東京海上日動システムズ株式会社

To Be a Good Company

東京海上日動システムズの GRCと情報セキュリティ管理の態勢 ～価値創出を目指したGRC改革～

2015年6月5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

稲葉　裕一

アブストラクト

東京海上日動システムズでは、ガバナンス、リスク管理、コンプライアンス（GRC）について統合的に対応することにより、効果的・効率的なガバナンス態勢を構築した。
これは、東京海上グループのITを担う企業として、グループ会社にITサービス提供を通じてお客様価値を提供するとともに、自社の企業価値を創造していくことを目指したものである。
このようなGRC態勢への改革について、さらには、GRC態勢の重要領域である情報セキュリティ管理の改革について、背景や経緯、築いた態勢の概要、定着に向けた考慮点、もたらされた効果等について説明する。

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
   - 2.1　GRC改革に至る背景
   - 2.2　構築したGRC態勢
   - 2.3　定着に向けた取り組みと振り返り

3. 東京海上日動システムズの情報セキュリティ改革

4. 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 1,378名 (2015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

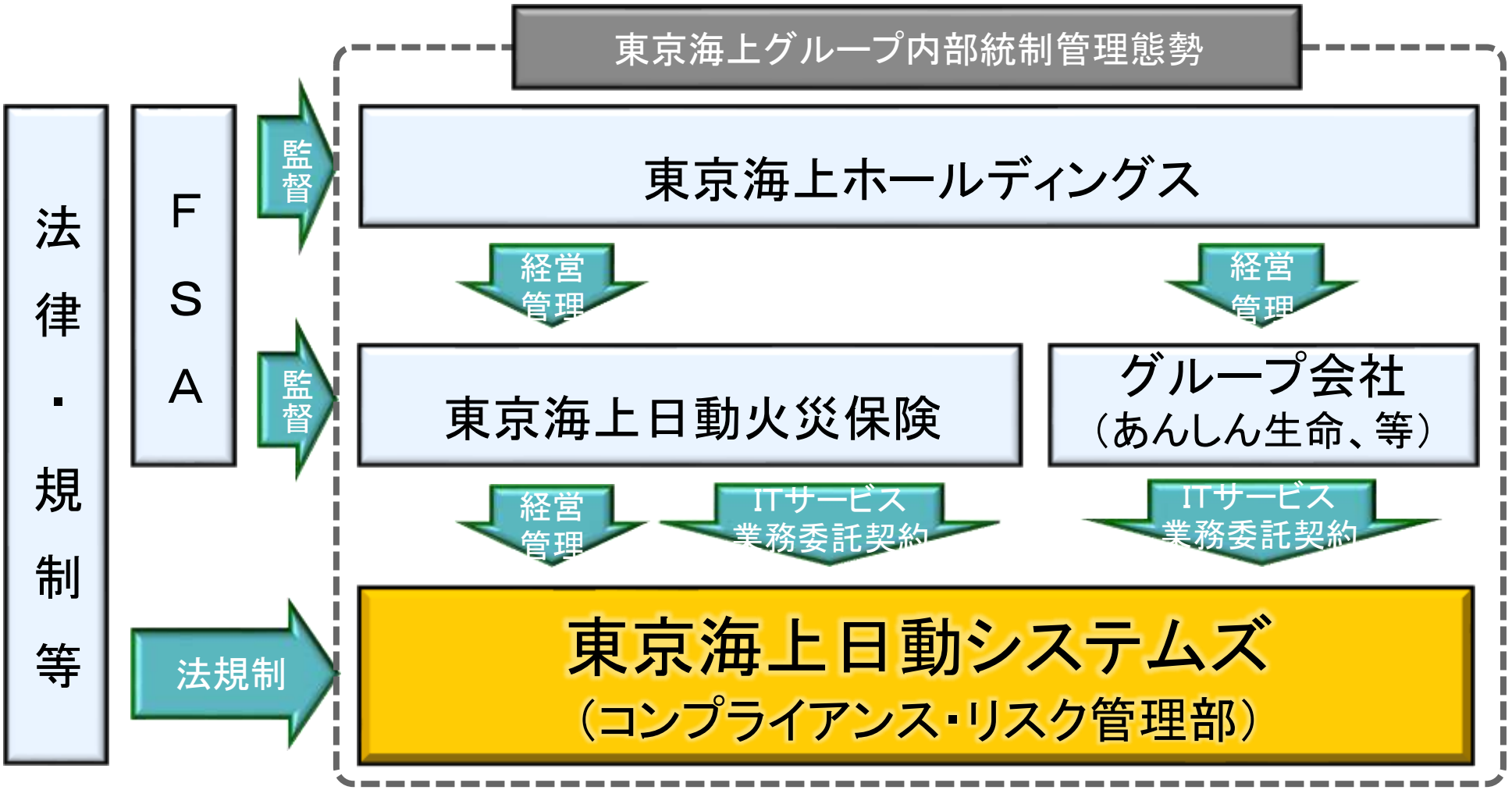
1. はじめに　～　自己紹介 と 自社紹介

2. 東京海上日動システムズのGRC改革
   - 2.1　GRC改革に至る背景
   - 2.2　構築したGRC態勢の概要
   - 2.3　定着に向けた取り組みと振り返り

3. 東京海上日動システムズの情報セキュリティ改革

4. まとめ

背景 ～ 弊社を取り巻く環境



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

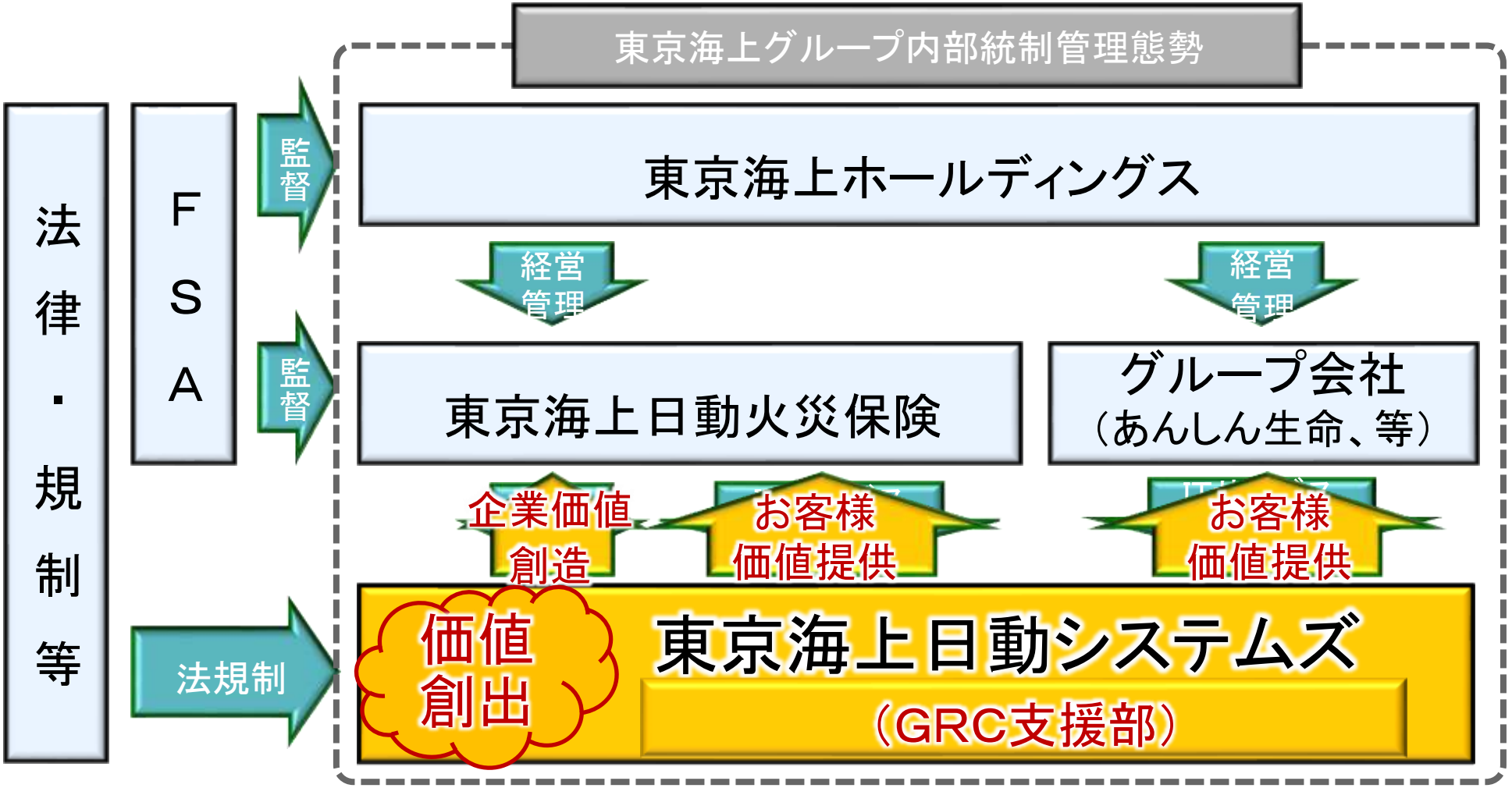
経営者の想いを形に　～　GRC

- ✓ 経営者はコーポレートメッセージ「**ITでグローバルに東京海上グループを支えるGood Company＝光り輝くシステムズ**」に基づき、経営の舵取りを行っている
- ✓ これを「GRC」という言葉で見える化した

(G) ガバナンス目標：　価値の創出
(R) リスク管理目標：　リスクの最適化
(C) コンプライアンス目標：　社会の期待に応える

東京海上グループの内部統制フレームワークを使用して、
G、R、Cに統合的かつ効率的、効果的に対応

価値創出を目指した攻めのGRCへ ～ GRC支援部



本日のアジェンダ

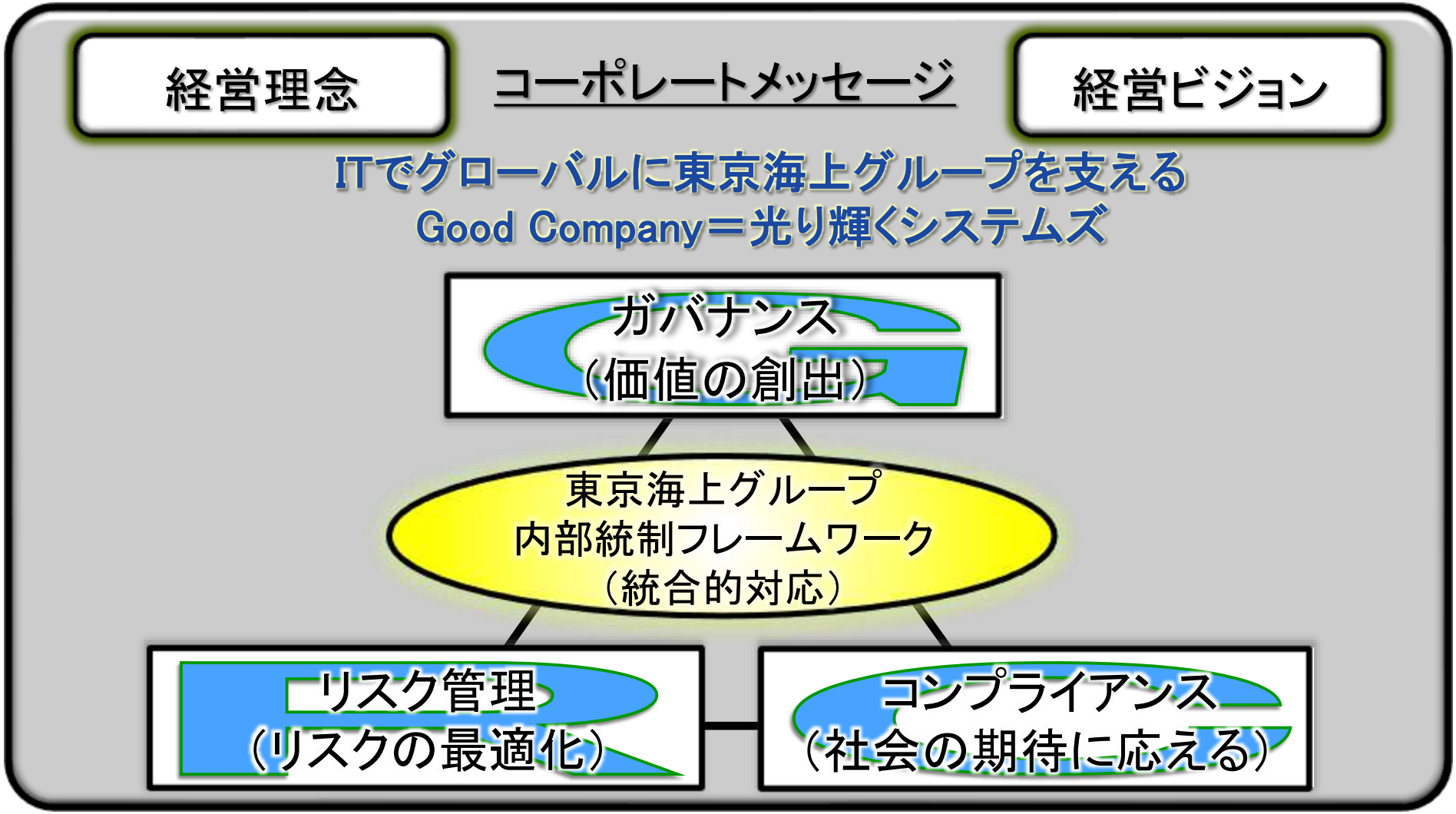
1. はじめに　～　自己紹介 と 自社紹介

2. 東京海上日動システムズのGRC改革
   - 2.1　GRC改革に至る背景
   - 2.2　構築したGRC態勢の概要
   - 2.3　定着に向けた取り組みと振り返り

3. 東京海上日動システムズの情報セキュリティ改革

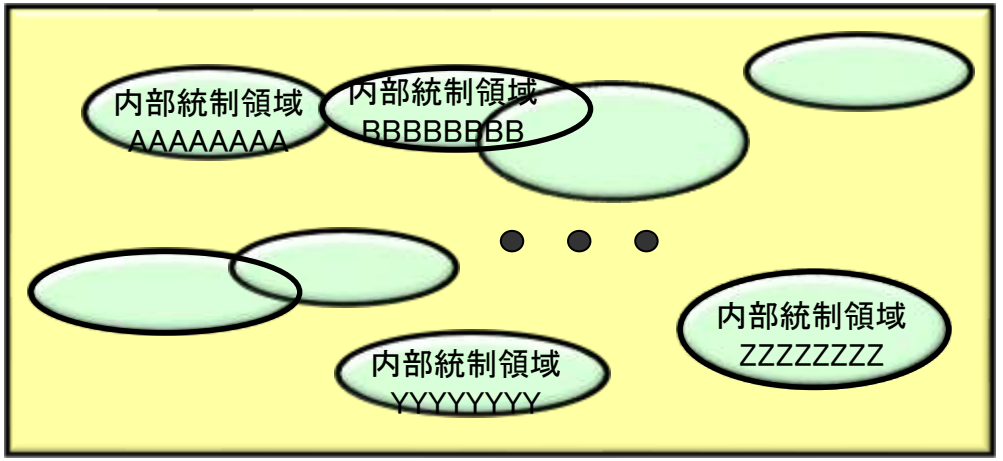
4. まとめ

経営者の想いを形に ～ GRC態勢の概念



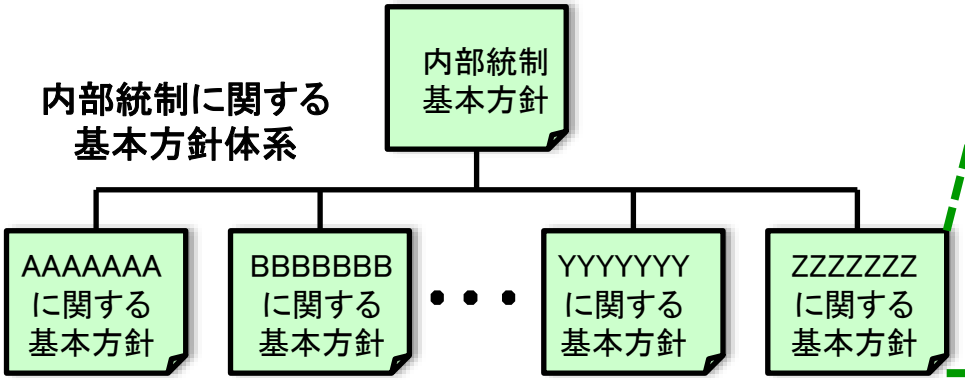
東京海上グループの内部統制フレームワーク

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



各内部統制の
基本方針を定義

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）
・・・

各基本方針に内部統制の達成目標を定義

□□□□□□□□に関する基本方針

第1条（目的） → 内部統制の目的
・・・

第2条（定義等） → 言葉の定義
・・・

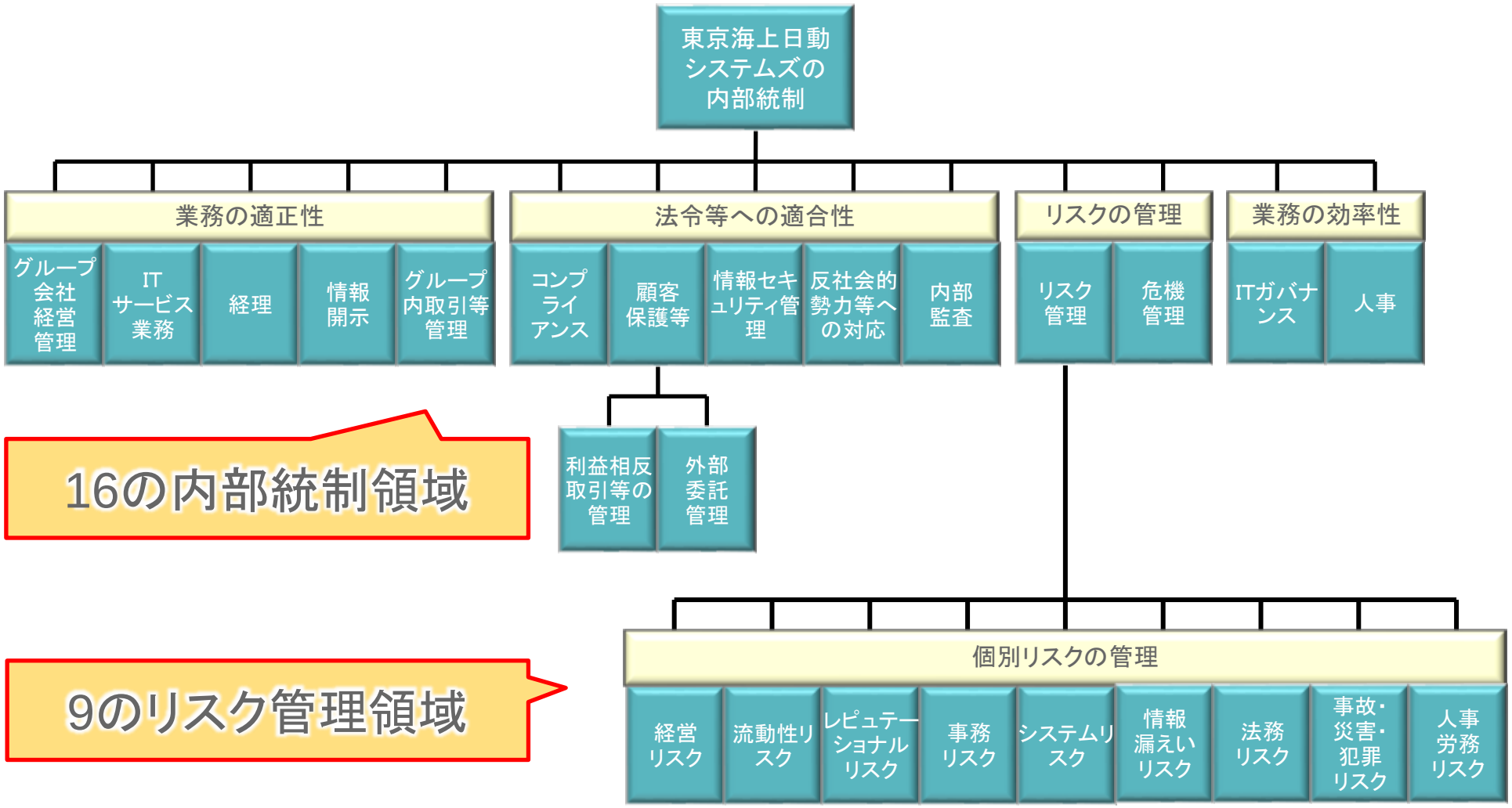
第3条（基本的考え方） → カルチャー、プリンシプル等を定義
・・・

第4条（態勢の整備） → 方針・規程等、組織体制、評価改善活動を定義
・・・

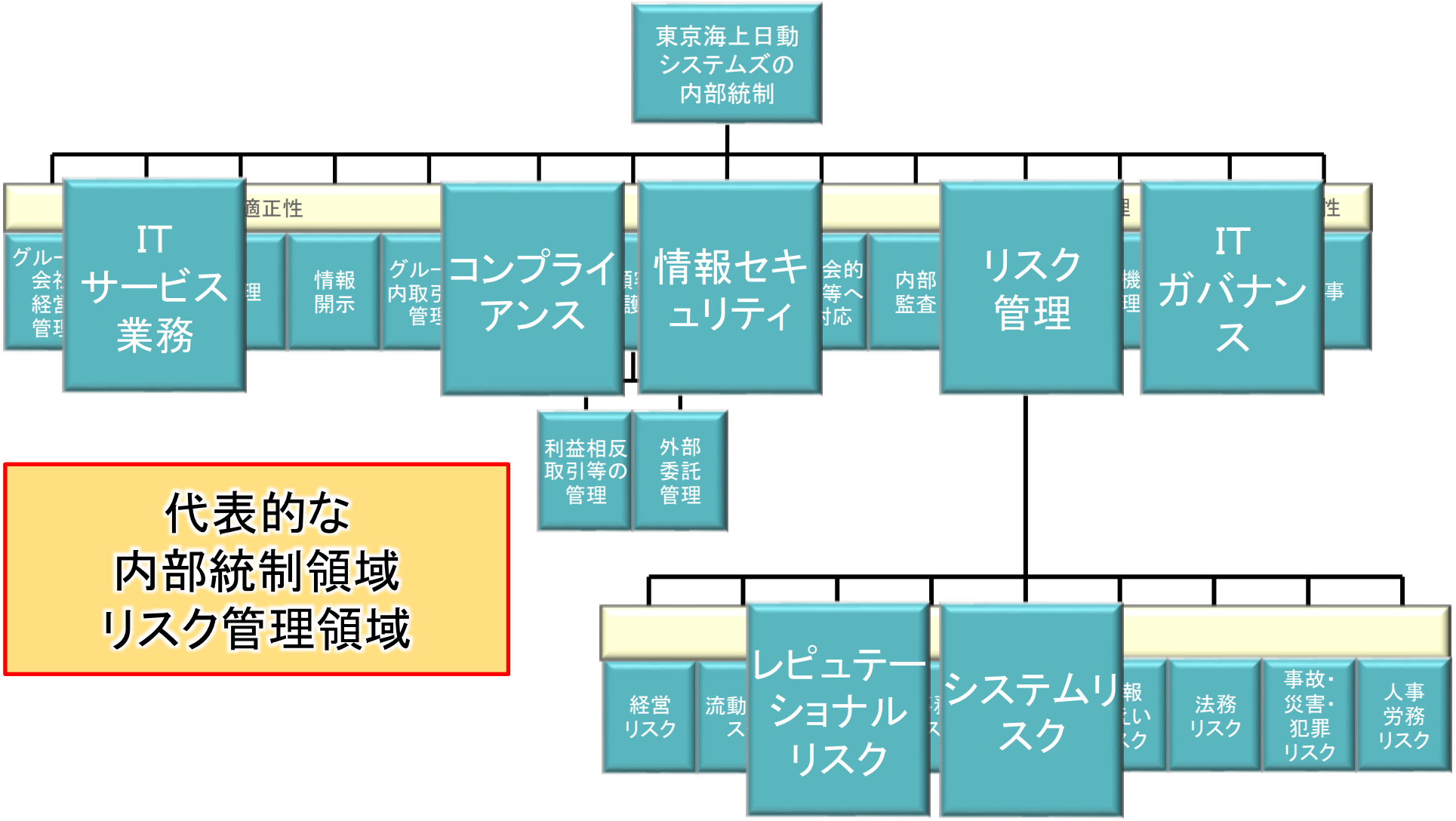
第5条（子会社としての役割） → 親会社への事前承認事項、報告事項等
・・・

第6条（改廃）
・・・

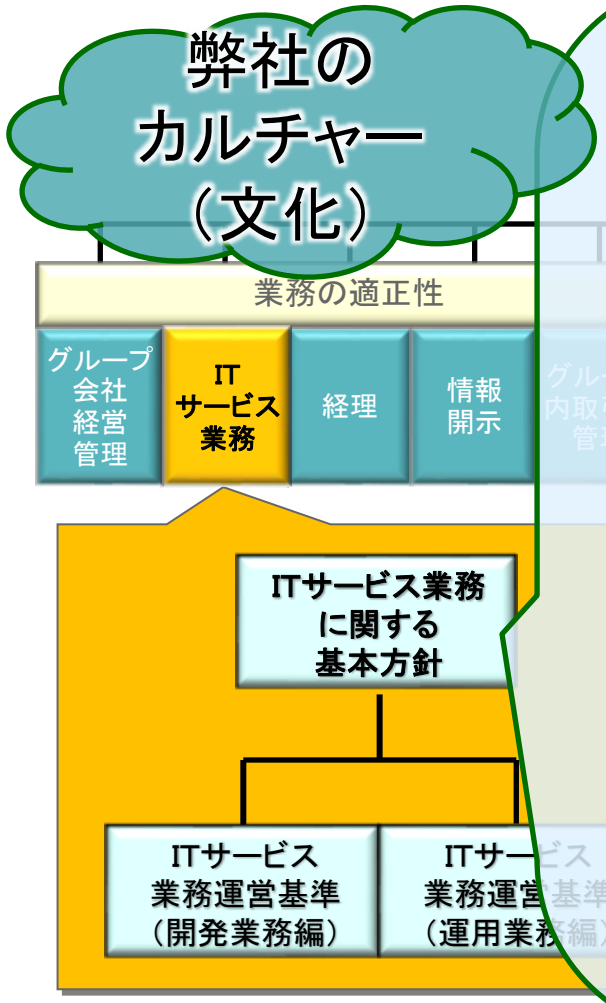
東京海上日動システムズの内部統制



東京海上日動システムズの内部統制



価値創出の源泉～ITサービス業務



第3条　（基本的考え方）

当社は、次に掲げる方針に基づき行う。

（1）お客様の事業戦略を具体的なビジネスプロセスに落とし込み、お客様と同じ想いをシェアしながら業務を推進する。

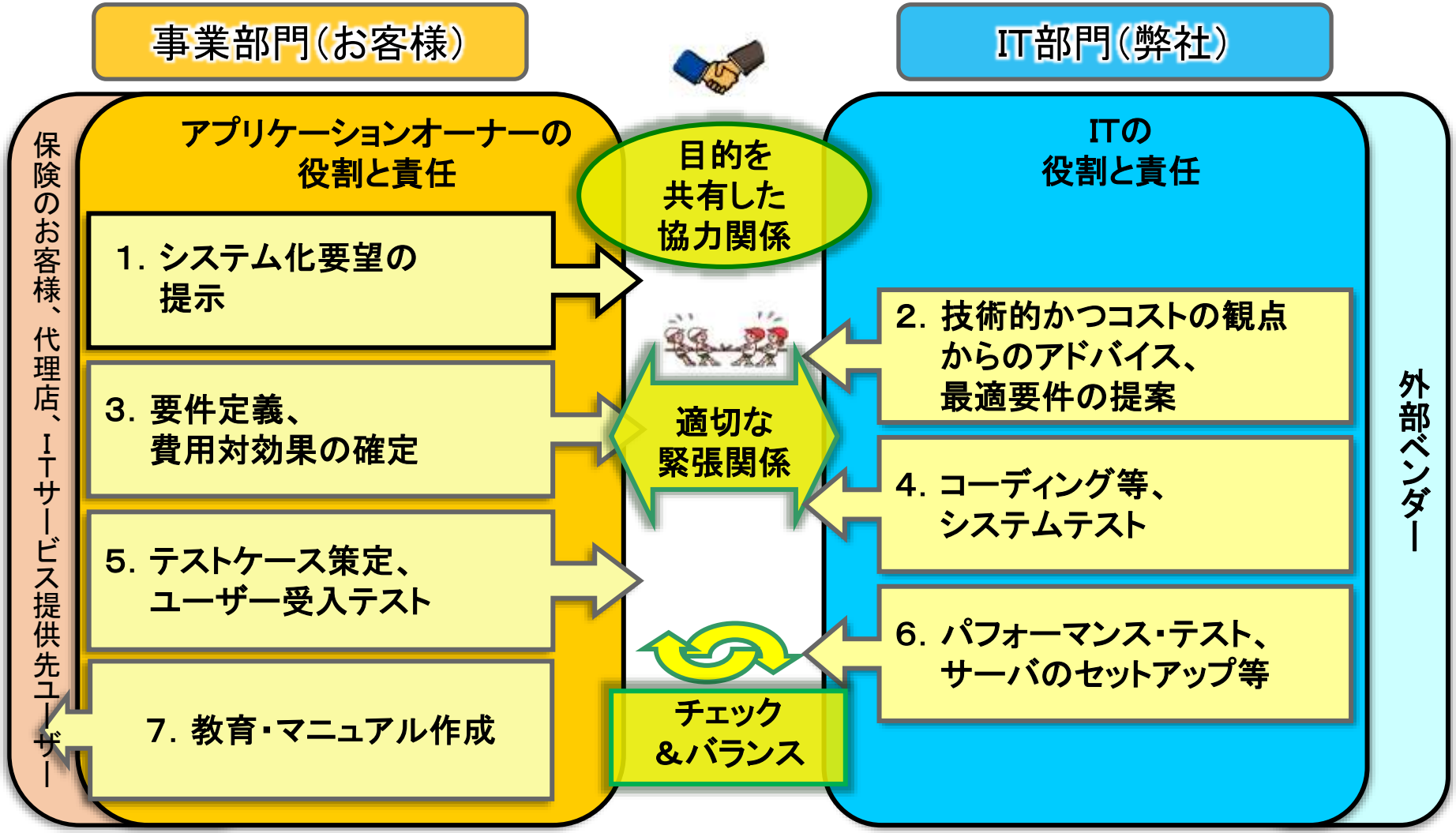
（2）お客様のビジネスサイドに深く踏みこんでアプリケーションオーナーと協働し、お客様の価値を共に創造する。

（3）プログラムの生産量をなるべく少なく、ビジネス効果を大きく、スピードを上げることで、「システムズの品質」の極大化を共に推進する。

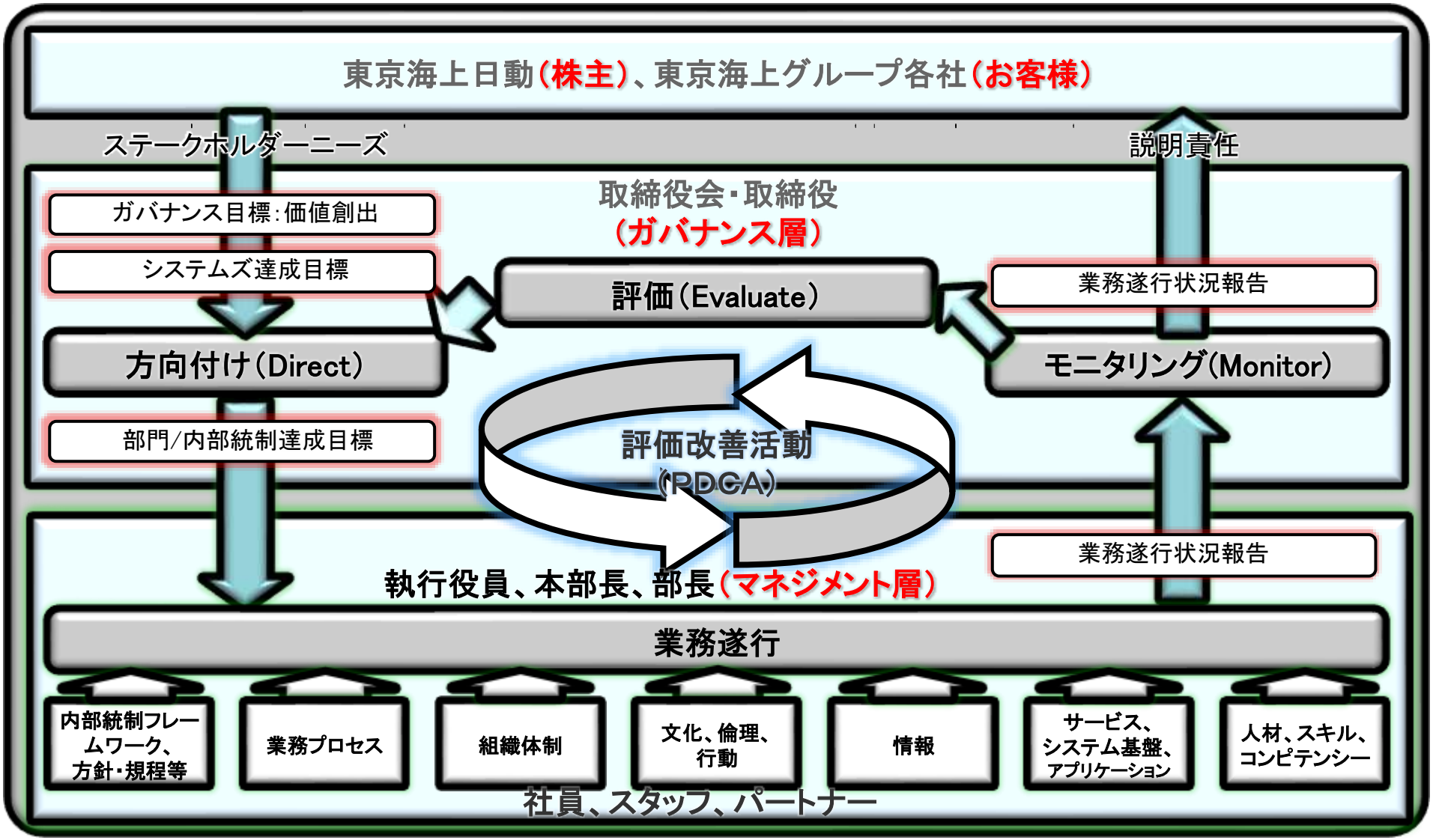
（4）開発と運用に関する職責を分離した上で、適切なタイミングで開発と運用の連携に基づいた業務運営を行う。

アプリケーションオーナー制度を支えるITサービス業務

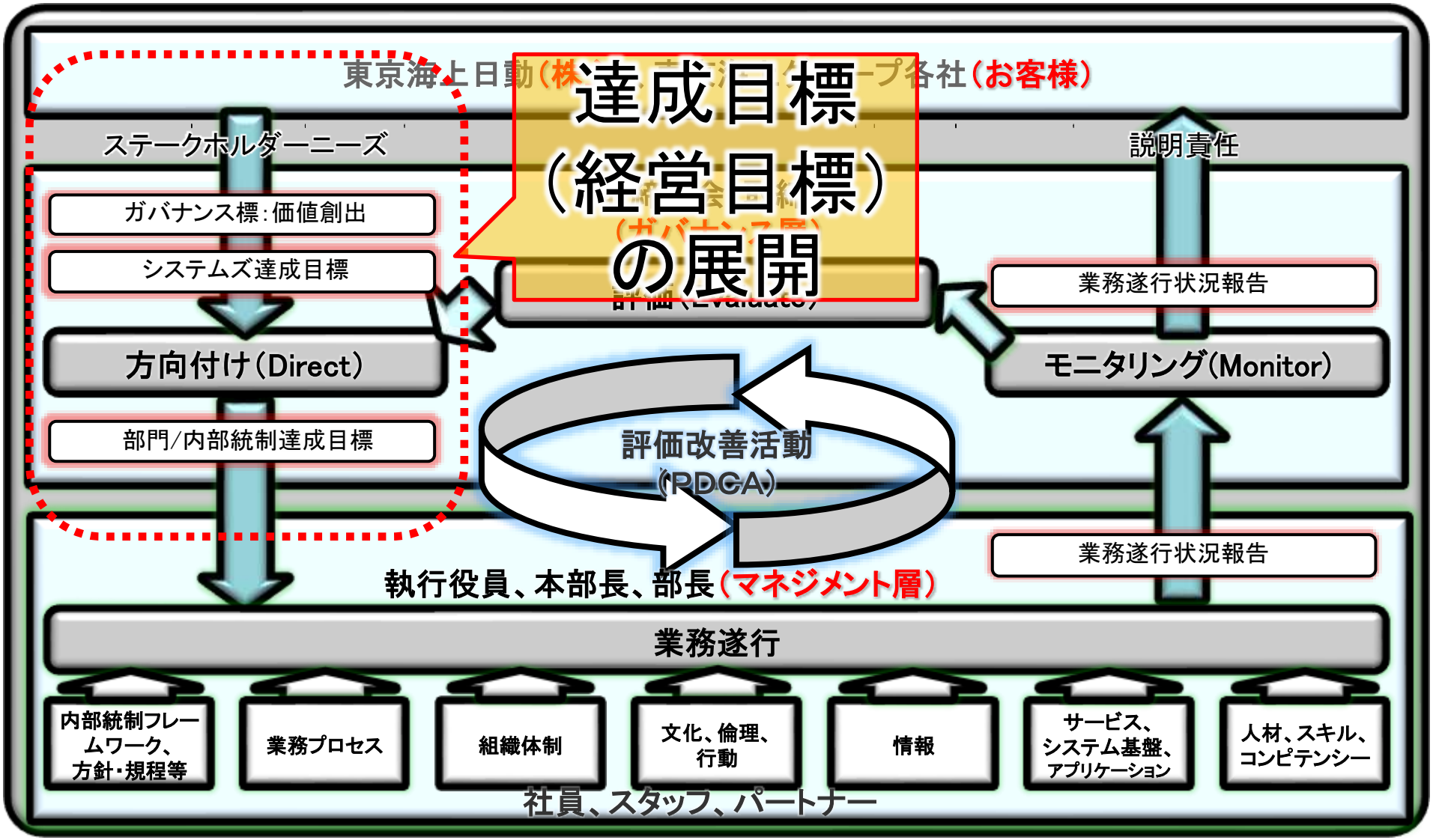
東京海上グループのアプリケーションオーナー制度



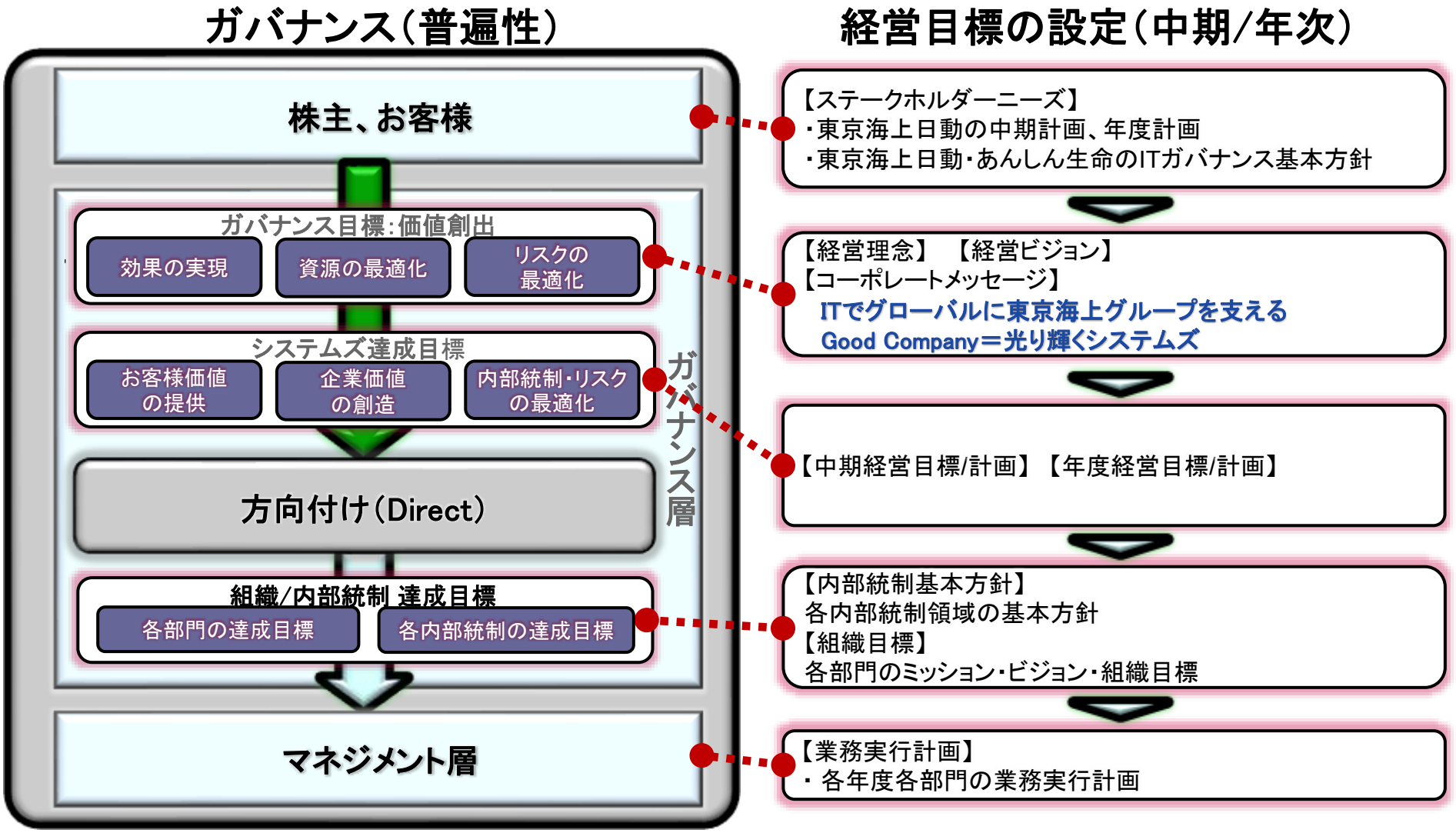
東京海上日動システムズのGRCプロセス



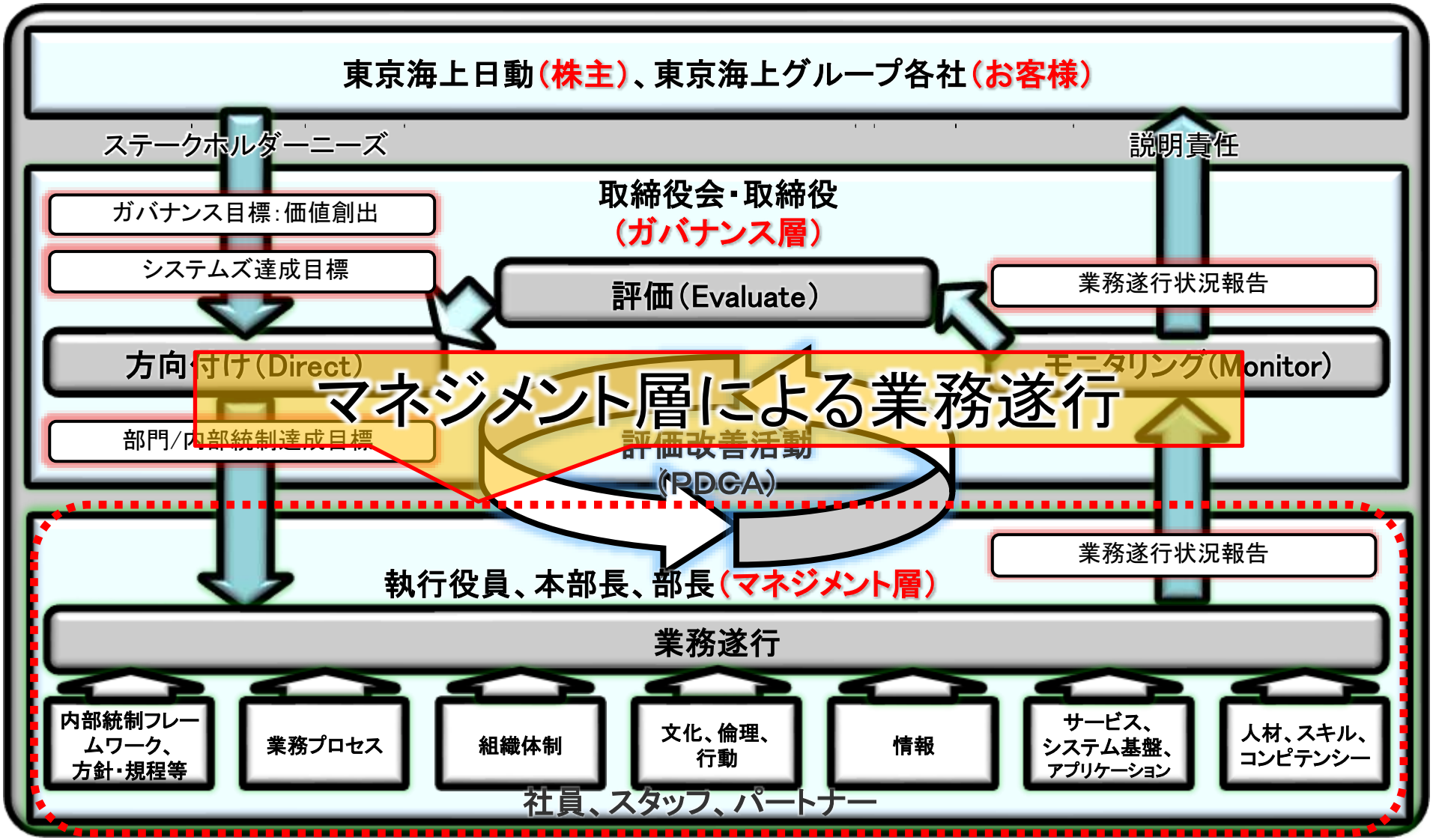
達成目標の展開


東京海上日動（お客様）
ステークホルダーニーズ
説明責任
ガバナンス標：価値創出
システムズ達成目標
達成目標
（経営目標）
の展開
業務遂行状況報告
方向付け（Direct）
モニタリング（Monitor）
部門/内部統制達成目標
評価改善活動
（PDCA）
業務遂行状況報告
執行役員、本部長、部長（マネジメント層）
業務遂行
内部統制フレームワーク、方針・規程等
業務プロセス
組織体制
文化、倫理、行動
情報
サービス、システム基盤、アプリケーション
人材、スキル、コンピテンシー
社員、スタッフ、パートナー

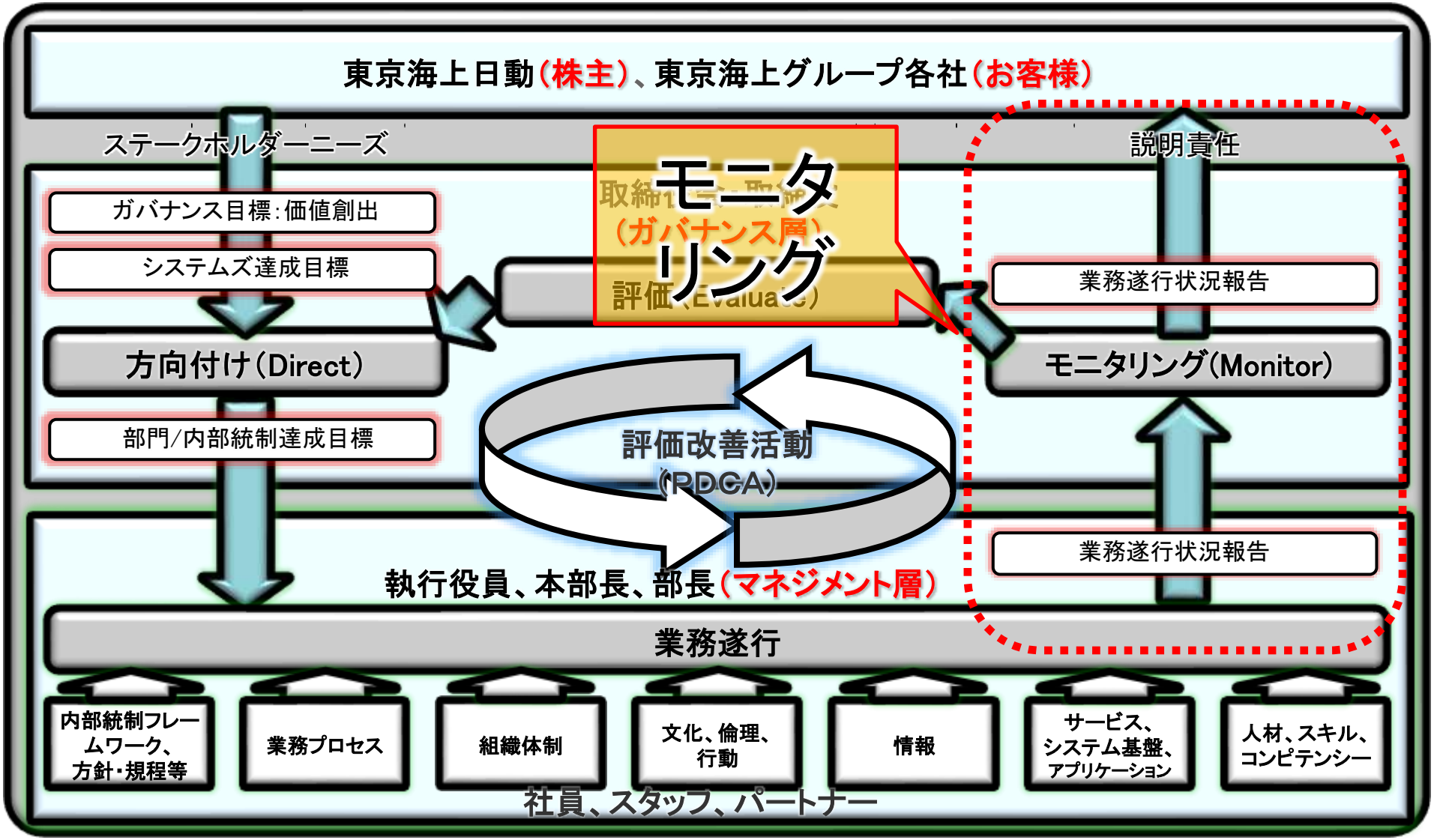
システムズの達成目標の設定



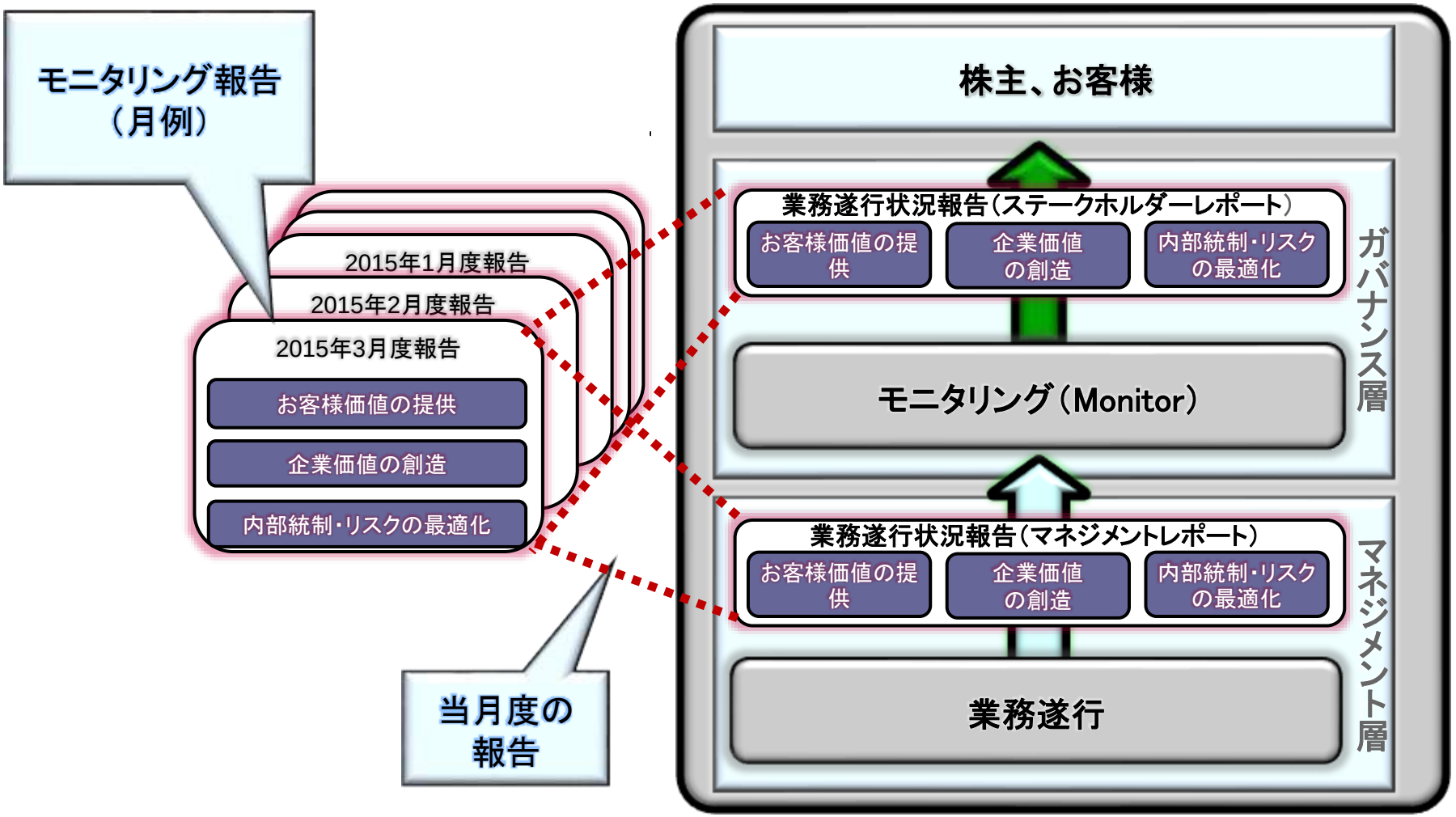
業務遂行


東京海上日動（株主）、東京海上グループ各社（お客様）
ステークホルダーニーズ
説明責任
取締役会・取締役
（ガバナンス層）
ガバナンス目標：価値創出
システムズ達成目標
評価（Evaluate）
業務遂行状況報告
方向付け（Direct）
モニタリング（Monitor）
マネジメント層による業務遂行
部門/内部統制達成目標
評価改善活動
（PDCA）
業務遂行状況報告
執行役員、本部長、部長（マネジメント層）
業務遂行
内部統制フレームワーク、方針・規程等
業務プロセス
組織体制
文化、倫理、行動
情報
サービス、システム基盤、アプリケーション
人材、スキル、コンピテンシー
社員、スタッフ、パートナー

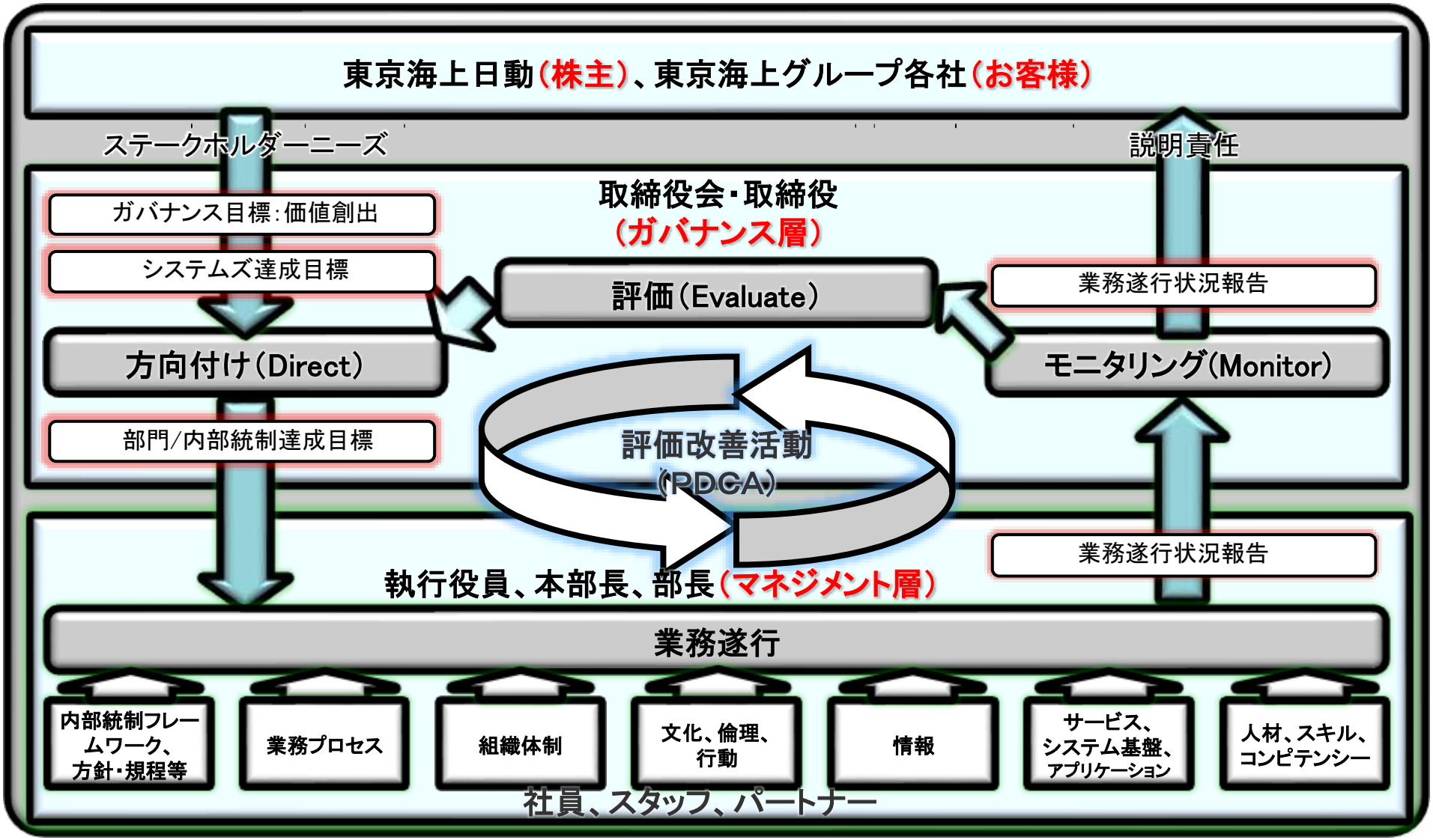
モニタリング


東京海上日動（株主）、東京海上グループ各社（お客様）
ステークホルダーニーズ
説明責任
ガバナンス目標：価値創出
システムズ達成目標
モニタリング
（ガバナンス層）
評価（Evaluate）
業務遂行状況報告
方向付け（Direct）
モニタリング（Monitor）
部門/内部統制達成目標
評価改善活動
（PDCA）
業務遂行状況報告
執行役員、本部長、部長（マネジメント層）
業務遂行
内部統制フレームワーク、方針・規程等
業務プロセス
組織体制
文化、倫理、行動
情報
サービス、システム基盤、アプリケーション
人材、スキル、コンピテンシー
社員、スタッフ、パートナー

マネジメントレポートとステークホルダーレポート



東京海上日動システムズのGRCプロセス



本日のアジェンダ

1. はじめに　～　自己紹介 と 自社紹介

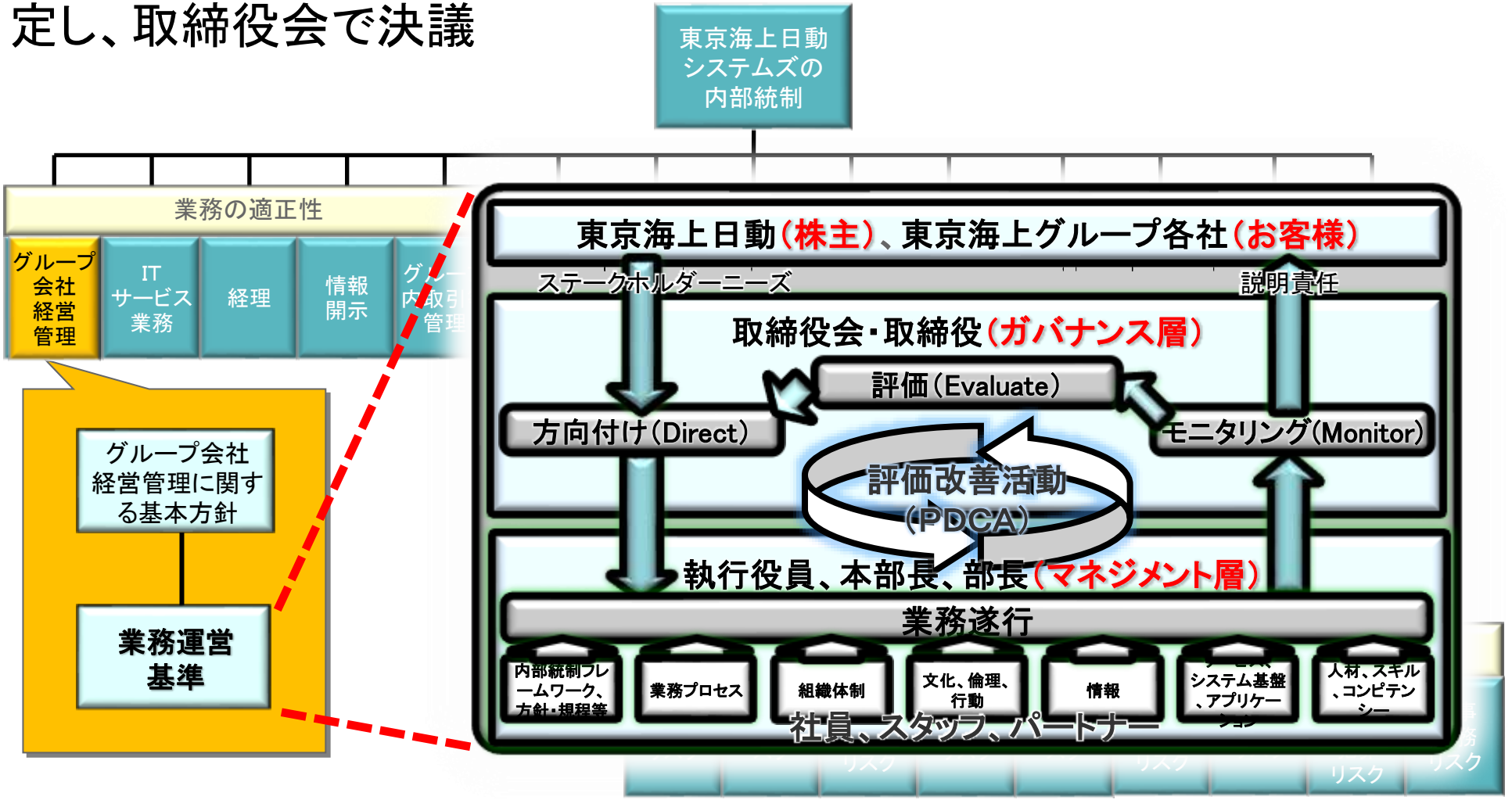
2. 東京海上日動システムズのGRC改革
   - 2.1　GRC改革に至る背景
   - 2.2　構築したGRC態勢の概要
   - 2.3　定着に向けた取り組みと振り返り

3. 東京海上日動システムズの情報セキュリティ改革

4. まとめ

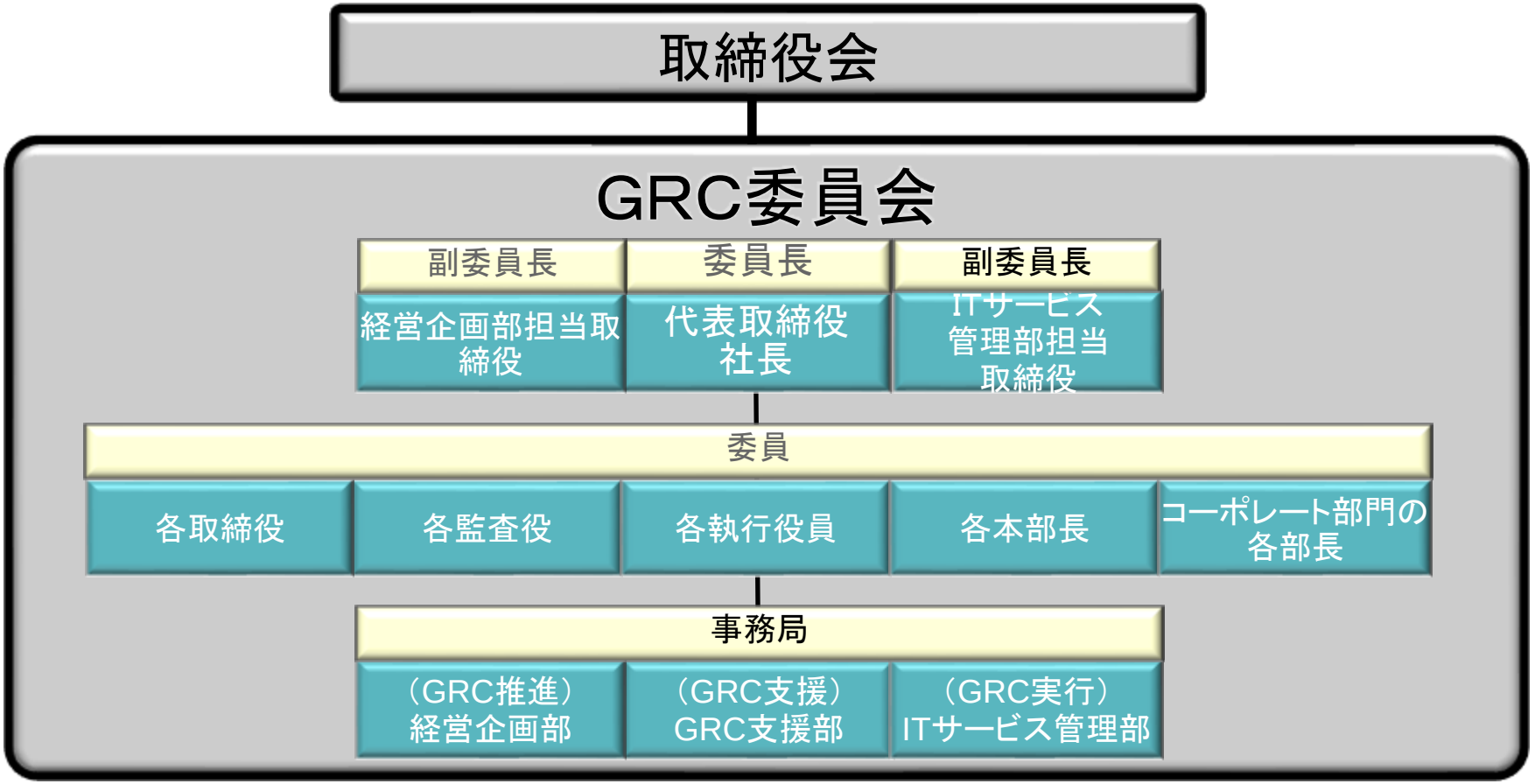
GRCプロセスのルール化～持続性の確保

✓ 経営者が自らを律するルールとして、GRCプロセスを「業務運営基準」に制定し、取締役会で決議



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



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、プロジェクトチームでは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価値を提供し、企業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、プロジェクトチームの感想をまとめたものであり、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

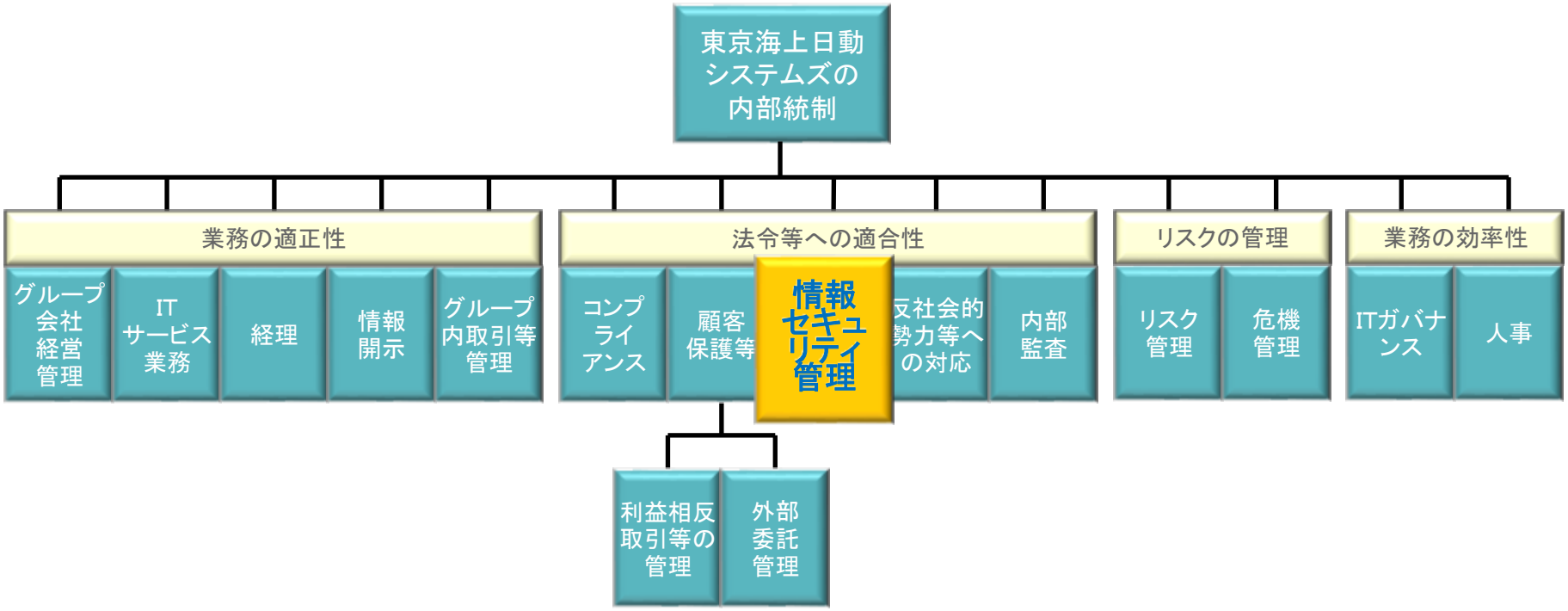
2. 東京海上日動システムズのGRC改革
   - 2.1　GRC改革に至る背景
   - 2.2　構築したGRC態勢の概要
   - 2.3　定着に向けた取り組みと振り返り

3. 東京海上日動システムズの情報セキュリティ改革

4. 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？

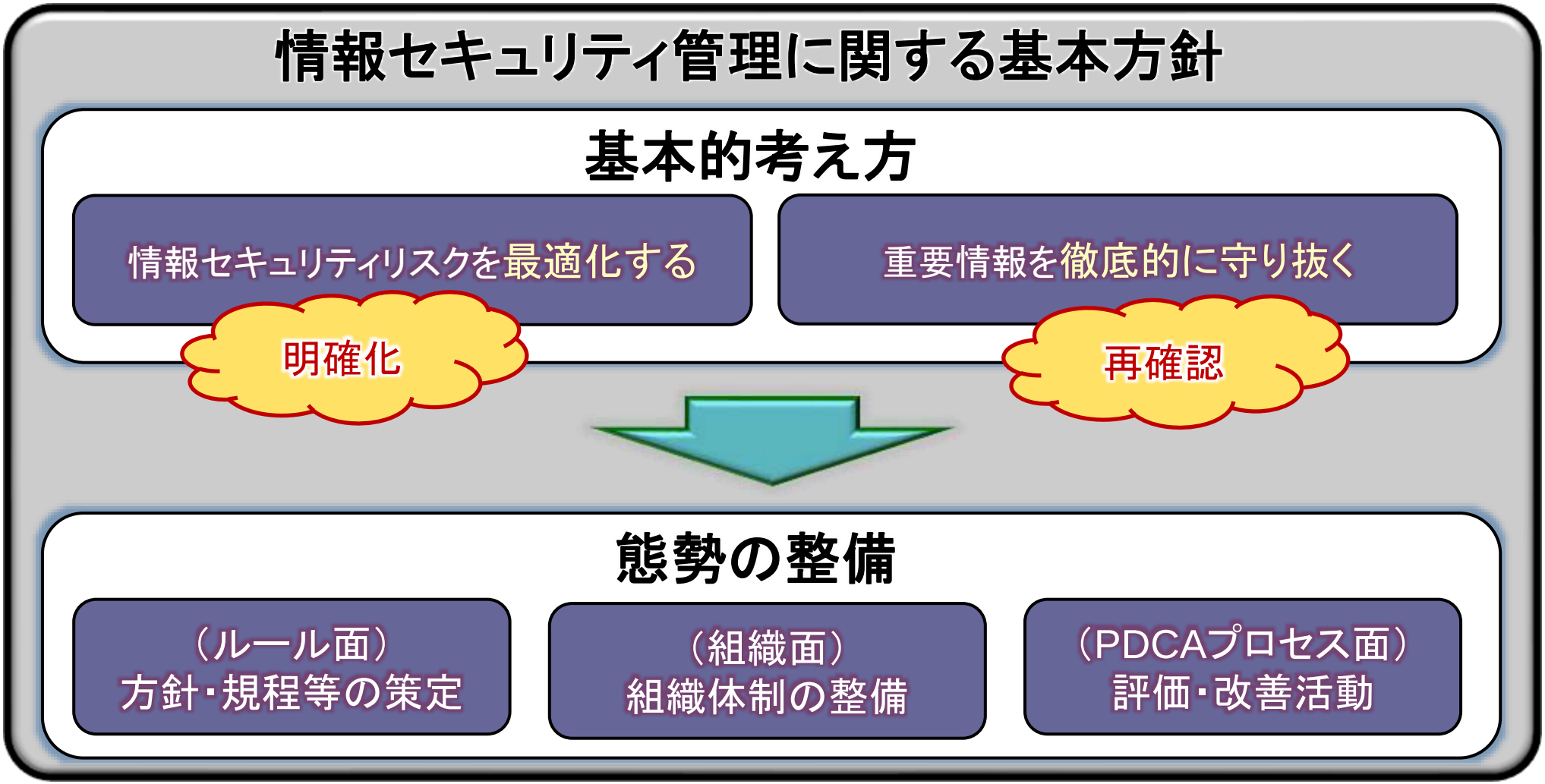
お客様と気持ちをシェアしてビジネス価値を共に創出しなければ・・・

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

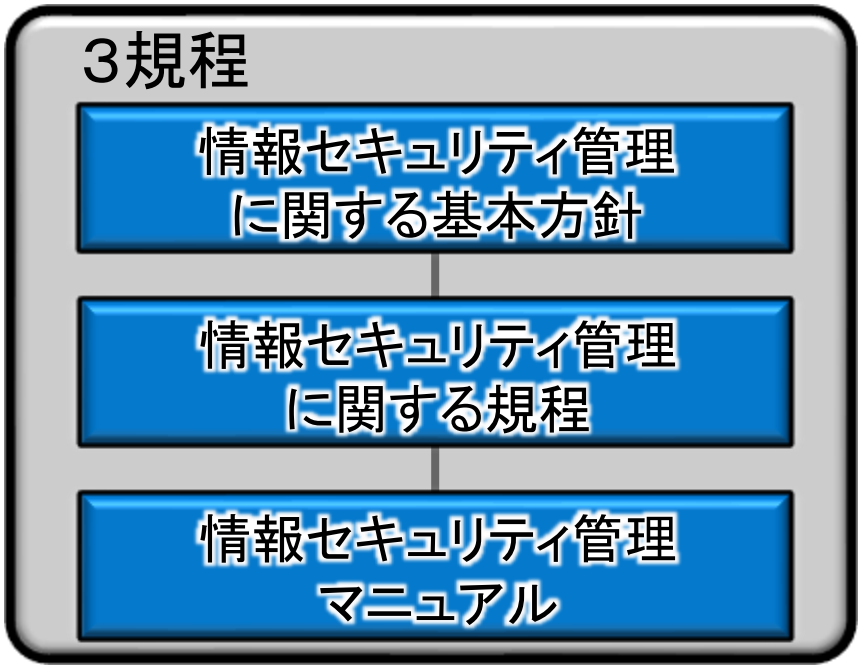
価値創出を目指した攻めの情報セキュリティへ

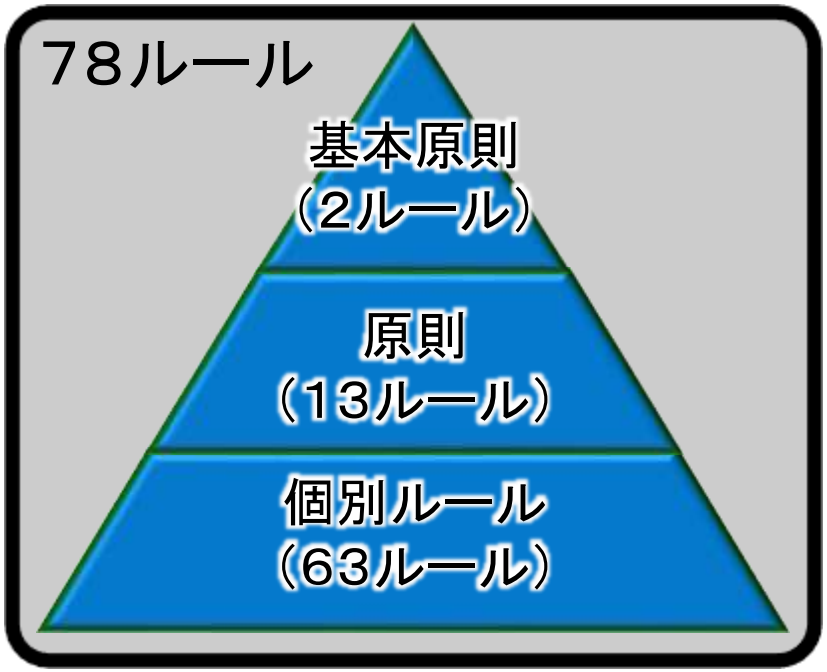
情報セキュリティに関するGRC



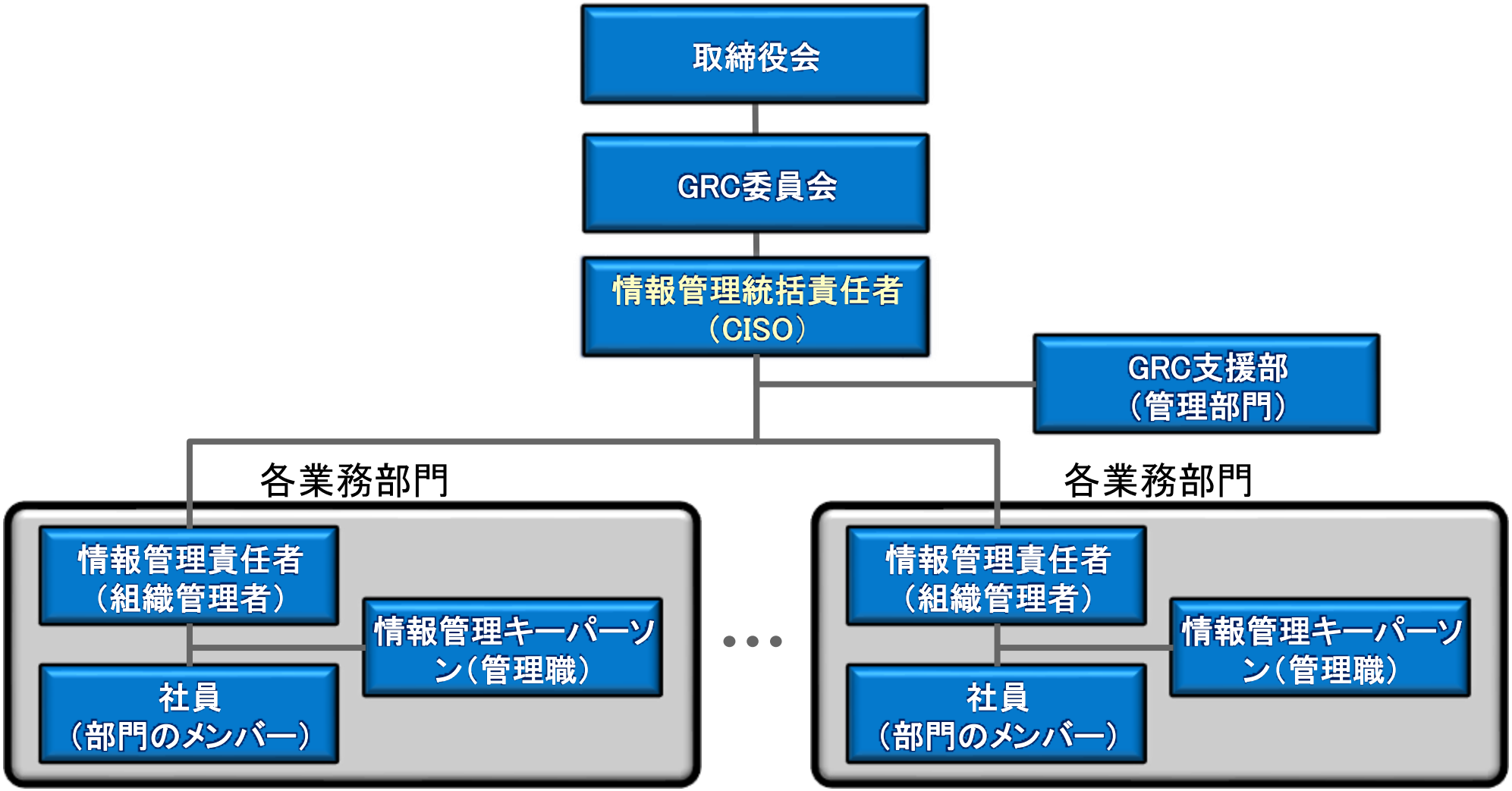
情報セキュリティルールの最適化、シンプル化

- 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

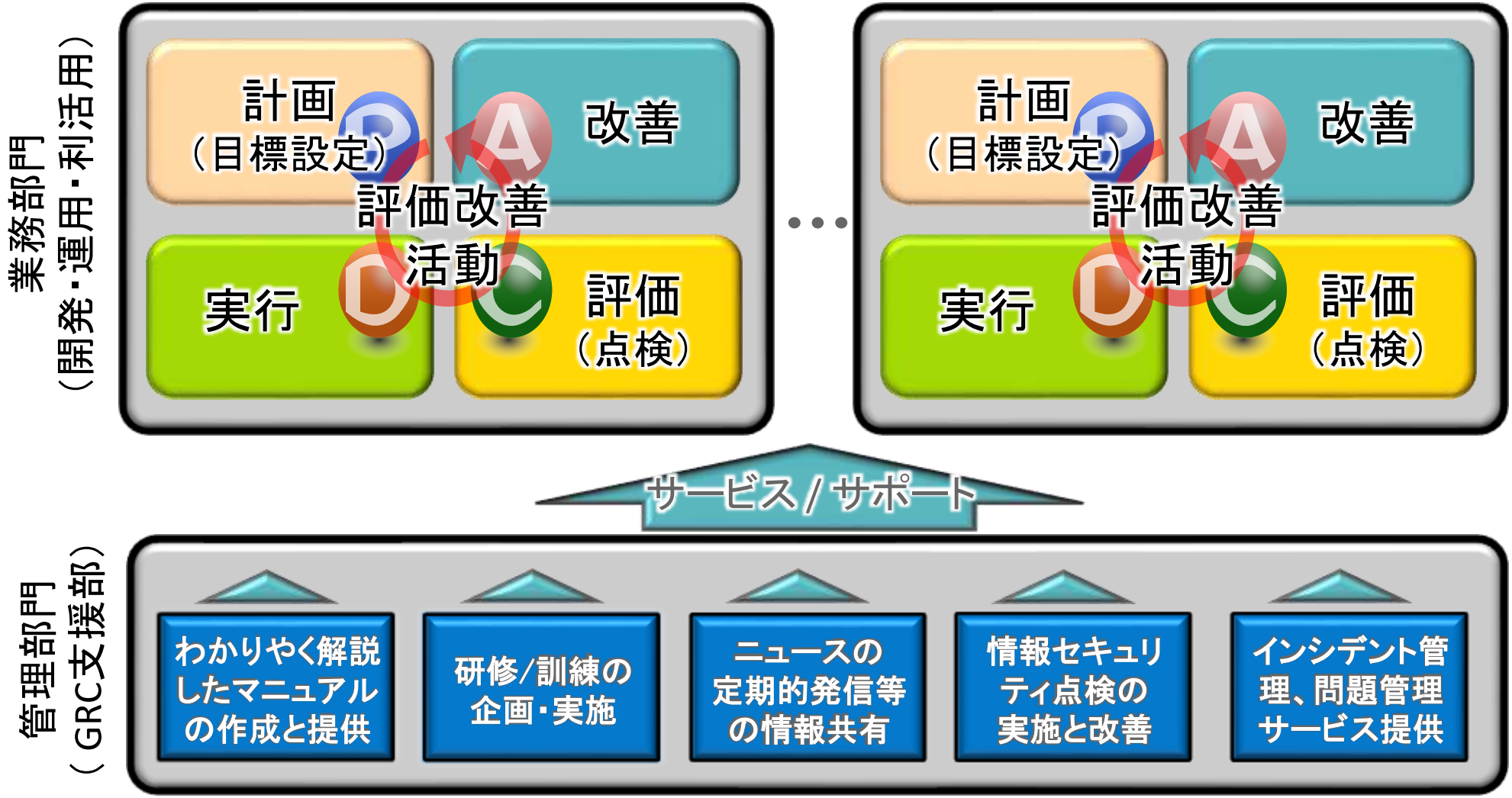




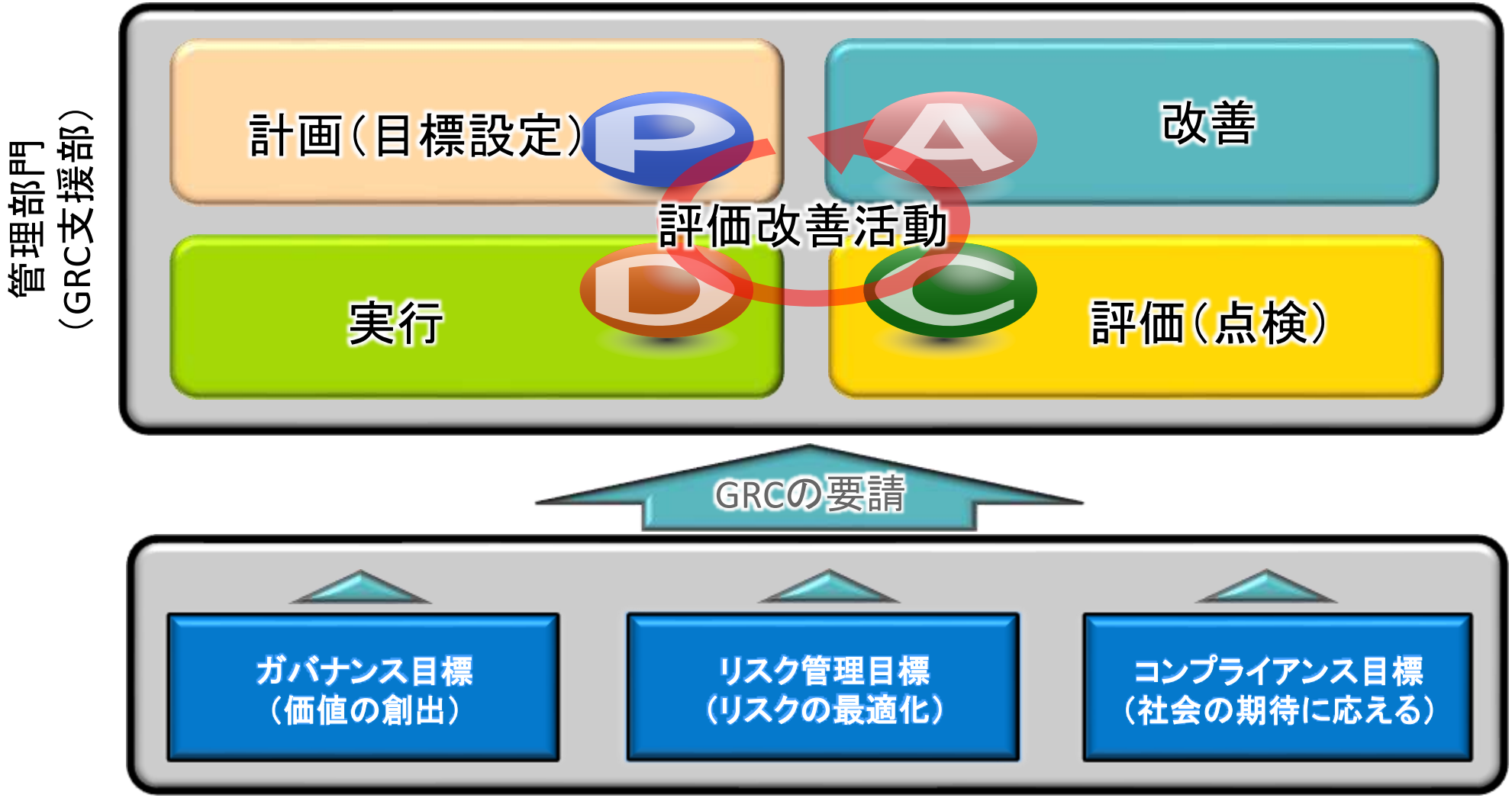
情報セキュリティ管理体制



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）



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、プロジェクトチームでは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、プロジェクトチームの感想をまとめたものであり、組織として総括した内容ではありません。

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2014年12月2日記事）

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
   - 2.1　GRC改革に至る背景
   - 2.2　構築したGRC態勢の概要
   - 2.3　定着に向けた取り組みと振り返り

3. 東京海上日動システムズの情報セキュリティ改革

4. まとめ

まとめ

東京海上日動システムズの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・情報セキュリティへ
- ✓ G（価値創出）とR（リスクの最適化）、C（社会の期待に応える）を統合的に対応し、効果的・効率的なガバナンス態勢を構築
- ✓ 経営者が交代しても「価値創出」し続ける持続性を確保
- ✓ 社員がいきいきとスピード感をもって、お客様価値を提供し企業価値創造している

ご静聴、ありがとうございました。

To Be a **Good Company**

東京海上日動システムズ株式会社