【ソフトバンクグループ会社の皆様へ】
東京海上日動システムズの
GRC/情報セキュリティ管理 態勢
～価値創出を目指したGRC改革～

2015年3月6日

東京海上日動システムズ（株）
GRC支援部 兼 経営企画部 上級エキスパート

ISACA（情報システムコントロール協会）
国際本部 委員 兼 東京支部 基準委員会 副委員長

稲葉　裕一

本日のアジェンダ

1. はじめに　～　自己紹介 と 自社紹介

2. 東京海上日動システムズのGRC改革

3. 東京海上日動システムズの情報セキュリティ改革

4. COBIT 5 活用のお勧め

5. まとめ

プロフィール

東京海上日動システムズ(株)
GRC支援部 兼 経営企画部　上級エキスパート
稲葉　裕一(いなば　ゆういち)
CISA, 技術士(情報工学部門)

- 東京海上グループ*会社のIT部門を歴任

年代	所属	活動
1992-1998	Tokio Marine Management, Inc (New York)	米国現地法人のIT管理全般
1998-2008	東京海上日動火災保険株式会社	2000年対応、合併プロジェクト管理、SOX対応、リスク管理
2008-2011	東京海上ホールディングス株式会社	グループITガバナンス態勢 の整備・普及活動
2011-現在	東京海上日動システムズ株式会社	GRC態勢 構築・整備・運用

*) 東京海上グループは、日本を拠点としてグローバルに保険事業を展開する企業グループです。

東京海上日動システムズ(株)会社概要

設立	1983年9月 東京海上のシステム開発会社として設立
	2004年10月 東京海上と日動火災の システムグループ会社3社が合併して 東京海上日動システムズが発足
社員数	1,381名 (2014年4月1日現在)
業務	東京海上グループの情報システムの 企画・提案・設計・開発・保守・運用
お客様	東京海上日動火災保険、 東京海上日動あんしん生命保険、等
HP URL ：	http://www.tmn-systems.co.jp/

本日のアジェンダ

1. はじめに　～　自己紹介 と 自社紹介

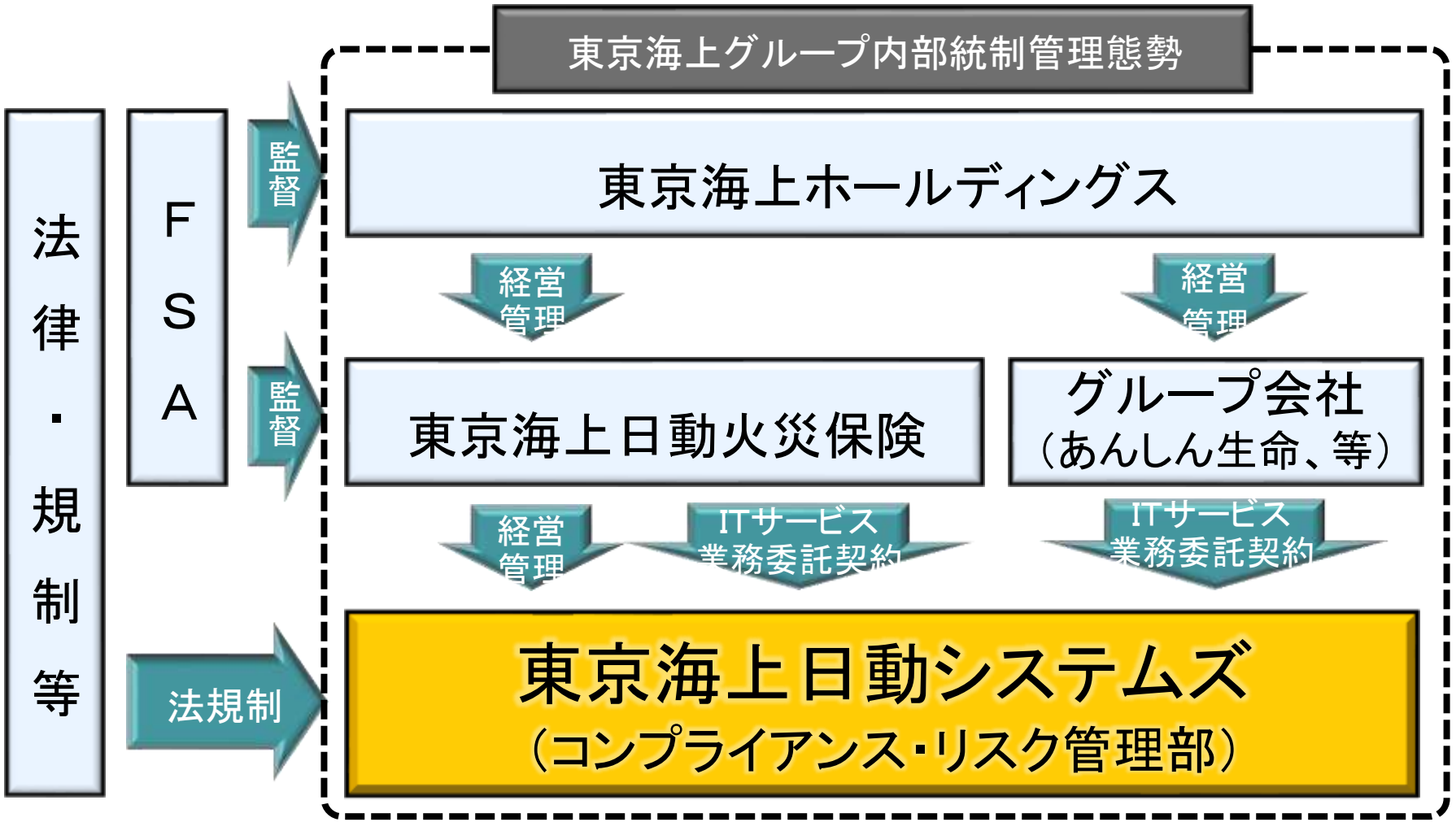
2. 東京海上日動システムズのGRC改革

3. 東京海上日動システムズの情報セキュリティ

4. COBIT 5 活用のお勧め

5. まとめ

弊社を取り巻く環境


東京海上グループ内部統制管理態勢
法律・規制等
FSA
監督
監督
法規制
東京海上ホールディングス
経営管理
経営管理
東京海上日動火災保険
グループ会社
（あんしん生命、等）
経営管理
ITサービス業務委託契約
ITサービス業務委託契約
東京海上日動システムズ
（コンプライアンス・リスク管理部）

守りのコンプライアンス・リスク管理

会社法施行

金融庁の規制
（保険検査マニュアル）

東京海上グループの
内部統制管理態勢に準拠

東京海上日動の求めるリスク
管理・コンプライアンスに対応

内部統制・リスク管理・コンプライアンスばかりで後ろ向き

新しいことは何もしないで、リスク回避、規制対応するのが楽だけど・・・

東京海上日動システムズの未来は？？？

守りのRCから価値創出を目指した攻めのGRCへ

守りのコンプライアンス・リスク管理 ～ 会社の将来への不安

お客様（ビジネス部門）と気持ちをシェアしてお客様価値を共に創出

社員がいきいきとスピード感を持って業務遂行できるように

そのためには、人材育成など企業価値を向上したい

価値創出を目指した攻めGRCへ

東京海上日動システムズの経営者の想い

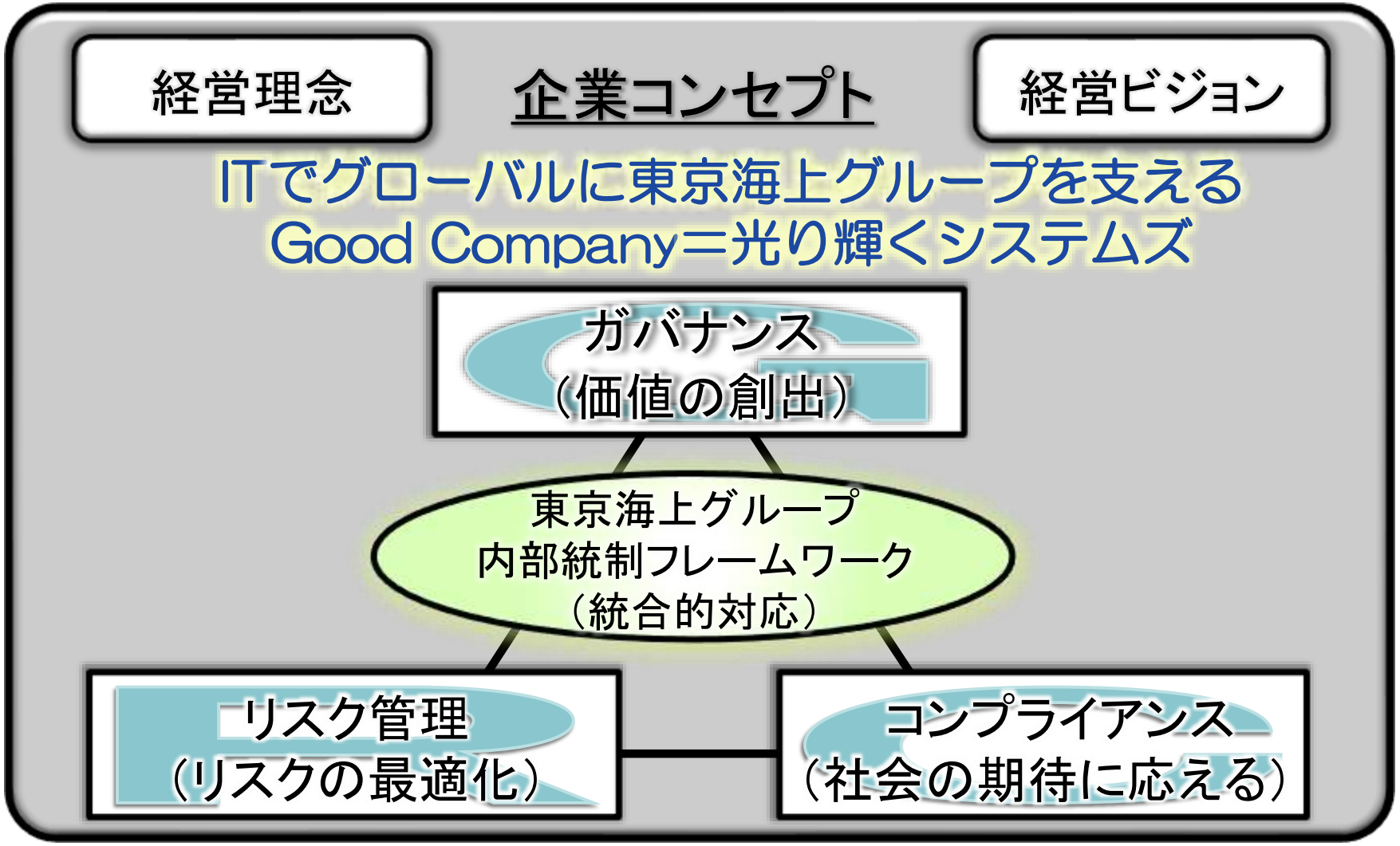
リスク最小化やコンプライアンスは
とても大事

だけどこればかりで、チャレンジを
忘れると会社の未来は危うい

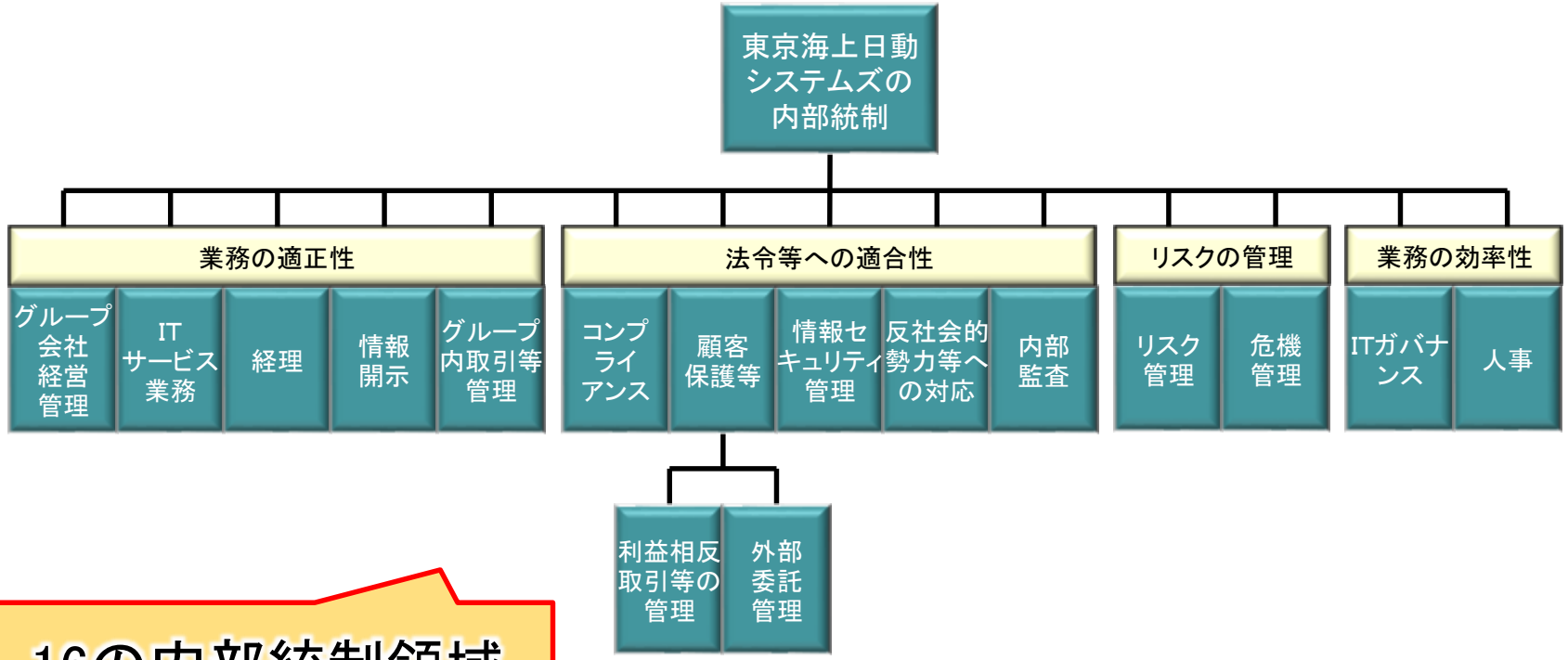
企業の使命は価値を創り出すこと
ではないか

そのための経営の舵取りが必要

経営者の想いを形に ~ GRCの概念

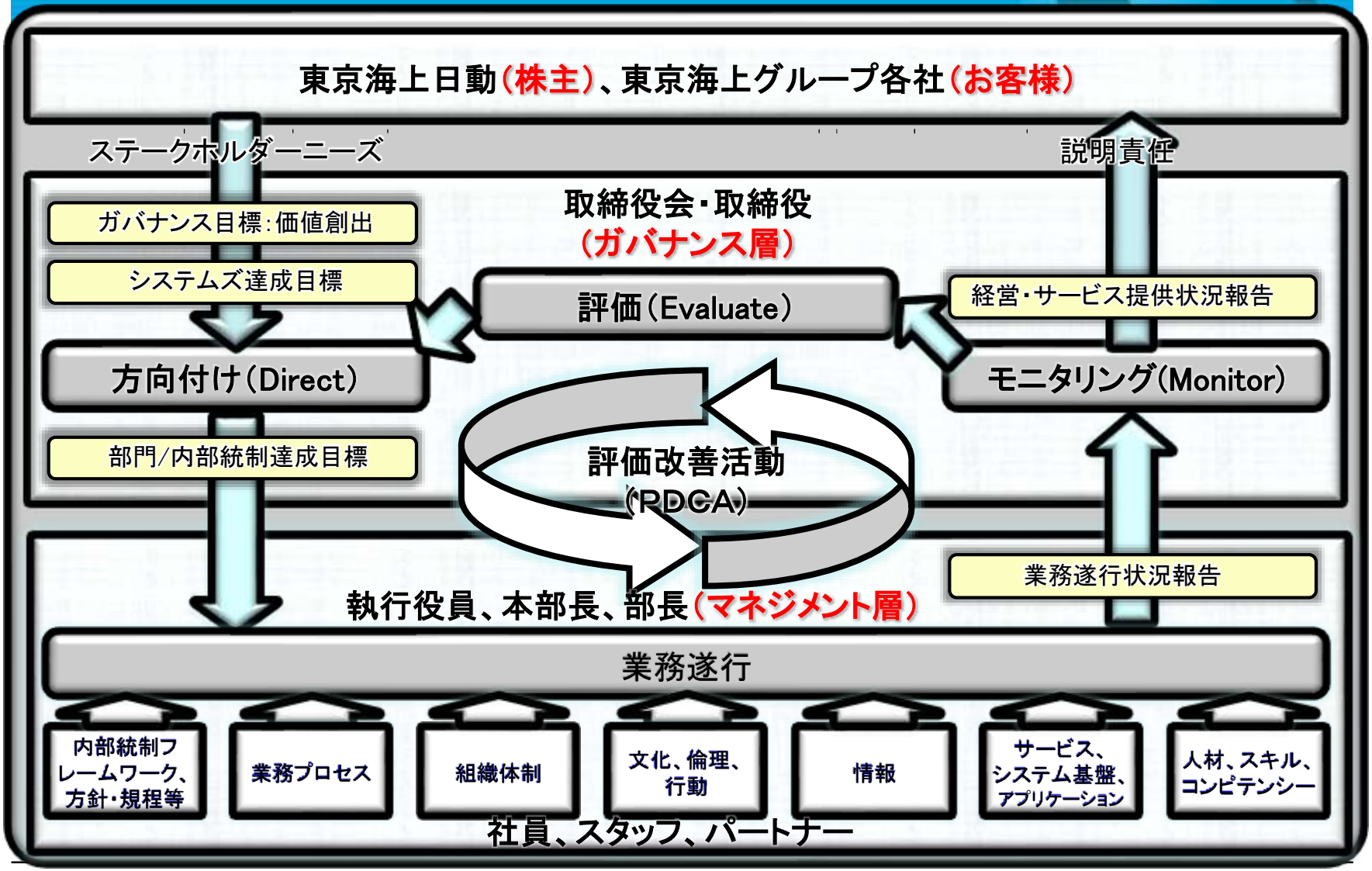


東京海上日動システムズの内部統制



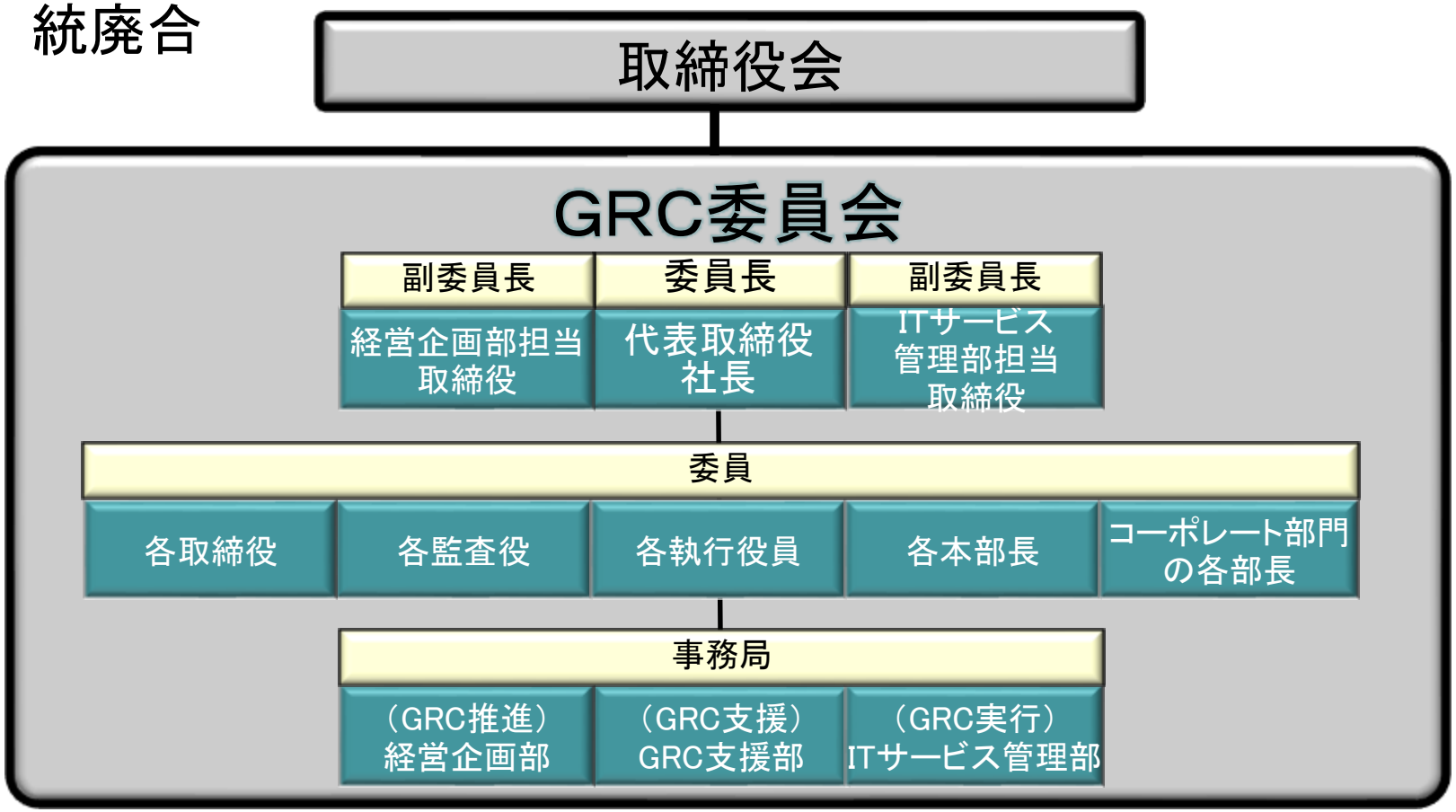
16の内部統制領域

東京海上日動システムズのGRC態勢

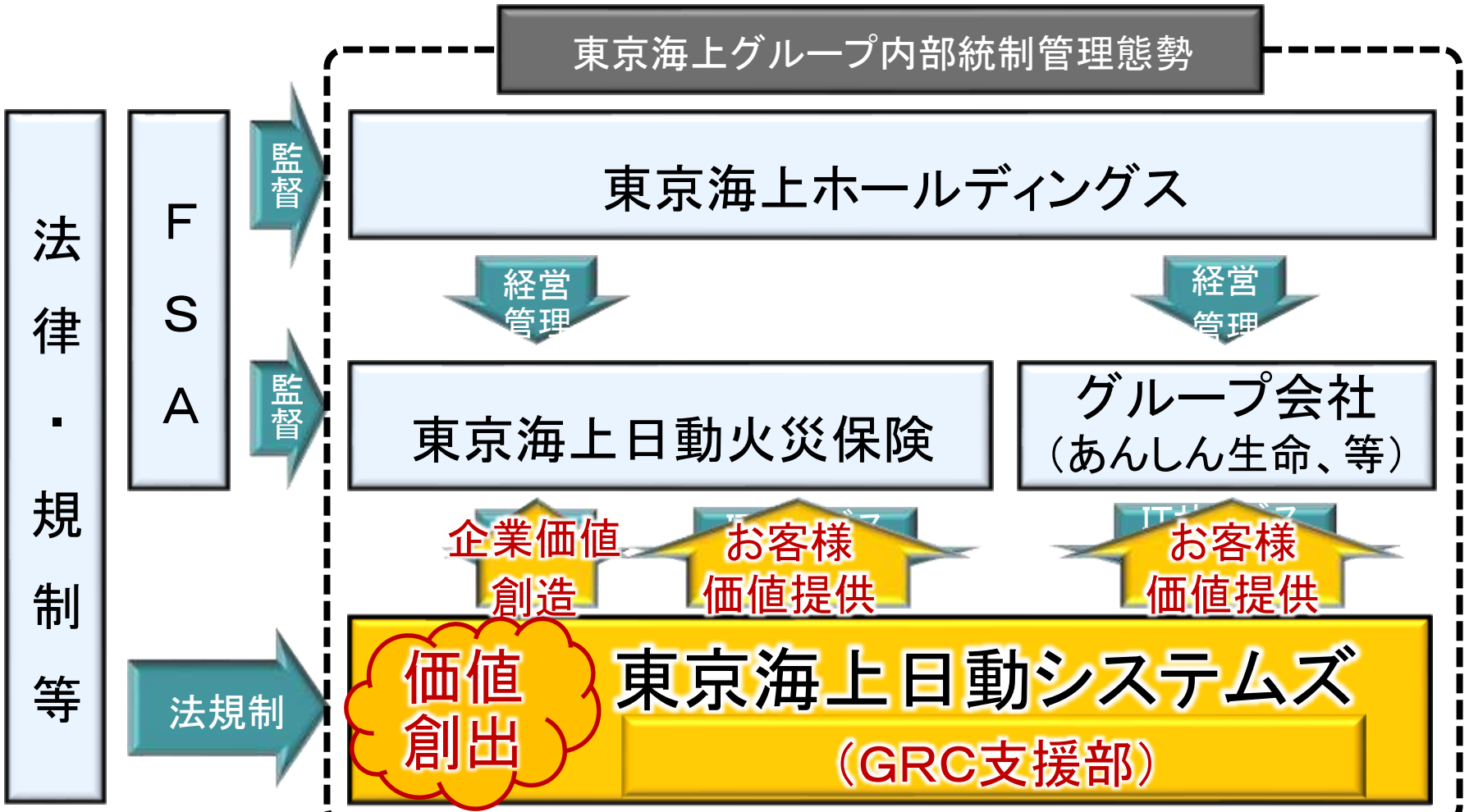


GRC委員会～継続的改善の推進エンジン

- ✓ GRCに関する論議の場を設置 ～ GRC委員会
- ✓ 旧3委員会（情報セキュリティ、コンプライアンス、危機管理）を統廃合



価値創出を目指した攻めのGRCへ



GRC改革の過程で苦労した点、良かった点

GRC改革を振り返って、個人的に次のように感じました。

<u>苦労した点</u>

- ✓ プロジェクト開始当初、各領域責任者の能動的参画を得ること
- ✓ 親会社（各内部統制・リスク所管部署）の承認を得ること
- ✓ 社員全員との「価値創出」の一体感を醸成すること

<u>良かった点</u>

- ✓ 経営トップの理解・支援（Buy in）と方向付け（Direct）
- ✓ 最終的に改革チーム全員の一体感を感じたこと
- ✓ 社員がいきいきとスピード感を持ってお客様の価値を創造していること
- ✓ 改革チームが社内MIP賞を受賞し認められたこと

（注）これらは、プロジェクトリーダーであった稲葉個人の感想であり、組織として総括した内容ではありません。

本日のアジェンダ

1. はじめに　～　自己紹介 と 自社紹介

2. 東京海上日動システムズのGRC改革

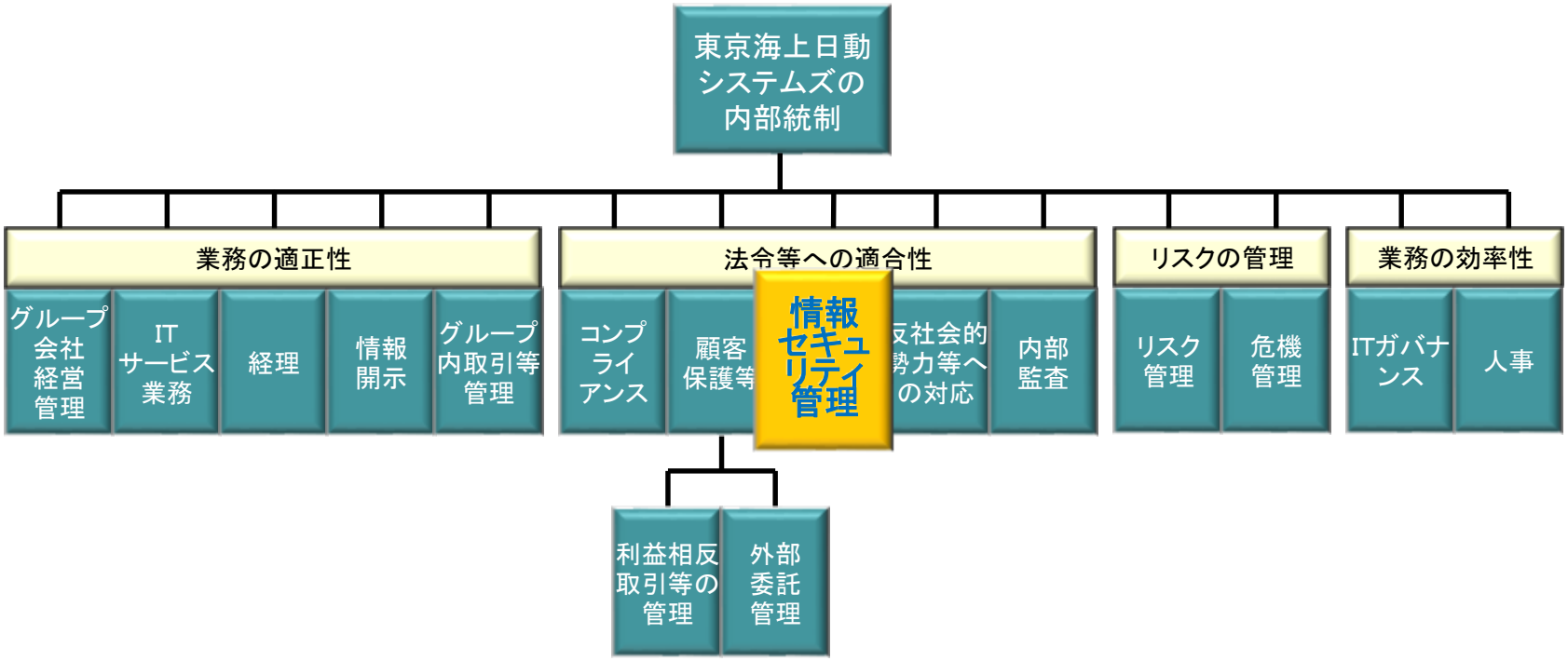
3. 東京海上日動システムズの情報セキュリティ改革

4. COBIT 5 活用のお勧め

5. まとめ

情報セキュリティ管理　～GRCの重要領域

- GRC態勢により以下の16の内部統制領域をガバナンス
- 「情報セキュリティ管理」はその中心的な領域に位置づけられる



守りから攻めに転じる情報セキュリティへ

守りの情報セキュリティばかりで大変、
お客様（ビジネス部門）のビジネスにブレーキをかけているのではないか？

お客様と気持ちをシェアしてビジネス価値を共に創出しなければ・・・

新しい技術を積極的に活用し、お客様が保険サービスを通じて世の中の
人々のニーズに応えることをサポートしたい

ビジネス戦略の実現を加速させる情報セキュリティであるべき

価値創出を目指した攻めの情報セキュリティへ

情報セキュリティに関するGRC

情報セキュリティ管理に関する基本方針

基本的考え方

情報セキュリティリスクを最適化する

明確化

重要情報を徹底的に守り抜く

再確認

態勢の整備

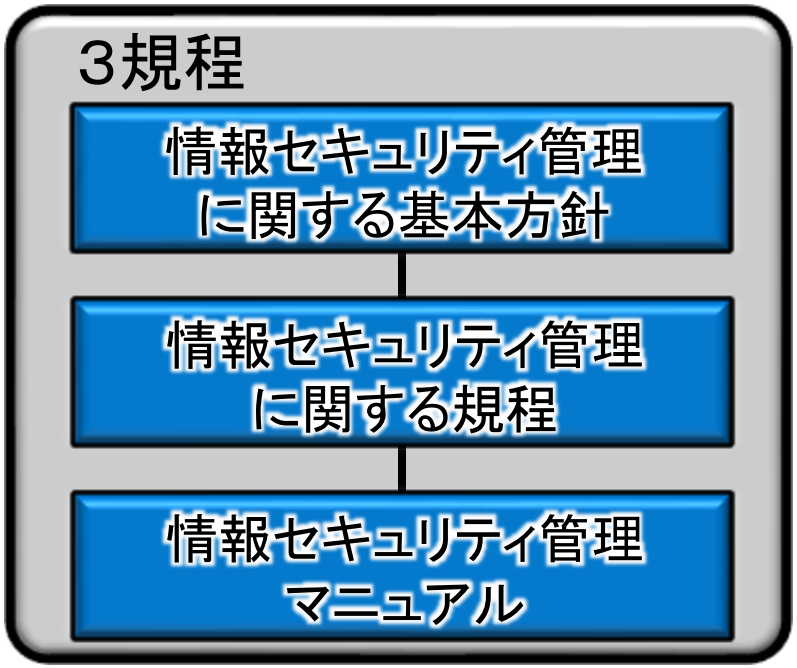
（ルール面）
方針・規程等の策定

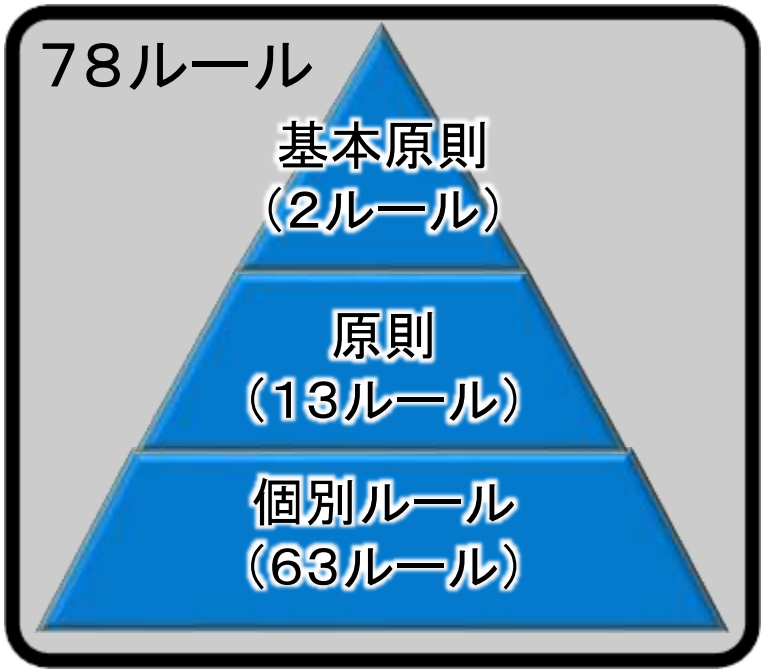
（組織面）
組織体制の整備

（PDCAプロセス面）
評価・改善活動

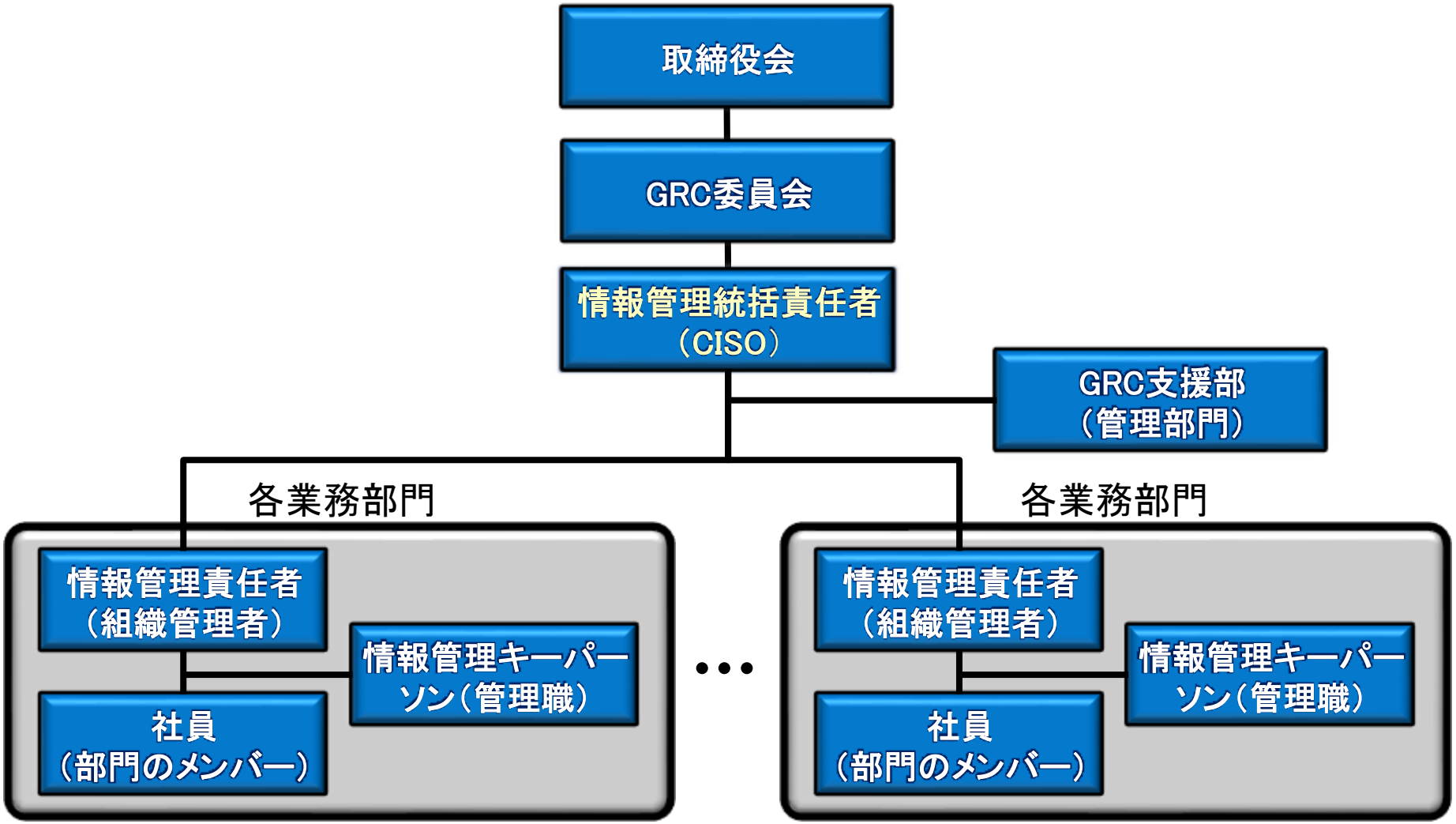
情報セキュリティルールの最適化、シンプル化

- 徹底的なルールの見直し
  - ✓【最適化】サイバーセキュリティをはじめとする重要リスク、新しいリスクにしっかり向き合い、過剰な統制ルールをとことん軽減・廃止する
  - ✓【シンプル化】プリンシプルベースでルールを統廃合する
- 成果：（改革前）15規程318ルール　➡　（改革後）3規程78ルール

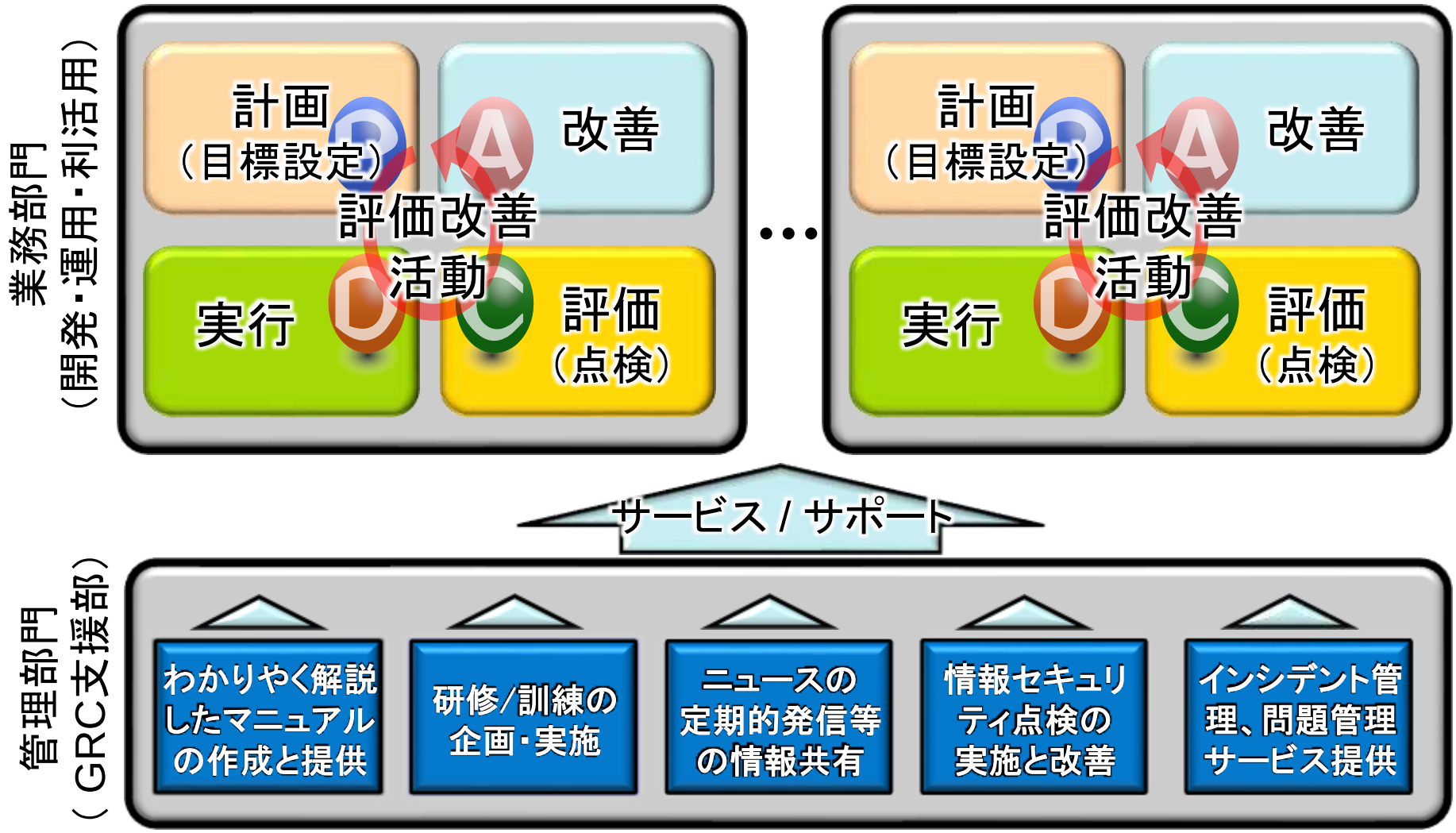




情報セキュリティ管理体制



情報セキュリティ管理　評価・改善活動（業務部門）



情報セキュリティ管理　評価・改善活動（管理部門）

管理部門
（GRC支援部）

GRCの要請

ガバナンス目標 （価値の創出）	リスク管理目標 （リスクの最適化）	コンプライアンス目標 （社会要請への対応）

CISO of the Year No.1 Awardを受賞

日本CISO協会様の2014年度「CISO 10 Award」において、弊社のCISO 宇野代表取締役社長が「CISO of the Year No.1」を受賞
（副賞としてベストCEO賞、ベスト・イノベーション賞を合わせて受賞）
http://www.cisojapan.org/award/report.html

“CISO of the Year No.1 Award：
東京海上日動システムズ 代表取締役社長
宇野直樹 氏

情報セキュリティに関する規程やルールの抜本的な刷新に対し、CEOの立場で鋭意推進し、多くの組織に対してもモデル（規範）となる実績を残した。“

（出典：IT Media エンタープライズ12月2日記事）

情報セキュリティ改革の過程で苦労した点、良かった点

情報セキュリティ改革を振り返って、個人的に次のように感じました。

苦労した点

- ✓ 散在する多数の細かなルールの「なぜ」の追求と関係整理
- ✓ 「重要情報をしっかり守ること（損失の最小化）」と「ビジネスを加速させる武器とすること（効果の最大化）」の両立
- ✓ 社員が情報セキュリティについて自ら考え行動してもらう一方で、詳しいマニュアルによりルールを理解しやすいようにする工夫

良かった点

- ✓ 経営トップの強力なリーダーシップが得られたこと
- ✓ プリンシプルベースのわかりやすいルールとし、「箸の上げ下ろし」はルールの実践事例として解説するようなマニュアルを整備できたこと
- ✓ 各業務部門が情報セキュリティのPDCAを自主的に回しながら、社員がいきいきとスピード感をもってお客様へ価値を提供していること

（注）これらは、プロジェクトリーダーであった稲葉個人の感想であり、組織として総括した内容ではありません。

本日のアジェンダ

1. はじめに　～　自己紹介 と 自社紹介

2. 東京海上日動システムズのGRC改革

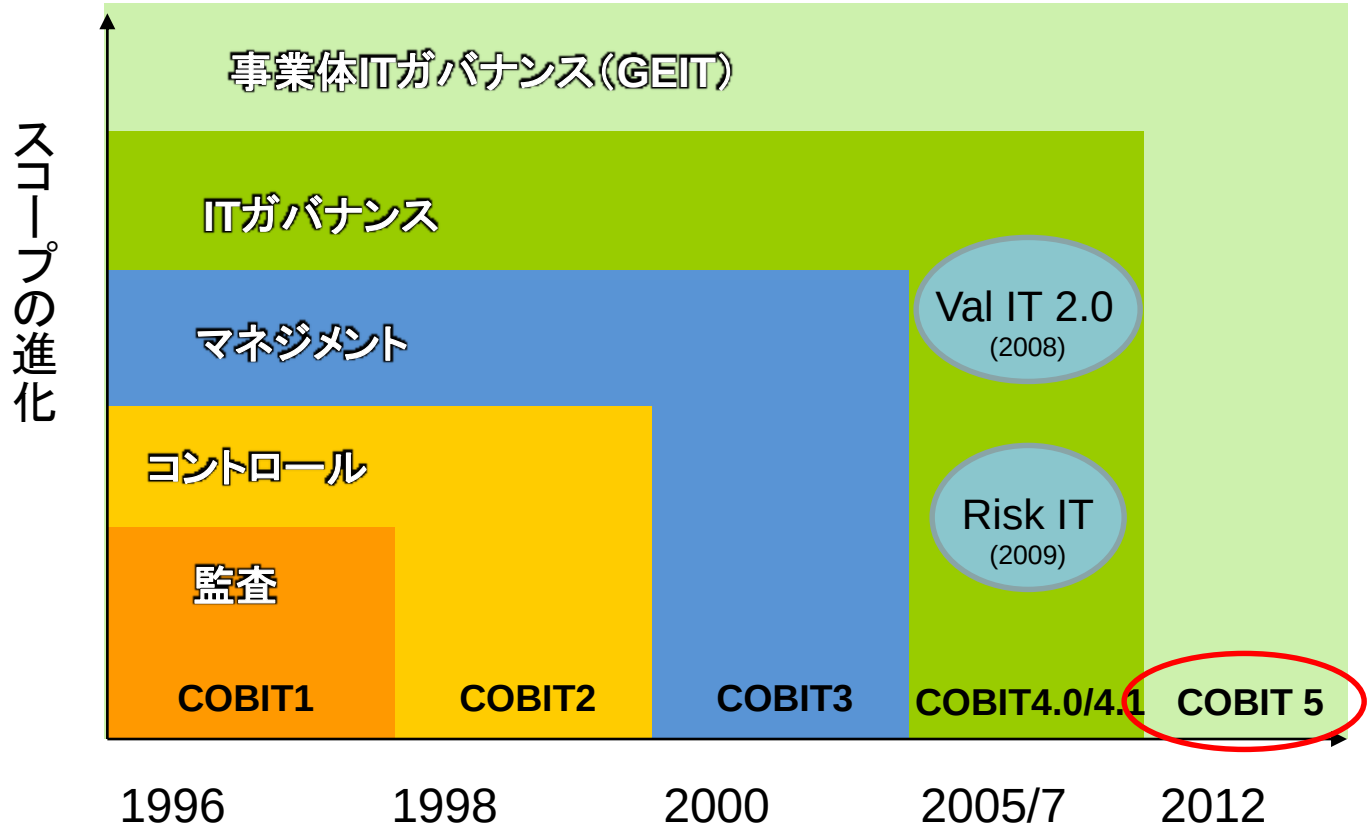
3. 東京海上日動システムズの情報セキュリティ改革

4. COBIT 5 活用のお勧め

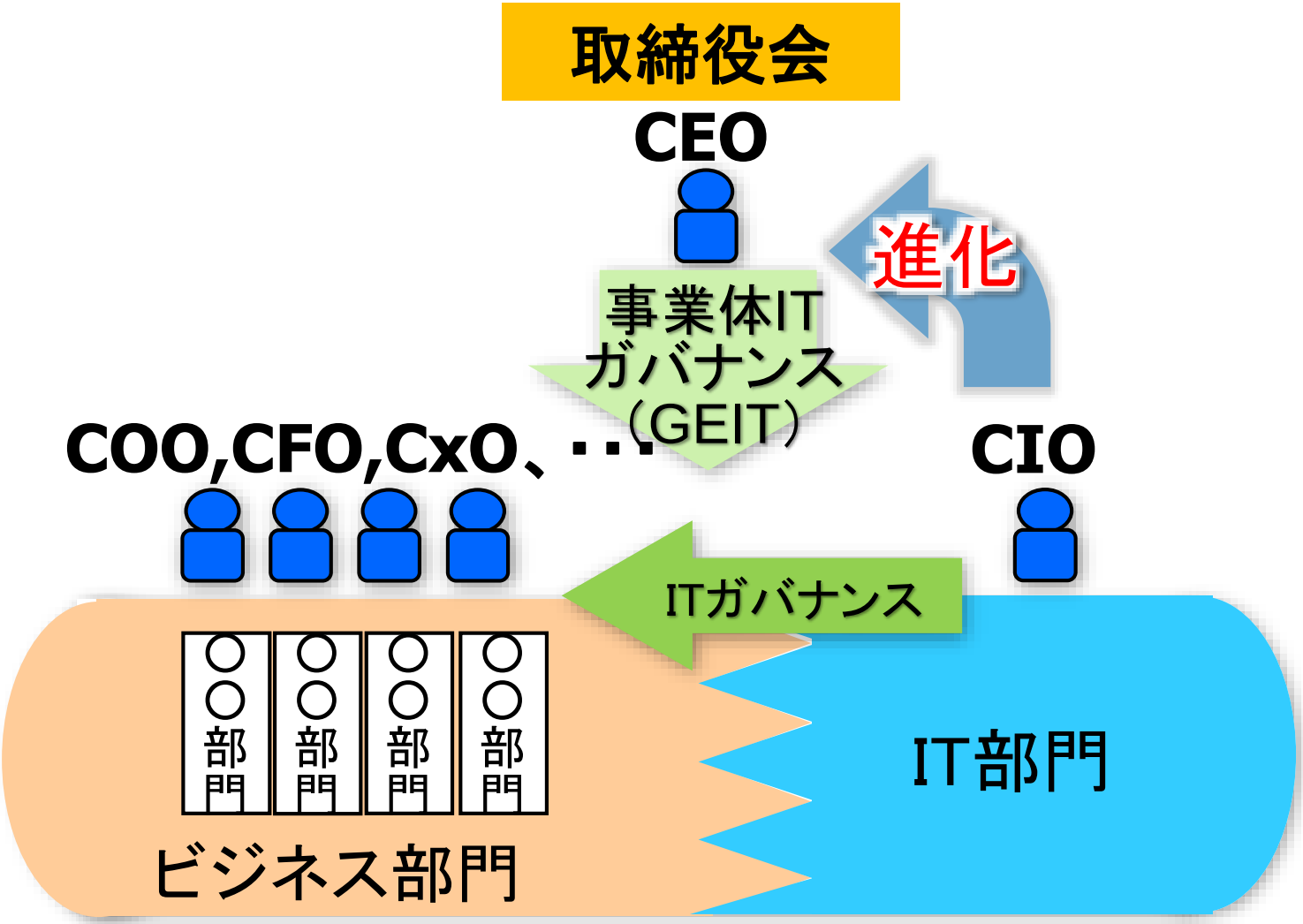
5. まとめ

COBIT 5 ～ ITガバナンスから事業体ITガバナンスへ

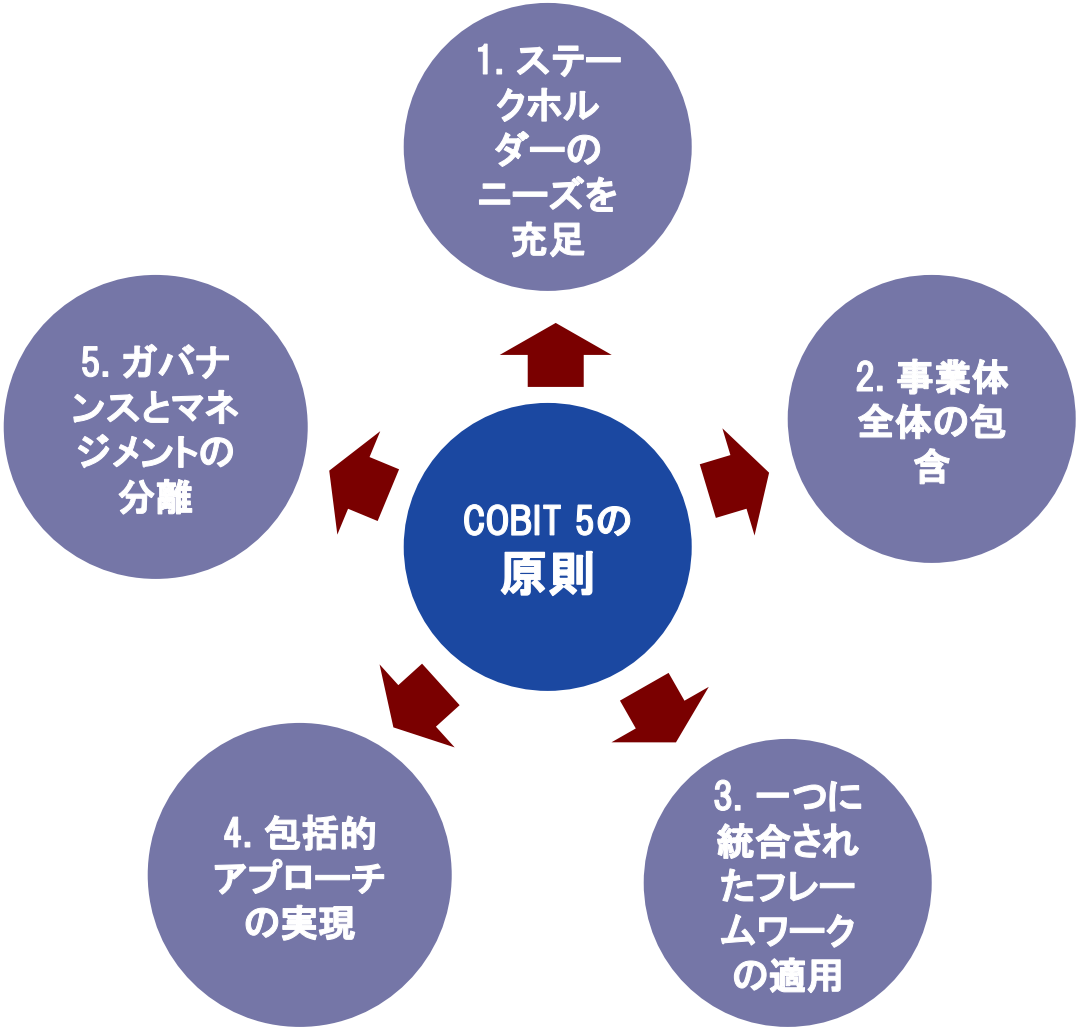
COBIT 5はISACA（情報システムコントロール協会）が提供する事業体ITガバナンスのためのフレームワークです。www.isaca.org/cobit



事業体ITガバナンス　～　CEOの視点へ

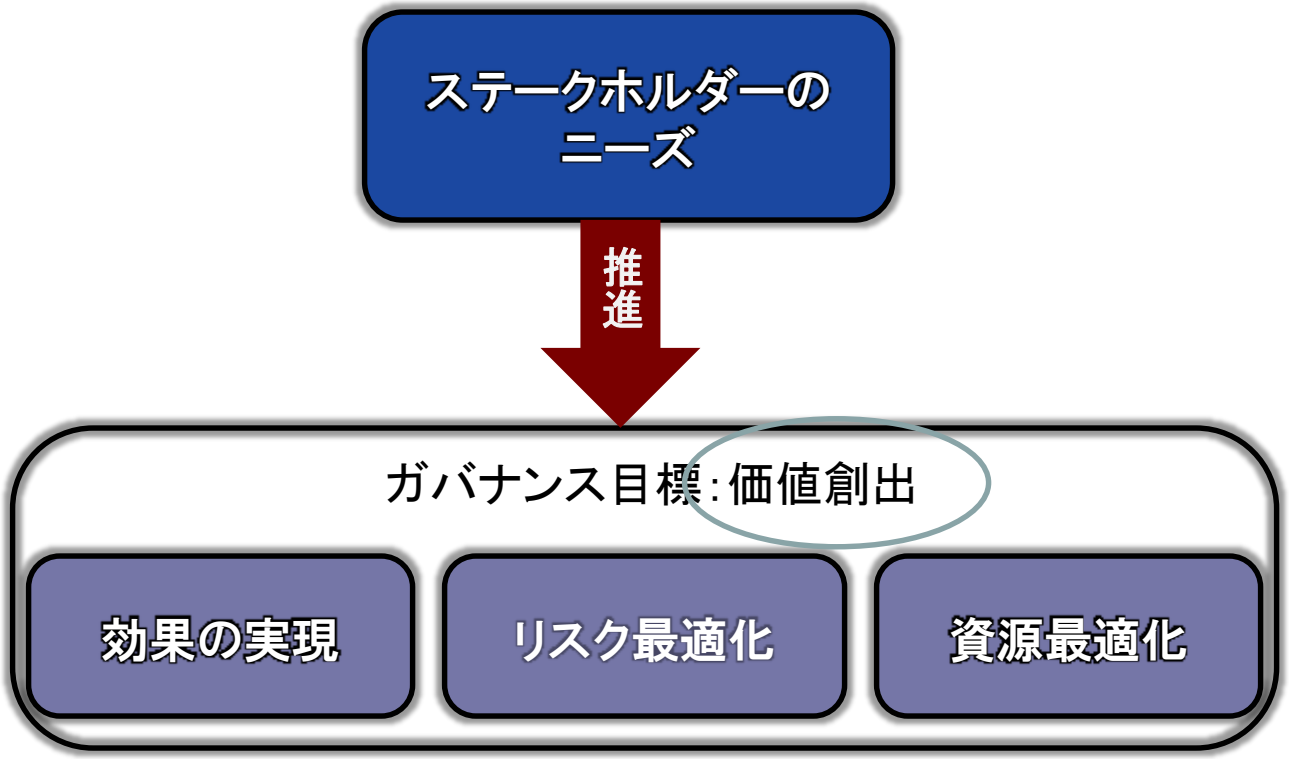


COBIT 5 の 5つの原則 ～ 事業体ITガバナンス



COBIT 5 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。

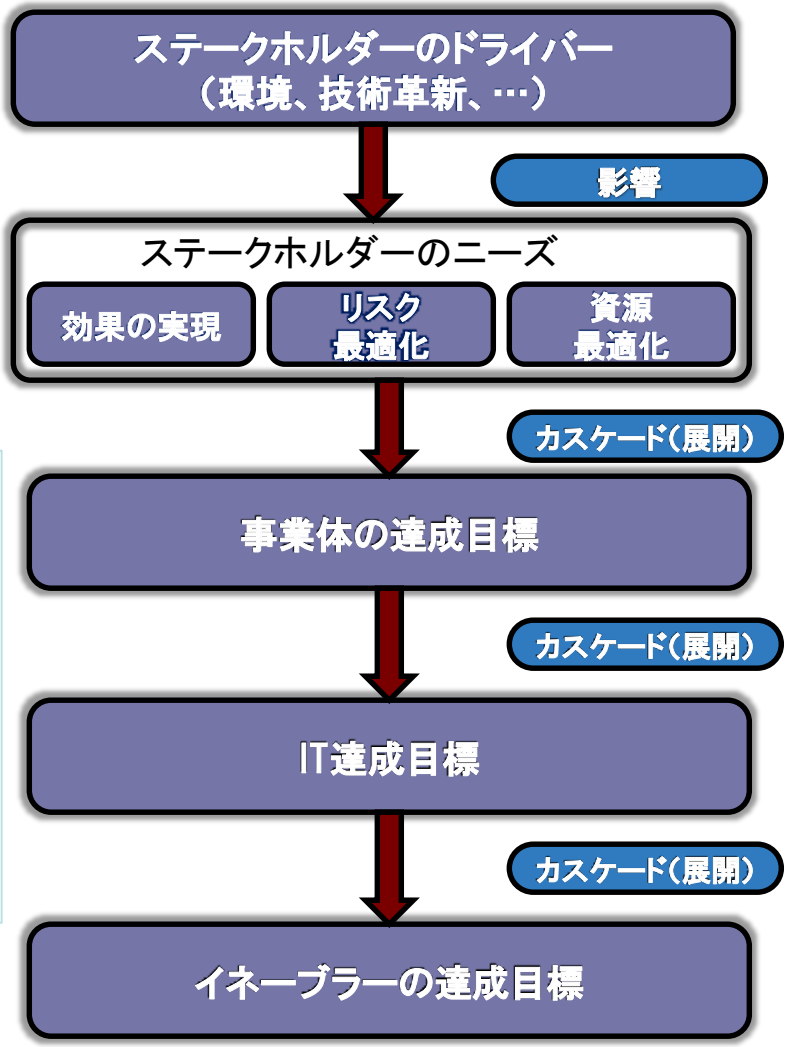


出典: COBIT® 5 日本語版, 図表3.. © 2012 ISACA® All rights reserved.

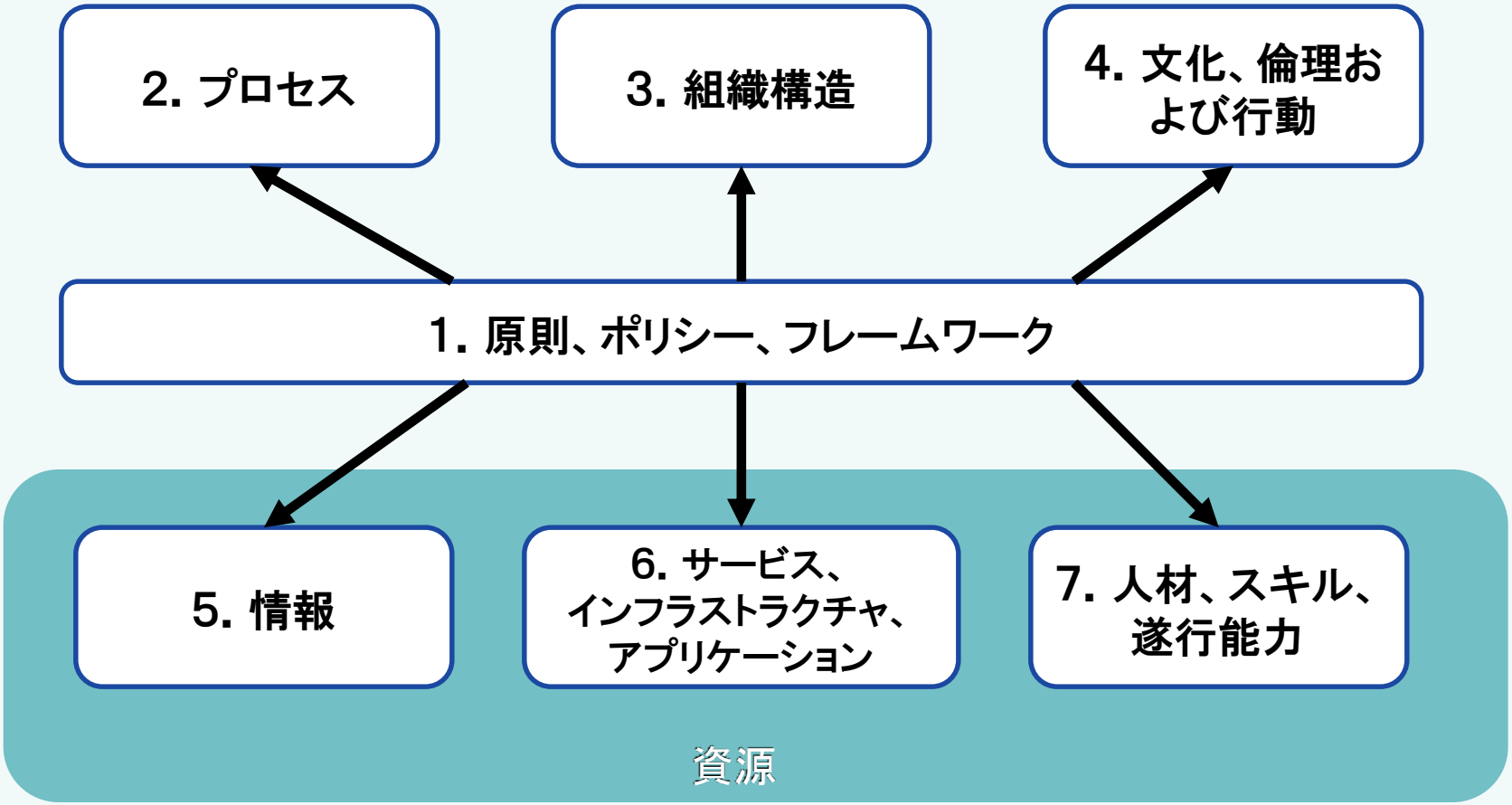
COBIT 5 原則1. ステークホルダーのニーズを充足

- 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)

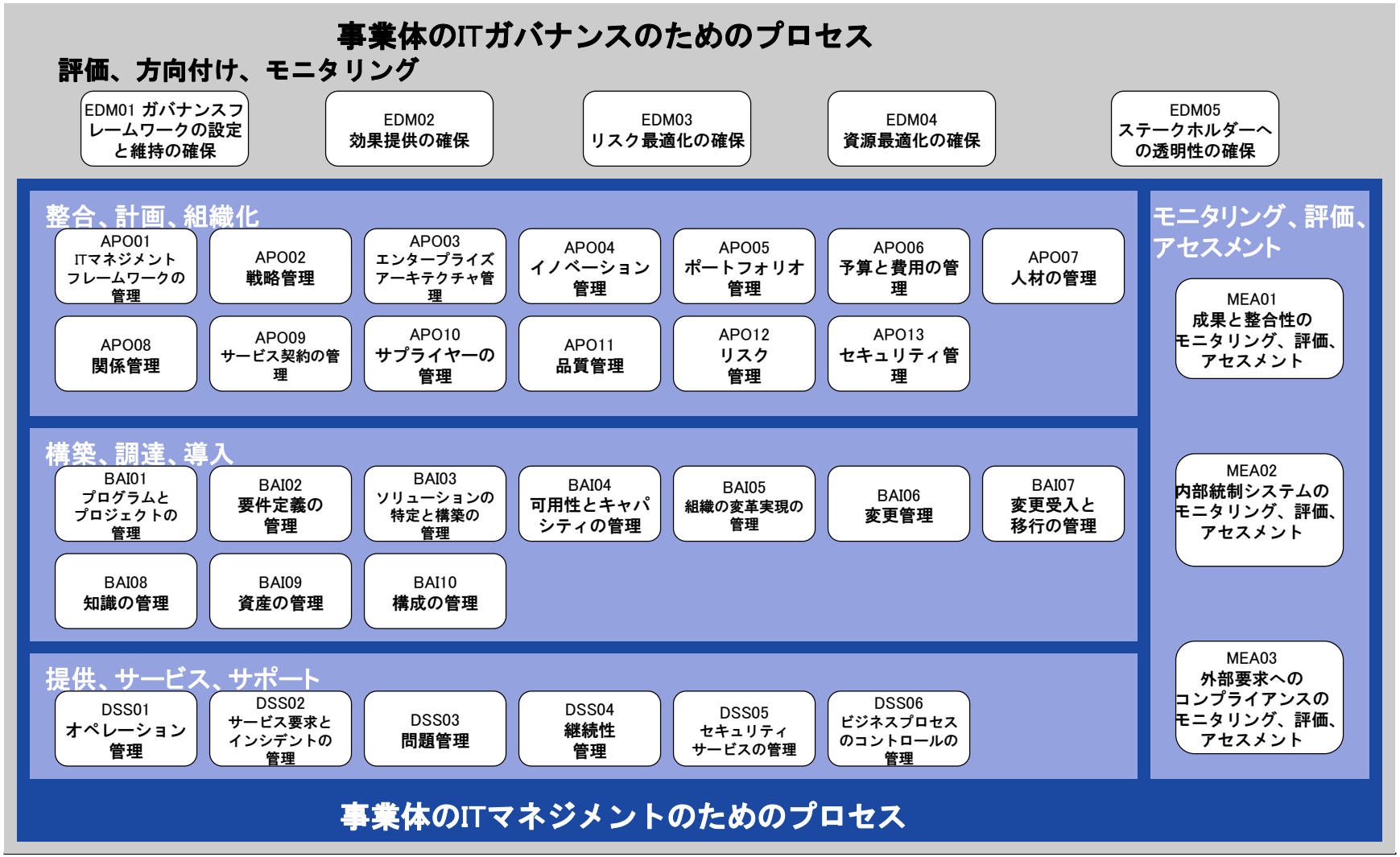
ステークホルダーのニーズから
➡事業体の達成目標
➡IT達成目標
➡イネーブラーの達成目標
へ展開する



COBIT 5 の7つのイネーブラー

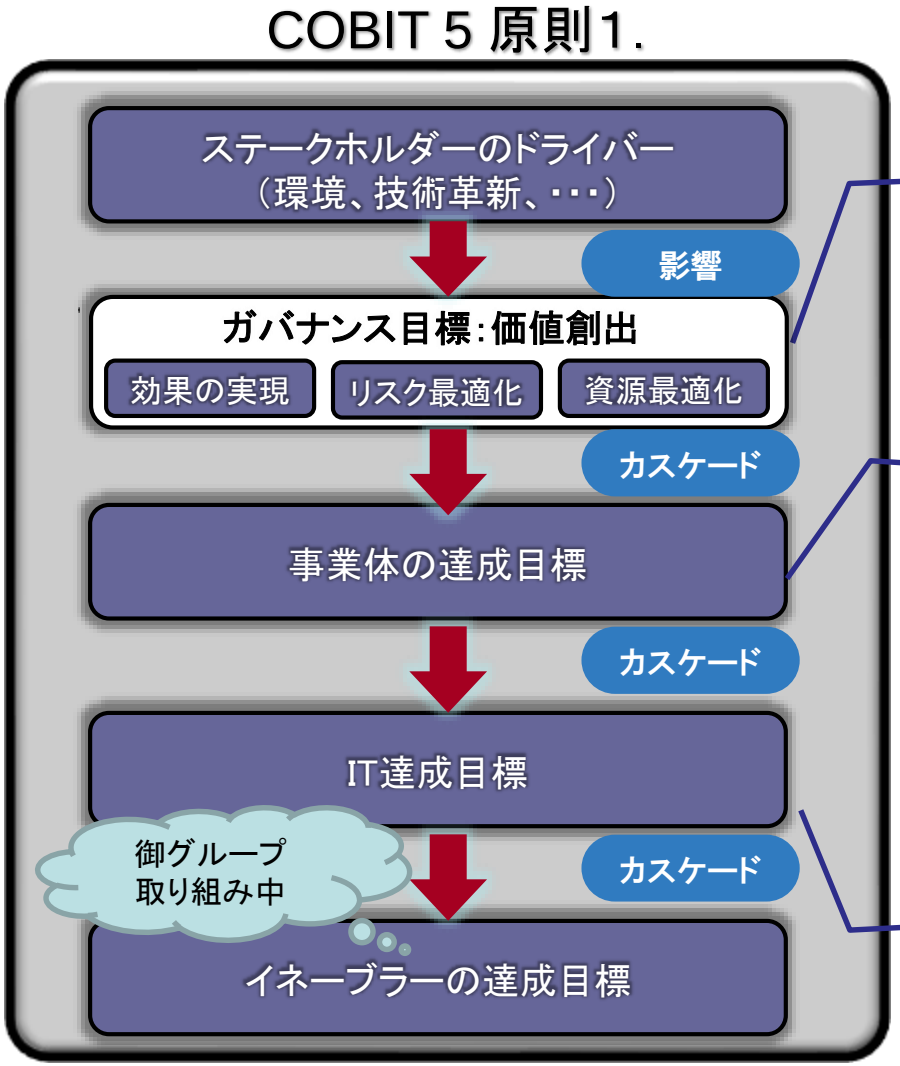


COBIT 5 のプロセス参照モデル



出典: COBIT® 5 日本語版, 図表16.

私の理解した御グループのガバナンス



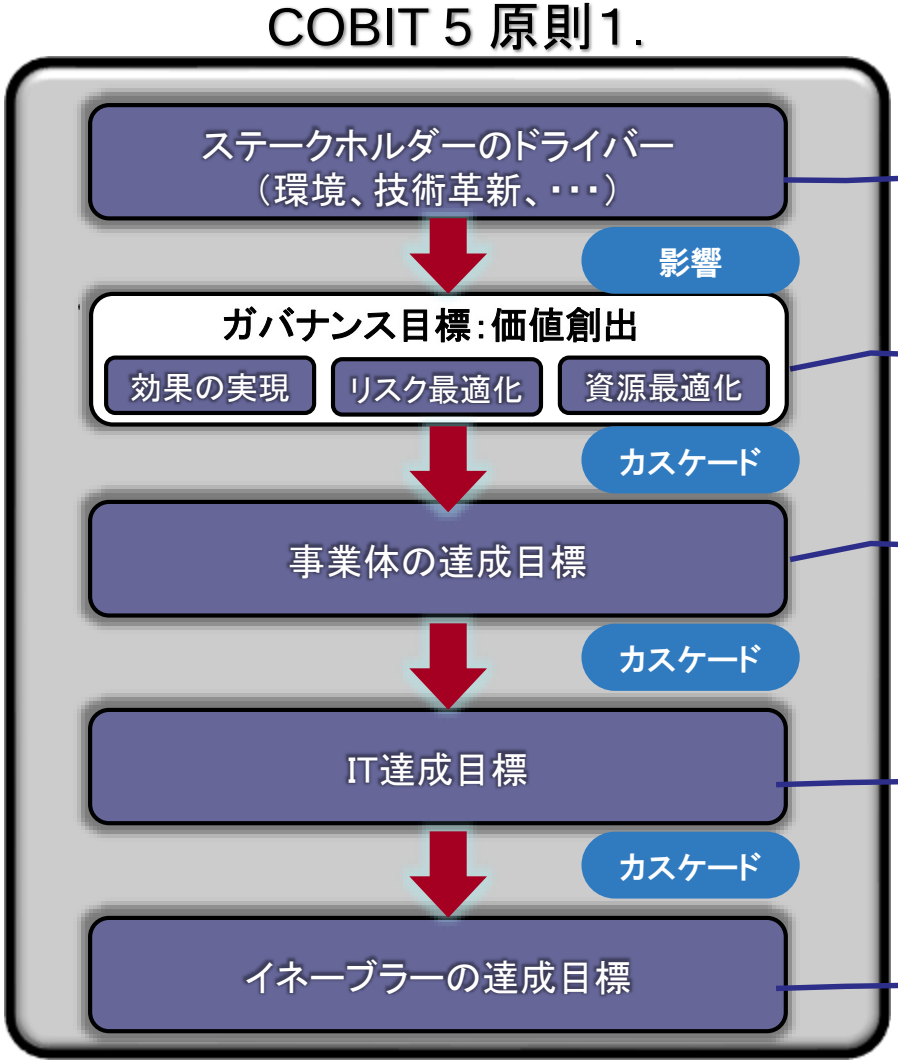
御グループのガバナンス

【経営理念】
情報革命で人々を幸せに

【経営ビジョン】
300年成長のDNA
世界の人々から必要とされる企業へ
【経営戦略】
戦略的シナジーグループ（情報産業）
自律×分散×協調：自己進化＋自己増殖

【 G-ITGビジョン】
ITガバナンスでコラボレーションを活性化する
【 G-ITG戦略】
・イノベーション/モチベーションを誘発する仕組みの構築
・グループ企業が事業に専念してもうためのIT環境の提供（IT共通化）

各グループ会社でもCOBIT 5を活用いただければ・・・



各グループ会社個社のガバナンス

御グループの経営理念、経営ビジョン、経営戦略、G－ITGビジョン、G－ITG戦略
御社のお客様のニーズ

各グループ会社個社の経営理念

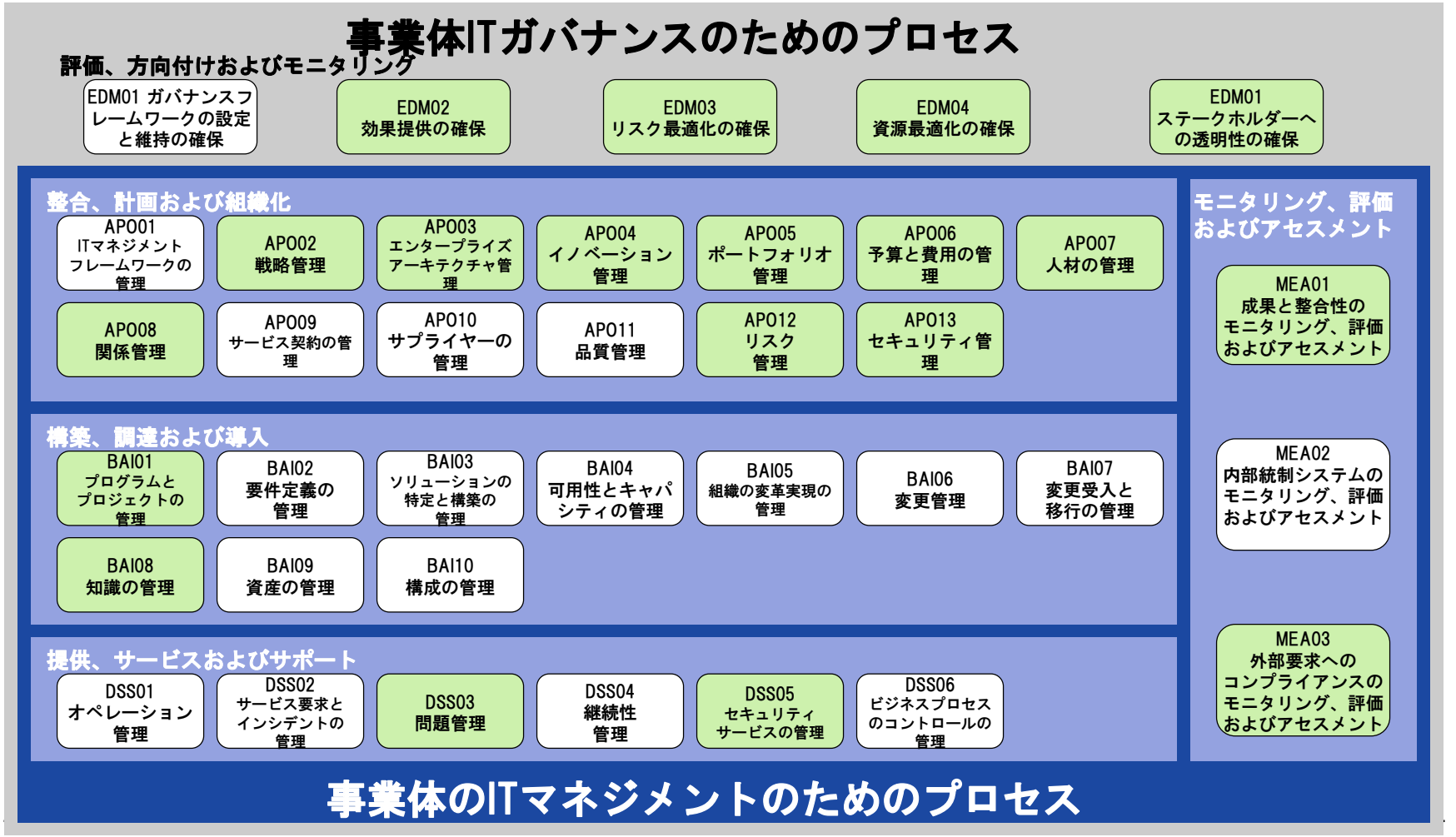
各グループ会社個社の経営ビジョン、経営戦略

各グループ会社個社のITビジョン、IT戦略

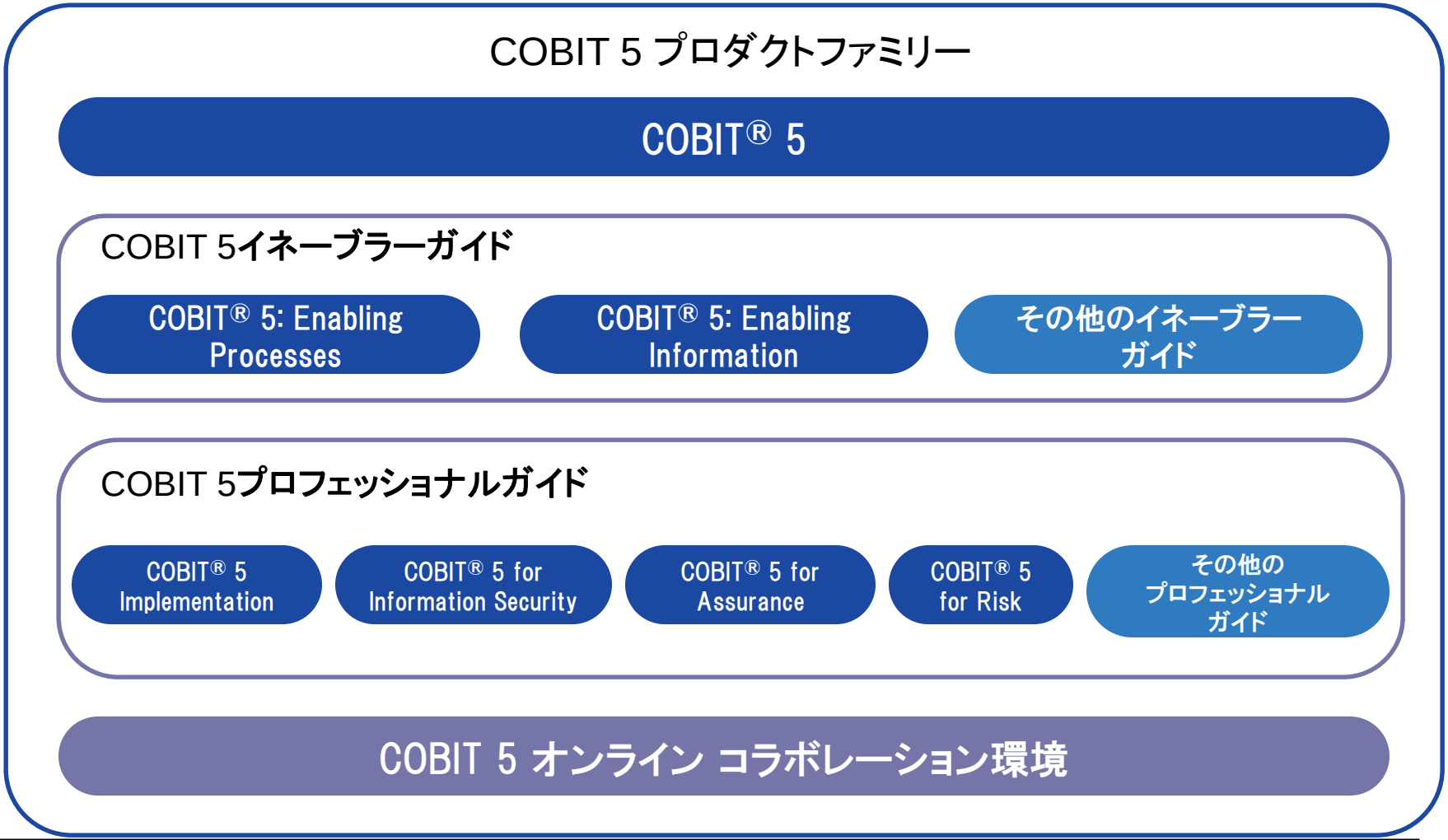
各グループ会社個社のIT戦術
（7つのイネーブラーの目標）

COBIT 5プロセス参照モデル

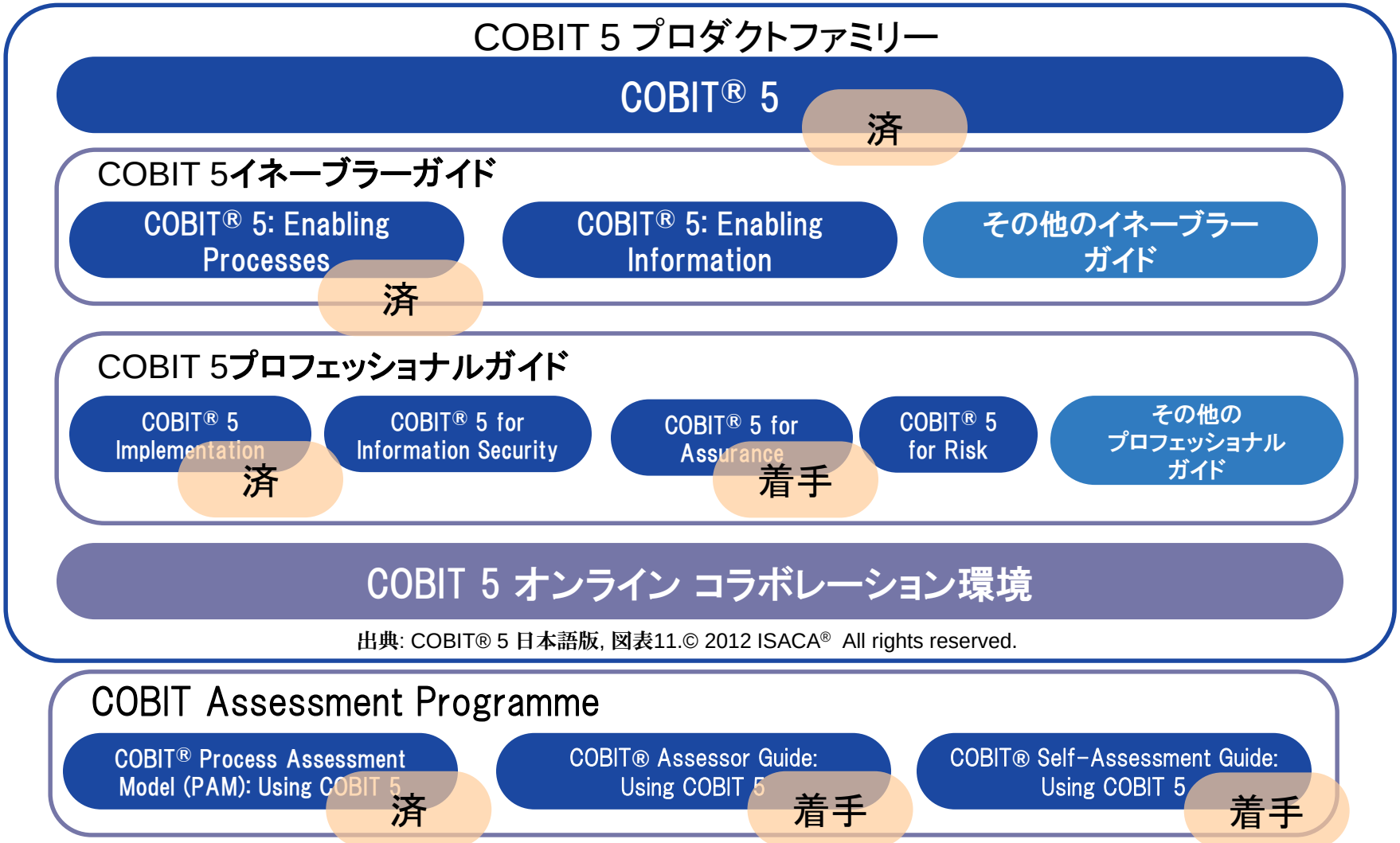
Focusプロセスの例（薄緑は私見によるイメージです）



COBIT 5 プロダクトファミリー



COBIT 5 プロダクトファミリー日本語版



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

本日のアジェンダ

1. はじめに　～　自己紹介 と 自社紹介

2. 東京海上日動システムズのGRC改革

3. 東京海上日動システムズの情報セキュリティ改革

4. COBIT 5 活用のお勧め

5. まとめ

まとめ

弊社のGRC・情報セキュリティ改革を紹介

- ✓東京海上日動システムズの「価値創出」を目指したGRC改革、情報セキュリティ改革
- ✓守りのコンプライアンス・リスク管理から攻めのGRCへ
- ✓改革にはCOBIT 5のガイダンスを最大限活用

まとめ

ソフトバンクグループ様へのCOBIT 5活用のお勧め

- ✓ 御グループにおかれましては、「情報革命により人々を幸せに」を実現するために、COBIT 5が「役に立つ」、「参考になる」と確信しています
- ✓ COBIT 5は「標準」や「基準」ではありません。ガバナンス目標を「価値創出」に設定した優れたフレームワーク、ガイダンスです
- ✓ 5つの原則、プロセス参照モデル（Enabling Processes）、導入の手引き（Implementation）など、参考になるところ、使えるところをつまみ食いしてください
- ✓ 私見ですが、COBIT 5の原則は、偉大な経営者の方々が、経験から得られ暗黙のうちに行動している「真理」をあらわしていると感じています

（注）背景のイメージはソフトバンク株式会社様の「新30年ビジョン」の資料から抜粋させていただきました。