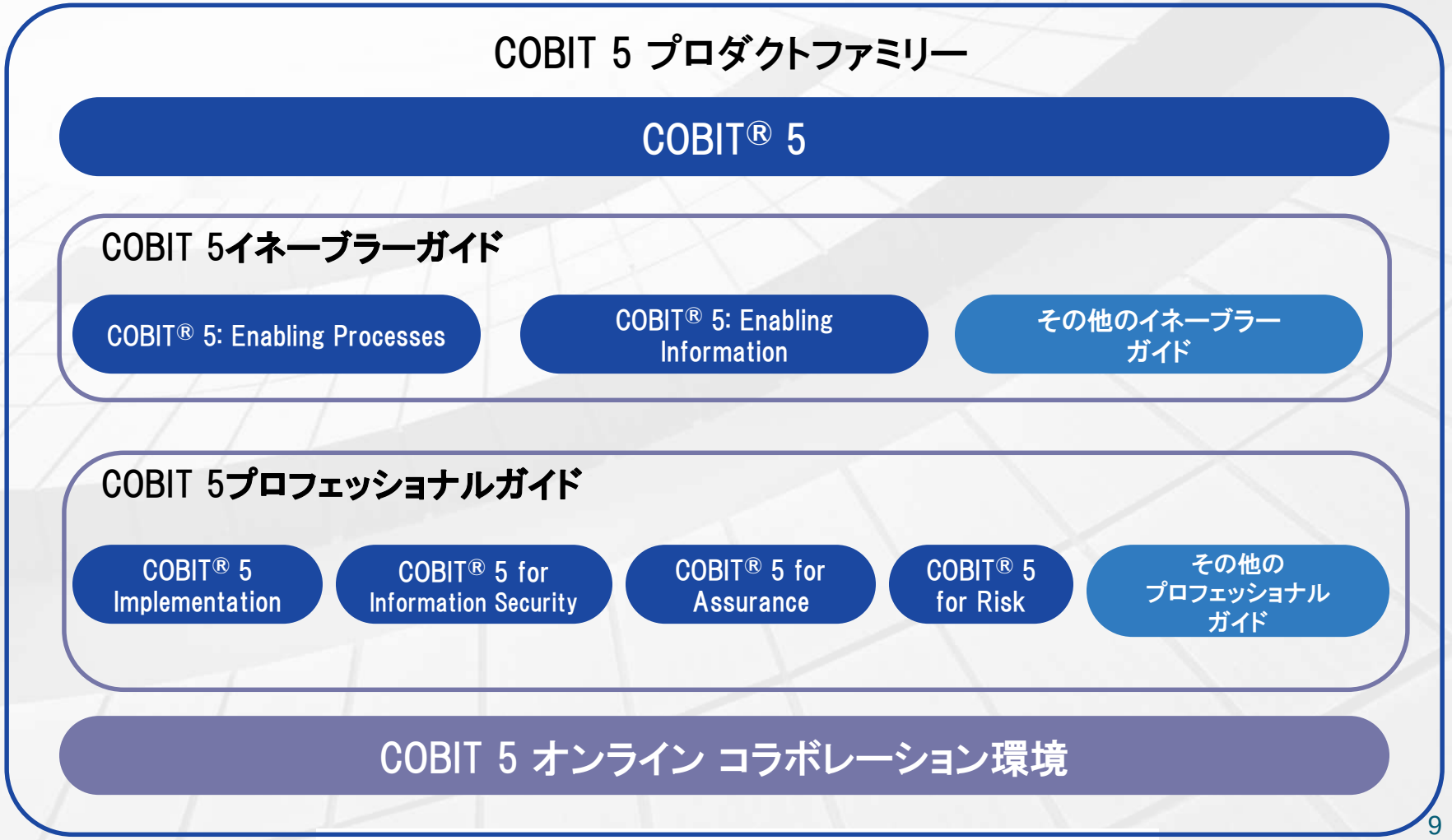
原則2. 事業体全体の包含



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

COBIT5　5つの原則（その3）

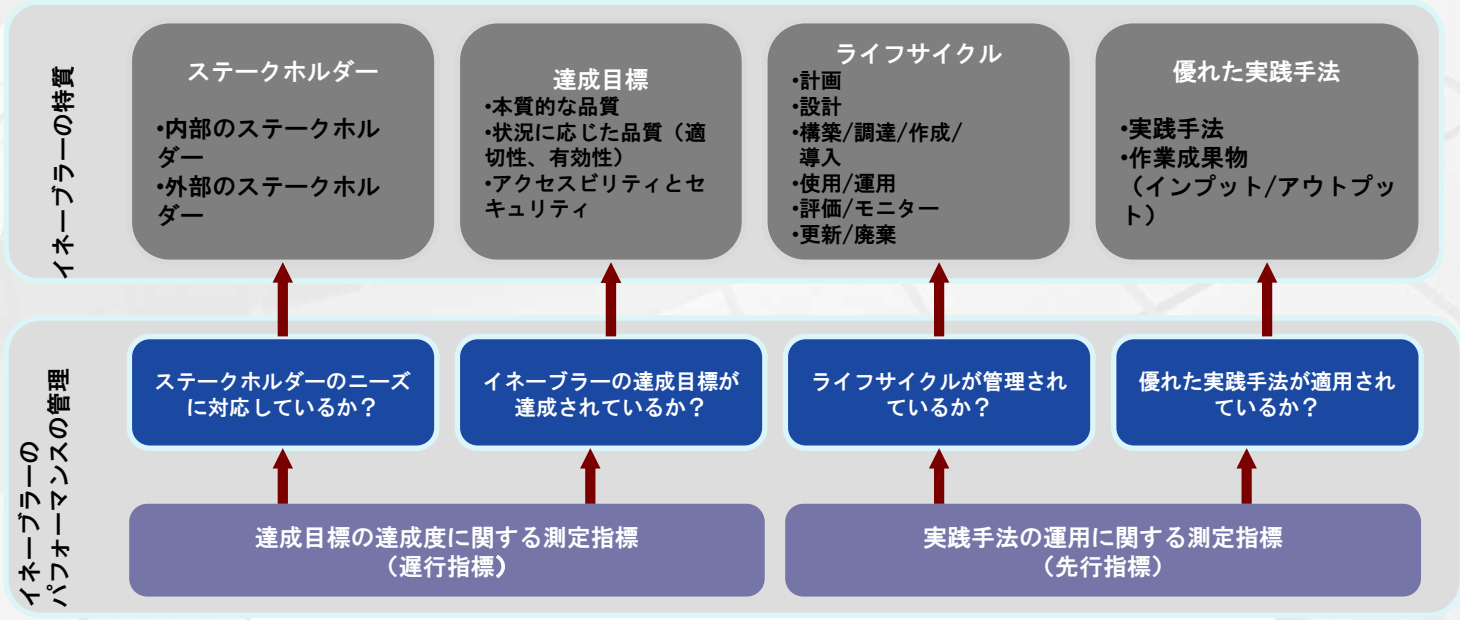
原則3. 一つに統合されたフレームワークの適用



COBIT5　5つの原則（その4）

原則4．包括的アプローチの実現（イネーブラー）

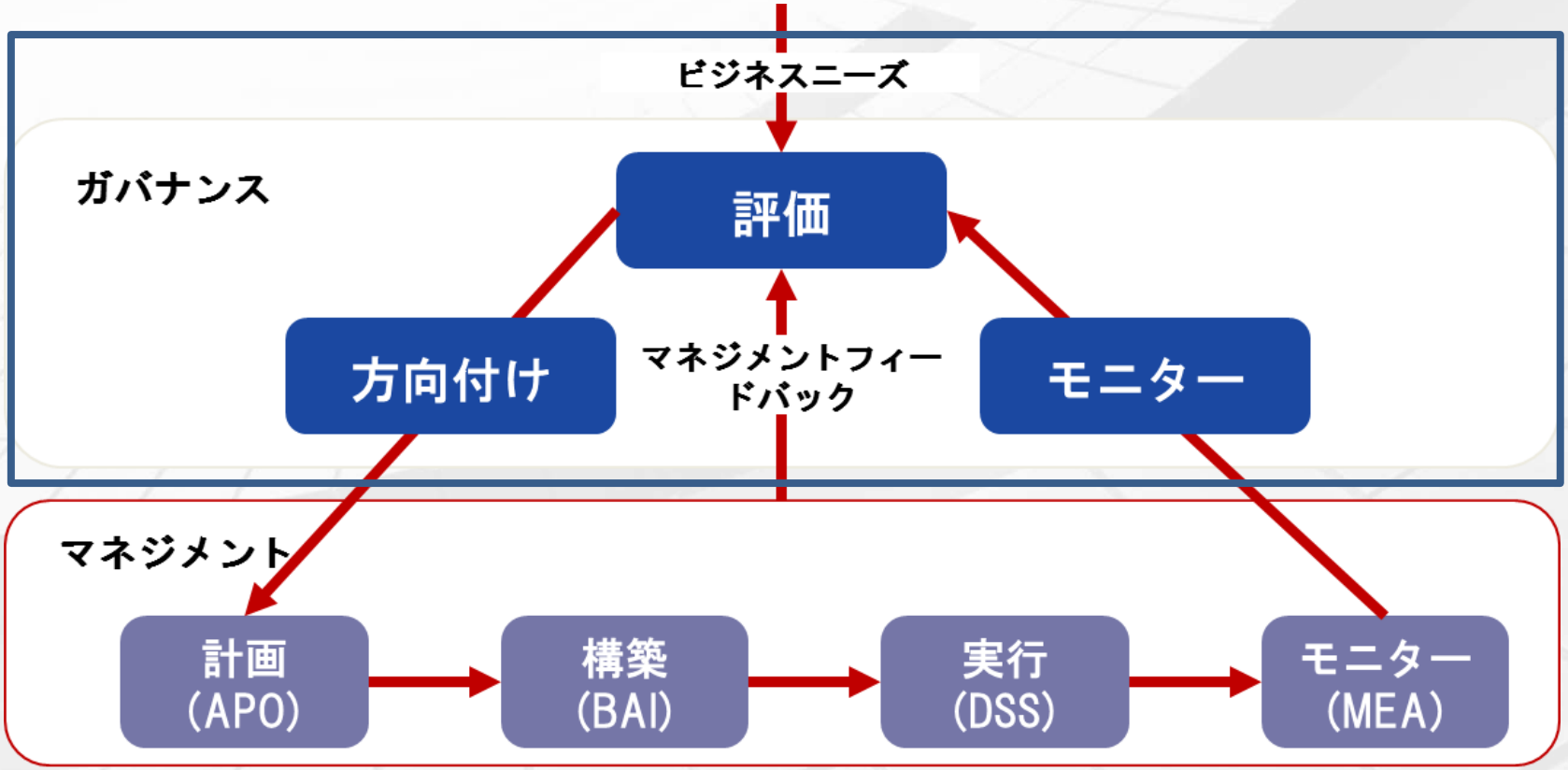
- イネーブラーを扱うため、共通、シンプルで構造化された方法
- 組織エンティティが複雑な相互作用を管理することが可能
- イネーブラーの成果達成を促進



出典: COBIT® 5 日本語版, 図表13.© 2012 ISACA® All rights reserved.

COBIT5　5つの原則（その5）

原則5.ガバナンスと マネジメントの分離



出典: COBIT® 5 日本語版, 図表15. © 2012 ISACA® All rights reserved.

COBIT5の37プロセス

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 ステークホルダーからみた透明性の確保

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
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 サービス契約の管理
APO10 サプライヤーの管理
APO11 品質管理
APO12 リスク管理
APO13 セキュリティ管理

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 知識管理
BAI09 資産管理
BAI10 構成管理

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 ビジネスプロセスコントロールの管理

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 外部要件への準拠性のモニタリング、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

サイバーセキュリティ翻訳活動①

“NIST Cybersecurity Framework”

- 2016年4月から着手し最終レビュー中
- ISACAがNISTフレームワーク策定に大きく関与
- NISTとCOBITフレームワークとの互換性を強調
- IPAのNIST CSF翻訳も参考に使用

サイバーセキュリティ翻訳活動②

“NIST Cybersecurity Framework” COBIT5　5つの原則との対応付け

NIST CSF　7つのステップ	COBIT5　5つの原則
ステップ1　優先順位付けを行い、範囲を決定する。	原則1. ステークホルダーのニーズを充足する。
ステップ2　方向付けを行う。 ステップ3　「現在のプロファイル」を作成する。 ステップ4　リスクアセスメントを実施する。 ステップ5　「目標のプロファイル」を作成する。 ステップ6　ギャップを特定・分析し、優先順位付けを行う。	原則2. 事業体全体の包含 原則3. 一つに統合されたフレームワークの適用
ステップ7　行動計画を実施する。	原則4. 包括的アプローチの実現
なし	原則5. ガバナンスとマネジメントの分離

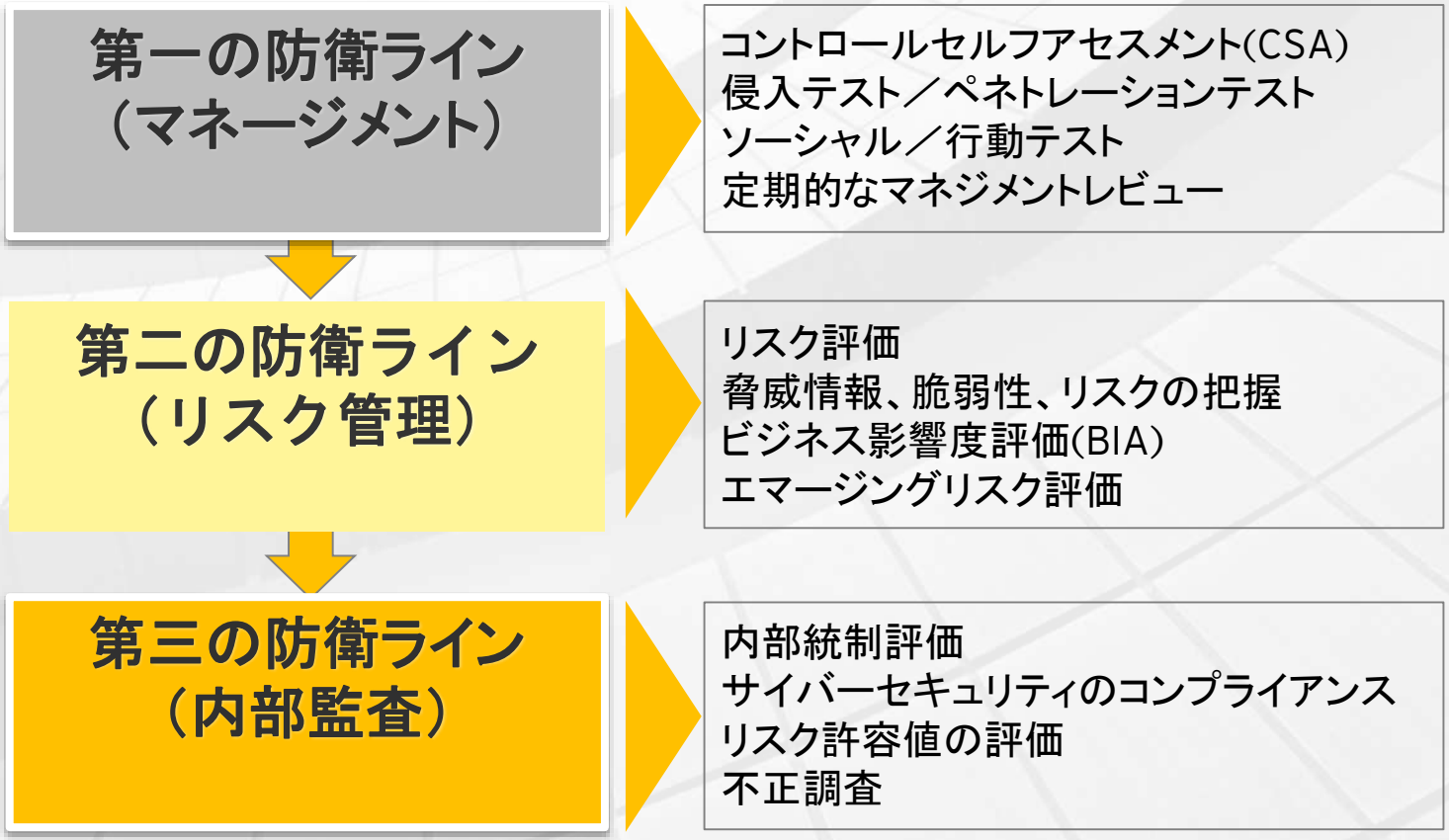
サイバーセキュリティ翻訳活動③

“Transforming Cybersecurity”

- 2016年7月から着手するも現在、レビュー中
- アメリカセキュリティの歴史から解説
- 日本語翻訳の訳語の検討に課題（例示）
  Emergence（訳語統一化）:
  出現、登場、カタカナなどケースバイケース
  Traveling user（日本語化）:
  外出時に公衆ネットワークに繋ぐ人？
  Generation Y:（アメリカ歴史等の理解）
  アメリカのY世代(1980-90年代生まれ)で
  インターネットを駆使する世代のこと

サイバーセキュリティ翻訳④

“Transforming Cybersecurity”
各防衛ラインで行うサイバーセキュリティ対応を整理。



※“Transforming Cybersecurity” © 2012 ISACAより改版＆引用

End