システム監査と事業継続マネジメントシステム（BCMS：Business Continuity Management System）ー持続的成長と人財育成の関係 ー

The Relationship of Sustainable Growth and Human Resource Development

2014年06月06日

リスクマネジメント研究プロジェクト

報告者　足立　憲昭

イオンエンターテイメント㈱

システム監査学会RM研究プロジェクト

「リスクマネジメント研究プロジェクト」 メンバー

主査　　：森宮　康（明治大学）
副主査　：黒澤　兵夫（TAKE国際技術士研究所）
メンバー：植野　俊雄（ISU）
　　高野　美久（NECソリューションイノベータ㈱）
　　高橋　孝治（公認会計士事務所）
　　堀越　繁明（みずほ証券株式会社）
発表者　：足立　憲昭（イオンエンターテイメント㈱）

昨年度までの到達点：

・SCMにおけるBCMSとSAのモデル化　（H19年度）
・チェックリストの作成　（H20年度）
・ガイドラインの作成と試行　（H21年度）
・JRMS2010の小売SCM適用について　（H22年度）
・JRMS2010の適用・・・成熟度の違い　（H23年度）
・社会的責任への道程・・・レベル3の壁　（H24年度）

会合	日程	おもな検討内容
1回目	平成25年07月24日(水)	前回振り返りとﾌﾘｰ・ﾃﾞｨｽｶｯｼｮﾝ①
2回目	平成25年09月30日(月)	フリー・ディスカッション②
3回目	平成25年10月21日(月)	特別講座
4回目	平成25年12月02日(月)	報告（案）の説明と協議①
5回目	平成26年01月27日（月）	報告（案）の説明と協議②
6回目	平成25年03月10日(月)	報告書（たたき台）の検討会
7回目	平成25年04月24日(木)	報告書（確定分）最終検討会

1-1.RMプロジェクトで話しあった意見（今年1～5回目）

JR北海道の脱線事故
モラルハザードの問題
（人財の流出、経営優先）

原発汚染水漏れの報告遅れ
モラルハザードの問題
（情報の共有化、部分最適）

海外子会社の経理不正
情報共有化、ネットワーク不足
（言葉・風土・法律の壁）

記録的な大雨・異常高温
農業・漁業の産地変化
築き上げたブランド失う

日中・日韓関係の問題
地政学リスクが増大
（個人・企業ネットワーク重要）

知的財産権の侵害
企業機密情報の漏洩
（リストラで信頼関係変化）

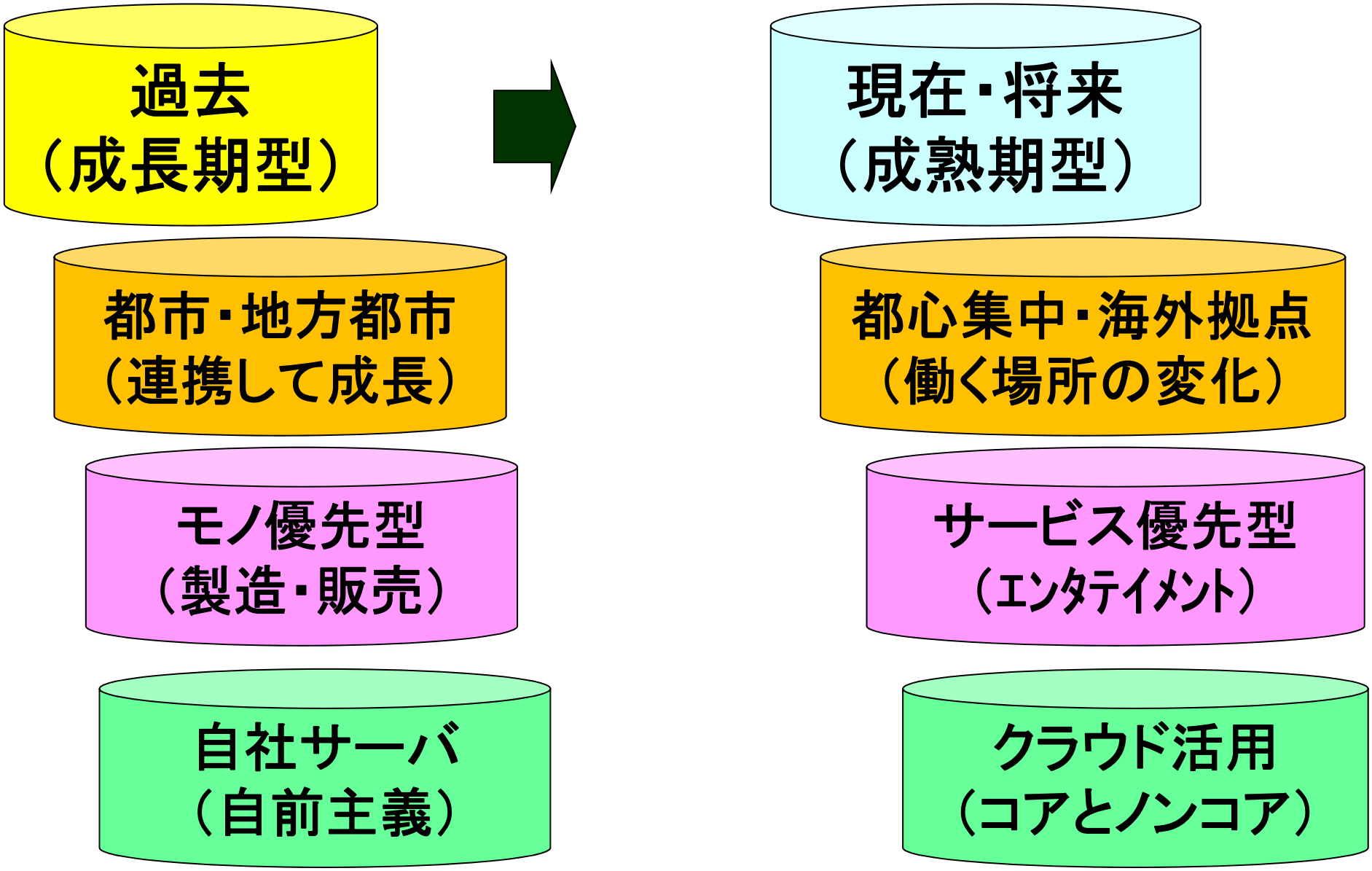
欧米式の株主利益偏重
効率化（労働を経費とみる）
人的資産、現場力の競争

システム監査学会RM研究プロジェクト

1-2.急激な社会環境の変化

1.小売業が地元顧客（ローカルニーズ）へ対応
　ネットスーパー、御用聞き復活、オムニチャネル
2.買物頻度の増加（毎日）とコミュニケーションの
　場を求める⇒時間帯別、年代別ニーズへ対応
3.単身世帯急増⇒少量パック（使いきり）、冷凍食品
4.健康志向（無添加、有機農法、カロリー表示）

1-3.急激な環境変化に組織が対応遅れになる



システム監査学会RM研究プロジェクト

1-4.なぜ、事故報告が再発防止に繋がらない？

リスク情報の共有化

受容したリスクを記録

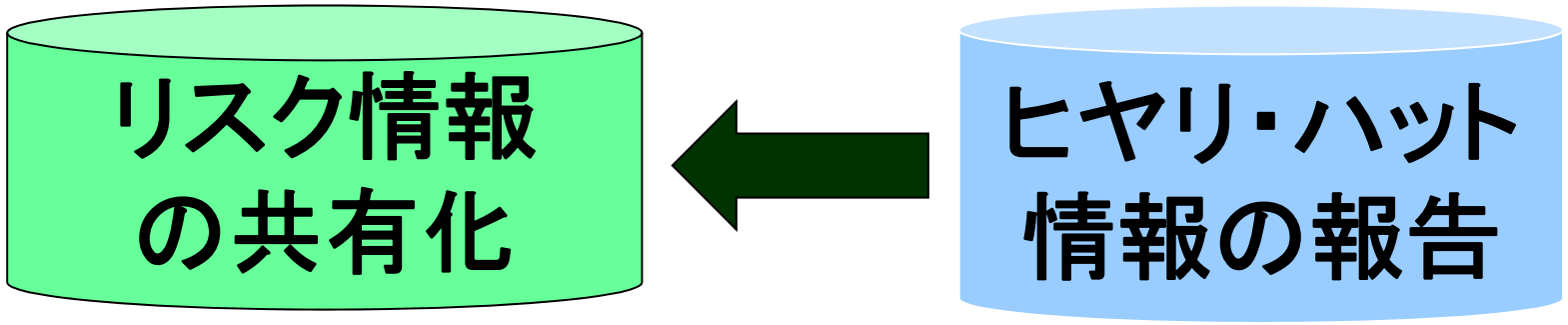
執行部門（株主要求）
短期利益の追求と投資効果

1.第三者委員会の必要性・・・業界の常識が非常識
　専門性と独立性の両立 **組織内**

2.事故報告書に真実が現れない・・・身内で処理
　「真のリスク情報（失敗・事故）」

3.多くの業界・学会・官公庁が協同で取組み
　異業種の専門家がネットワーク（Co-working）

1-5.なぜ、事実が埋もれてしまうのか？



1.事実調査と評価（又は犯人探し）を分離

事件の真相が闇に埋もれる（記録が不完全）

関係者が無口になる、マスコミの過激報道

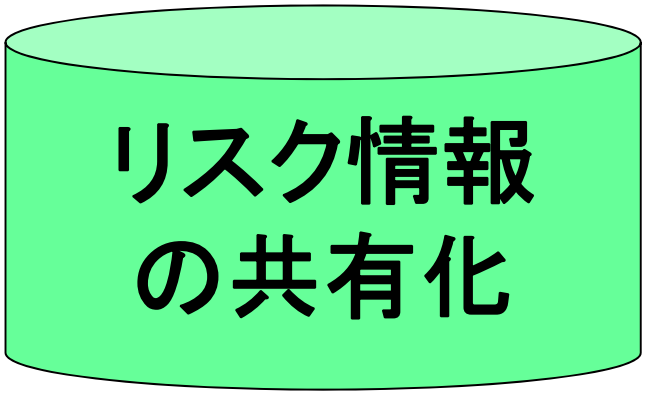
※告発すれば、傷つく（組織からマイナス評価）

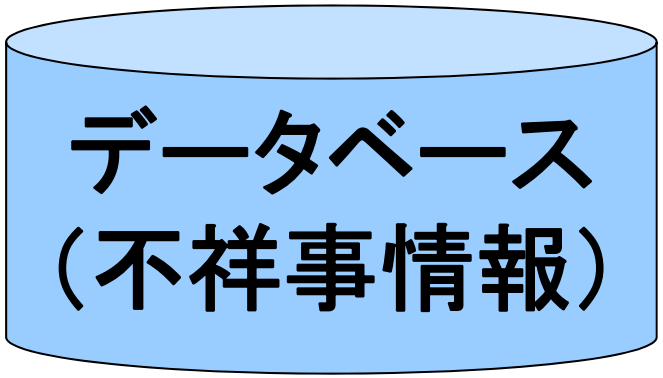
2.組織的不正・・・蔓延する（組織全体）

個人的不正・・・虫がつく（取り除ける）

※人が介在する

1-6.不祥事発生時の情報・記録が活用されない





1.役員（トップ）が持つ情報⇒悪い報告が上がらない

2.「株主・経営者の視点」に偏り「従業員の視点」が弱い

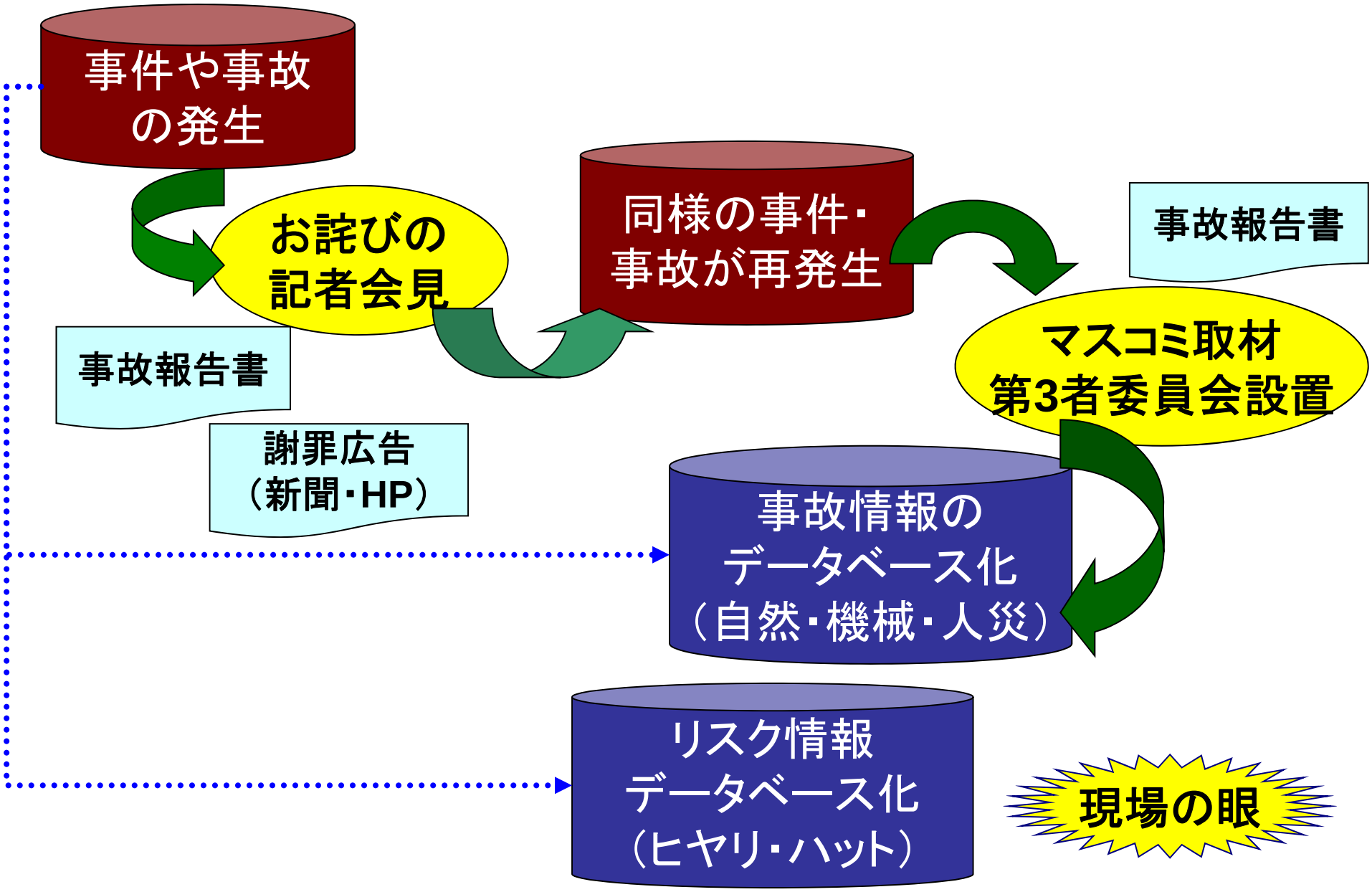
3.従業員の忠誠心薄れる（リストラ、非正規雇用の影響）

4.同業の情報に偏り、他の業界に関心が少ない

5.サプライチェーンの構築遅れ（パートナー意識が弱い）

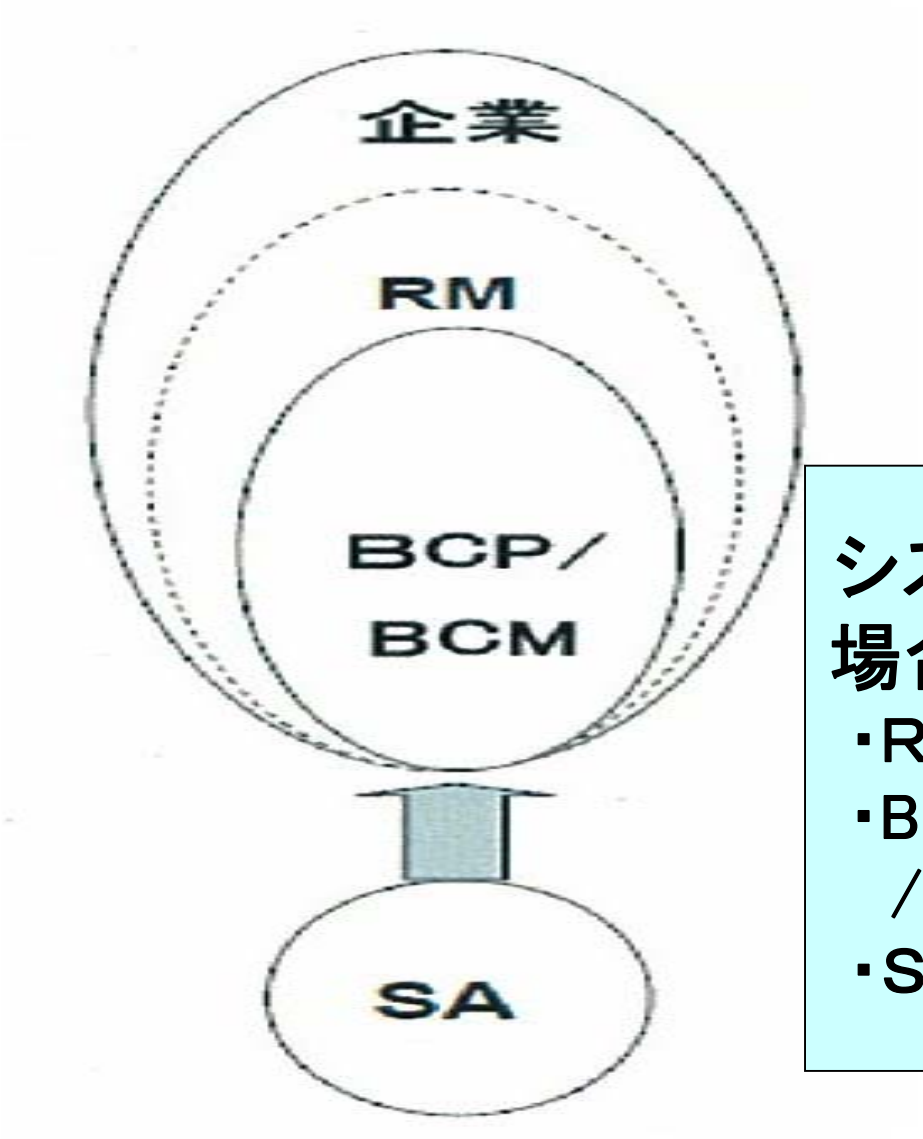
6.利害関係者へアカウンタビリティ不足（経営の透明性）

1-7.繰り返す事件・事故・・・データベースが活きない



システム監査学会RM研究プロジェクト

2-1. RM、BCP/BCMSとSAの関連（主眼SA）



システム監査（SA）を主眼とした場合の関係

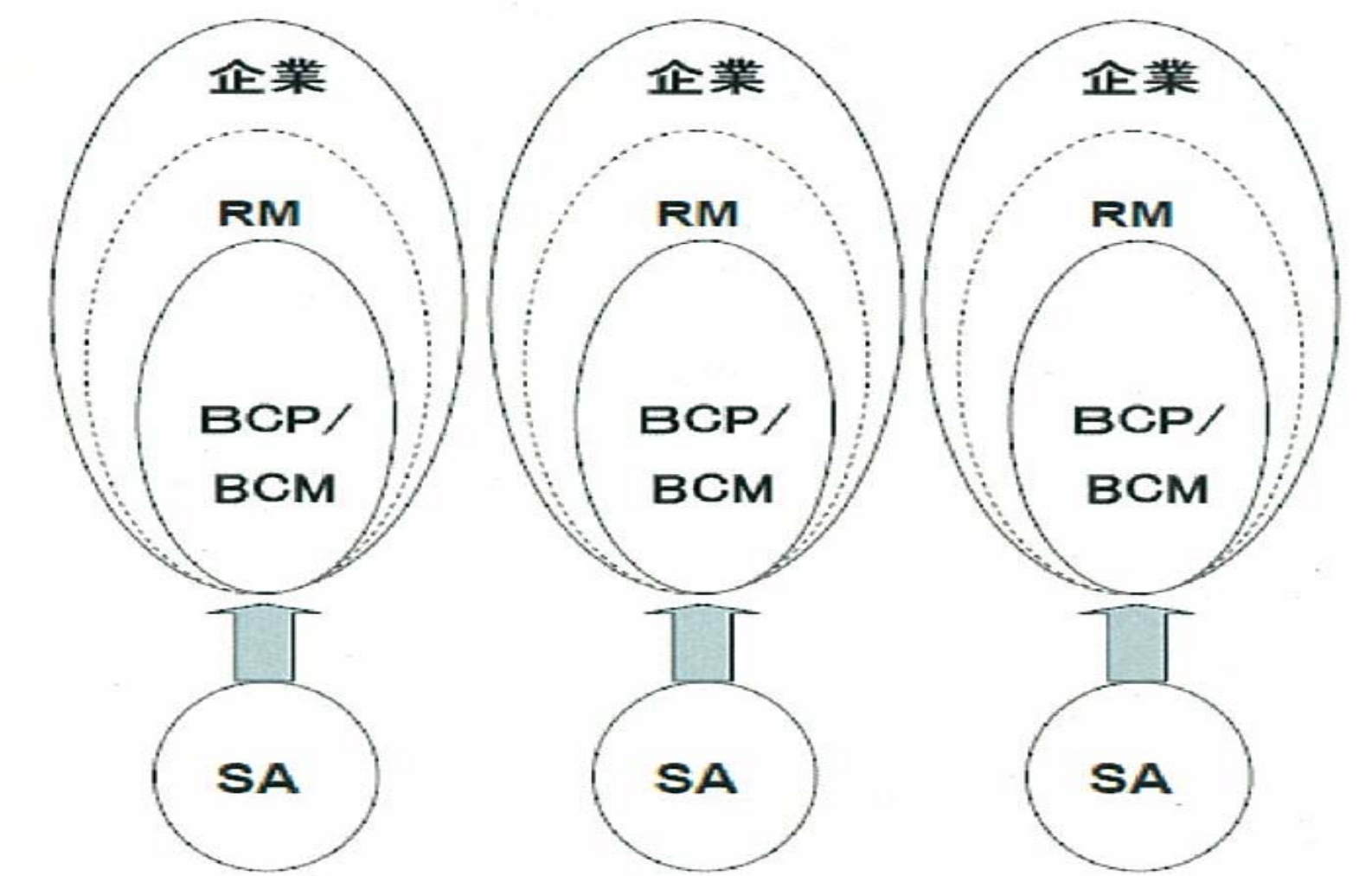
- RM（リスクマネジメント）
- BCP(事業継続計画）
  /BCMS（事業継続ﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ）
- SA（システム監査）

2-2. 単一ソリューションシステムの統合と単一監査

成熟度モデル（JRMS2010）

ﾚﾍﾞﾙⅡからﾚﾍﾞﾙⅢに該当

（部門ﾚﾍﾞﾙ）　　（会社ﾚﾍﾞﾙ）

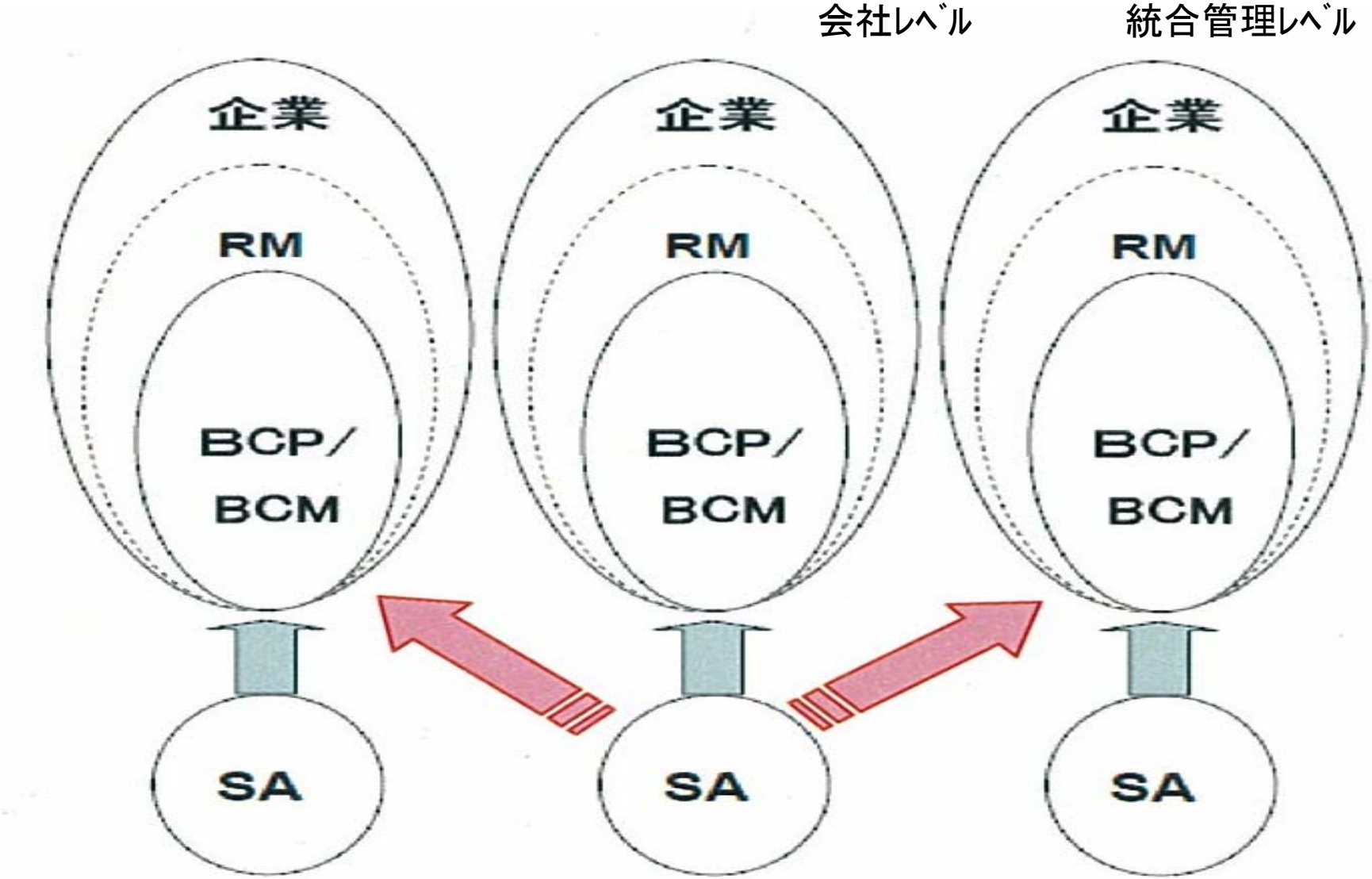


ｼｽﾃﾑ監査学会RM研究ﾌﾟﾛｼﾞｪｸﾄ

2-3. 他企業／他組織のシステムと連携したSAの実施

ﾚﾍﾞﾙⅢからﾚﾍﾞﾙⅣに該当

会社ﾚﾍﾞﾙ　　統合管理ﾚﾍﾞﾙ

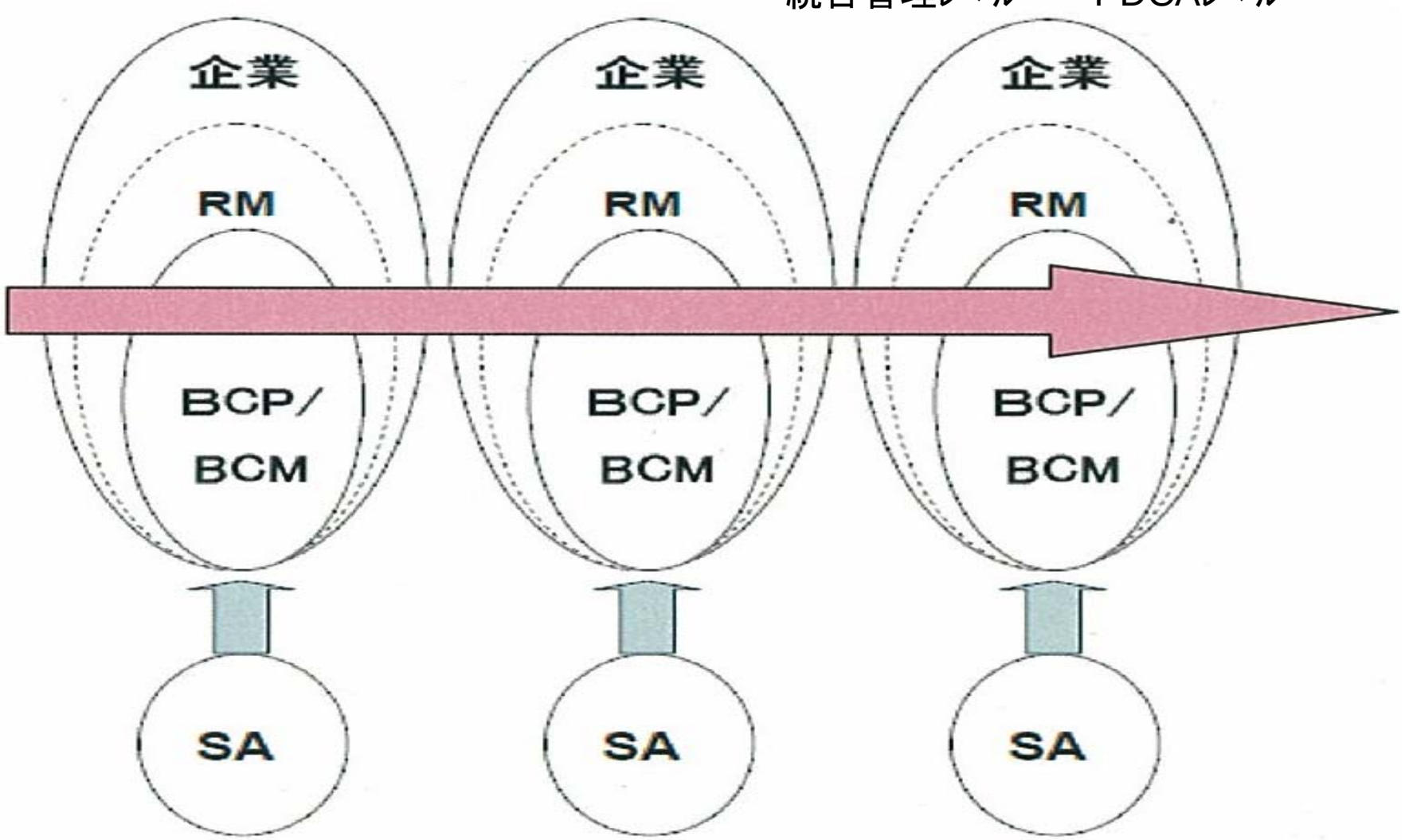


ｼｽﾃﾑ監査学会RM研究ﾌﾟﾛｼﾞｪｸﾄ

2-4. 統合システムのSAとSCMシステムの横断SAの実施

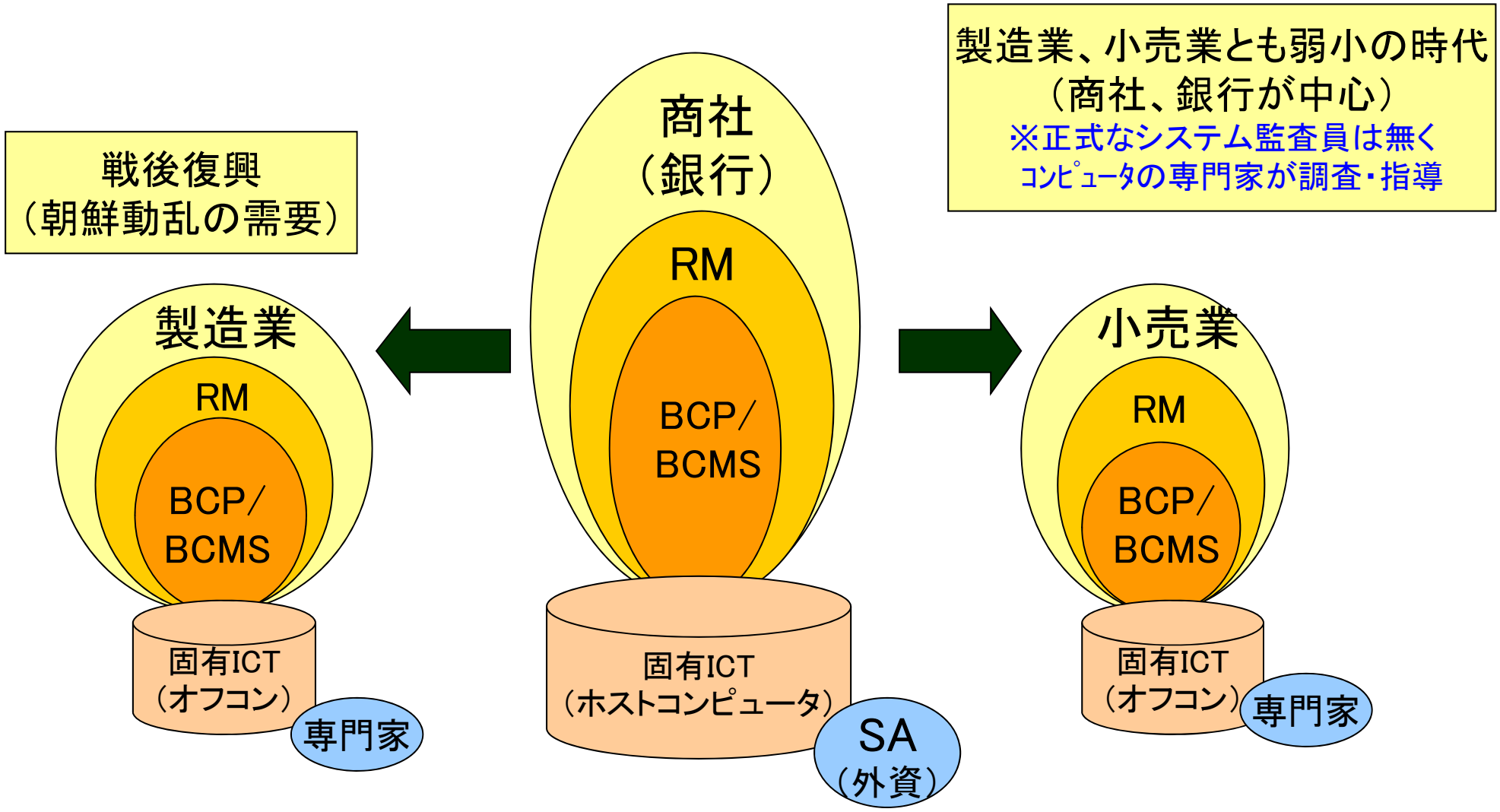
ﾚﾍﾞﾙⅣからﾚﾍﾞﾙⅤに該当

統合管理ﾚﾍﾞﾙ　　PDCAﾚﾍﾞﾙ



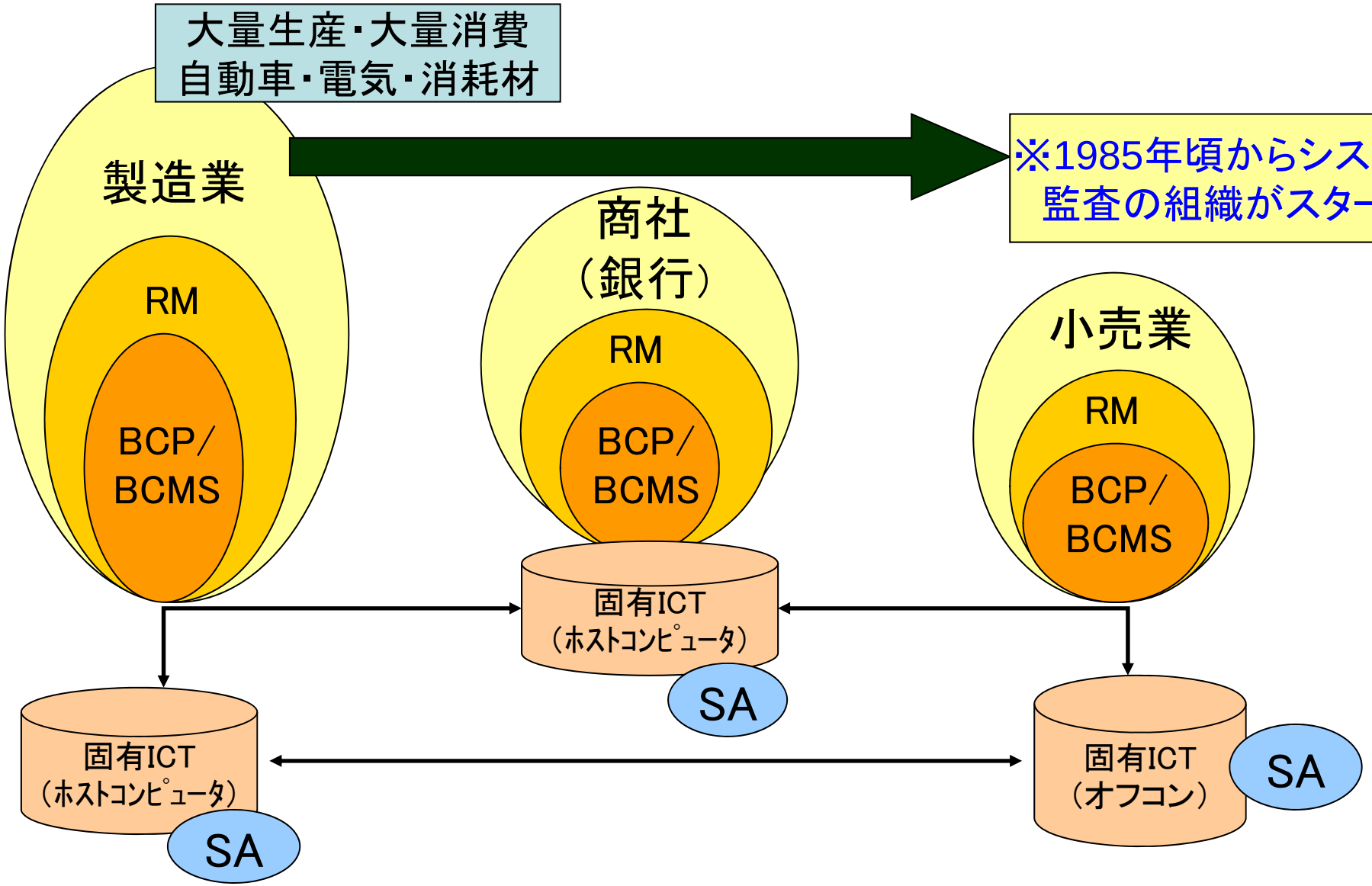
ｼｽﾃﾑ監査学会RM研究ﾌﾟﾛｼﾞｪｸﾄ

3-1.サプライチェーンの発展Ⅰ（1950～60年代イメージ）



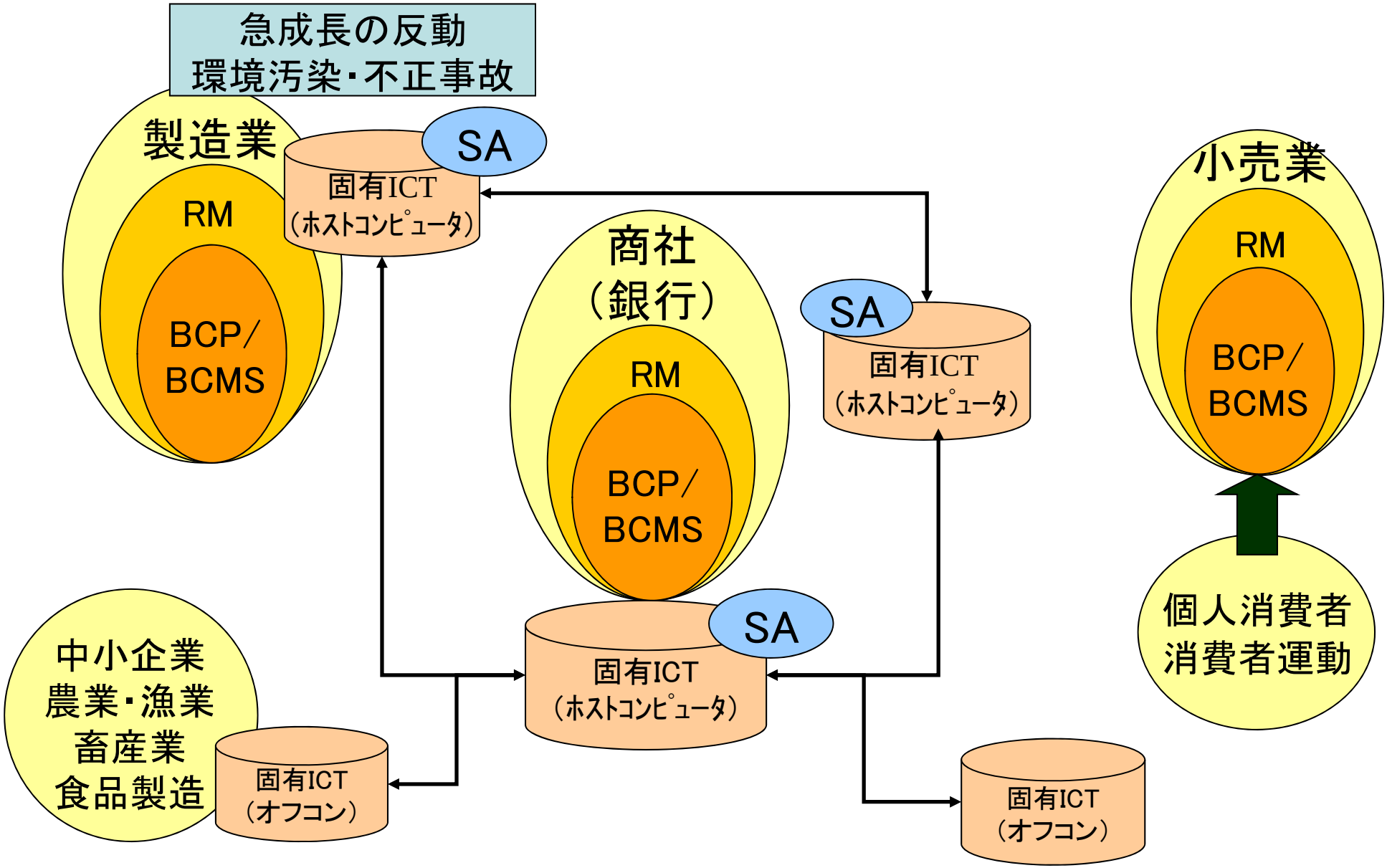
システム監査学会RM研究ﾌﾟﾛｼﾞｪｸﾄ

3-2.サプライチェーンの発展Ⅱ（1970～80年代イメージ）



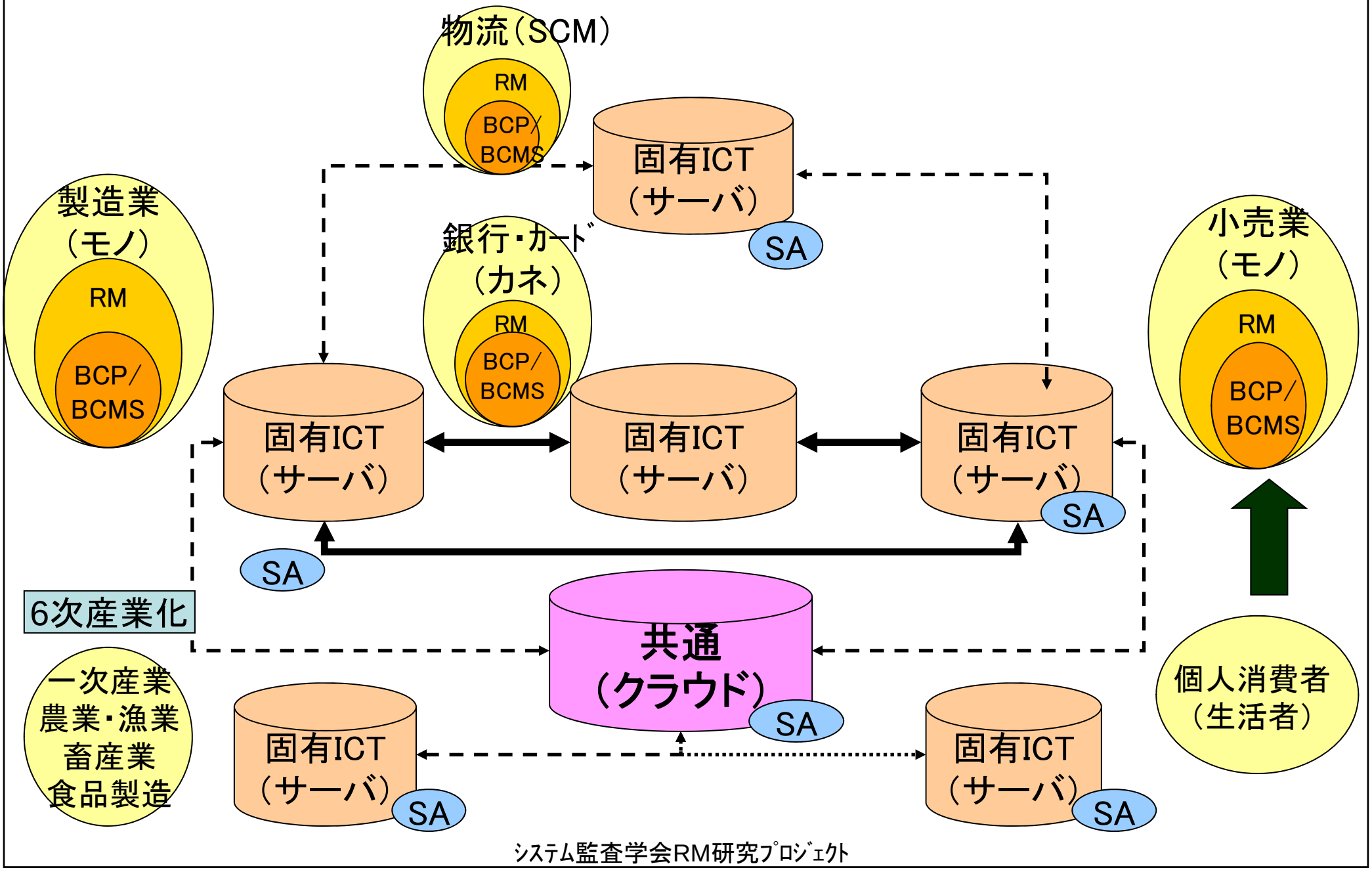
システム監査学会RM研究プロジェクト

3-3.サプライチェーンの発展Ⅲ（1990～2000年イメージ）



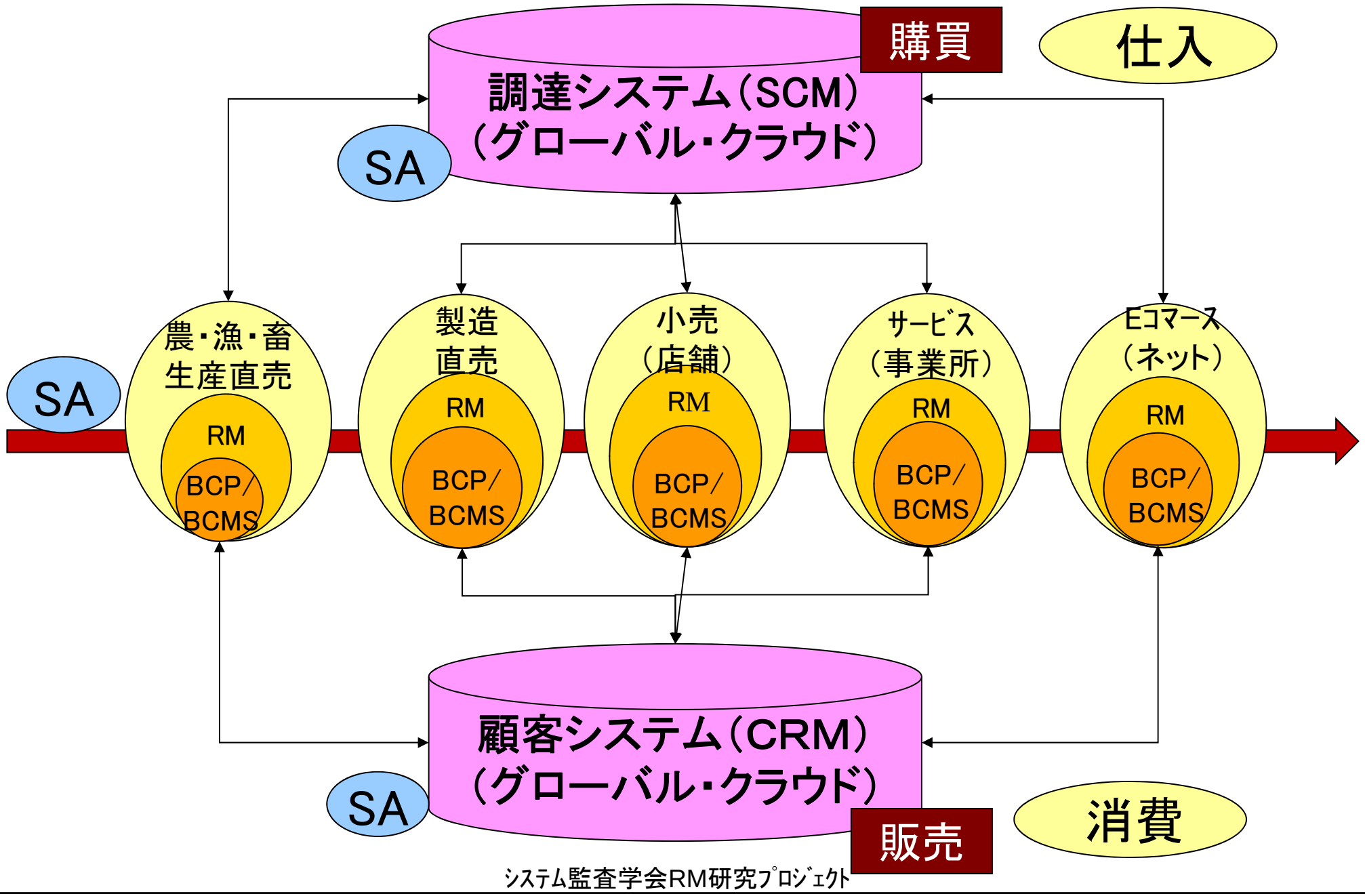
システム監査学会RM研究プロジェクト

3-4.サプライチェーンの発展Ⅳ（2001～2012イメージ）



システム監査学会RM研究プロジェクト

3-5.サプライチェーンの発展過程Ⅴ（2013～20イメージ）

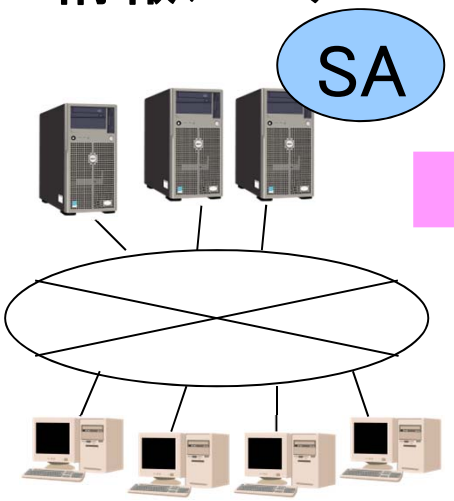


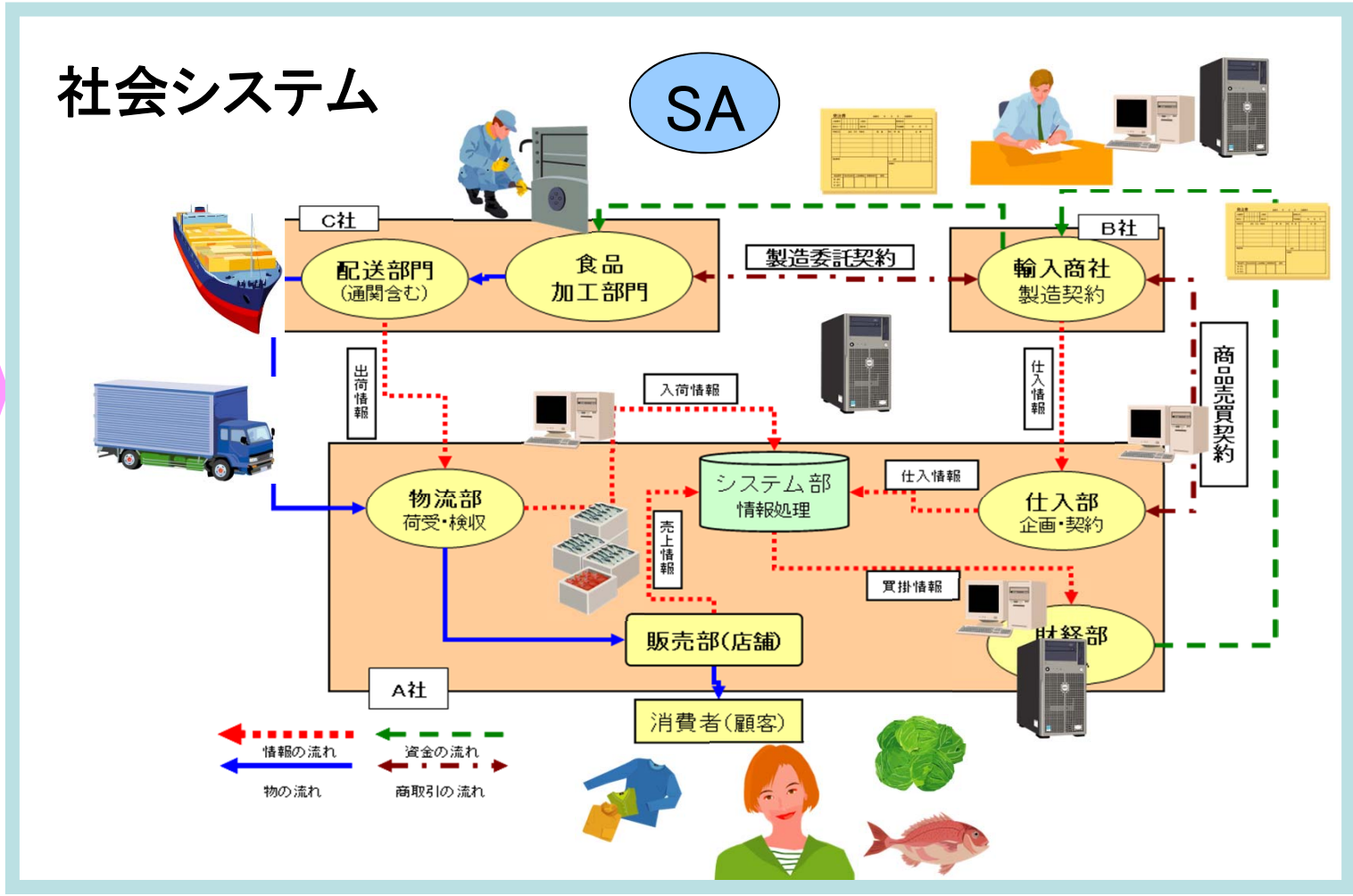
システム監査学会RM研究プロジェクト

4-1.小売業のリスクマネジメント対象範囲モデル

参考資料

【留意点】
・情報システムという視点でなく、材料／物の流れから対象範囲を決定していく。
・取引形態（B to C、B to B、B to P）によって、対象が異なる。



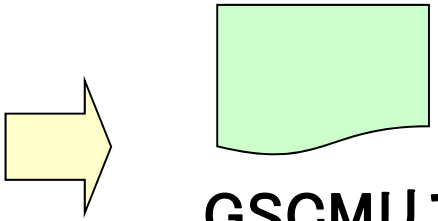


システム監査学会RM研究プロジェクト

4-2.GSCMにおけるリスクの一般化

システム管理基準
第Ⅰ項　情報戦略　第5項　事業継続計画（5項目）
第Ⅳ項　共通業務　第7項　災害対策（13項目）
7.1　リスク分析（3項目）
7.2　災害時対応計画（6項目）
7.3　バックアップ（2項目）
7.4　代替処理・復旧（2項目）

参考資料



GSCMリスク
チェックシート

GSCMリスクチェックシートの全体構成
Ⅰ．全体確認シート
①基本事項
・システム管理基準を参考
・教育関連は個別リスク確認シートの「人財」に移管
Ⅱ．個別リスク確認シート
①調達
②品質
③風評
④インフラ
⑤ファイナンシャル
⑥人財

GSCMのリスクにかかる要因

- 調達
- インフラ
- 品質
- ファイナンシャル
- 風評
- 人財

対象を“情報システム”だけでなく
“社会情報システム全体”として
考えざるを得ない

システム監査学会RM研究プロジェクト

4−3.情報システムの進化のシステム監査の概念図

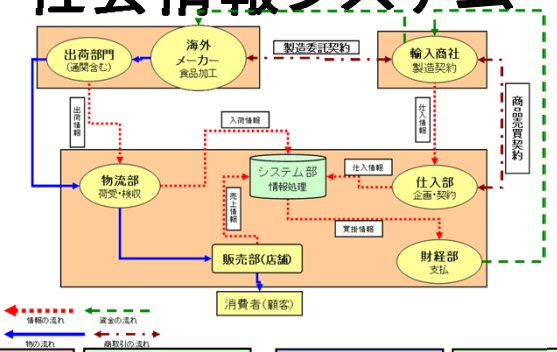
参考資料

【注記】 世の中の流れから
環境、社会が重要になってきた

品質
環境
ファイナンシャル
インフラ
ICTの深耕化／
国際社会におけるSCMSのインフラ化
人財
調達
社会
風評

情報システム
インフラ

社会情報システム



インフラ　環境　人財　品質
ファイナンシャル　調達　風評　社会

BCP/BCMの策定（ISO31000に準拠）

取引先にBCP/BCMを要請するのではなく、“社会情報システム”として全体を包含して監査する。

システム監査の実施

GSCMリスクチェックシート

システム監査学会RM研究プロジェクト

4-4.GSCMにおけるリスクの一般化（再整理）　参考資料

調達
原料高騰、納期遅延、在庫過剰
⇒品質ﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ（ISO9001）

環境
大気汚染、水質汚濁、放射能汚染
⇒環境ﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ（ISO14001）

品質
異物混入、不衛生、表示ミス
⇒食品安全ﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ

ファイナンシャル
資金不足、取引先倒産、為替変動
⇒COSO、COBIT、IFRS

インフラ
情報システム、サプライチェーン
⇒事業継続ﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ

人財
労務災害、過重労働、後継者不足
⇒労働安全ﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑOHSAS

風評
中国餃子の毒物混入、
福島原発の農産・水産へ影響
⇒事故発生後の対応（開示）

社会・政治
靖国訪問による日中関係悪化
ウクライナ情勢、歴史認識の違い
⇒ｶﾝﾄﾘｰﾘｽｸ、現地のｺﾐｭﾆｹｰｼｮﾝ

4-5.リスクマネジメントの成熟度モデルの考え方

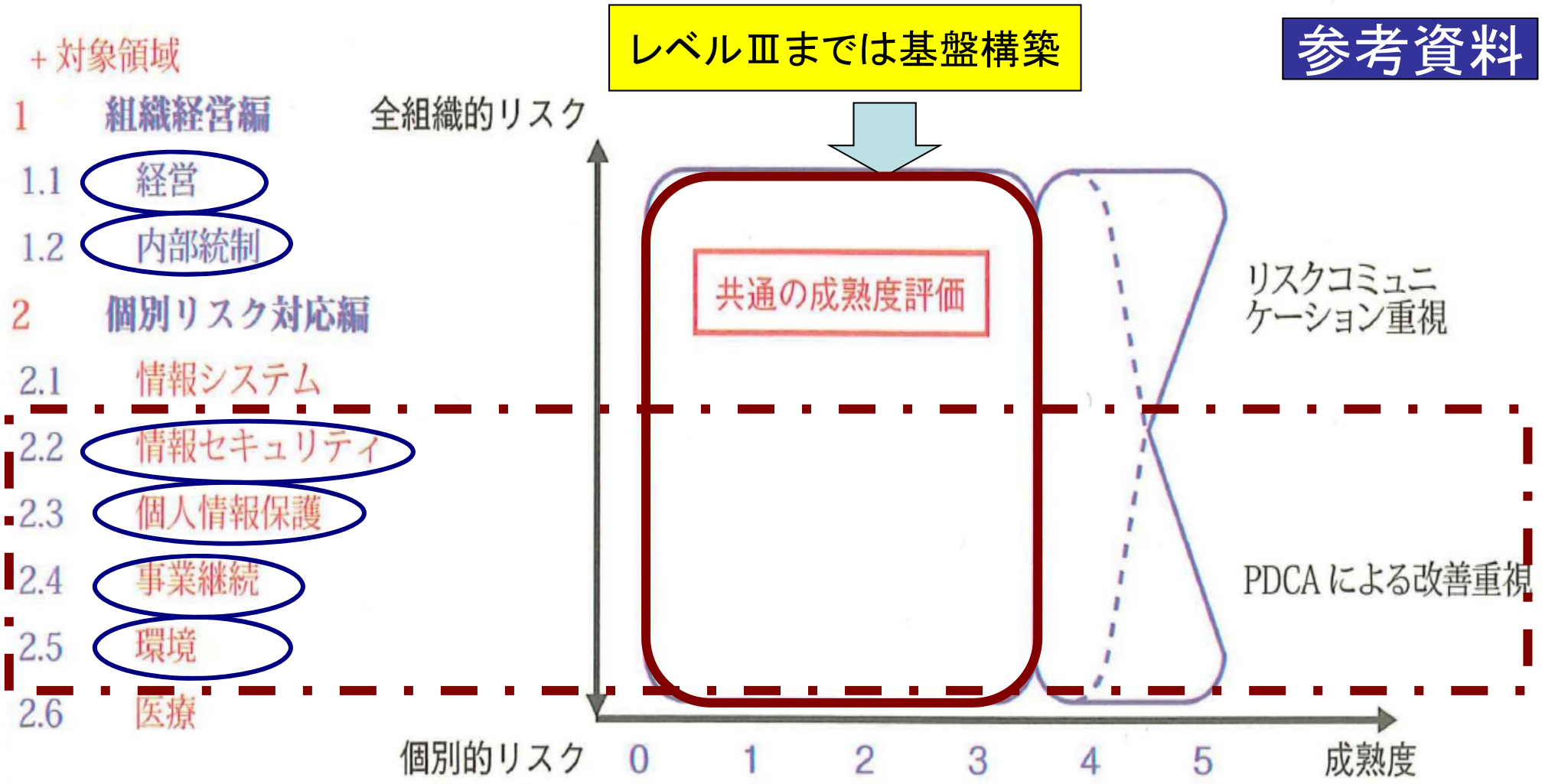


図 1-3.　リスクマネジメントの対象領域と成熟度の定義

参考：リスク社会で勝ち抜くためのリスクマネジメント-JRMS2010，JIPDEC

システム監査学会RM研究プロジェクト

4-6. 成熟度モデル活用による現場の実感！

参考資料

表 1-1.　JRMS2010 の成熟度の評価

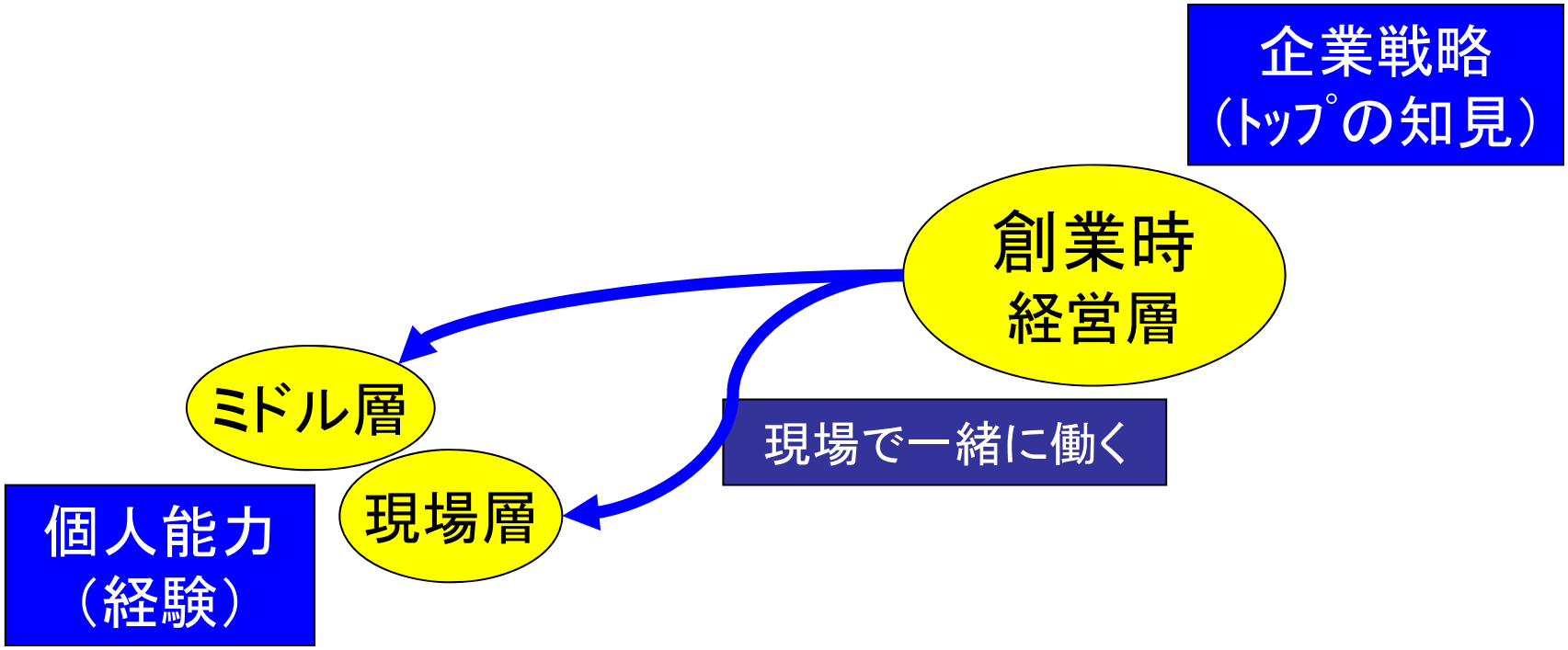
成熟度の評価レベル		定　義	摘要例
0	未認識・未対応	対象のリスクに対して、インシデントの発生まで何の対応もしていない。	・対象のリスクに対する認識もリスクを管理する認識もなく、対応方法について知識を持っている要員もいない。 ・インシデントの発生により、最大限の被害を受ける。
1	個人ごとによる対応	対象のリスクに対して個人的な対応を実施している。	・対象のリスクに対する認識や対応方法は、個人に依存している。 ・発生した個別のインシデントに対し、各個人が個人的な対応を行う。 ・インシデントの発生による被害は、誰が対応したかにより、大きく異なる。
2	部門ごとによる対応	対象のリスクに対する対応は部門ごとに統一されているが、全組織で統一した対応は行われていない。	・同一のリスクに対して、支店等の部門ごとに対応が定められ、文書化もされている。 ・発生した個別のインシデントへの対応は、その部門では統一されているが、部門が異なると、違った対応がある。 ・インシデントの発生による被害は、どの部門が対応したかにより、大きく異なる。
3	全組織による対応	対象のリスクに対する対応が全組織で標準化され、組織的な承認を得ている。	・同一のリスクに対して、全組織としての対応が定められ、文書化が行われており、手続き等も定められている。 ・実施された対応にバラツキ・ブレがあっても、その把握はできていない。 ・インシデントの発生による被害は、対応が外部から見える（外部に対し客観的な説明ができる）。
4	全組織による管理された対応	全組織での標準化された対応に加え、対象のリスクへの対応が基準どおり実施されているかを管理している。または、外部へのリスクコミュニケーションを行っている。	・対応のバラツキやブレが、基準からの逸脱として把握されている。 ・一般公衆も含め、外部への情報開示が行われている。 ・リスクマネジメントシステム改善のための仕組みがある。
5	全組織による最適化された対応	管理された全組織での対応に加え、リスクへの対応を組織として継続的に改善している。または、リスクへの外部からのフィードバックを取り入れている。	・外部のリスクマネジメントについて組織的な情報収集を行い、その情報をリスクマネジメントシステム改善の PDCA サイクルに活用している。 ・全社的な CSR 活動との連携が図られている。 ・外部への情報開示に対するフィードバックを取り入れる仕組みができている。

第1の壁

第2の壁

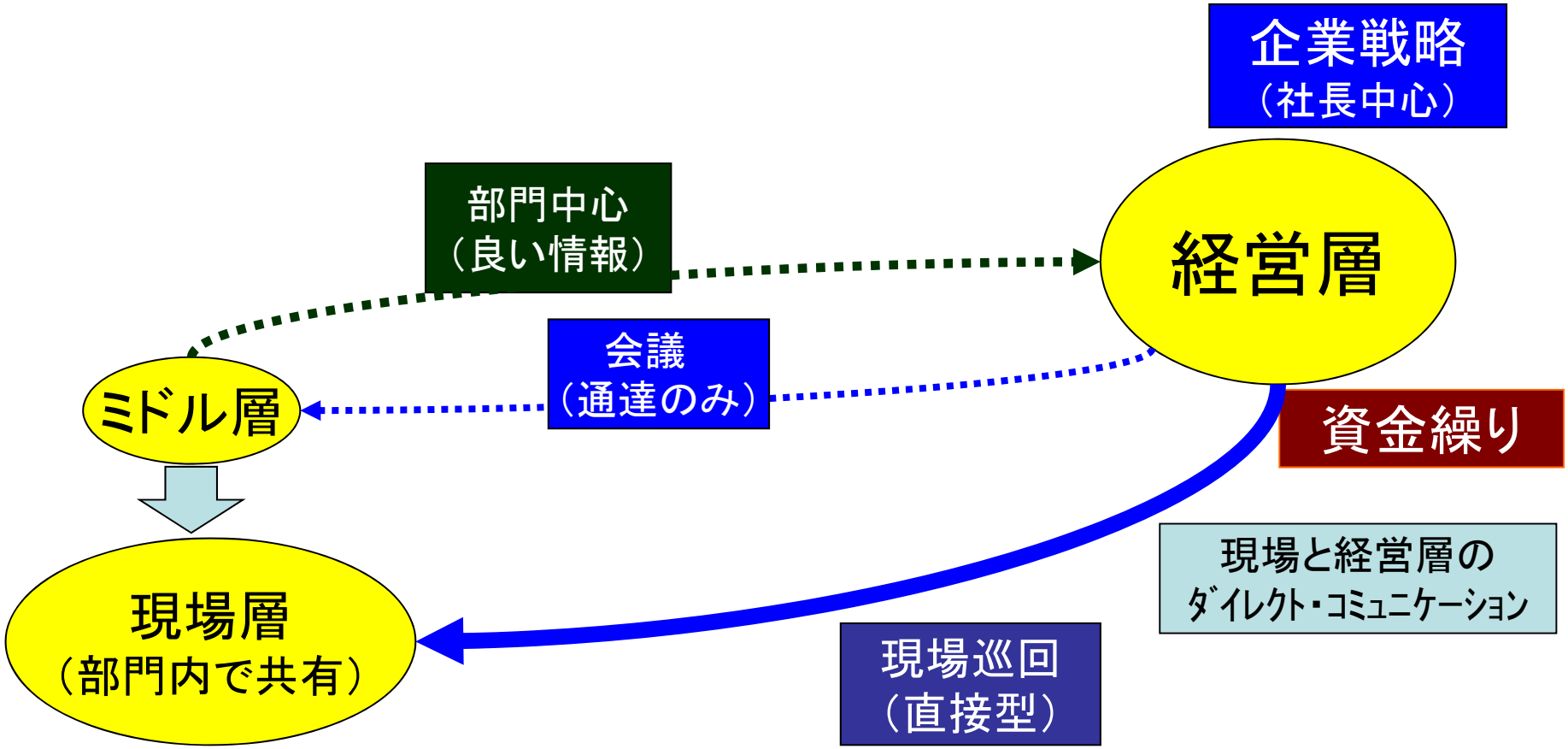
参考：リスク社会で勝ち抜くためのリスクマネジメント-JRMS2010，JIPDEC
システム監査学会RM研究プロジェクト

5-1.中小小売業の情報の流れ（成熟度Ｉのイメージ）



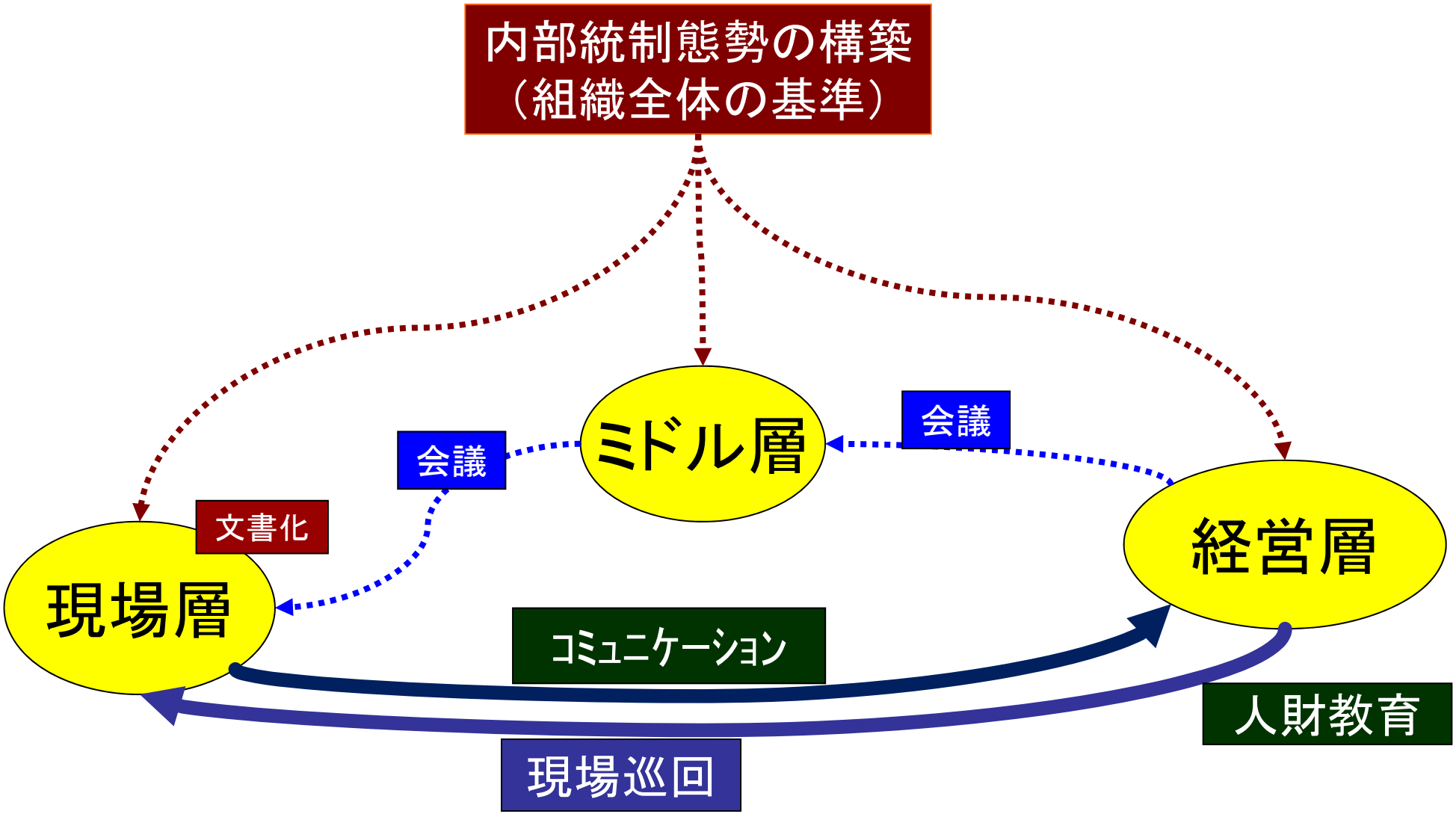
システム監査学会RM研究プロジェクト

5-2.中小小売業の情報（成熟度Ⅱのイメージ）



システム監査学会RM研究ﾌﾟﾛｼﾞｪｸﾄ

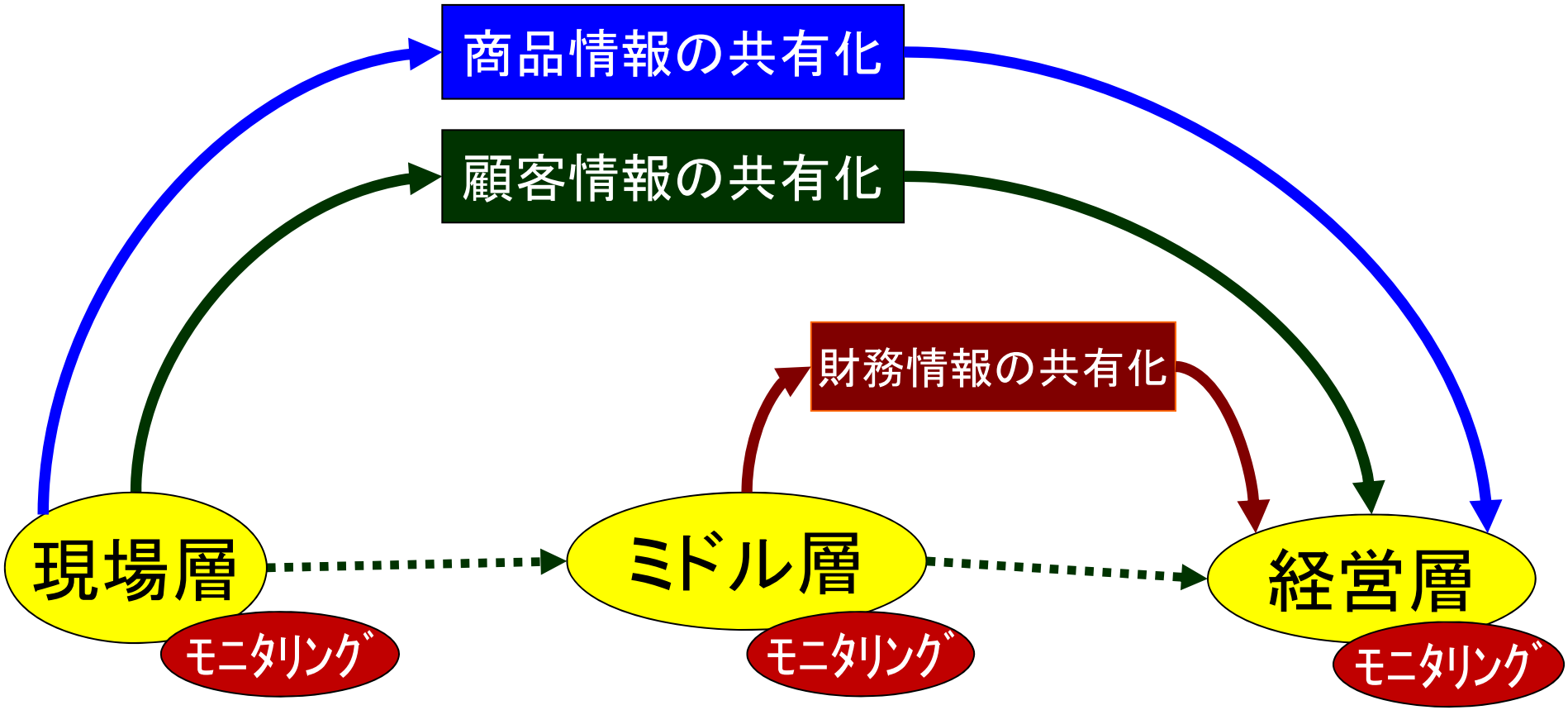
5-3.中小小売業における情報（成熟度Ⅲのイメージ）



システム監査学会RM研究プロジェクト

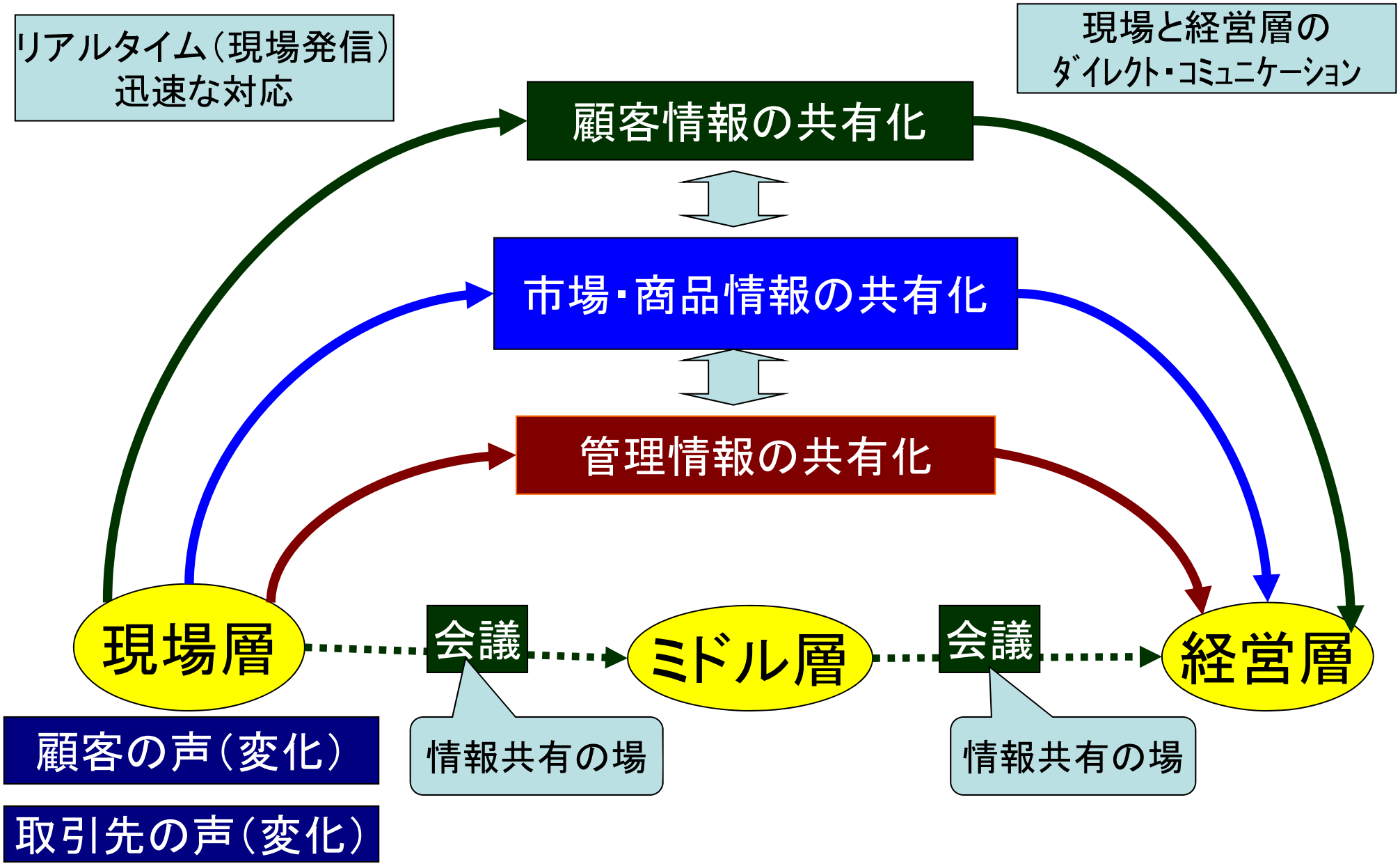
5-4.中小小売業における情報（成熟度Ⅳのイメージ）

現場層・ミドル層・経営層の
コミュニケーション（情報共有）



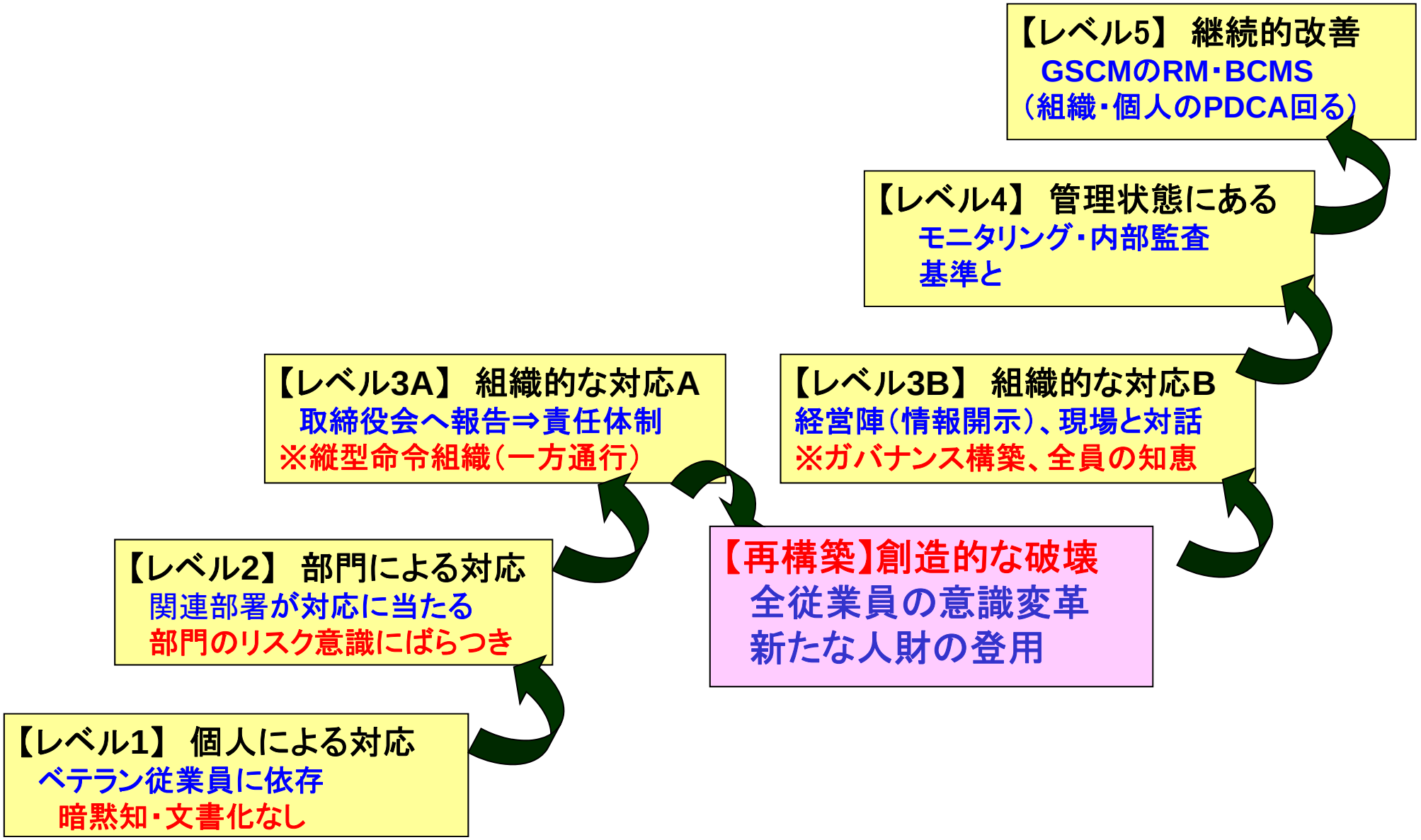
システム監査学会RM研究プロジェクト

5-5.中小小売業における情報（成熟度Ｖのイメージ）



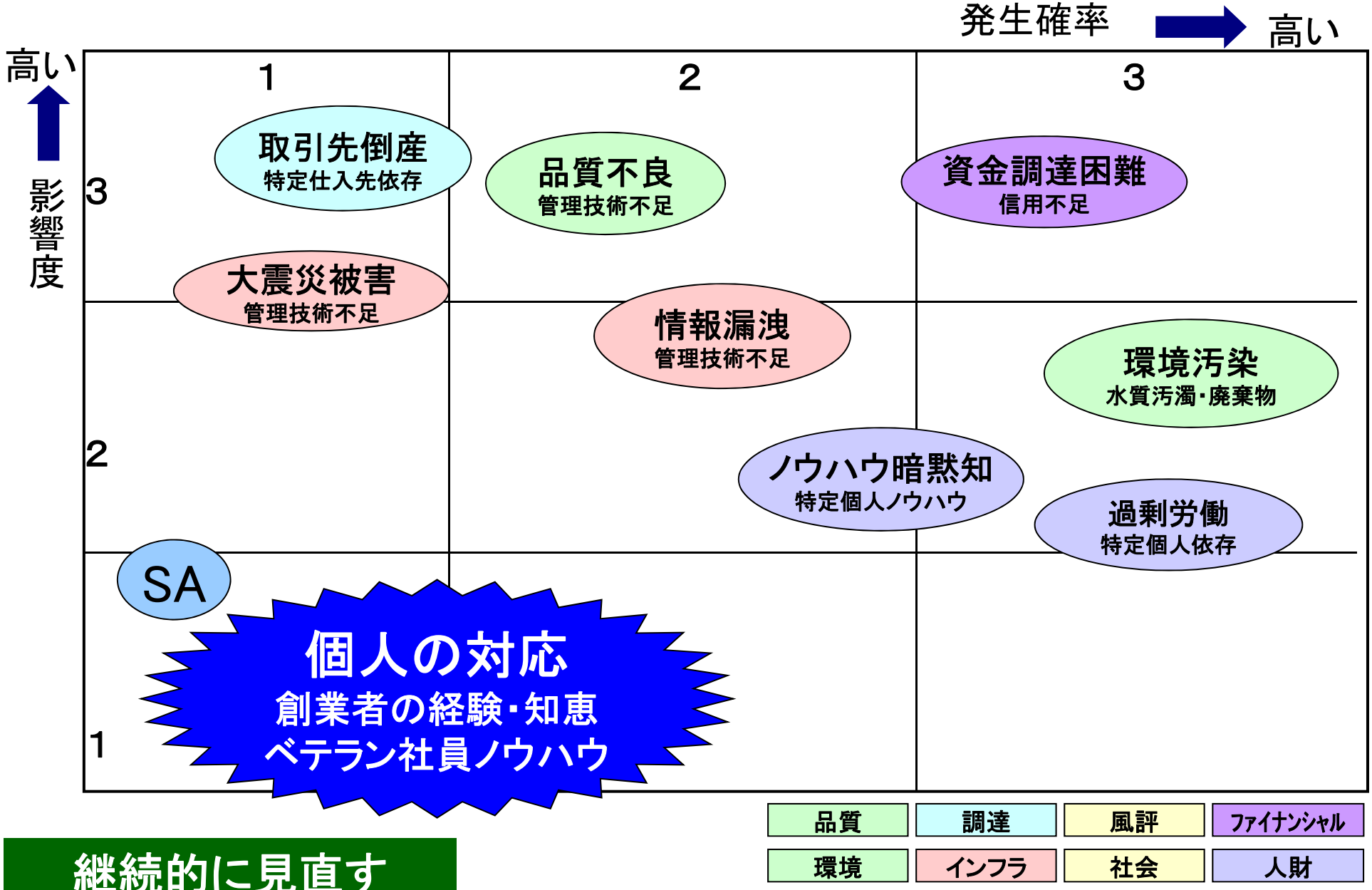
システム監査学会RM研究プロジェクト

5-6.中小小売業のリスクマネジメント成熟度（仮想モデル）



システム監査学会RM研究プロジェクト

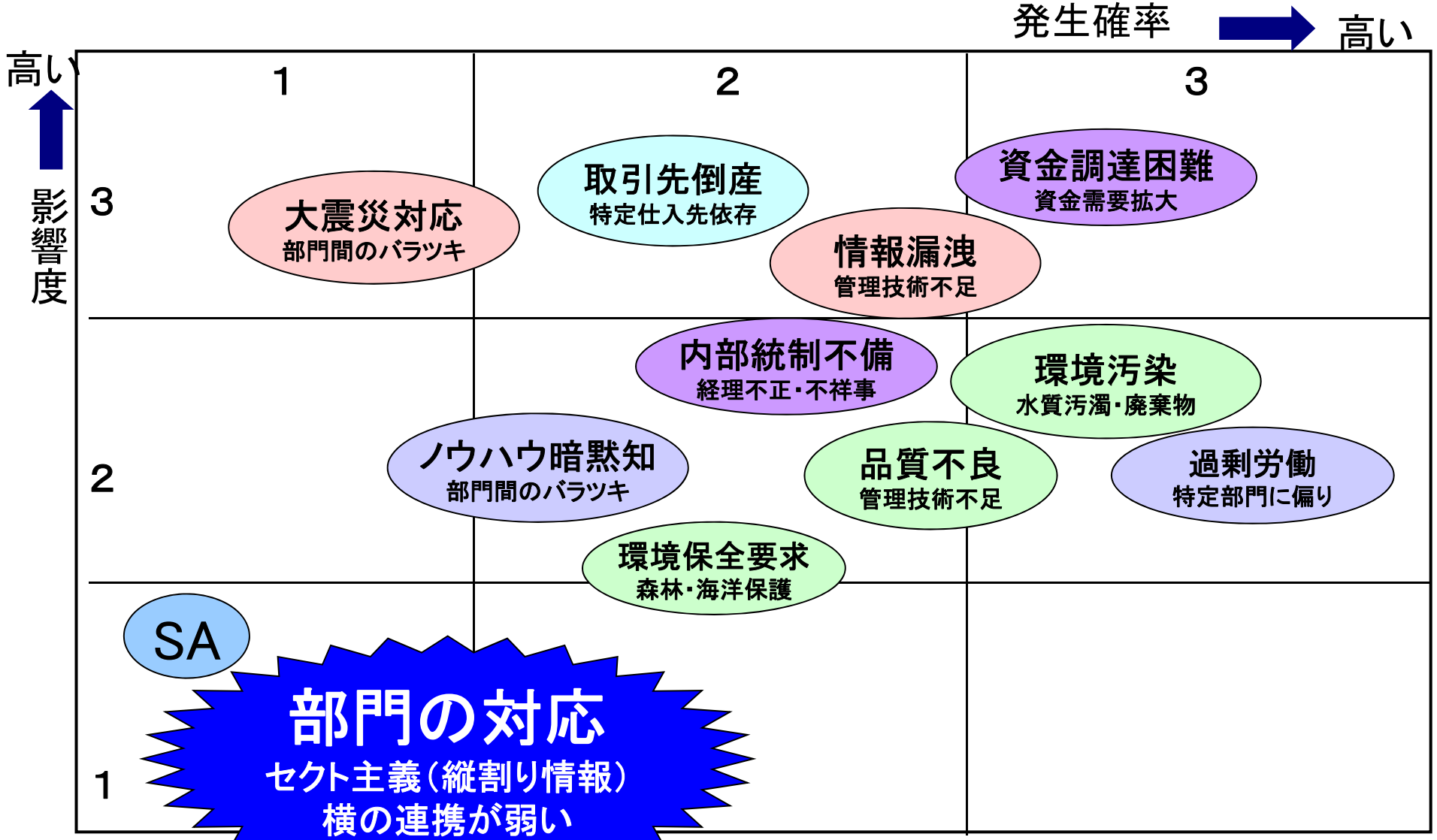
6-1.中小小売業のリスク評価ー（成熟度Ⅰ）イメージ



継続的に見直す

システム監査学会RM研究プロジェクト

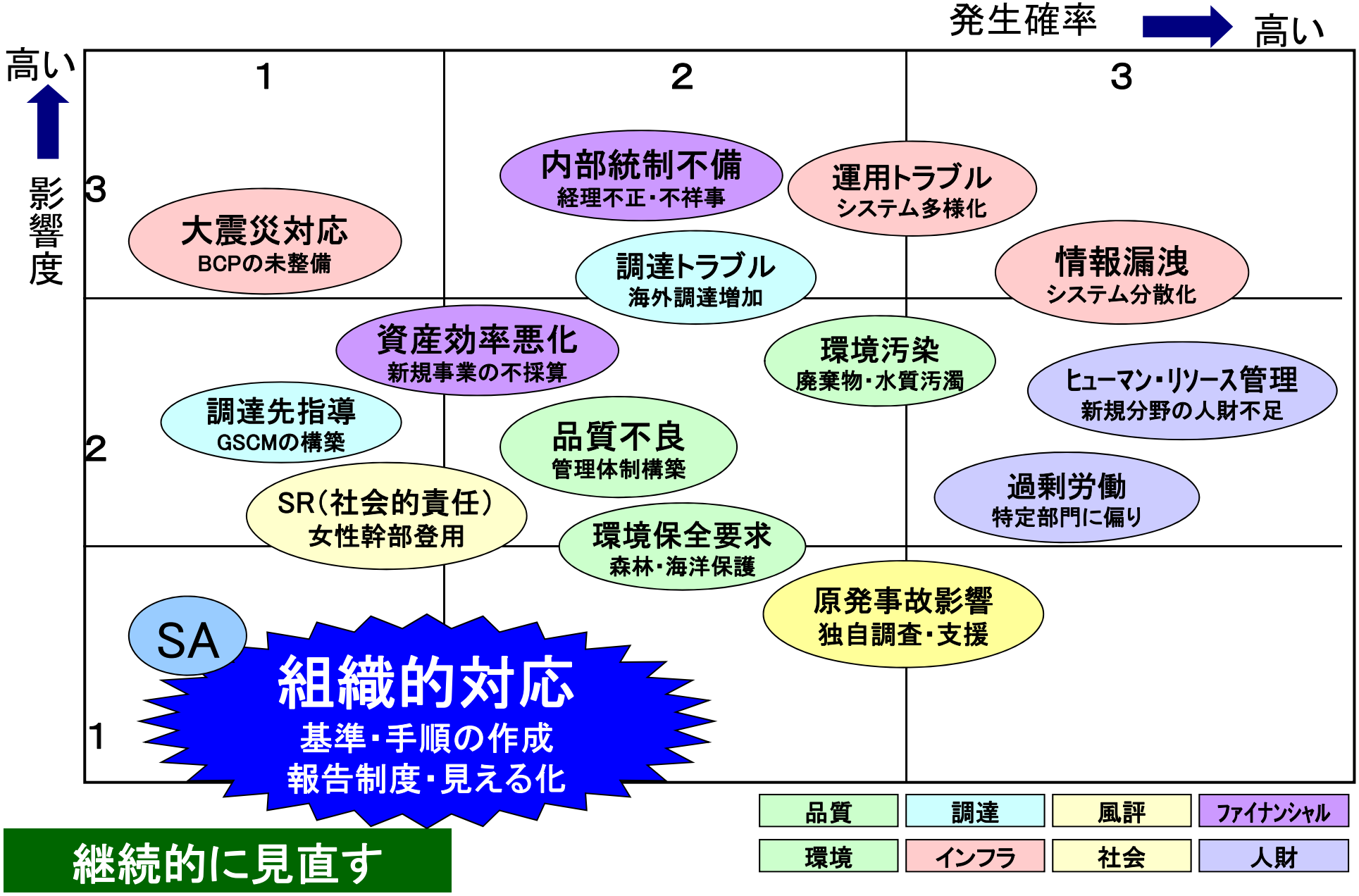
6-2.中小小売業のリスク評価ー（成熟度Ⅱ）イメージ



継続的に見直す

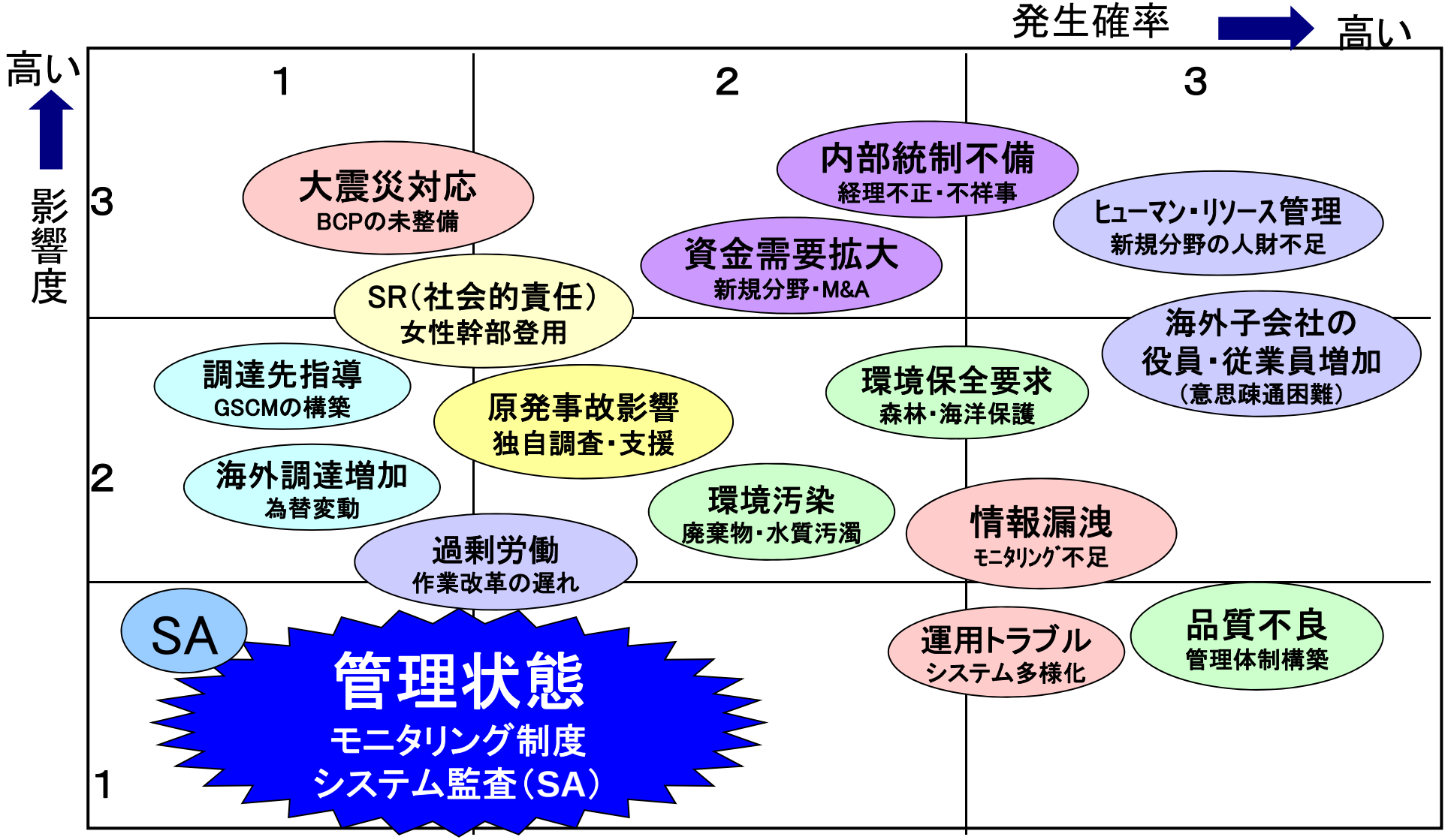
システム監査学会RM研究プロジェクト

6-3.中小小売業のリスク評価ー（成熟度Ⅲ）イメージ



システム監査学会RM研究プロジェクト

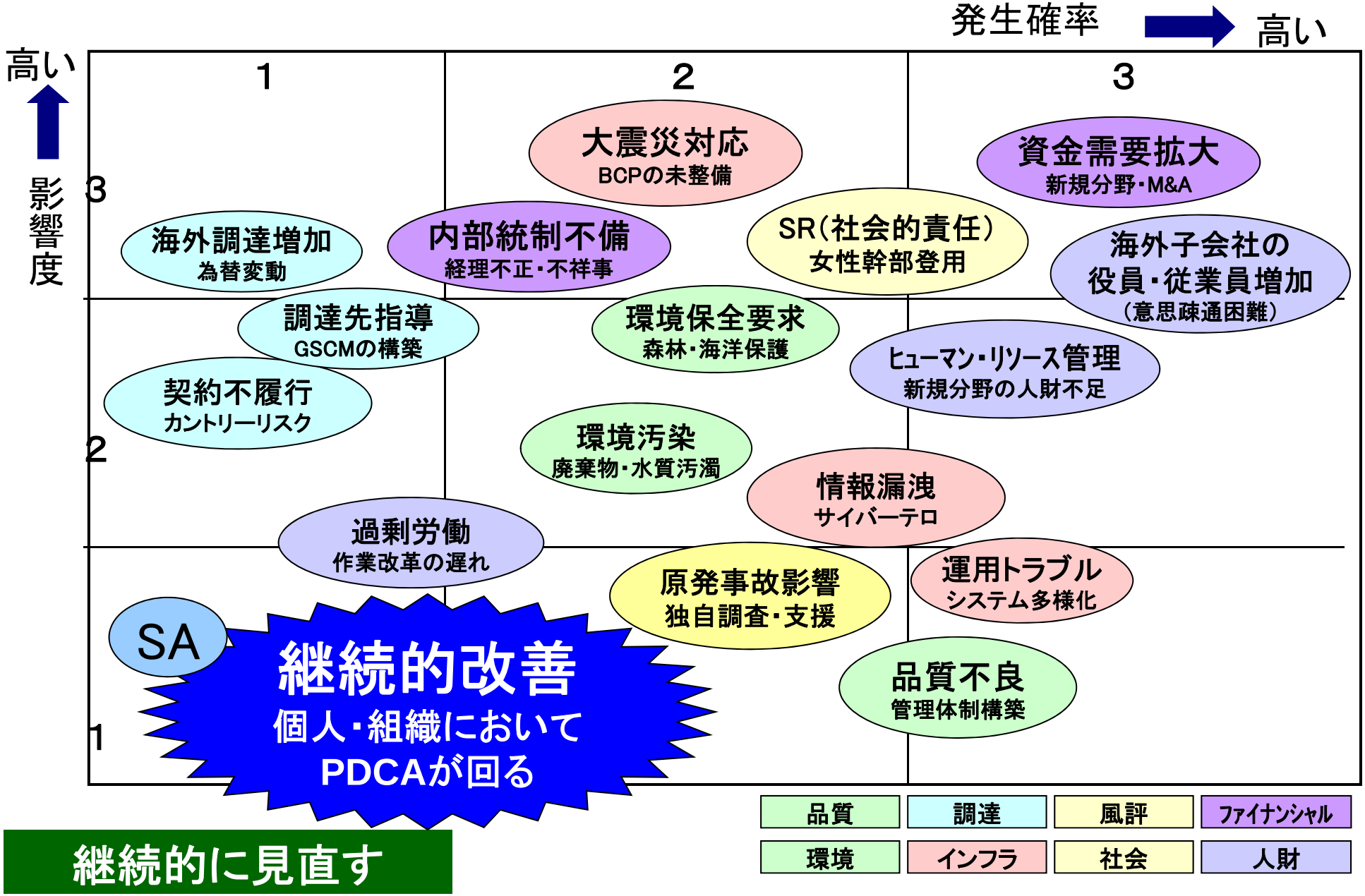
6-4.中小小売業のリスク評価ー（成熟度Ⅳ）イメージ



継続的に見直す

システム監査学会RM研究ﾌﾟﾛｼﾞｪｸﾄ

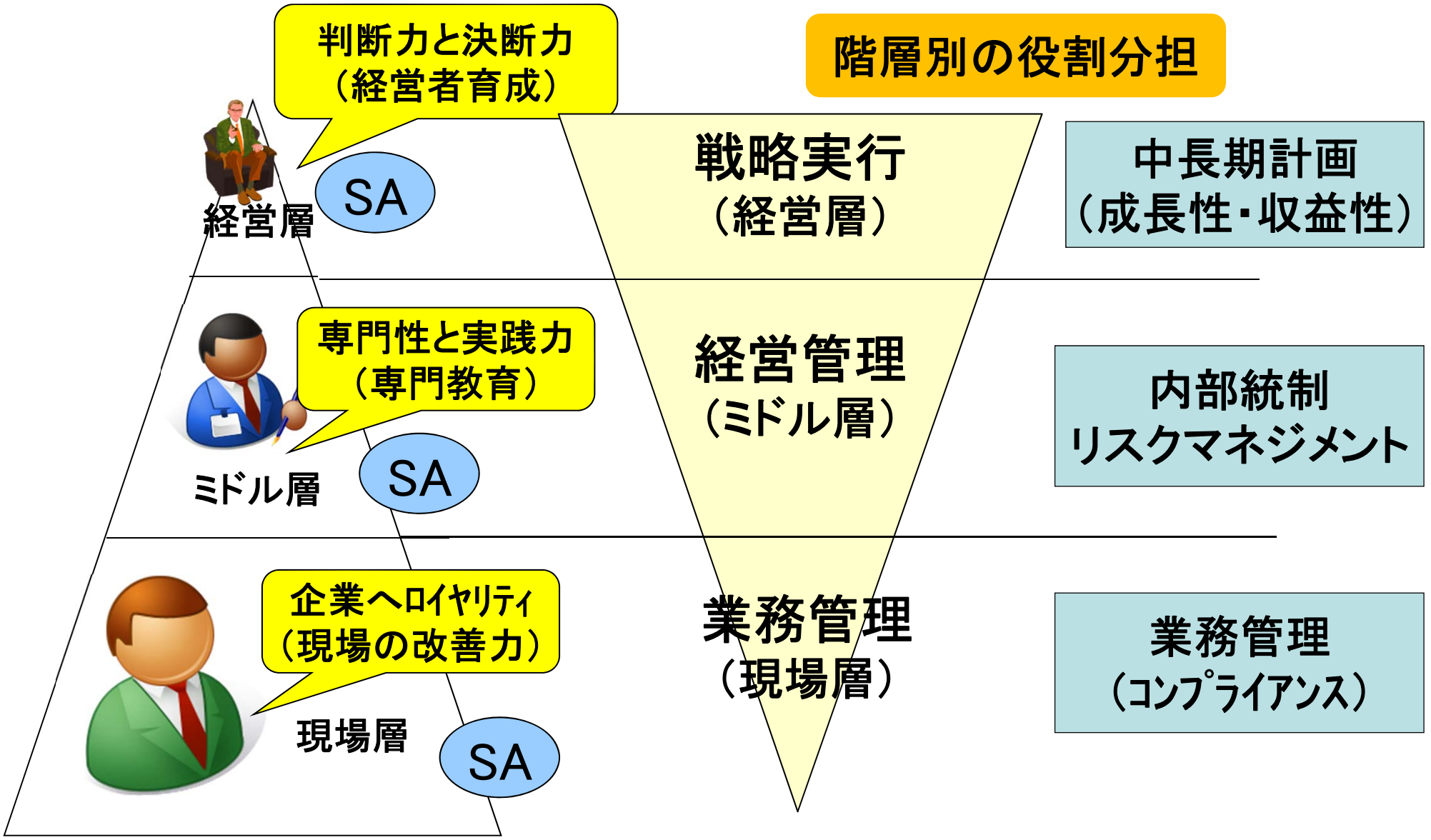
6-5.中小小売業のリスク評価ー（成熟度Ⅴ）イメージ



継続的に見直す

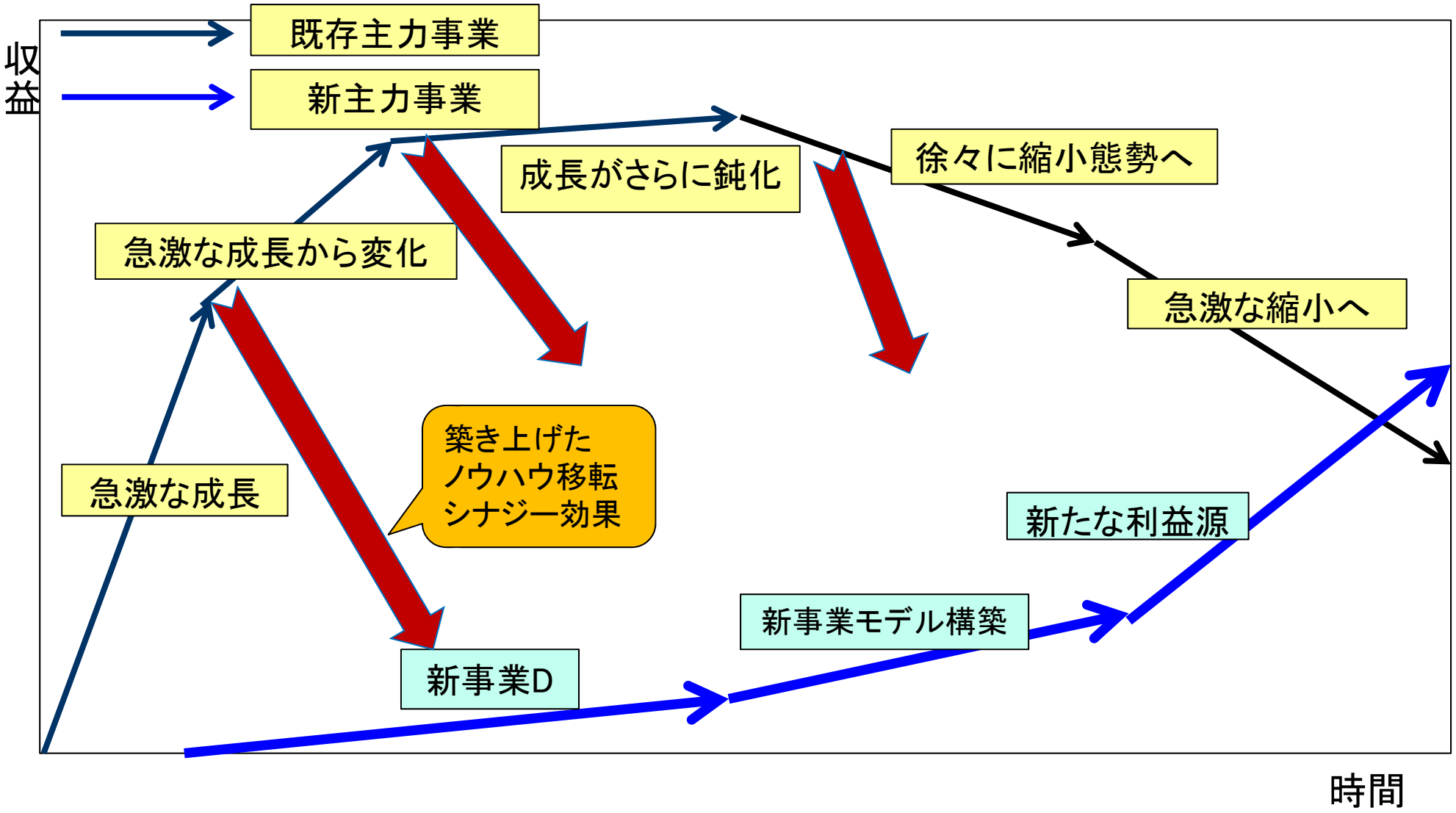
システム監査学会RM研究プロジェクト

7-1. 中小小売業の階層別リスクマネジメント



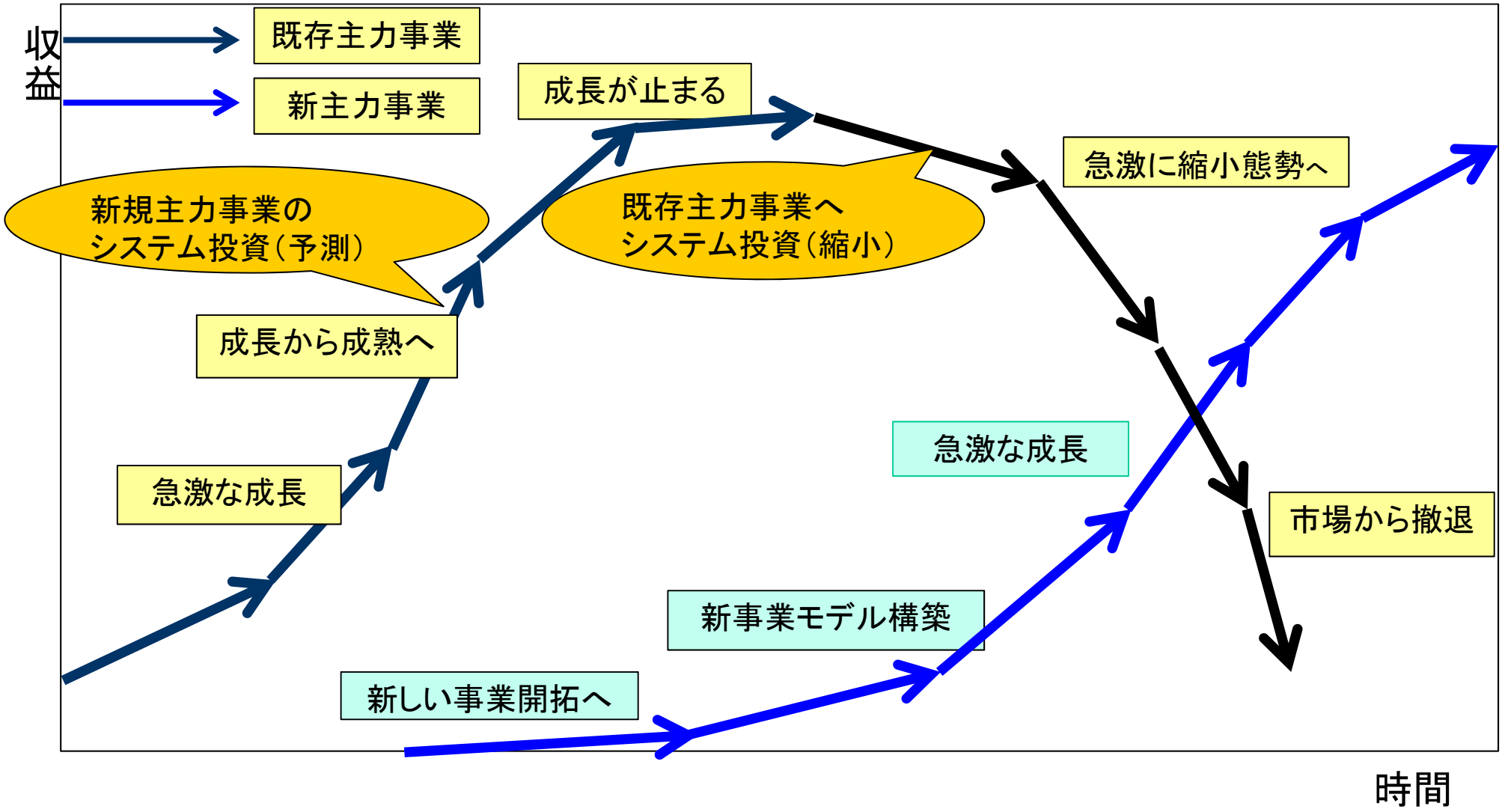
システム監査学会RM研究プロジェクト

7-2.転換期におけるヒト・技術・資金・情報の早期移転



システム監査学会RM研究プロジェクト

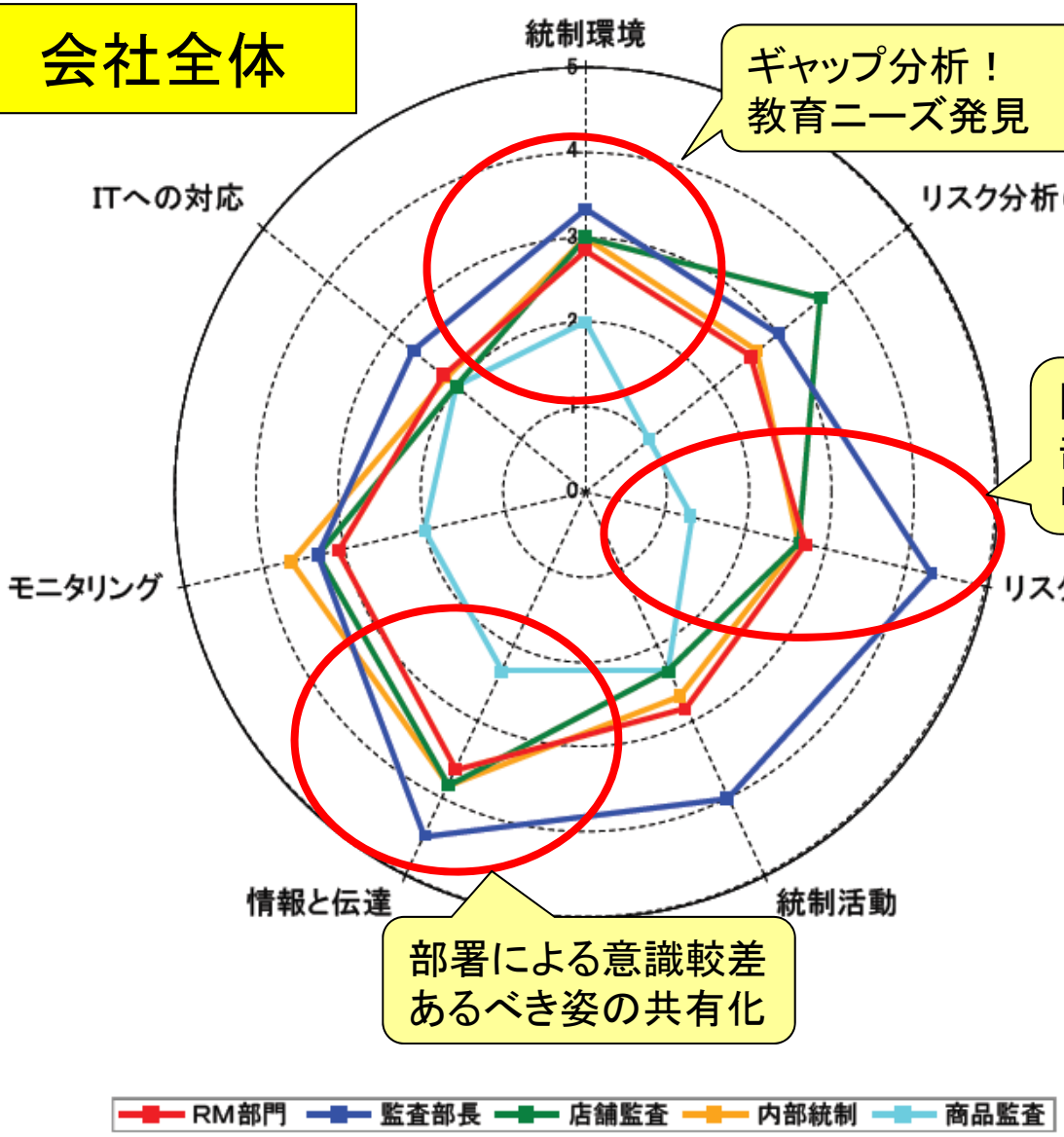
7-3.市場転換予測に基づくシステム投資の素早い移動



システム監査学会RM研究プロジェクト

7-4.評価レーダーチャート・・・内部統制（2013年）

会社全体



ギャップ分析！
教育ニーズ発見

問題に気づく！
部署間の温度差！
リスクリテラシー醸成

部署による意識較差
あるべき姿の共有化

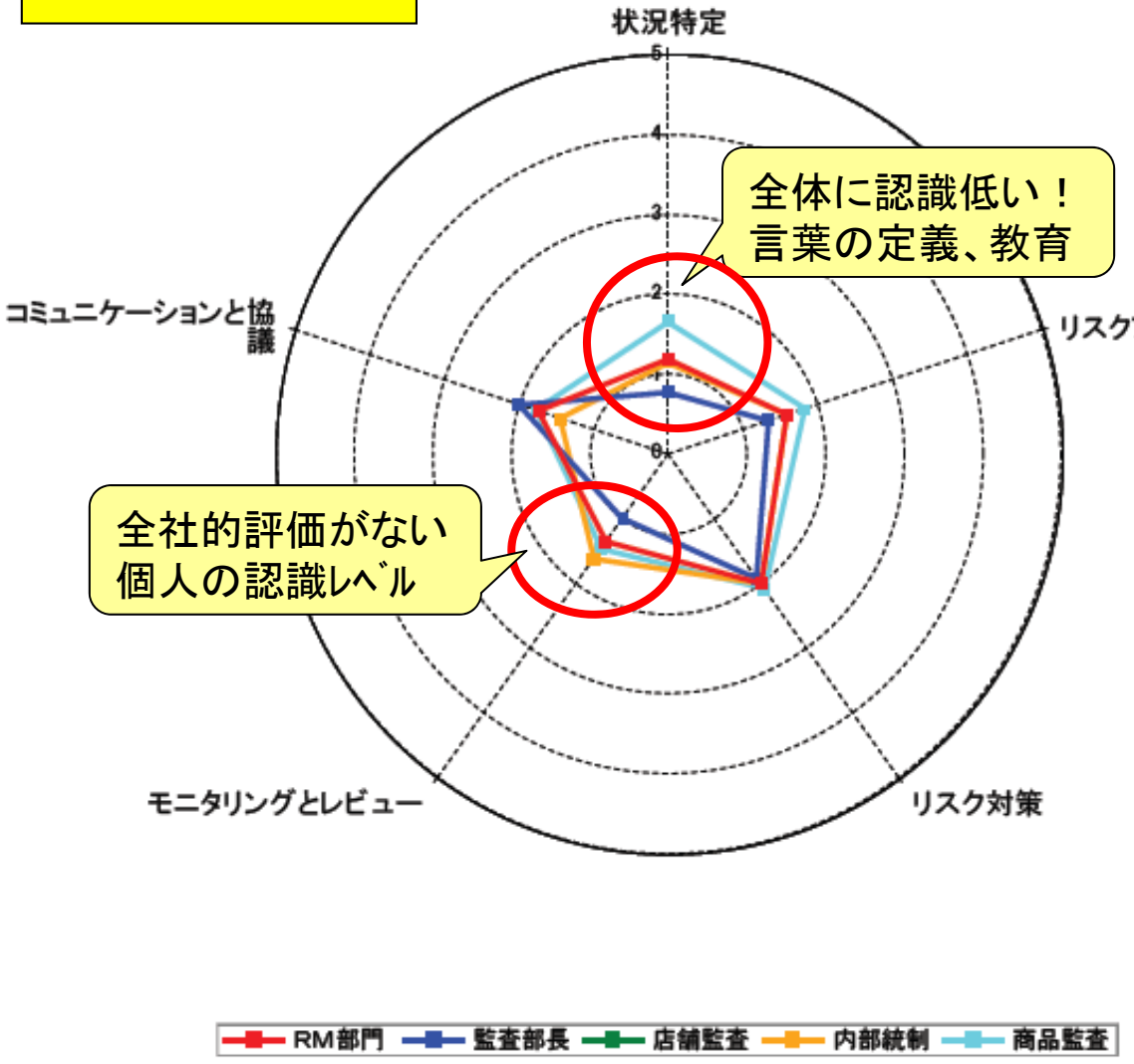
RM部門が評価して報告

【解説】 クィックスタート版
- リスク分析、リスク評価が進んだ
- 情報と伝達⇒コミュニケーションが良くなってきた
- 全体としてレベル3.0となっている
  ITへの対応が遅れている。

システム監査学会RM研究プロジェクト

7-5.評価レーダーチャート・・・事業継続（2013年）

会社全体



RM部門が啓蒙
安否確認訓練実施

【解説】 ｸｨｯｸｽﾀｰﾄ版
・全体としてレベル1.5となっているのはリスク訓練が行われた影響
・「3.11震災」の教訓から安否確認や緊急時組織の編成が進んだ。
・課題は全社・全従業員の意識改革

ｼｽﾃﾑ監査学会RM研究ﾌﾟﾛｼﾞｪｸﾄ

7-6.JRMS評価から気づいたこと

SAの“継続的モニタリングと報告”が経営陣を動かす
SAがC⇒Aを担っている（経営陣の理解と支援）

↓

SAは“関連部署と連携しながら”定着を図る
ファシリテーション技術で本部と現場を巻き込めた

↓

SAが“コストを上回るパフォーマンス”を発揮するには
ゆっくりと継続的に評価し続けて成果に繋がった

システム監査学会RM研究プロジェクト

7-7.成熟度モデルの新たな活用方法

企業統合（M&A）において成熟度モデルを
使うとそれぞれの過去を否定しない

↓

成熟度モデルでレベルⅢ、レベルⅣを会社内で
共有すると皆のベクトルが合ってくる

↓

成熟度レベルⅢまでは、全体像の見える化
成熟度レベルⅣ～Ⅴは、システム戦略の評価（SA）

システム監査学会RM研究プロジェクト

7-8.システム監査基準への活用について（案）

監査計画の立案で成熟度モデルを参考
⇒組織・個人の成熟度を勘案して修正できる

監査証拠の入手と評価で成熟度モデルを参考
⇒個人ノウハウ（暗黙知）を組織ノウハウ（形式知）

監査報告に基づく改善指導（フォローアップ）
⇒成熟度レベルに応じて、計画的に改善提案

ご静聴ありがとうございました。