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（成熟度モデルの実務活用）ー

2012/06/08

リスクマネジメント研究プロジェクト
報告者　足立　憲昭

「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）
　　植野　俊雄
　　喜入　博
　　小谷野　幸夫
　　高野　美久
　　高橋　孝治
　　野田　正美
　　北條　武
　　堀越　繁明　（五十音順）
発表　：足立　憲昭

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への適用について（H22年度）

今年度の到達点：

会合	日程	おもな検討内容
1回目	平成23年10月07日(金)	前回の反省と今後の計画
2回目	平成23年11月10日(木)	今後の展開について
3回目	平成23年12月19日(月)	報告の骨子について検討
4回目	平成24年　3月27日（火）	報告（案）の説明と協議・修正
5回目	平成24年　5月10日(木)	報告書（確定分）最終検討会

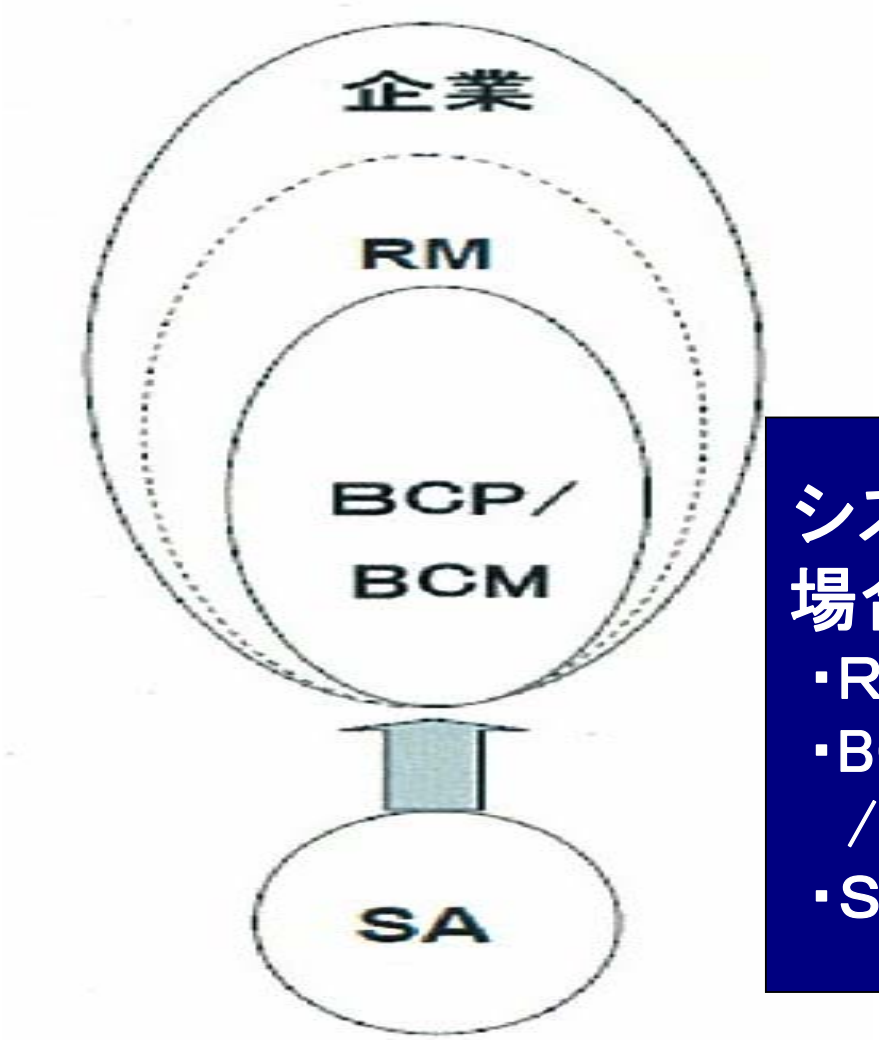
前回までのまとめ：

2007年～2008年
SCMにおけるBCMSとSAのモデル化

2009年～2010年　実際にモデルを使ってみる
GSCMリスクチェックシート　※システム管理基準参考

2011年　　成熟度モデルの概念を追加する
仮説モデルにJRMSを使ってみる

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. SCMの発展過程における統合システムのSA

評価尺度／達成度	段階	概要
Ⅰ	初期段階	部分的に行われている。
Ⅱ	定義段階	マニュアルがあり行われている。
Ⅲ	管理段階	組織化され、行われている。
Ⅳ	制御段階	定期及び不定期の訓練が行われ、且つ定量的な分析とフィードバック。（PDCA）が確立
Ⅴ	最適段階	サプライチェーンとして関連する会社を一体としてリスクマネジメントを推進している。

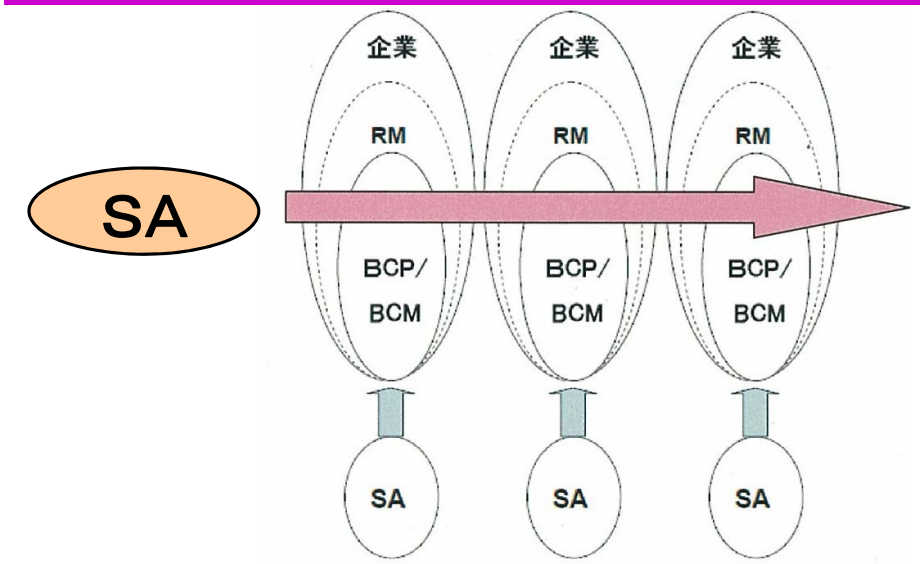
横の連携、相互の連携がない

単一監査

企業のシステム監査組織が関連のあるシステムをそれぞれ監査する

他企業／他組織と連携

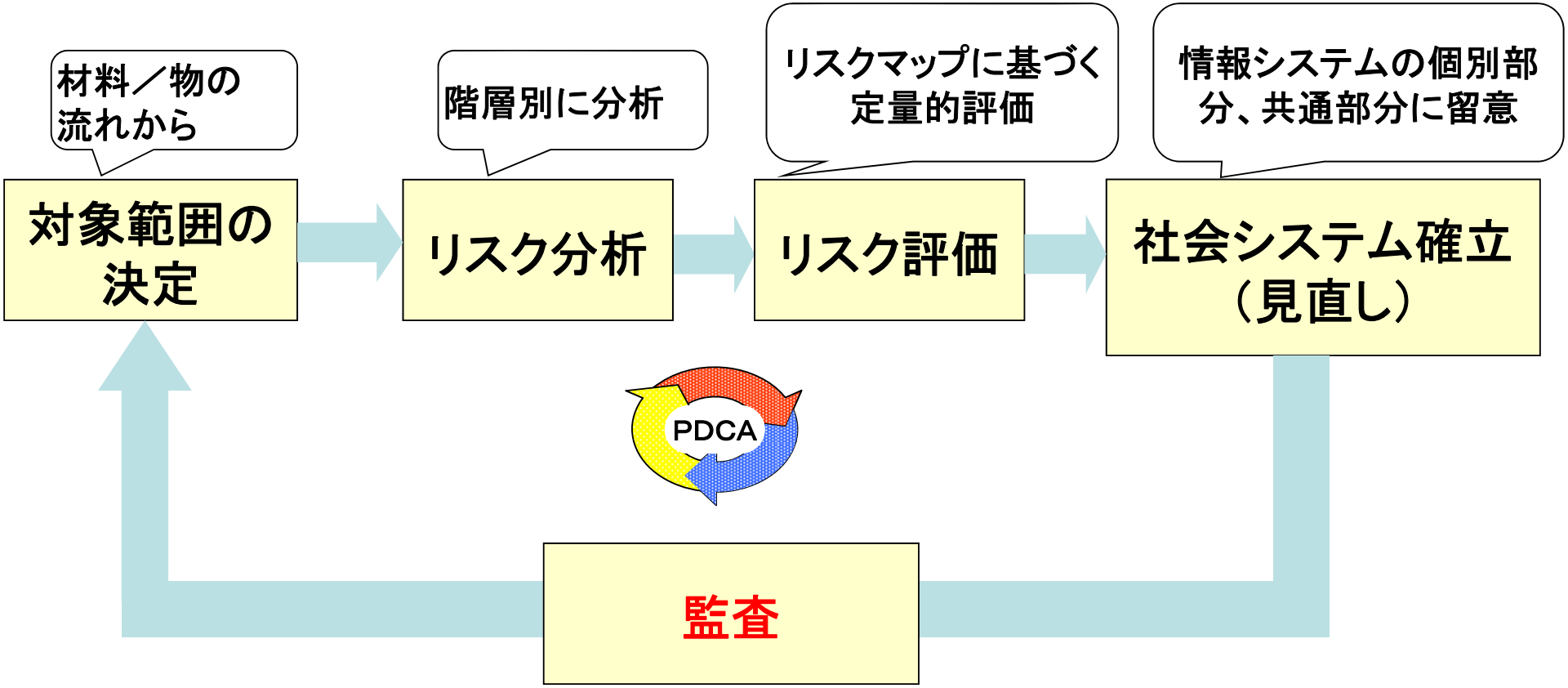
横断的な監査



レベルⅣ～Ⅴ

独立したシステム監査組織が横断的にチェックする

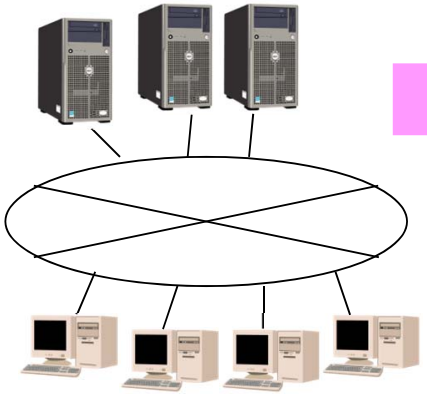
3. BCP/BCMSに関する作業の流れ



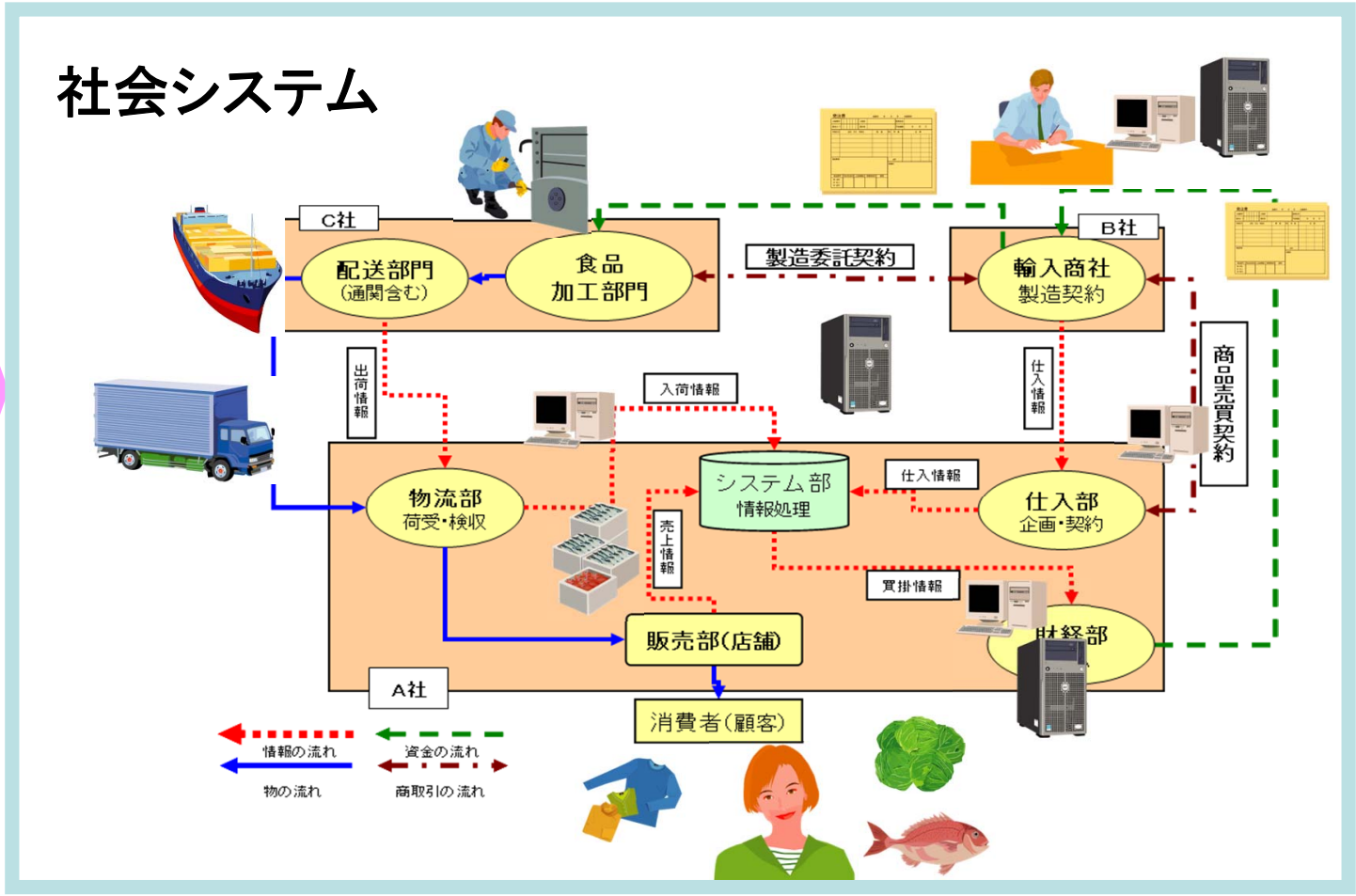
4.小売業のリスクマネジメント対象範囲モデル

【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。

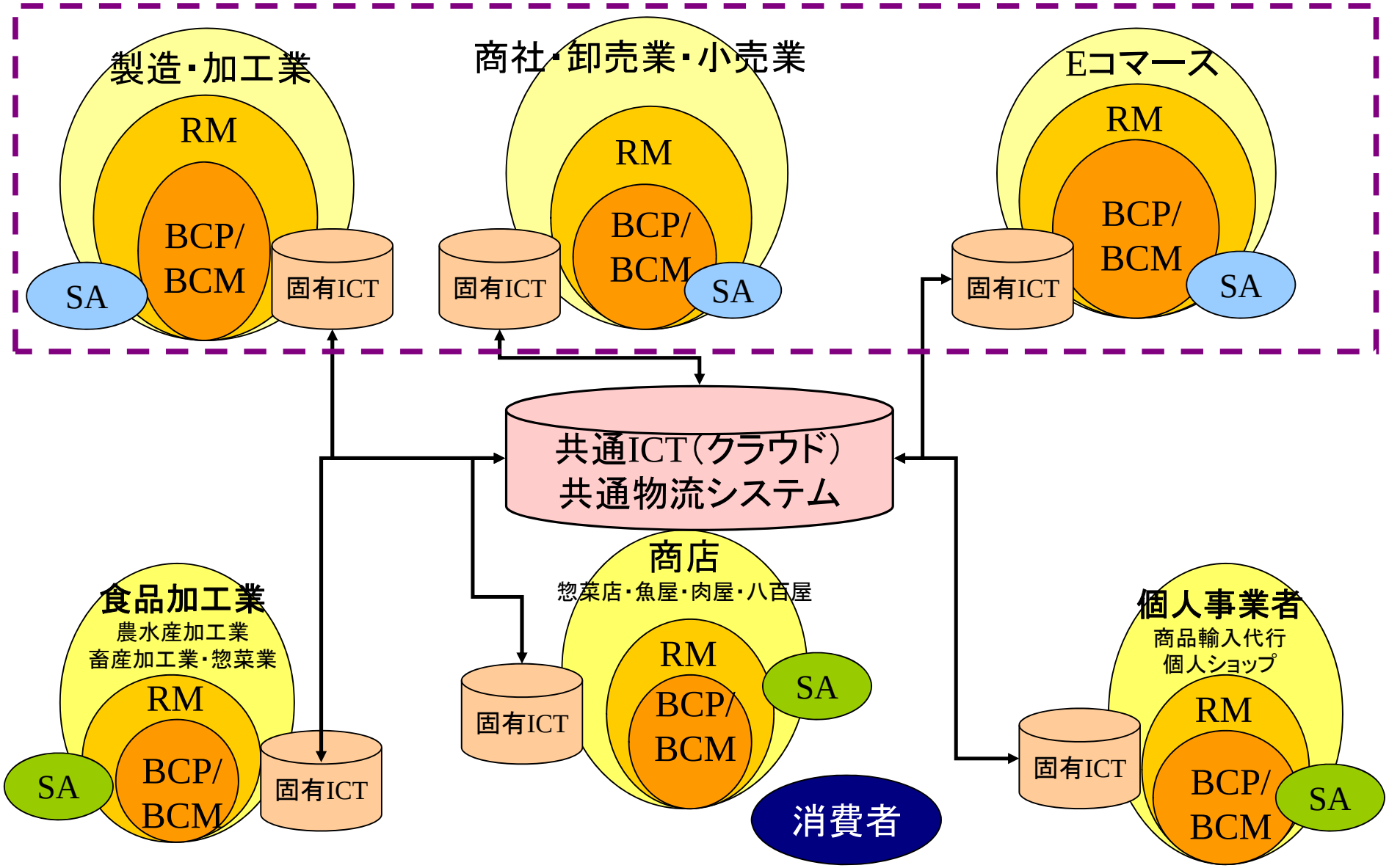
情報システム



社会システム



5.サプライチェーンの発展過程（仮想モデル）



6.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）

GSCMリスク
チェックシート

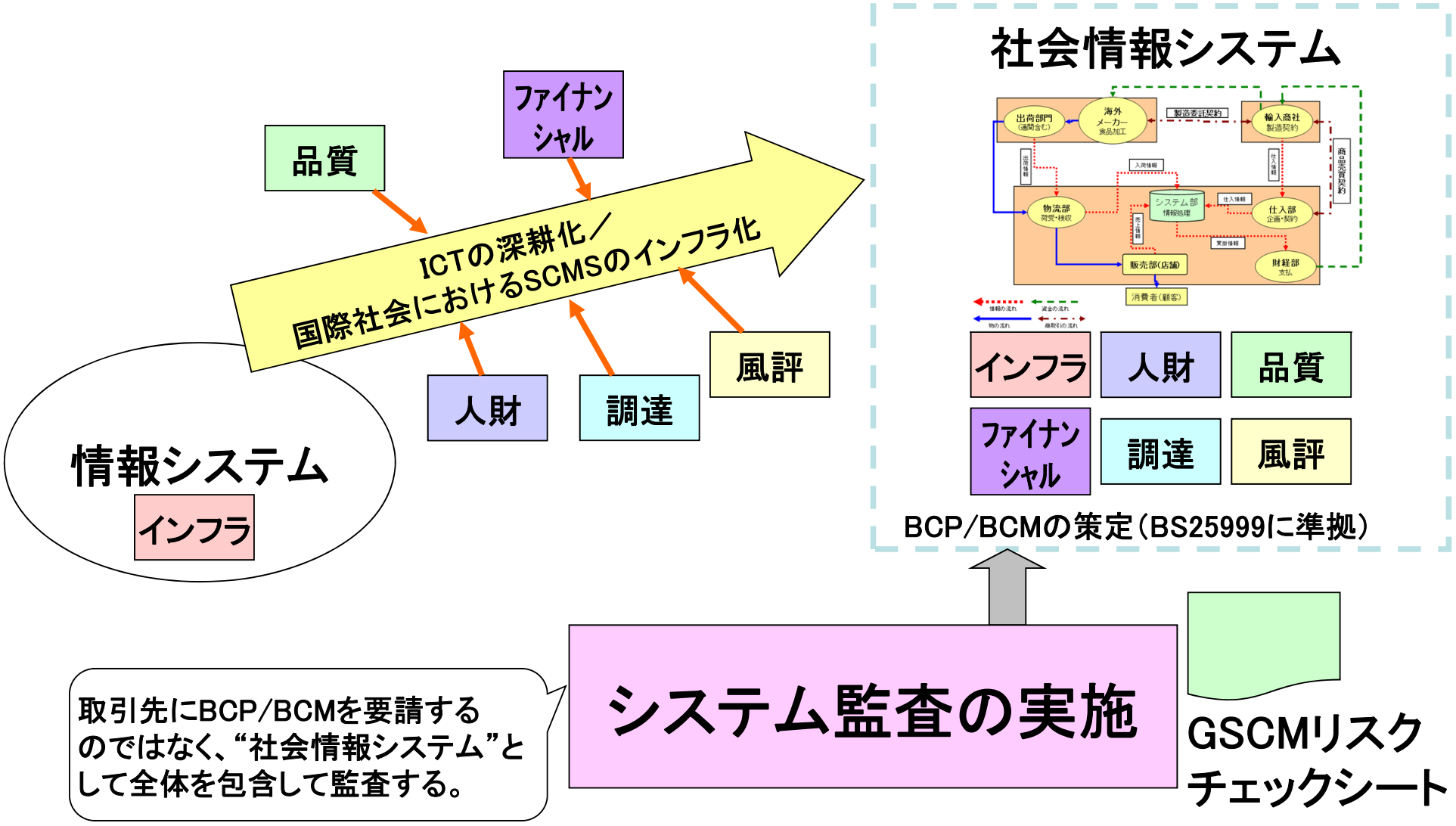
GSCMリスクチェックシートの全体構成
Ⅰ．全体確認シート
①基本事項
・システム管理基準を参考
・教育関連は個別リスク確認シートの「人財」に移管
Ⅱ．個別リスク確認シート
①調達
②品質
③風評
④インフラ
⑤ファイナンシャル
⑥人財

GSCMにおけるリスクの分類

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

7.情報システムの進化のシステム監査の概念図



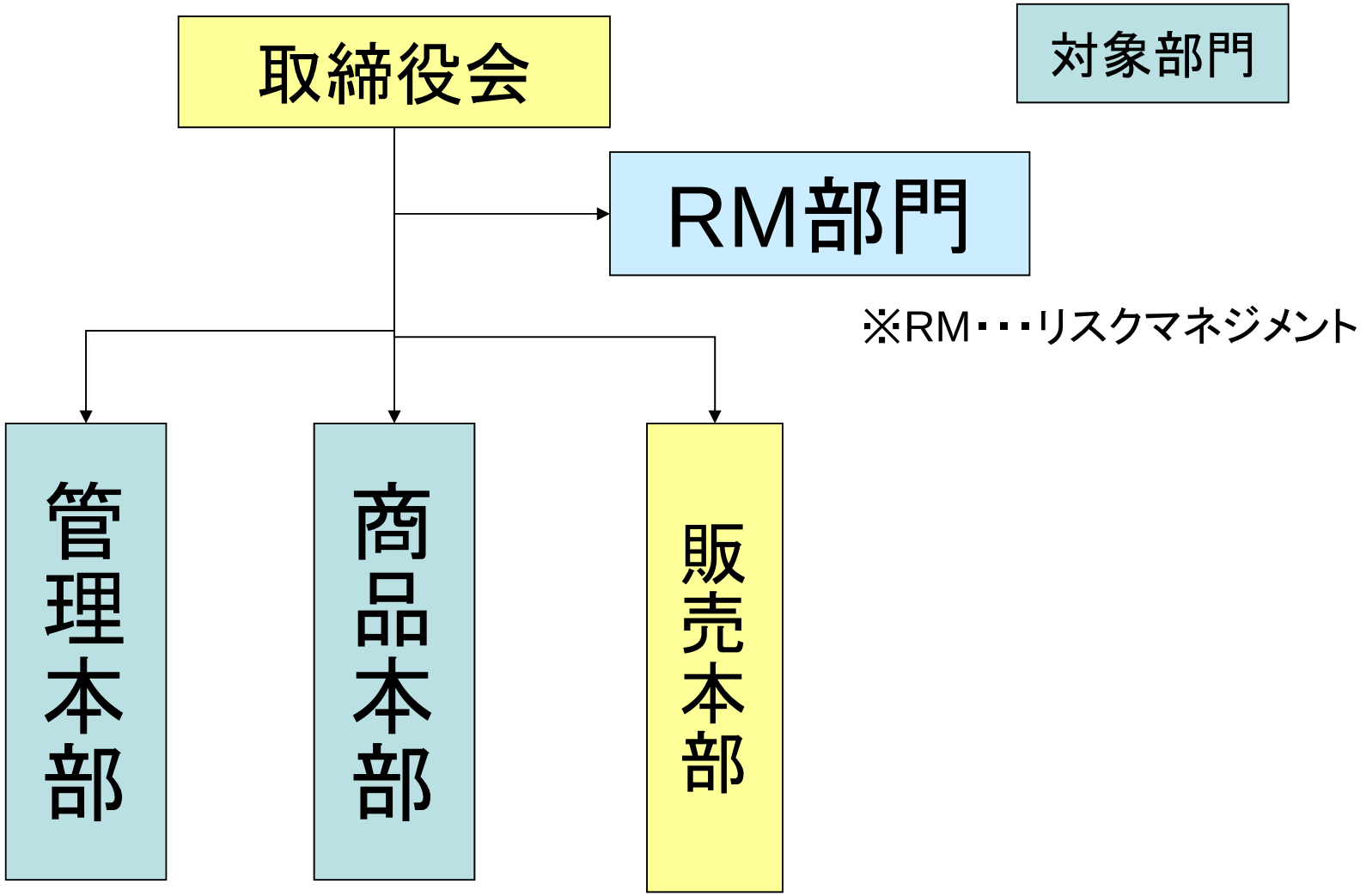
8. モデルに基づくリスクの洗い出し

分類	洗い出したリスク
調達	政変・大規模ストで海外物流（通関等）が停止してしまうリスク
調達	台風、大雪により配送されない等の天候に起因するリスク
調達	売れない商品（不振在庫）が溜まり、売れる商品（流行）を仕入できないリスク
品質	海外メーカー（製造加工）の品質管理に関するリスク
品質	海外工場（東南アジア）の検査体制不備による大量の不良品が発生するリスク
風評	解雇・退職した人（会社への不満を持つ）からの風評リスク
風評	マスコミ等の過剰対応による風評リスク（中国のギョーザ問題等）
インフラ	国内外の電力、ガス、水道、通信、情報システムetcの停止におけるリスク
インフラ	サイバーテロによるシステム停止、情報漏えい、改ざんのリスク
ファイナンシャル	国内外の金融危機に伴う契約先の倒産リスク（資金
ファイナンシャル	相手先倒産に対する財務的手当てが検討され
ファイナンシャル	物価の急激な変化に伴うコストリスク（原油など
人財	アウトソーシング先等の教育不徹底に基づくリスク（情報
人財	国内外工場の労務管理（児童労働等）に関するコンプライアンスリスク
人財	熟練者の技術やノウハウが継承されていないことからトラブルが発生するリスク

課題

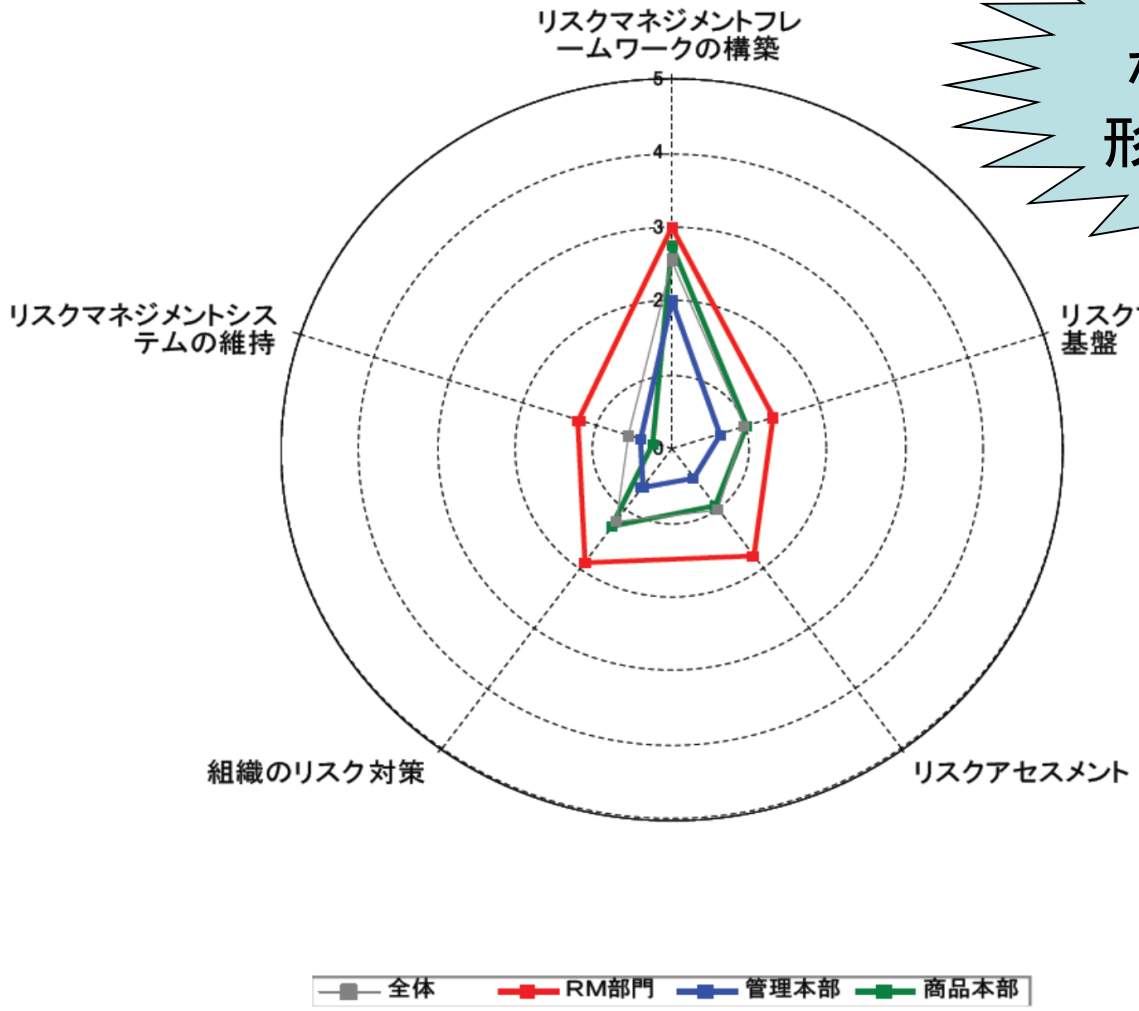
成熟度によってリスクの内容が変わってくる？

9.リスク評価の対象部門



10.評価レーダーチャート・・・経営（仮説モデル）

会社全体



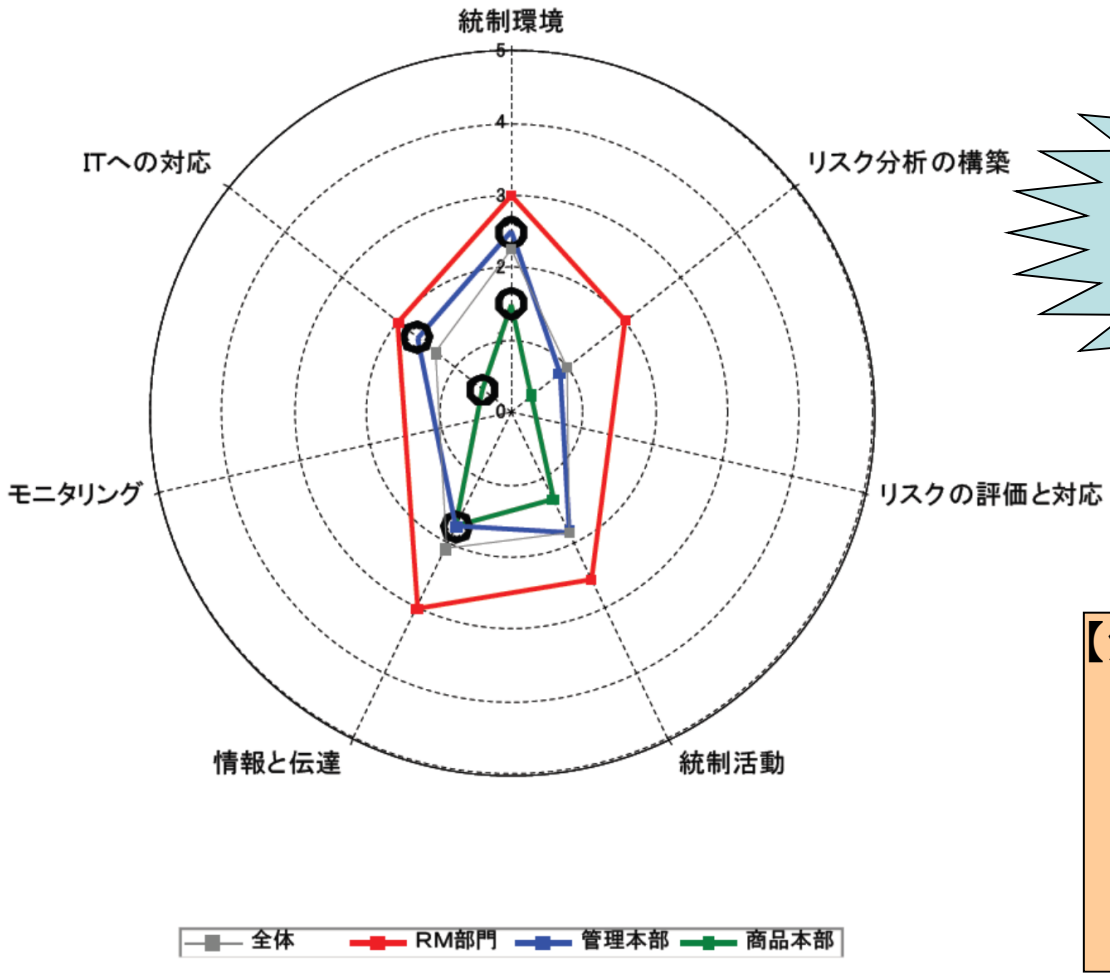
課題

なぜリスクマネジメントが
形だけで、進まないのか？

【解説】 クィックスタート版
- リスクマネジメントのフレームワークは理解されている　レベル3
- リスクアセスメントができていない
- 全体としてレベル1となっているのはリスクマネジメントの実施（対策）が弱い

11.評価レーダーチャート・・・内部統制（仮説モデル）

会社全体



課題

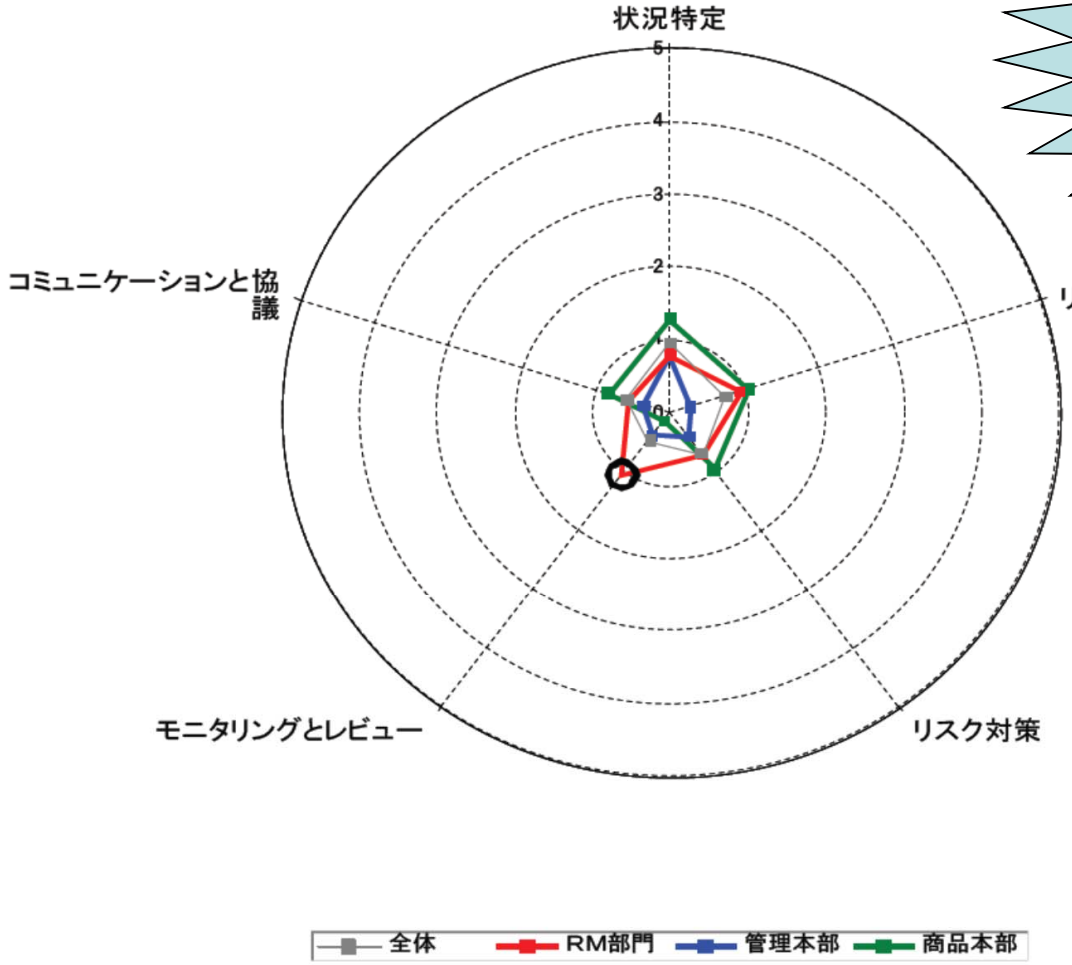
なぜリスク分析や評価が難しいのか？

【解説】 クィックスタート版

- リスク分析、情報と伝達にばらつき
- 商品本部の評価が低いのは教育機会が少ないため
- 全体としてレベル2となっている組織全体の対応になっていない

12.評価レーダーチャート・・・事業継続（仮説モデル）

会社全体



課題

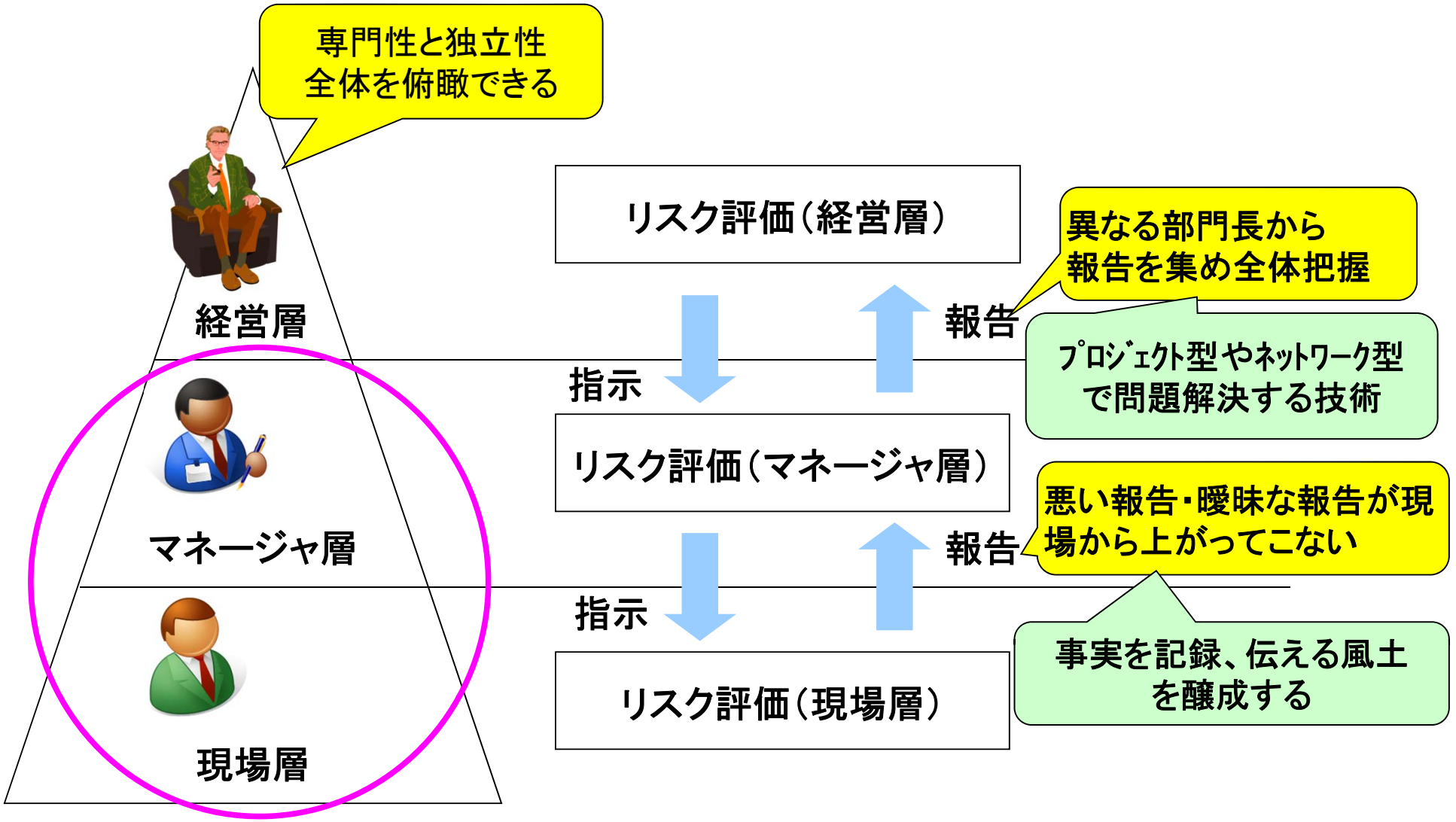
3.11東日本大地震後
意識が変化している
（今年中に評価）

【解説】 クィックスタート版
- 全体としてレベル1となっているのは事業継続の意味が理解されてない
- 事業継続について、社内教育が必要である。初心者用ガイドブックを作成して理解を深める。

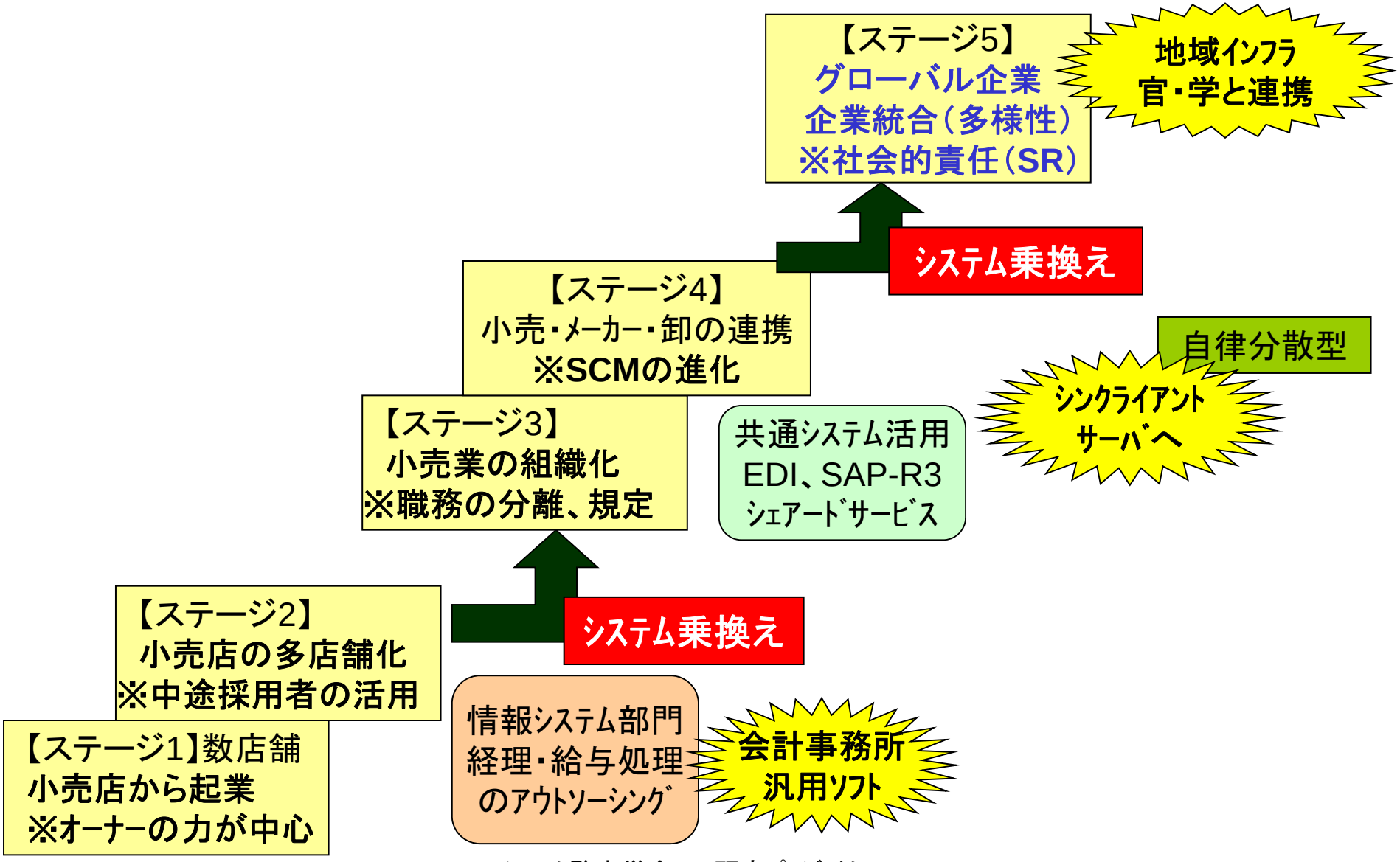
今年度の検討結果報告

- SCMの成熟度におけるリスクの変化
- 小売業におけるリスク評価モデル（仮想事例）
- JRMSツールの適用実験内容
  レベル1～2をレベル3へ・・・基盤構築と組織化
  レベル3をレベル4～5へ・・・PDCAと継続的改善
- システム事故事例の分析
  RM成熟度の違いとシステム監査の関連
- 今年度研究の結果総括と次年度への課題

13. 階層別リスクマネジメントの必要性



14.小売業の発展過程と情報システム変化



15.小売業のリスクマネジメント成熟度（仮想モデル）

継続的改善・・・RMS
地域とSCM全体のRM実施
レベル5へ引上げ！

※RM・・・リスク・マネジメント

※MR・・・マネジメント・レビュー

【レベル5】SR活動と一体RMS
GSCMが地域インフラとしてRM
関係者が社会貢献のマインド醸成
互いに長所・短所をネットワーク補完
RMS構築

【レベル4】 PDCAサイクル
情報共有化による迅速な対応
定期的内部監査とMRの実施
外部への情報開示
PDCA

【レベル3】 組織化・規定
取締役会の責任で対策本部
リスクマネジメント規程、リスク洗出し
事件・事故の時に稼動する
規程制定

【レベル2】 事故発生時対応
主管部署が対応に当たる
部門のリスク意識にばらつき
事故対応

【レベル1】 個人経験で対応
ベテラン従業員の経験に依存
暗黙知（見える化がない）

16.リスクマネジメントの成熟度（調達リスク　鶏インフルエンザ）

JRMSツールの活用で
レベルを知り変革を推進

【レベル5】 SR活動と連携
SCMとして地域へ安定供給
消費者・生産者と連携する
法基準を超えた安全を目指す

【レベル4】 フィードバックが効く
情報共有化による迅速な対応
定期的内部監査とMRの実施
外部への情報開示

消費者の安全確保と
生産地（者）を守るため
社会貢献できる体制！

【レベル3】 会社全体の対応
役員が責任者で本部設置
インシデントへの対応（見える化）
会社全体でクライシス対応

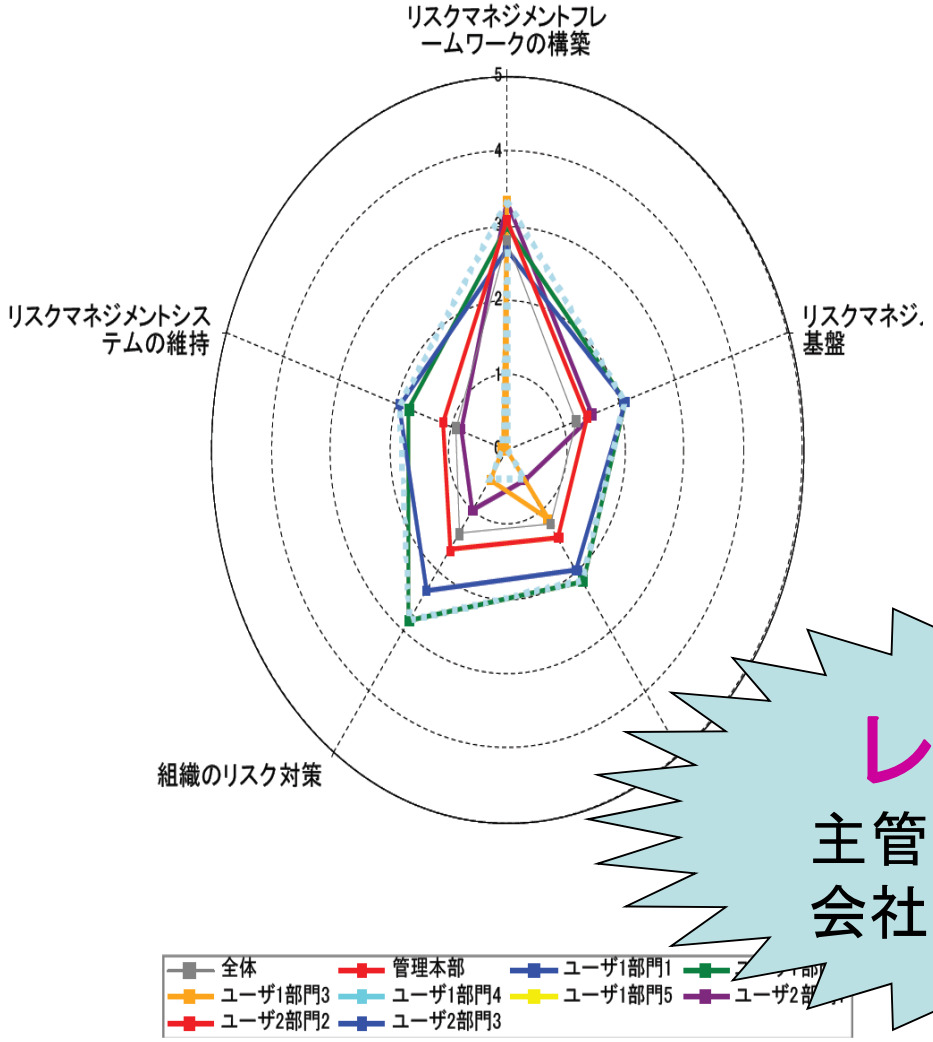
【レベル2】 主管部署で対応
精肉部が対応に当たる
部門のリスク意識にばらつき

RM組織が未熟な小売業は
同じ失敗を繰返し、対策が
遅れる！・・・大きな変革

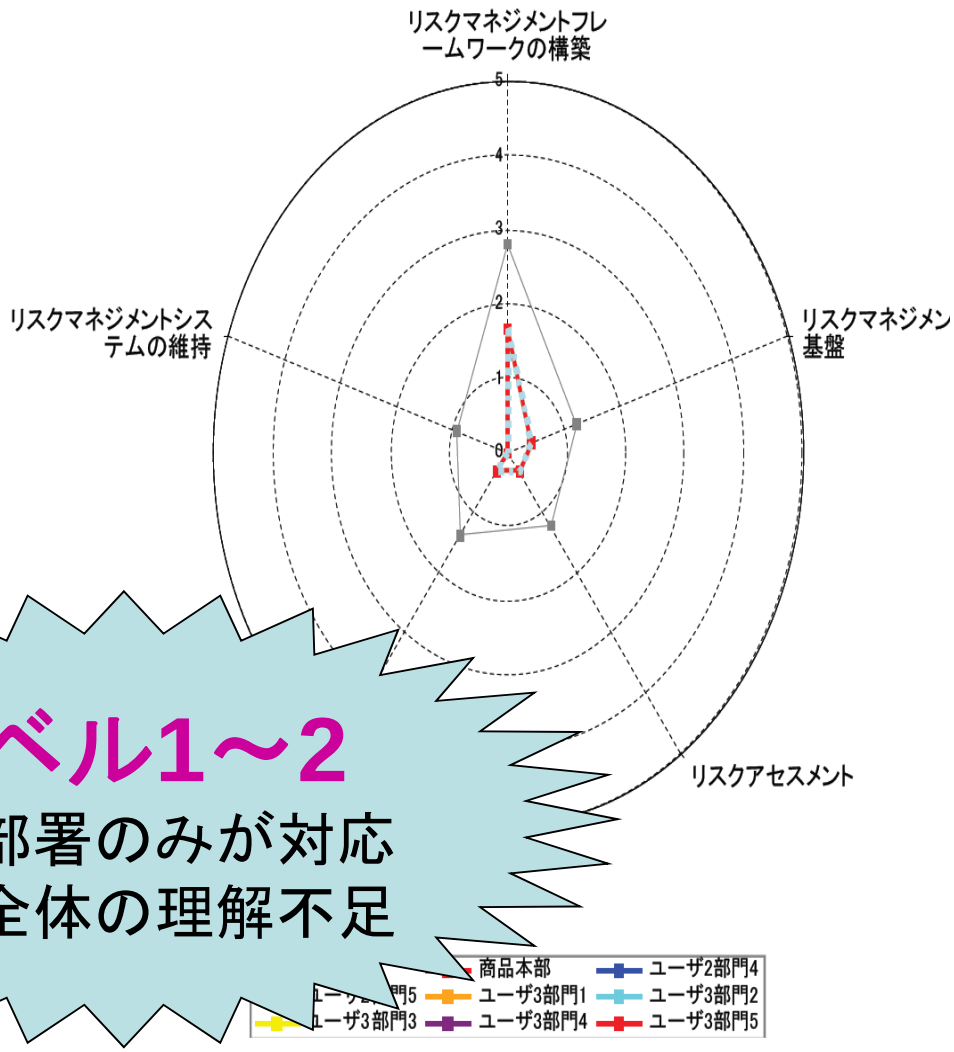
【レベル1】 個人経験で対応
ベテラン従業員の経験に依存
暗黙知（見える化がない）

17.評価レーダーチャート・・・経営（仮想モデル）

管理部門



商品部門



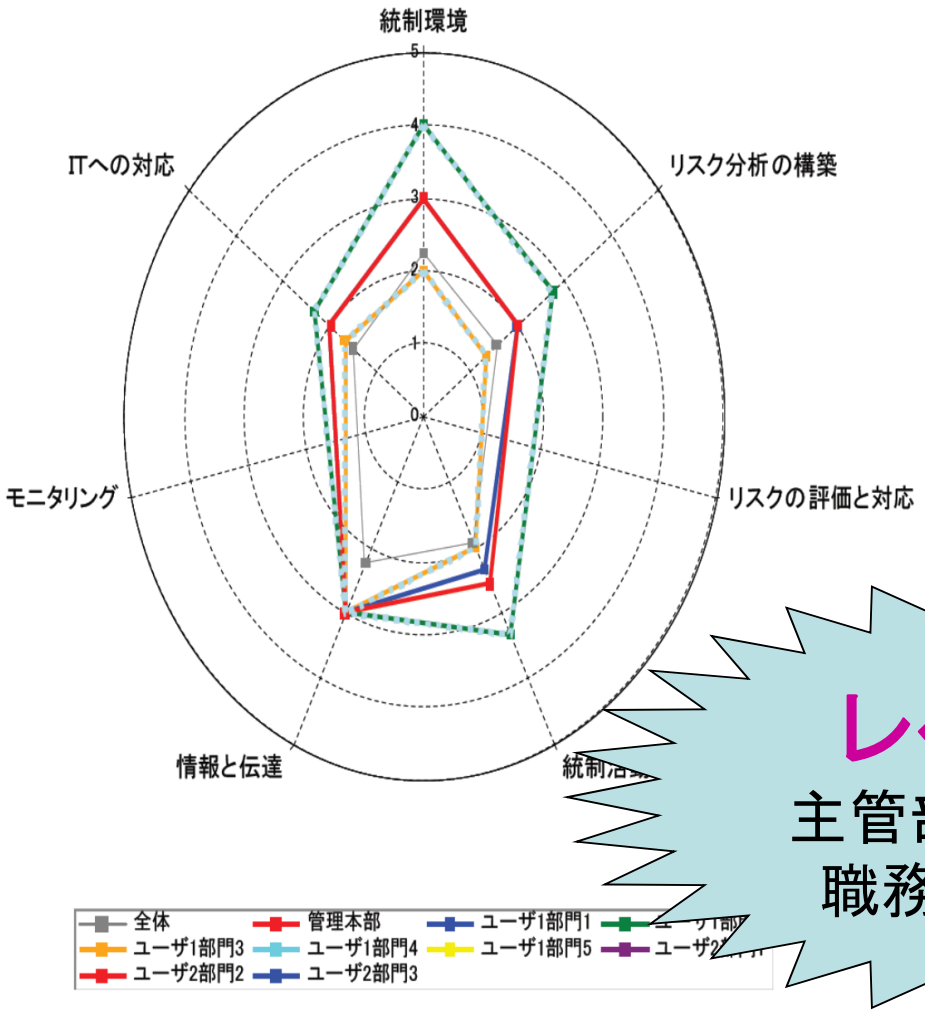
レベル1～2

主管部署のみが対応

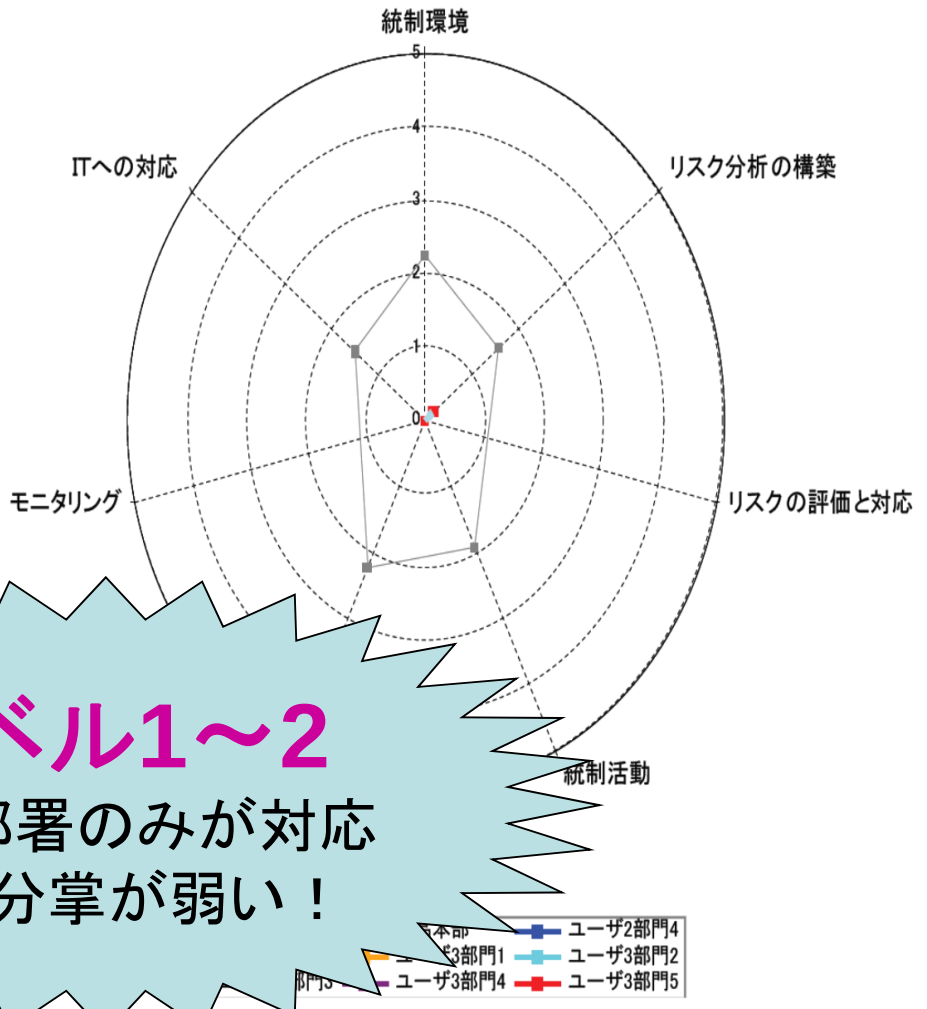
会社全体の理解不足

18.評価レーダーチャート・・・内部統制（部門モデル）

管理部門



商品部門



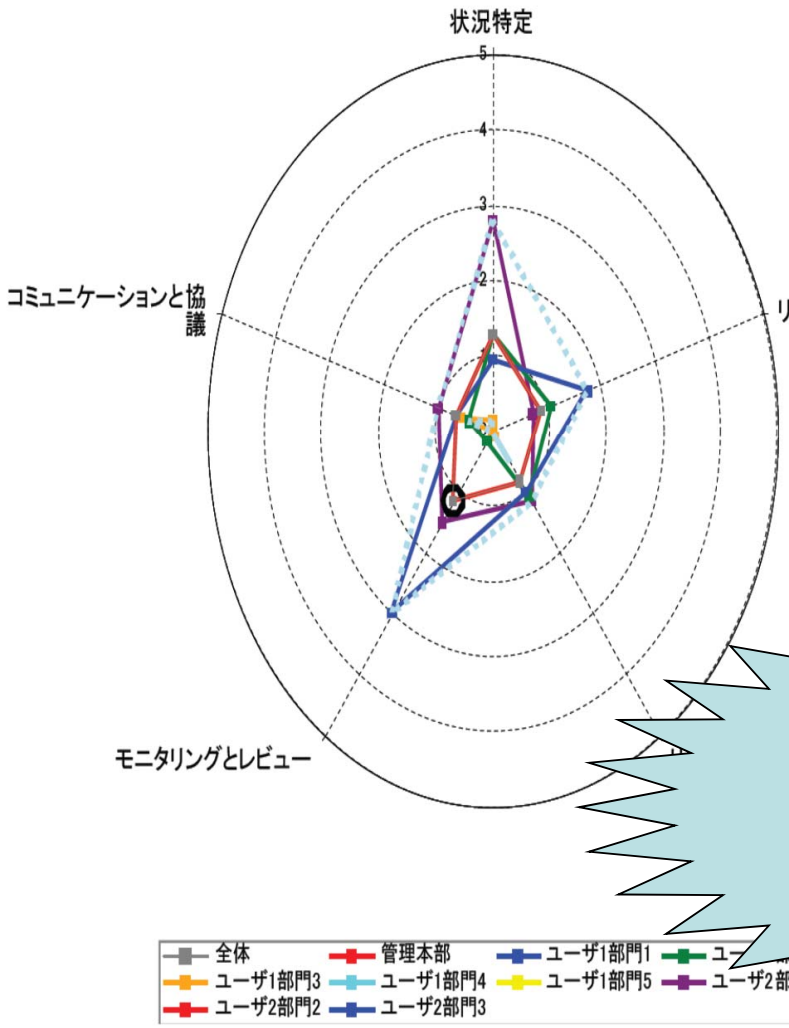
レベル1～2

主管部署のみが対応

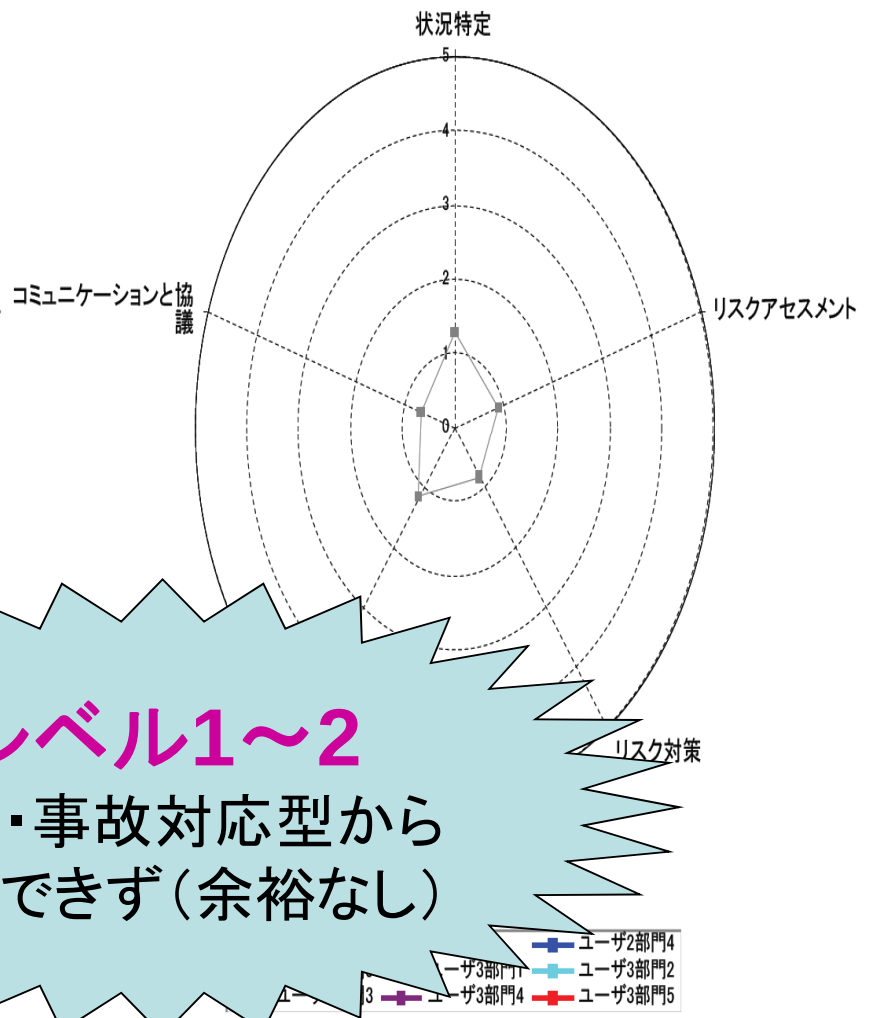
職務分掌が弱い！

19.評価レーダーチャート・・・事業継続（部門モデル）

管理部門



商品部門



レベル1～2

事件・事故対応型から
脱皮できず（余裕なし）

20. RMプロジェクトで話しあった意見（イメージ）

大王製紙やオリンパス事件
ガバナンス（企業統治）が欠如
役員会で反対できないムード
※分からないことを確認する勇気！

3.11の教訓は絆の大切さ
誰かに頼ったRMは命を捨てる
情報開示(悪い情報こそ）の勇気！

船場吉兆の使いまわし
老舗の驕りとﾜﾝﾏﾝ経営！
※企業倫理の醸成

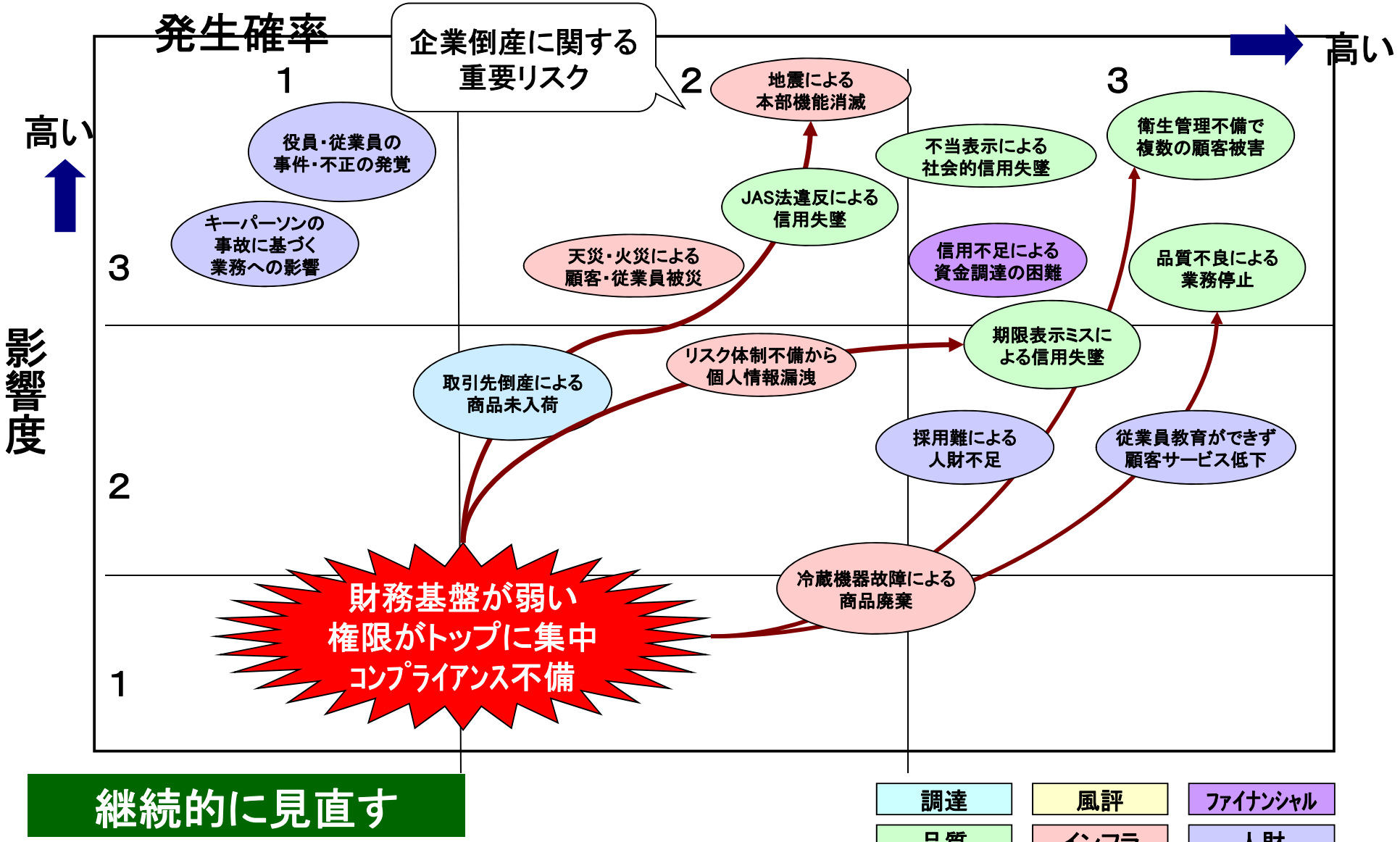
AIJの年金資産問題
金融（投資）ﾘｽｸをﾁｪｯｸできない
中小企業の専門職人財不足
※ﾓﾆﾀﾘﾝｸﾞされない怖さ！

赤福餅、不二家事件
消費期限の偽装！
※業界慣習が非常識！

福島原発の風評被害！
福島産・茨城産を販売しづらい
※安全確認して販売する勇気！

フーズフォーラスの焼肉事件！
最低限の衛生管理が守られない
※競争優先でﾘｽｸを犯す怖さ！

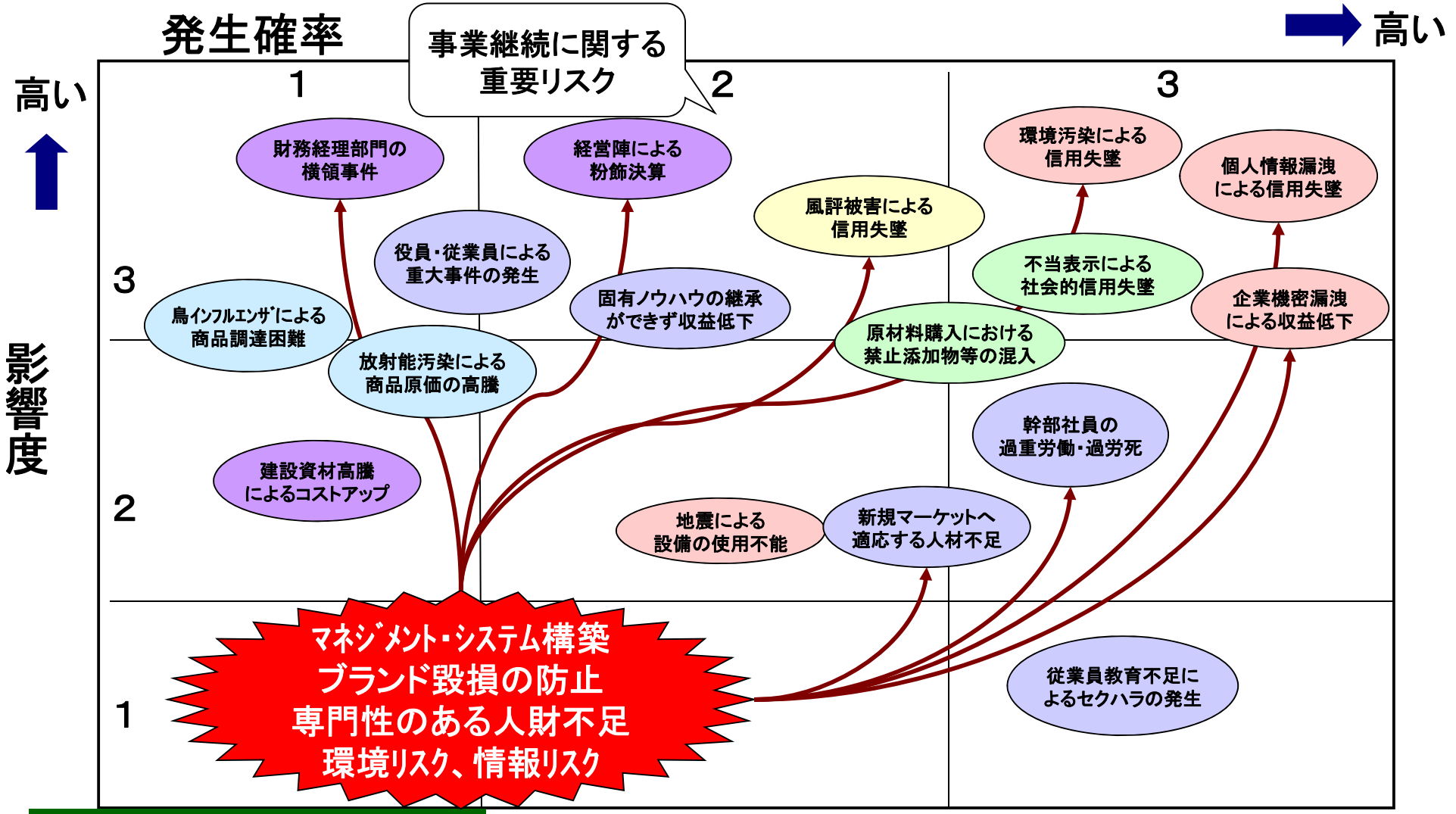
21. マップによるリスク評価ー（成熟度モデル　Ⅰ～Ⅱ）



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

22.マップによるリスク評価ー（成熟度ﾓﾃﾞﾙ　Ⅲ～Ⅳ）



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

23. レベル3に引き上げるための施策（イメージ）

成熟度モデルをレベル3に上げる⇒とにかく実践

↓

色々な場面で使ってみると・・・・意外な効果
過去の功績を評価したうえで新たなステージへ

企業が成長するための条件・・・仕組みを脱皮
個人に埋もれているやり方⇒会社の基準・手順へ

↓

トップ・一部門に集中している権限・・・職務分掌
情報の共有化と権限委譲で健全な葛藤が発生！

24.リスクマネジメントの成熟度モデルの考え方

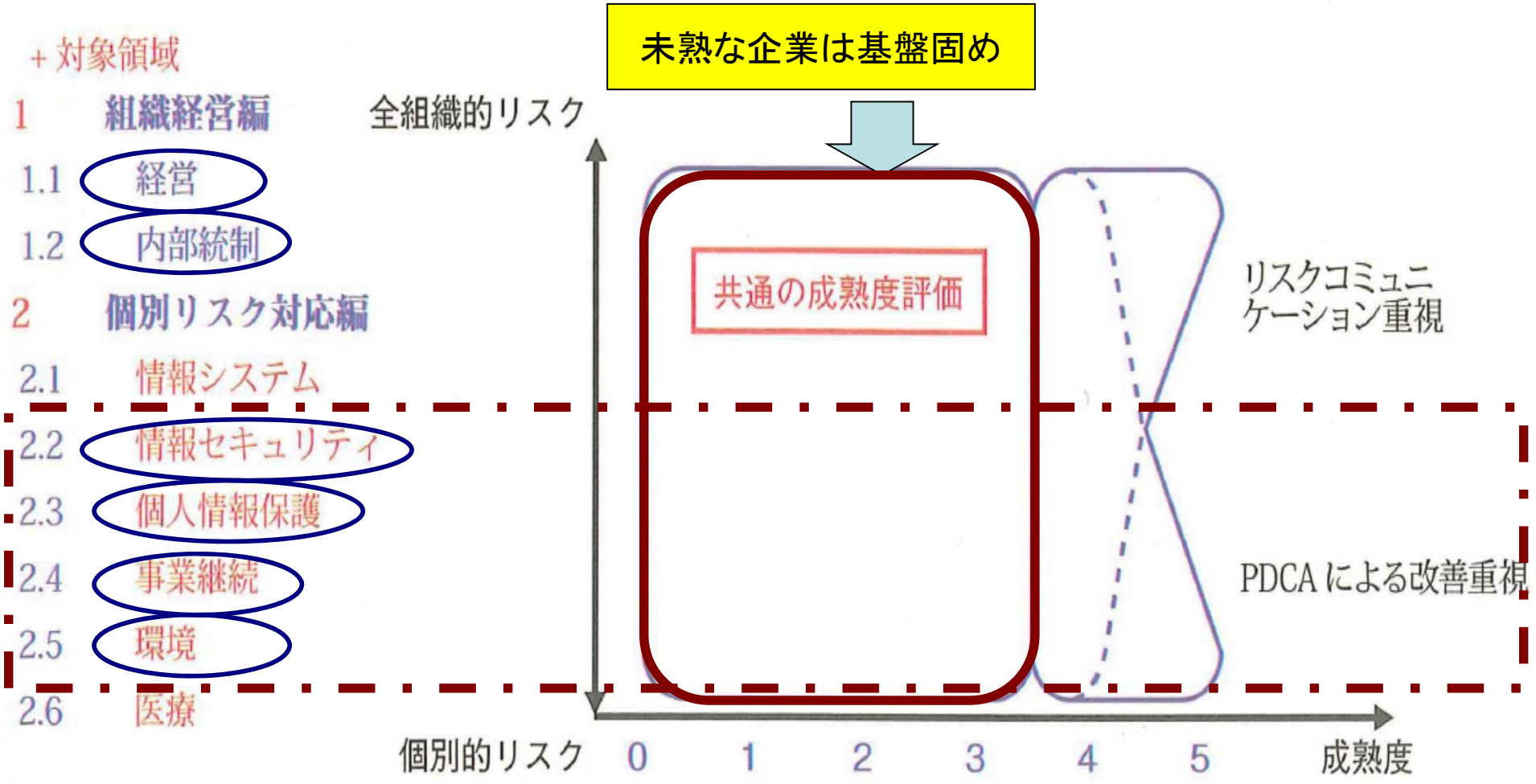


図 1-3.　リスクマネジメントの対象領域と成熟度の定義

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

25. 成熟度モデル活用による現場の実感！

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[illegible]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[illegible]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。

大きな壁

大きな壁

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

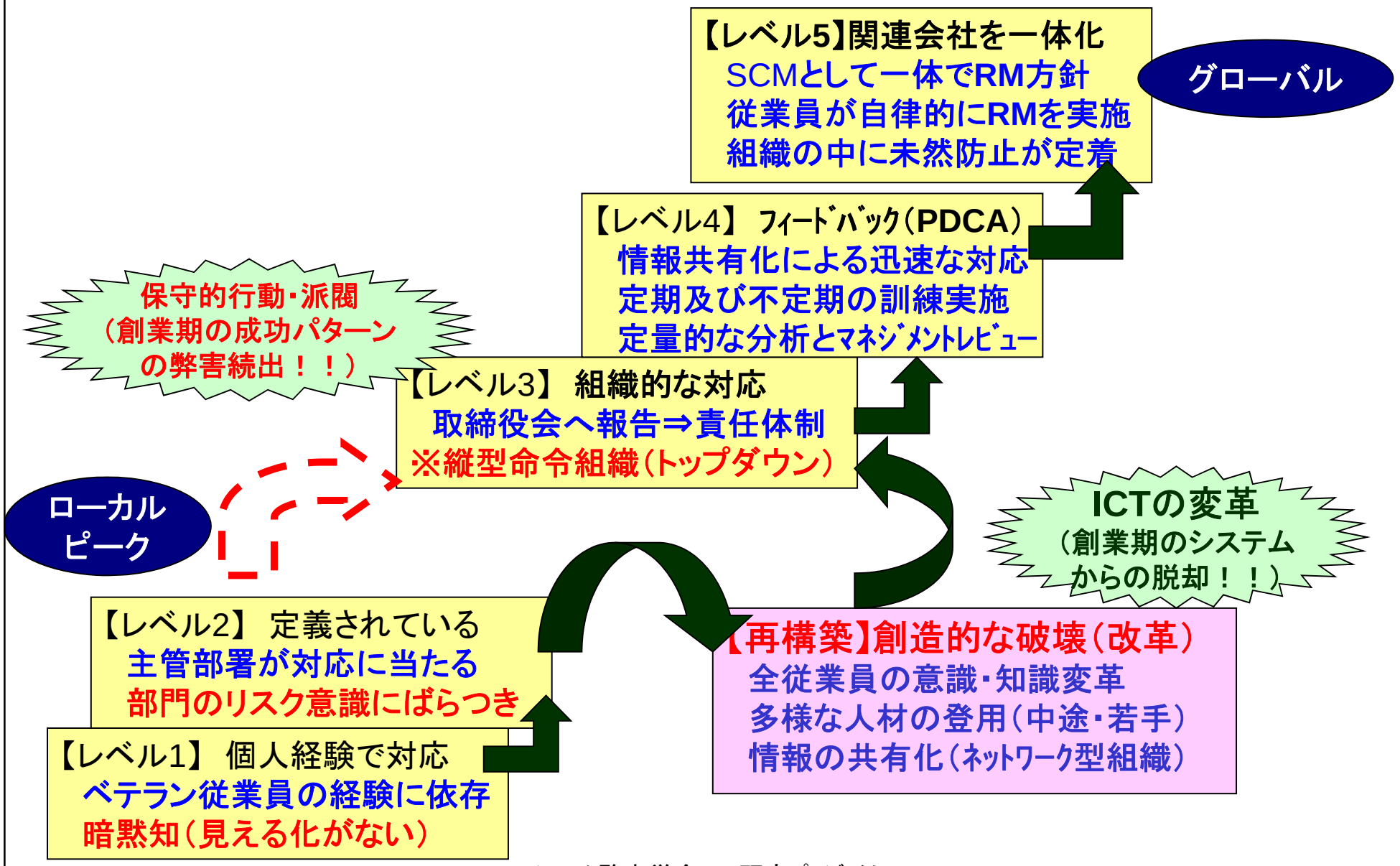
26.仮説事例・・・個人情報保護による評価

評価レベル		摘要例
0	未認識・未対応	・個人情報保護法について知らない。 ・個人情報の識別を行っていない。
1	個人ごとによる対応	・個人情報についての規則を決めた部門もなく、名刺を読み取ったファイルに個人的にパスワードロックをかけている人がいる。
2	部門ごとによる対応	・コールセンタでは、独自に個人情報保護についての規則を決めて、個人情報を保護している。
3	全組織による対応	・全社的な個人情報保護についての規則があり、全組織に配布されている。 ・全社的な個人情報保護について、担当する組織が作られている。
4	全組織による管理された対応	・個人情報保護について、規定どおりに実施されているかを定期的に監査し、経営者に報告している。
5	全組織による最適化された対応	・全社的な個人情報保護を担当する組織は、他の組織で発生した個人情報漏えいについて情報を収集し、自組織の対策に不足している点がないかを見直している。

情報管理レベル
1～3に差し掛かった位置
組織的に対応する枠組みが必要

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

27.小売業のリスクマネジメント成熟度（仮想モデル）



28.リスクマネジメント体制を定期的に評価

従業員の再教育/再訓練が必要な段階になってきた

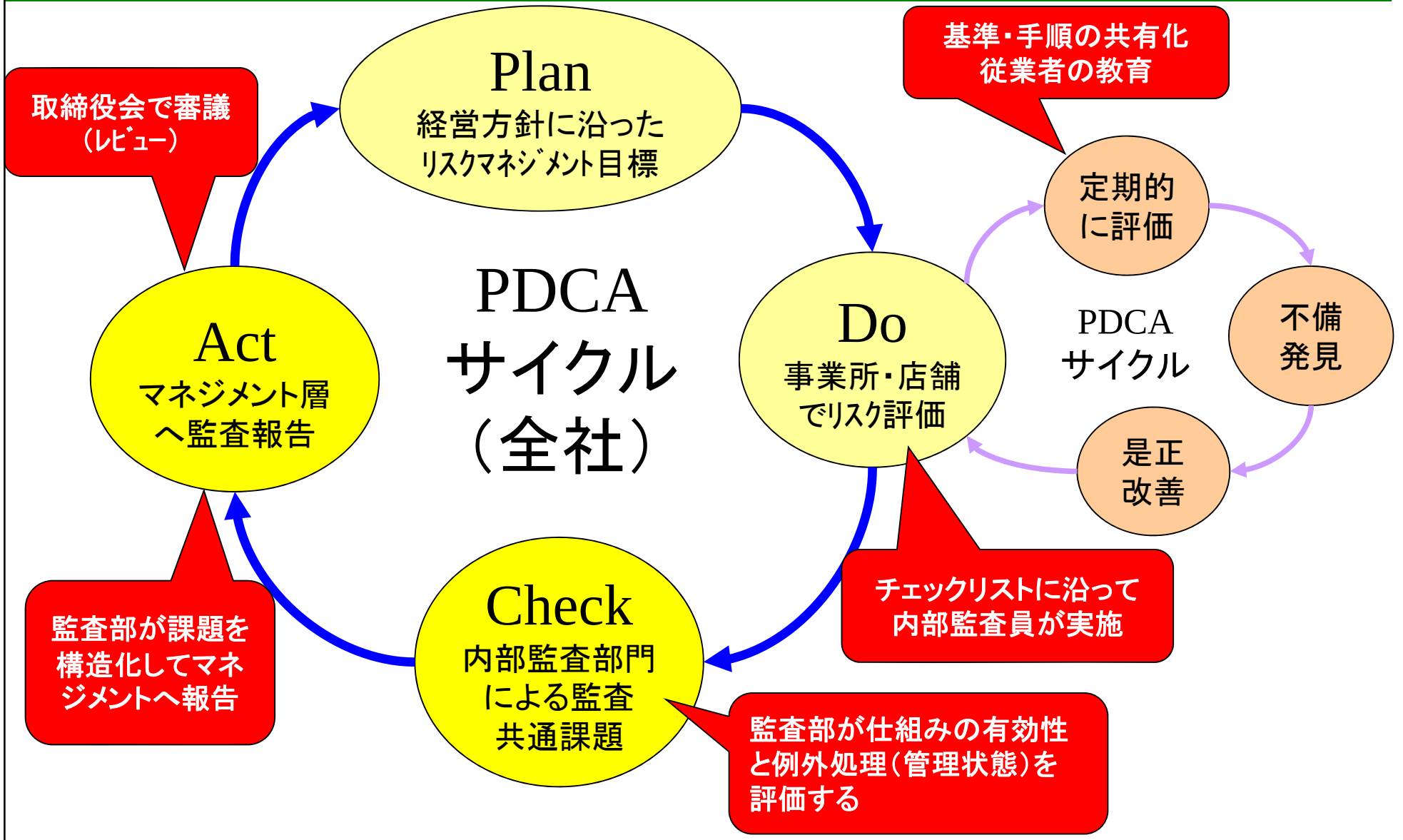
第4段階
未然防止・機会増大
（事業継続ﾏﾈｼﾞﾒﾝﾄ）

第3段階：自ら理解する
リスクマネジメント体制
（定期的に評価）

第2段階：何かあった時に対応
危機管理規程
（ｸﾗｲｼｽﾏﾈｼﾞﾒﾝﾄ）

第1段階：個人の技量で対応
リスクマネジメント規程
（内部統制構築）

29.リスクマネジメント評価の流れ（PDCAサイクル）



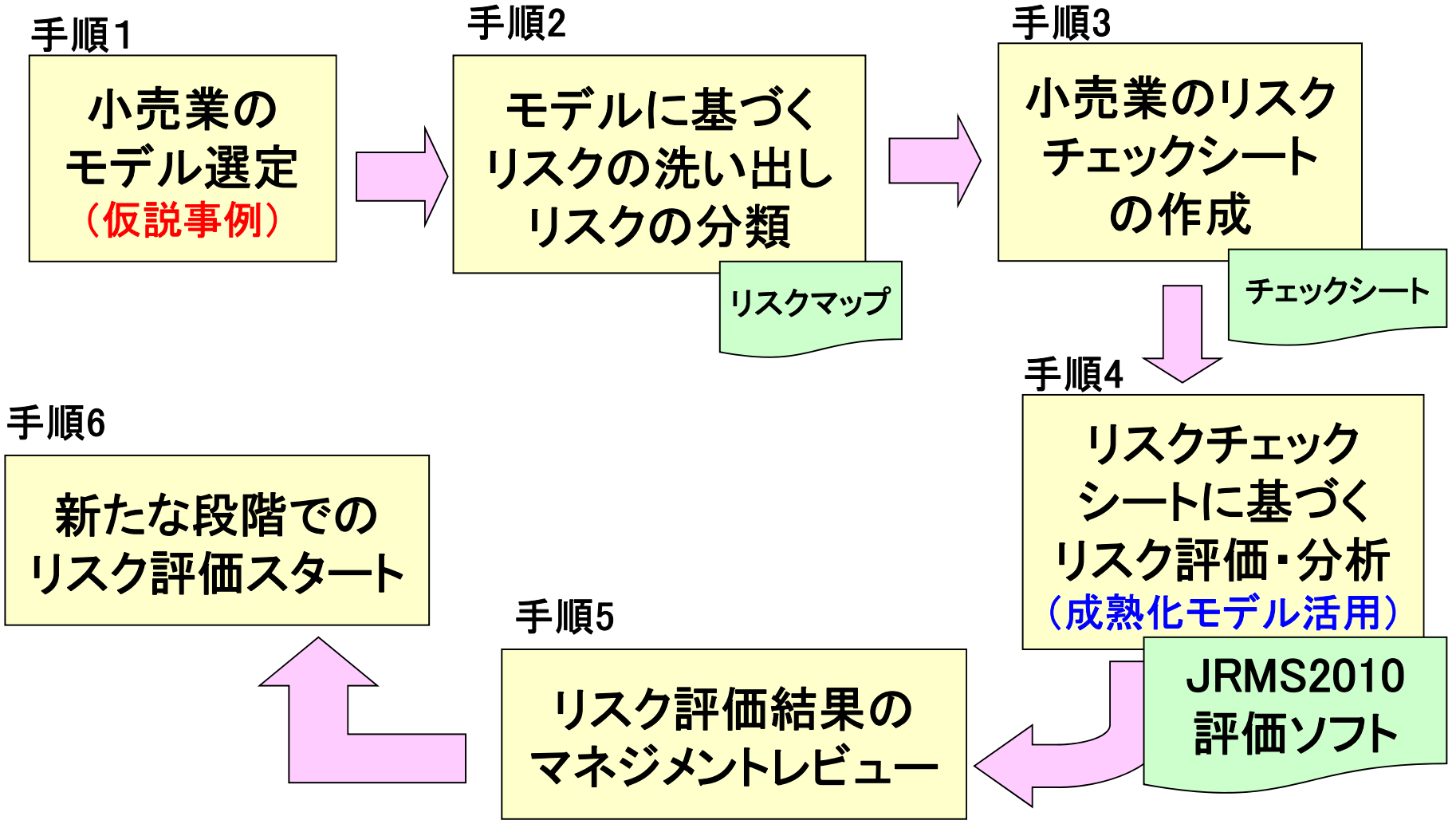
30.現状は小さいPDCAのみ回っている

大きいPDCAサイクル
アサーション
経営者の視点
《全体最適》

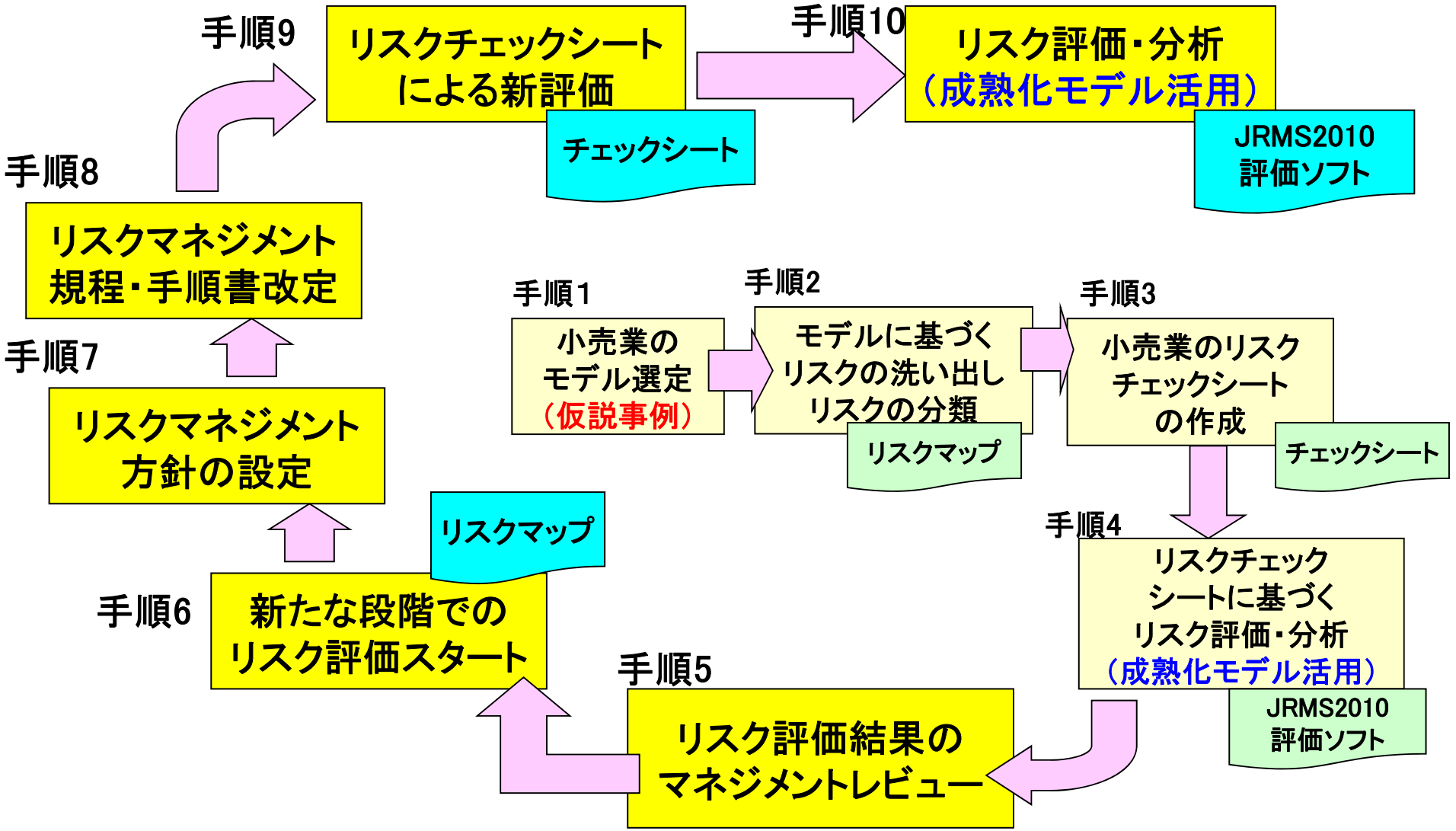
小さい
PDCAサイクル
現場に入り込み、
全体が見えない
《部分最適》

内部監査部門は悪さ
加減の共通点を
構造化し経営トップ
にあげていく

31.小売業のリスク評価の流れ（初年度）



32.小売業のリスク評価の流れ（評価2年目）



33.成熟度モデルを活用して見えてきた課題

大きな壁を乗り切るために！・・・3.11の教訓
個人がリスク感覚を醸成⇒情報共有化（情報開示）

事業継続における復旧方法は規模に関係なく
助け合うネットワーク（絆）と日常訓練（PDCAサイクル）

RMは成熟度レベルに関係なく開始すべきテーマ！
①コンプライアンス②組織化③継続的改善④社会責任

To Be Continued

ご静聴ありがとうございました。