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）
ー社会的責任（SR）への道筋 ー

2013/06/07

ﾘｽｸﾏﾈｼﾞﾒﾝﾄ研究ﾌﾟﾛｼﾞｪｸﾄ
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
　　堀越　繁明
　　高橋　孝治
　　野田　正美
　　小谷野　幸夫
　　桂　由紀子
　　高野　美久
　　喜入　博
　　北條　武（NTTデータ）
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）
- JRMS2010の適用・・・成熟度の違い（H23年度）

今年度の到達点：

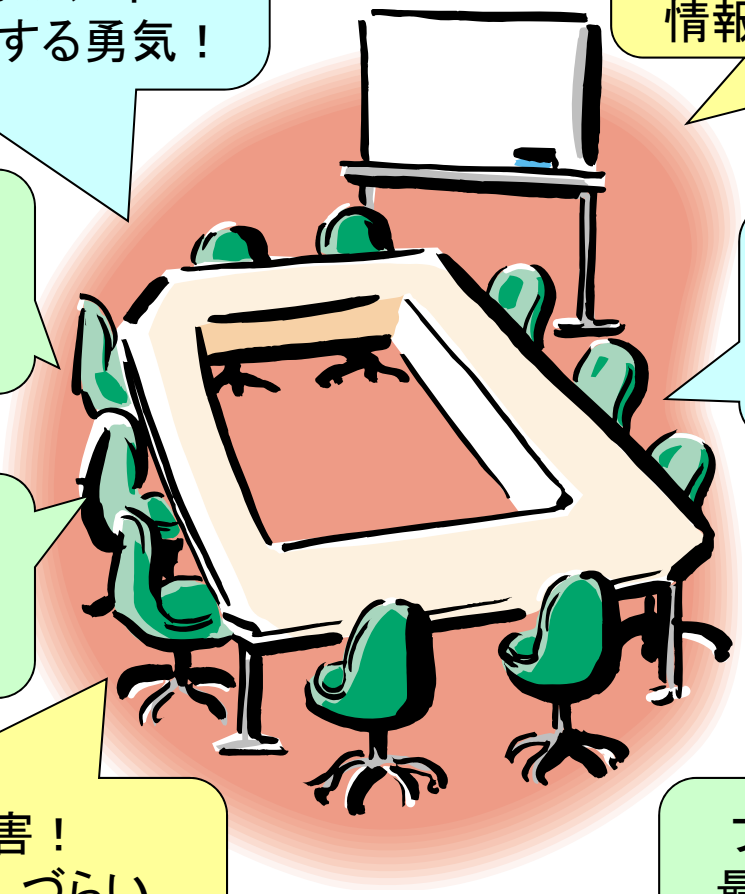
会合	日程	おもな検討内容
1回目	平成24年08月07日(火)	前回の反省と今後の展開
2回目	平成24年09月27日(木)	フリー・ディスカッション
3回目	平成24年12月07日(金)	前回振り返りとﾌﾘｰ・ﾃﾞｨｽｶｯｼｮﾝ
4回目	平成25年01月16日（水）	報告（案）の説明と協議・修正
5回目	平成25年03月07日（木）	報告（案）の説明と協議・修正
6回目	平成25年04月25日(木)	報告書（確定分）最終検討会

RMプロジェクトで話しあった意見（前年度）

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！

RMプロジェクトで話しあった意見（1～2回目）

経営計画に社会コストとして「環境保全」「フェアな雇用」「フェアな取引」「防災対策」を織り込むことが重要

信用は信者を作ること。そうすれば儲けに繋がる・・・

不正には、組織の利益（日本に多い）と個人の利益（欧米に多い）がある・・・

人材はヒト・モノ・カネ・情報の一つ。これからは社会に通用する「人財」つくりが他より重要！

経営陣に現状否定して「顧客ニーズからのズレ」を認識する意識が必要・・・・

埼玉のスーパーが「従業員の声」を大切にして、品揃えやサービスに繋げて成長している・・・・

「事故が起こってから対応」から、事故前の「ヒヤリハット情報へ対応」することがリスクマネジメント・・・

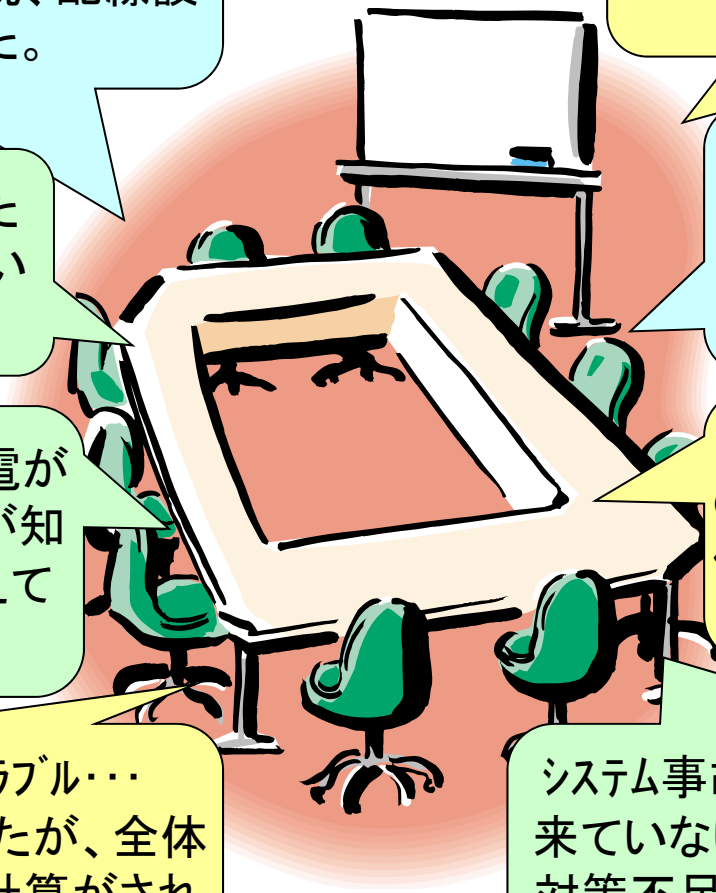
RMプロジェクトで話しあった意見（3～6回目）

メインフレームの時代は「ハードウェアエンジニア」「ソフトウェアエンジニア」「セールスエンジニア」が役割分担して、施設環境、配線設計、容量計算をした。

情報機器を販売するときに、便利なことしか説明しない。工学系のない顧客はトラブルで悩む！

コンピュータが「家電」になった時点から「動けば良い」という意識になった・・・

街の電気屋さんが居なくなって、大手通信会社の代理店業者が配線のため壁に穴をいくつも開けて知らん顔で帰っていく！



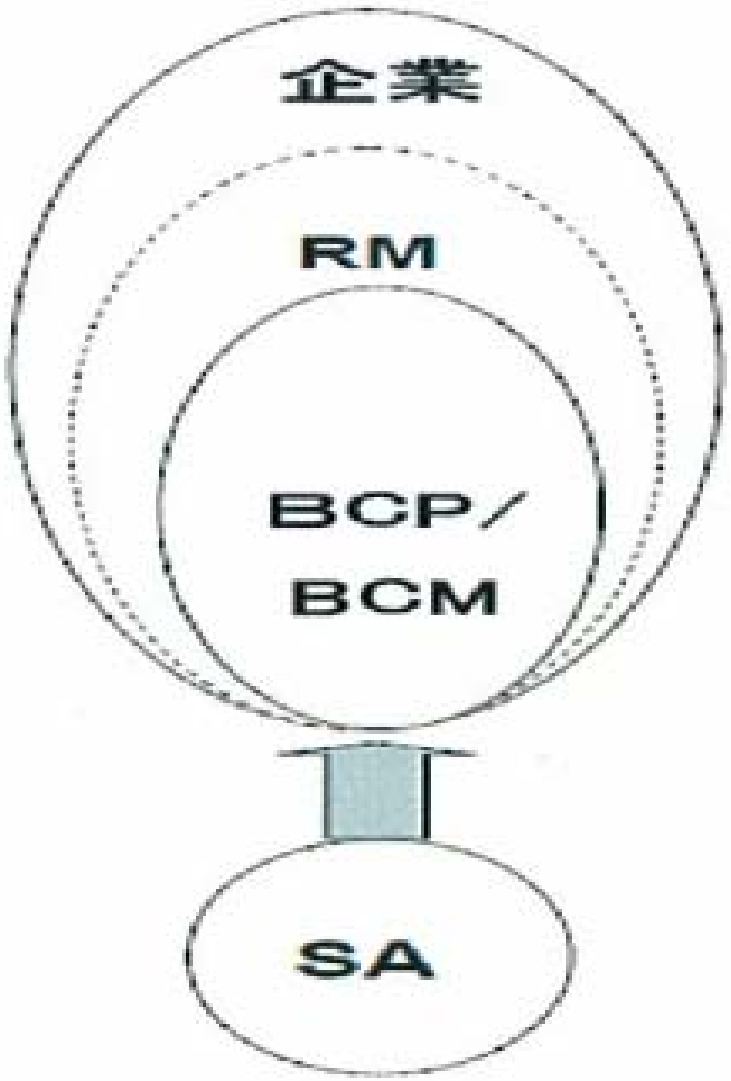
組込みコンピュータ、スマート家電が拡大してくるとシステム部門が知らないネットワーク機器が増えてケーブルが塊になる

メインフレームの時代⇒クライアントサーバーの時代⇒Webと端末の時代と変化。便利さだけが協調され、増大するリスクの全体像が見えない。

〇〇社の787ジェット機トラブル・・・
個別システムはテストされていたが、全体設計がなく、トータルの負荷計算がされていなかった！

システム事故の原因を辿っていくと「5S」が出来ていないことが多い。トラッキング事故、防塵対策不足、ゲリア洪水対策等、環境による事故が増えている

1-1. 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）

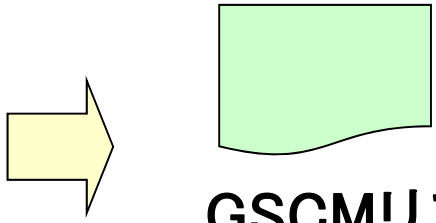
1-2.GSCMにおけるリスクの一般化

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）

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

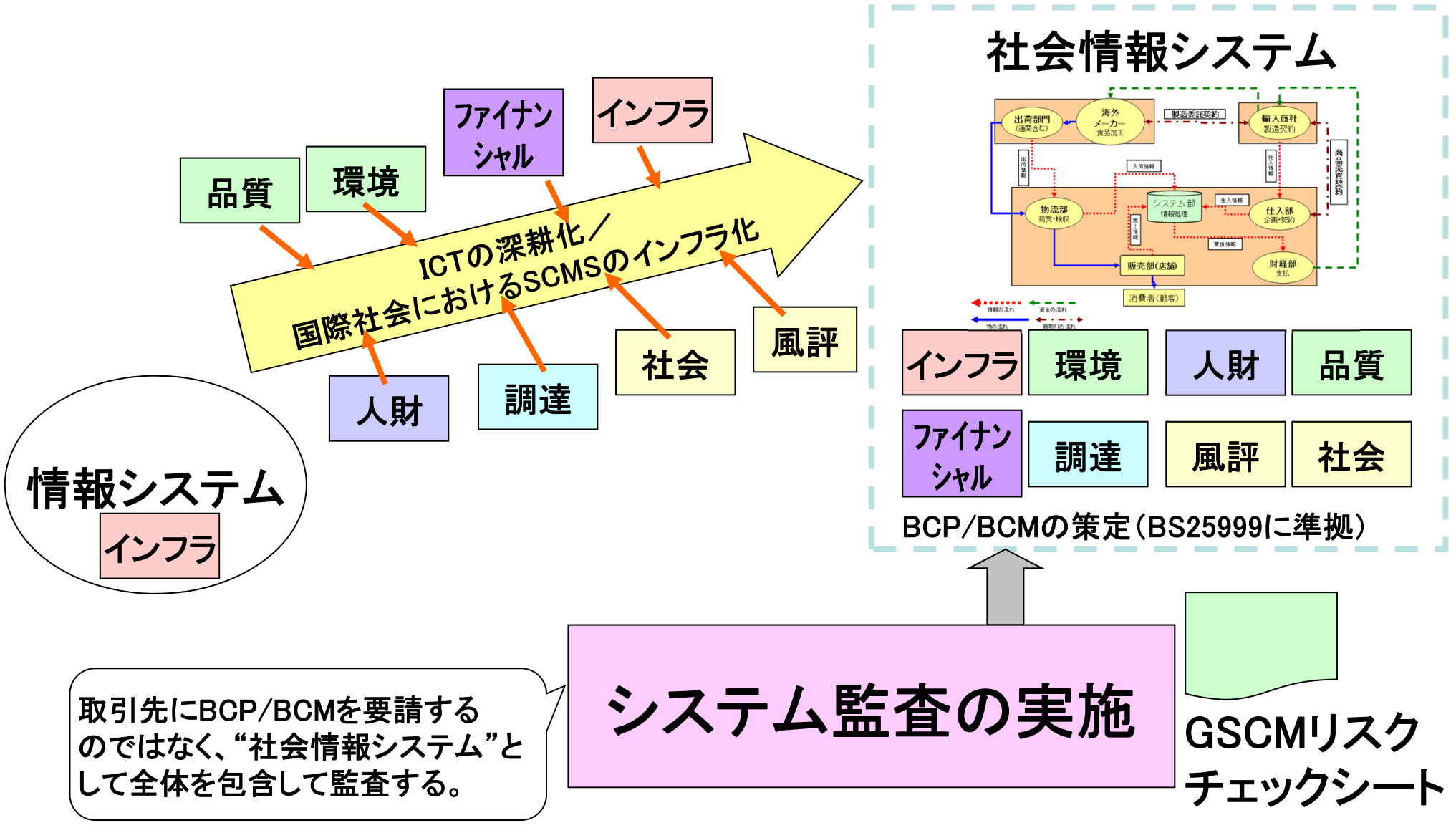
対象を“情報システム”だけでなく
“社会情報システム全体”として
考えざるを得ない



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

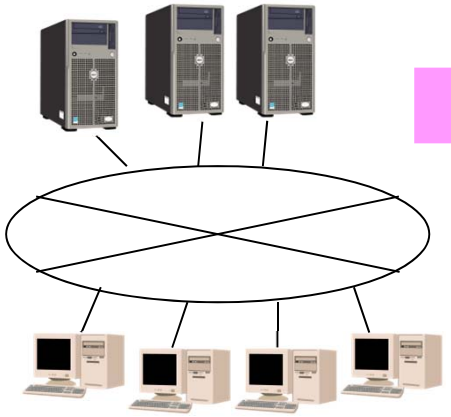
1-3.情報システムの進化のシステム監査の概念図



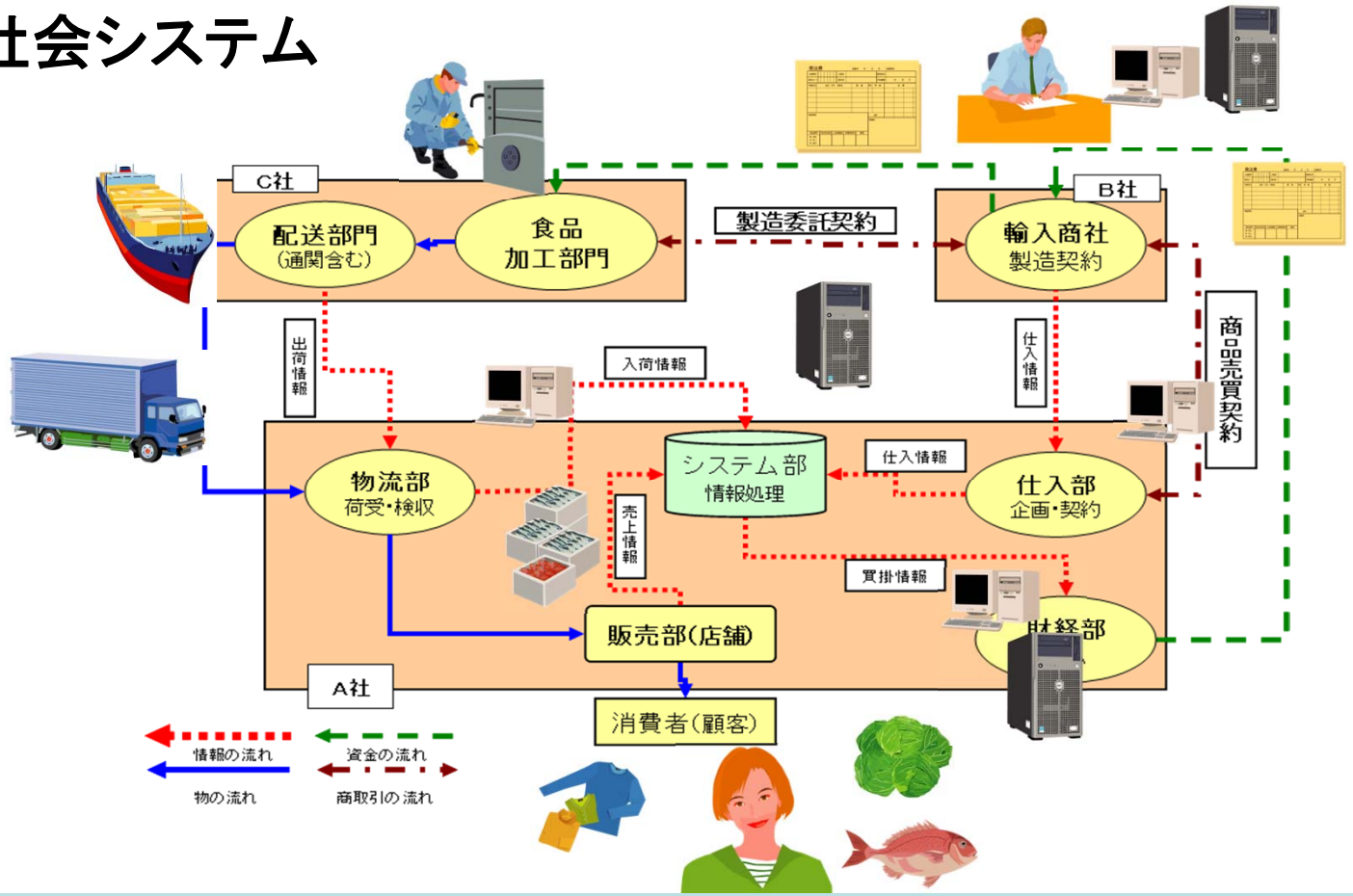
2-1.サプライチェーンのリスクマネジメント対象範囲モデル

【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



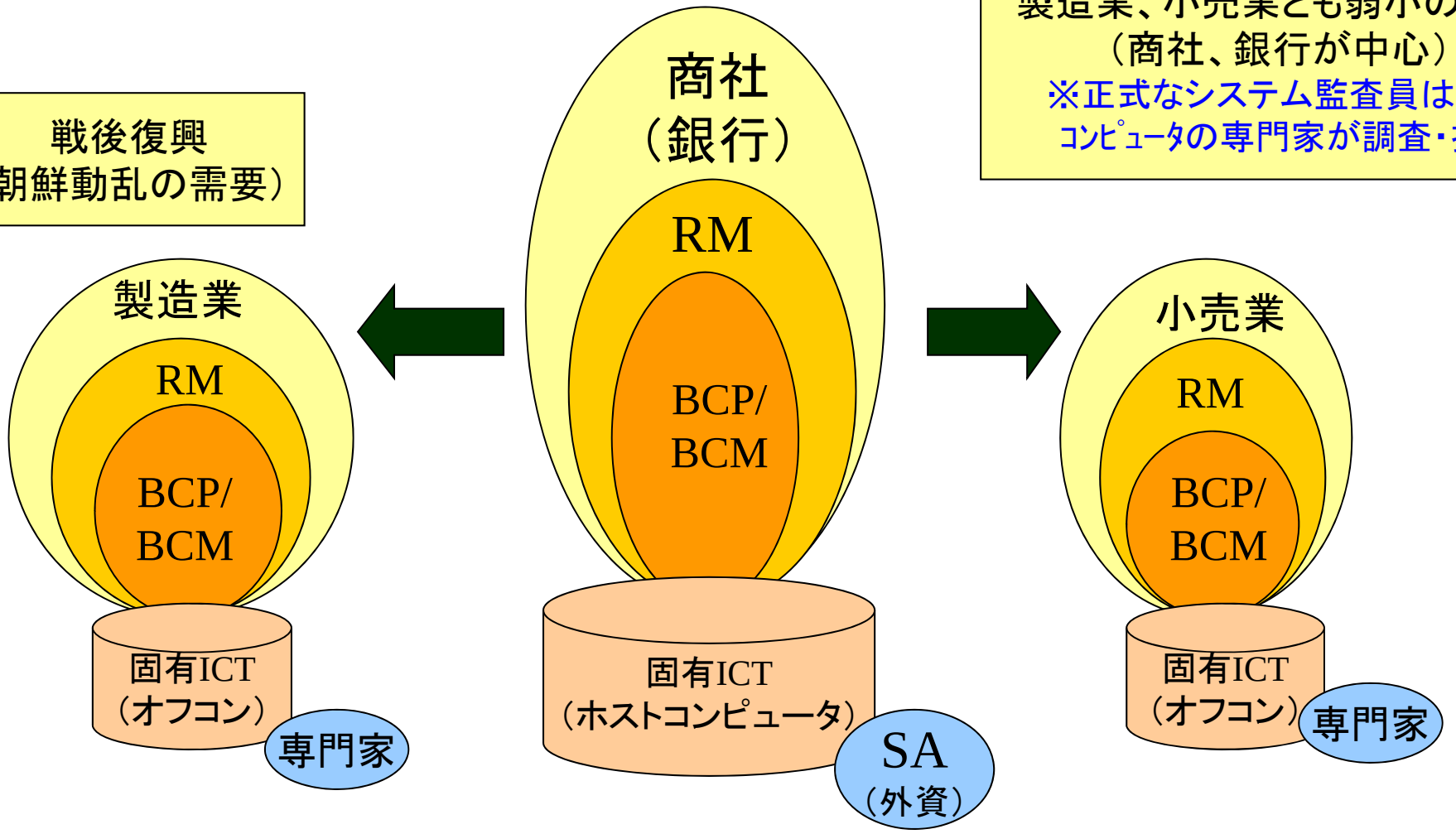
社会システム



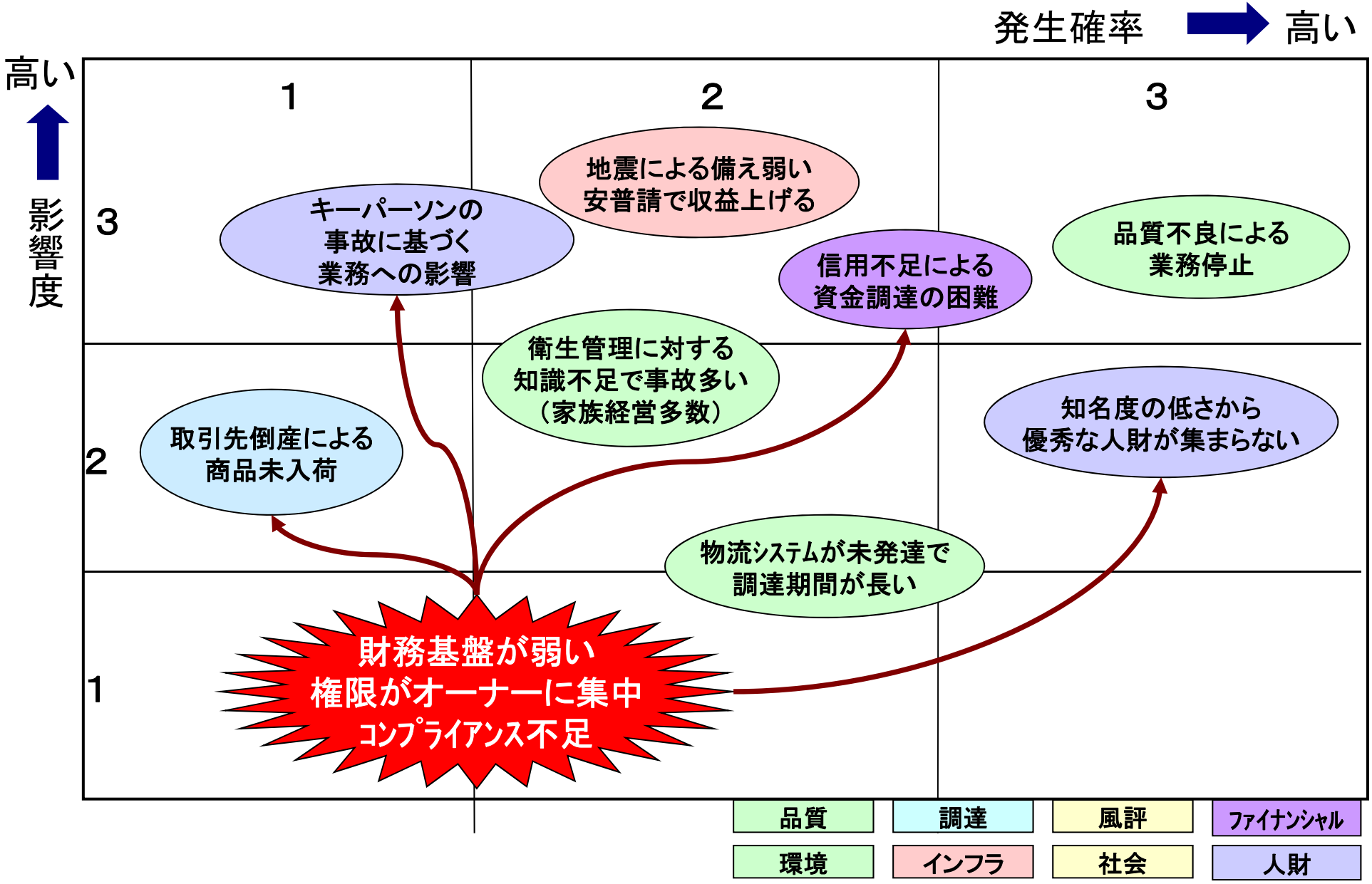
2-2.サプライチェーンの発展過程　Ⅰ　（1950～60年代）

製造業、小売業とも弱小の時代
（商社、銀行が中心）
※正式なシステム監査員は無く
ｺﾝﾋﾟｭｰﾀの専門家が調査・指導

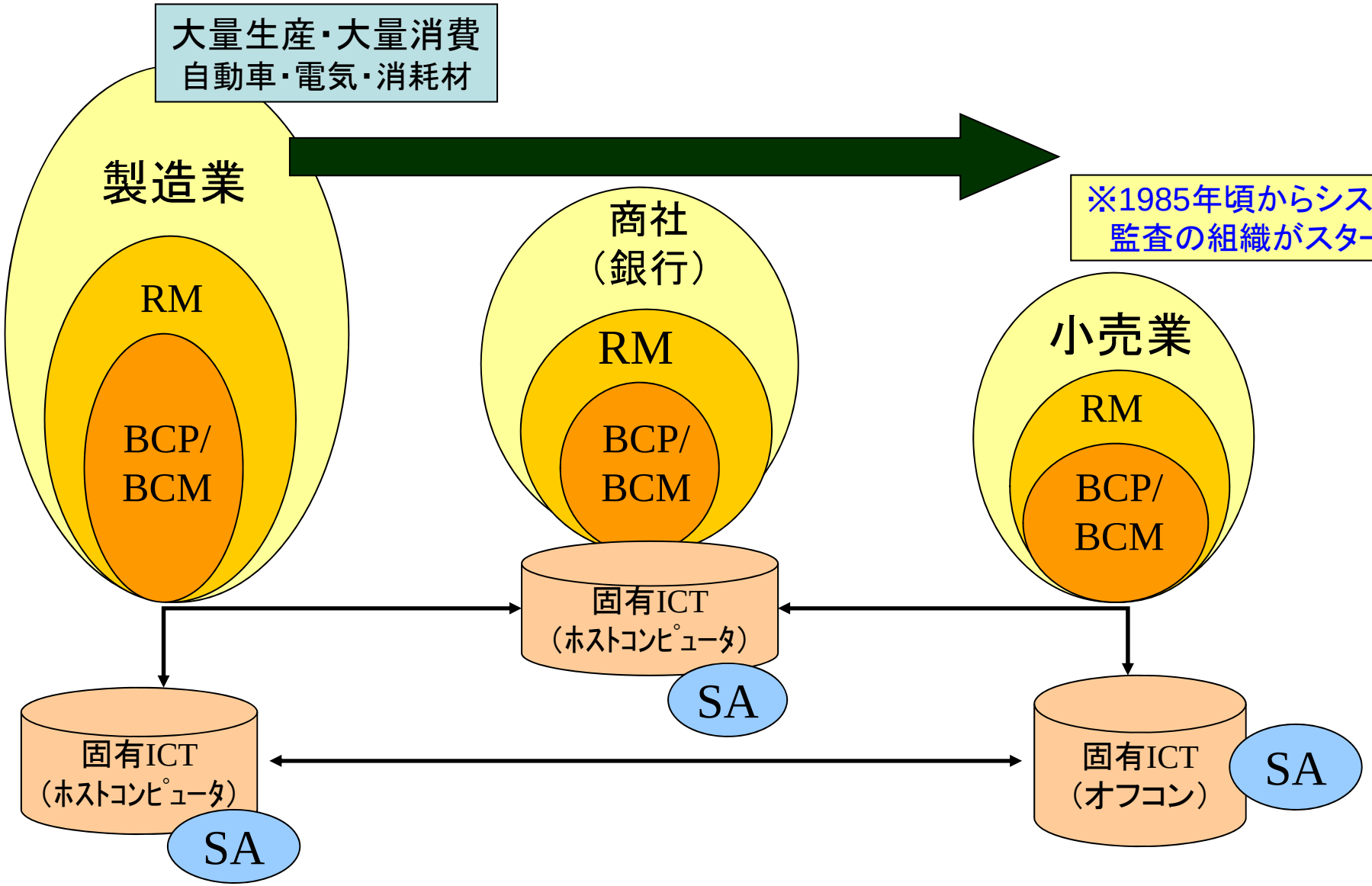
戦後復興
（朝鮮動乱の需要）



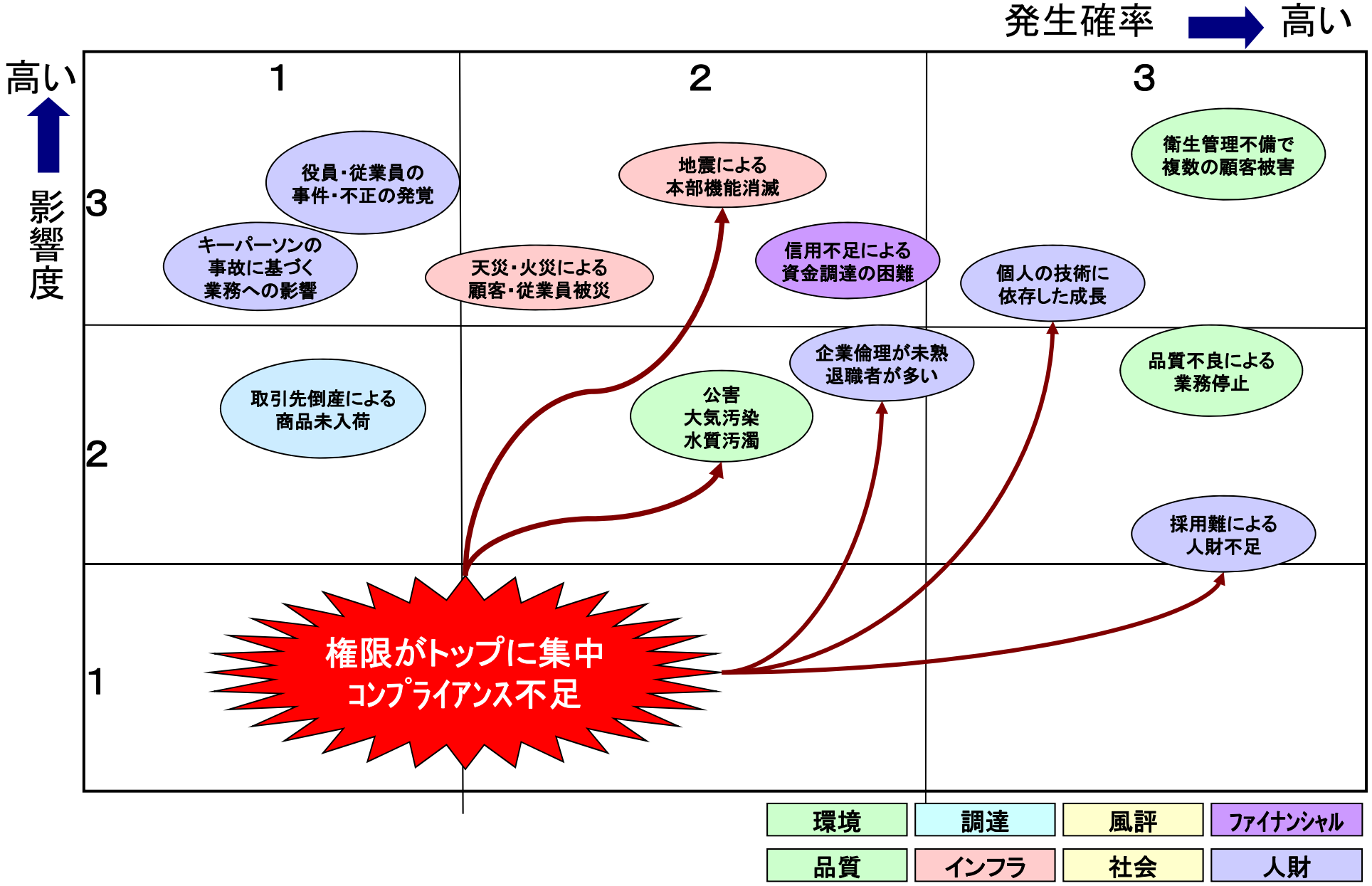
2-3.リスク評価ー（サプライチェーン　Ⅰ）



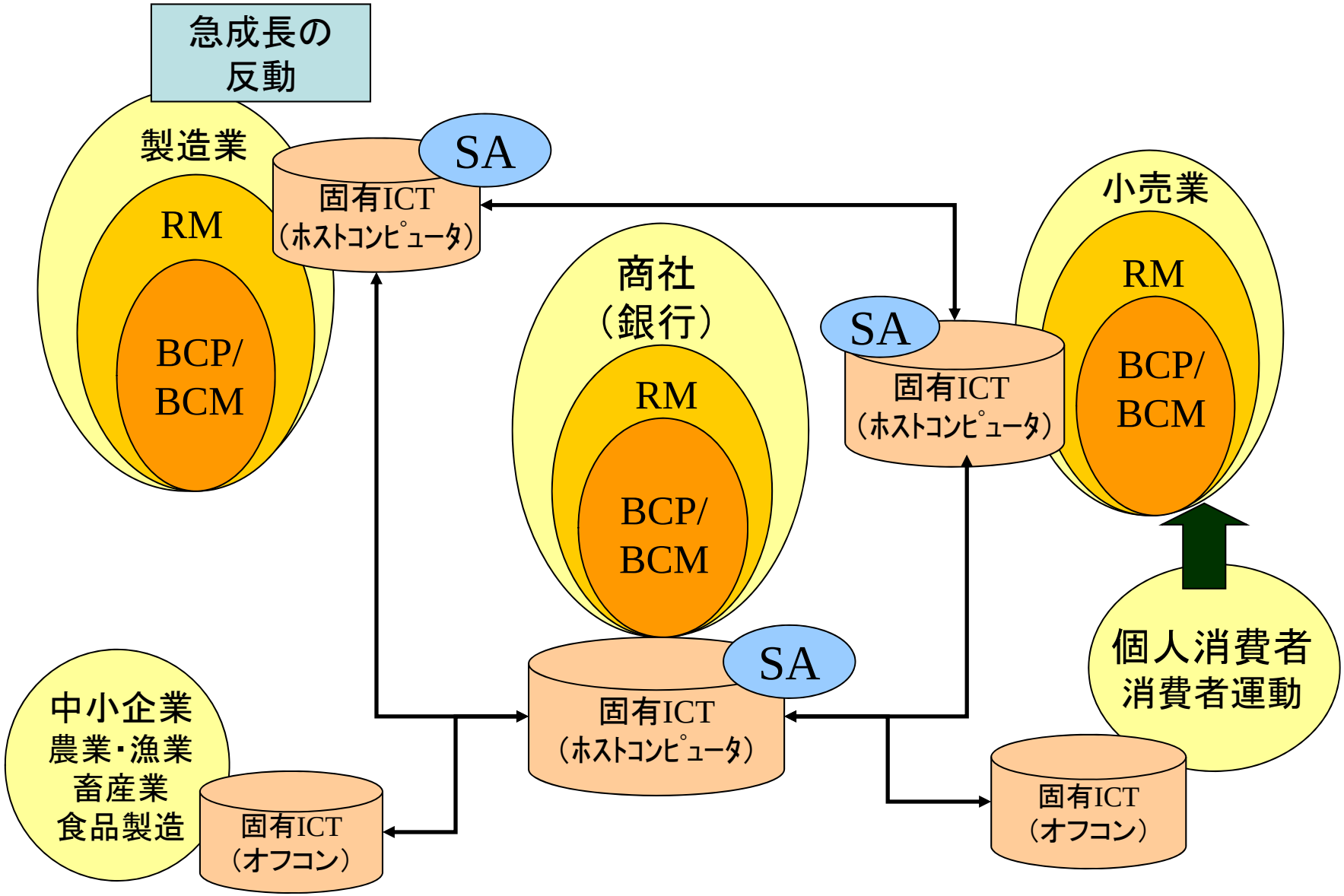
2-4.サプライチェーンの発展過程　Ⅱ（1970～80年代）



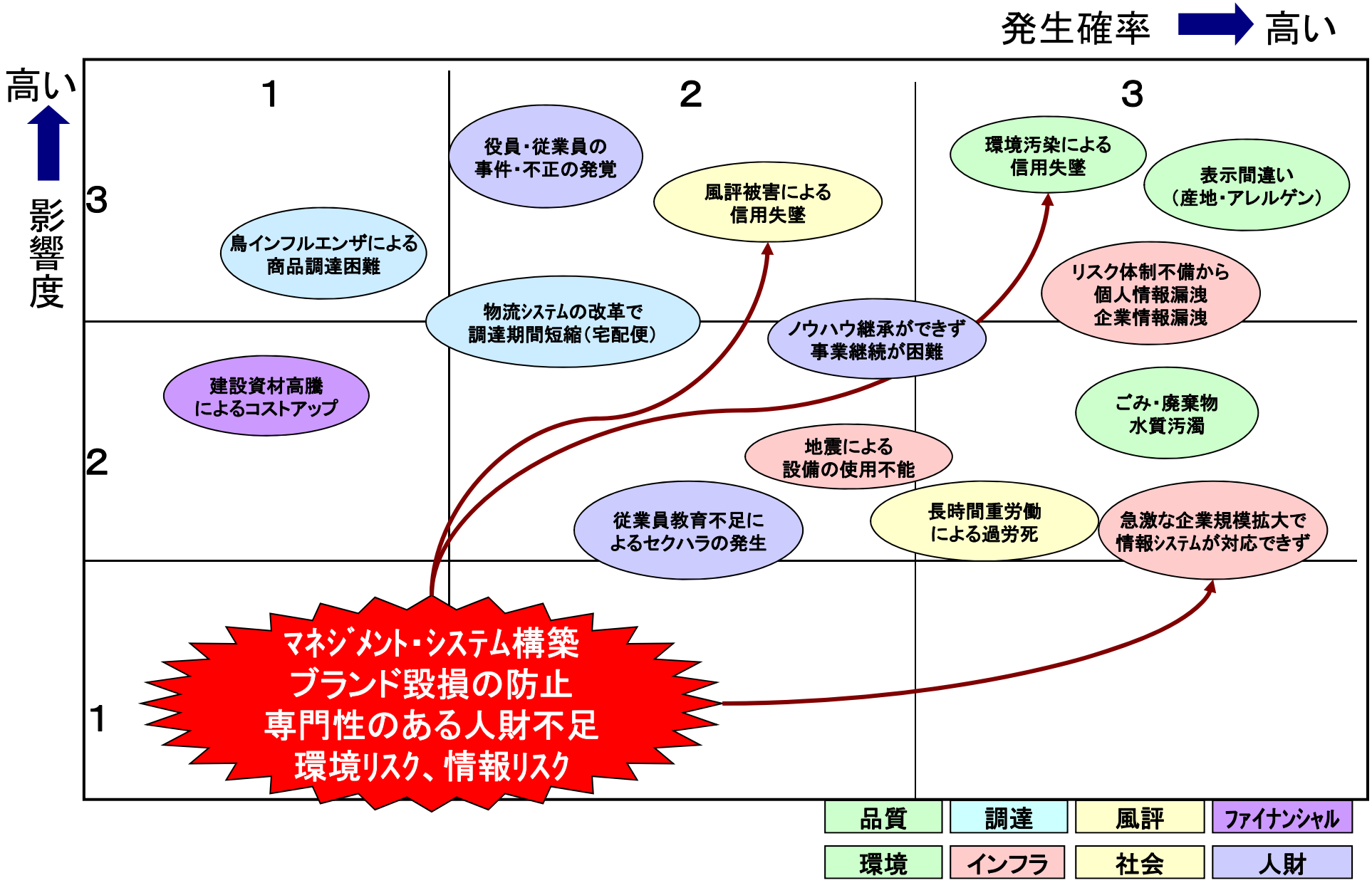
2-5.リスク評価ー（サプライチェーン　Ⅱ）



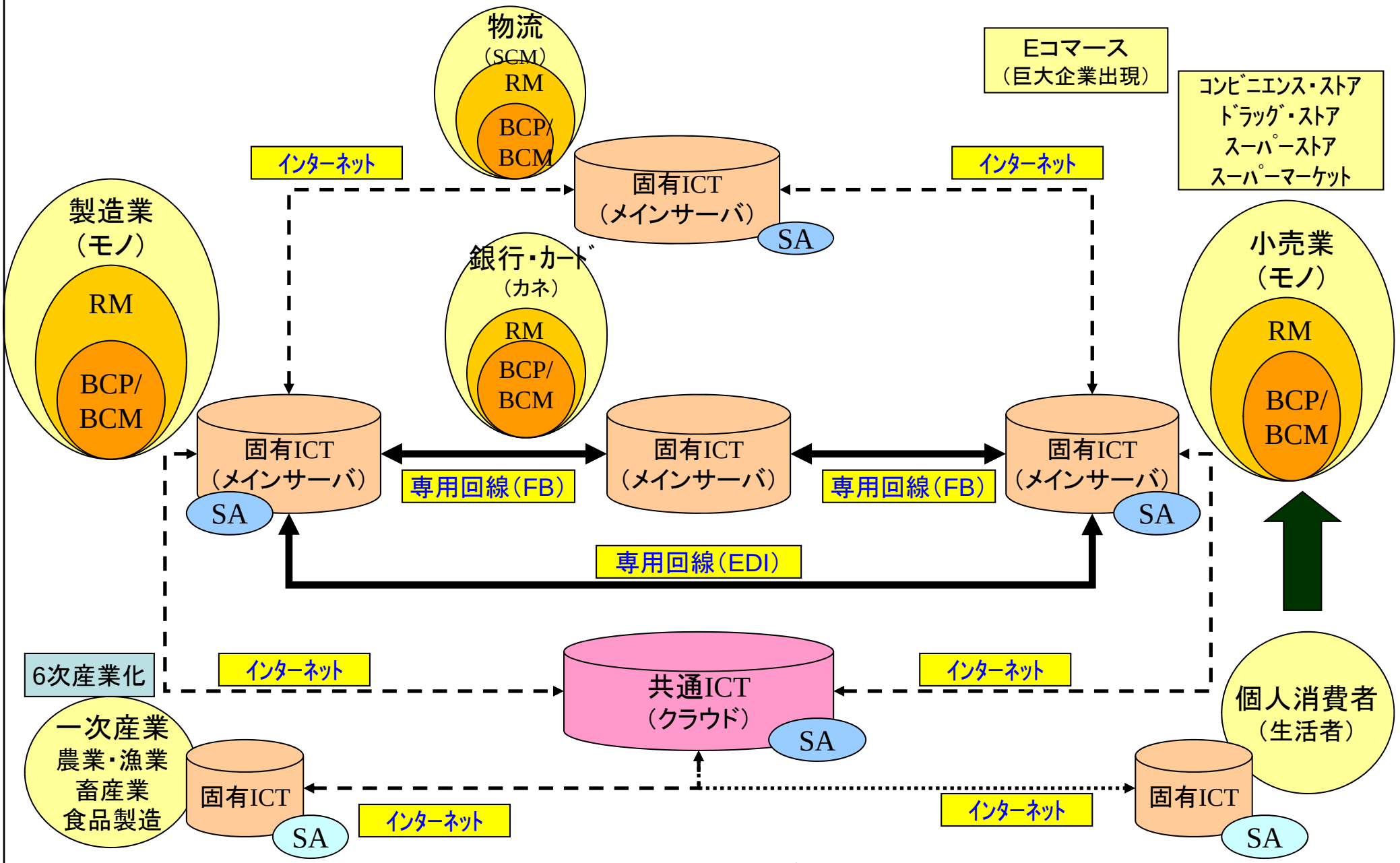
2-6.サプライチェーンの発展過程　Ⅲ（1990～2000年）



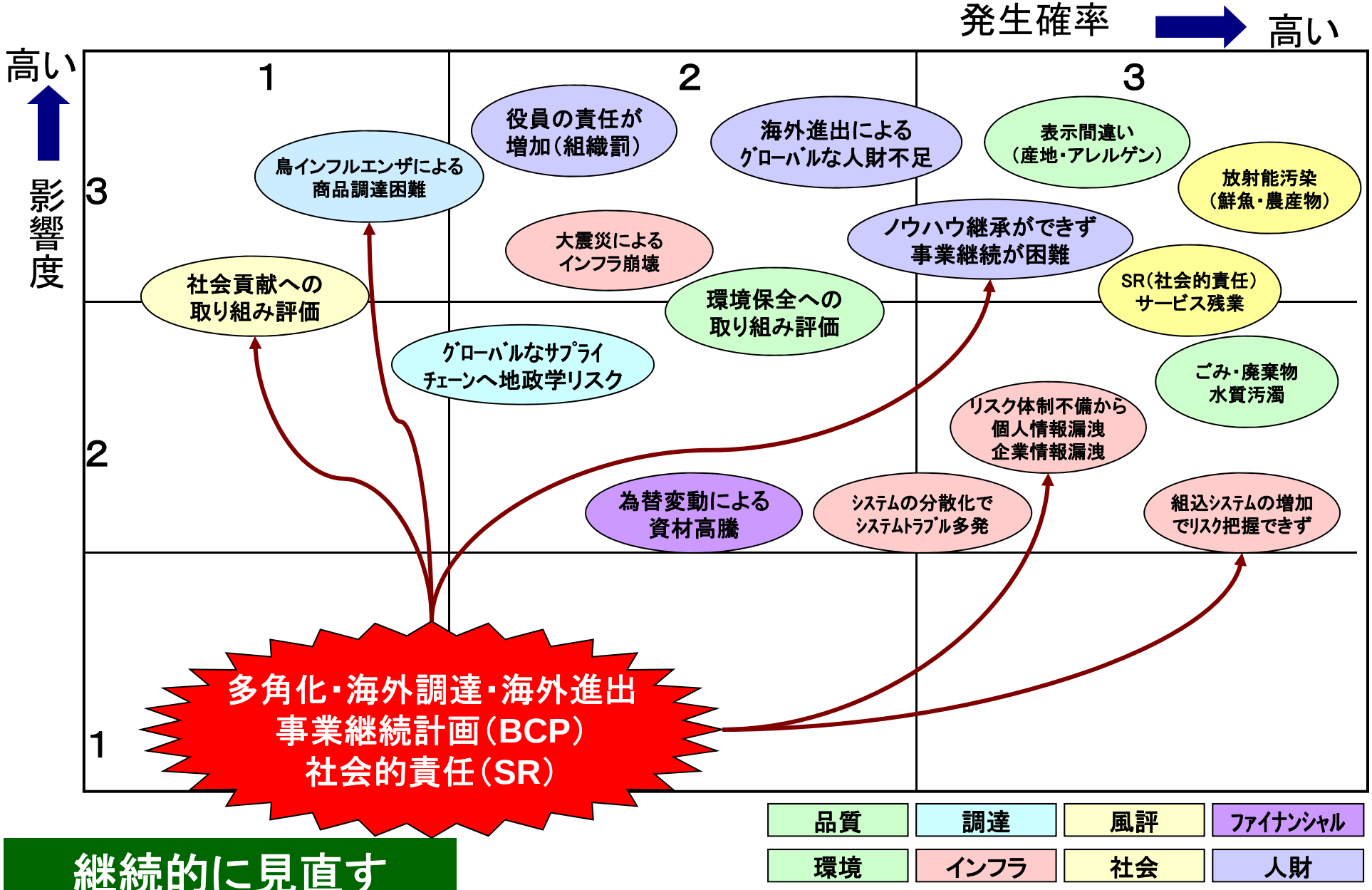
2-7.リスク評価ー（サプライチェーン　Ⅲ）



2-8.サプライチェーンの発展過程　Ⅳ（2001～現在）

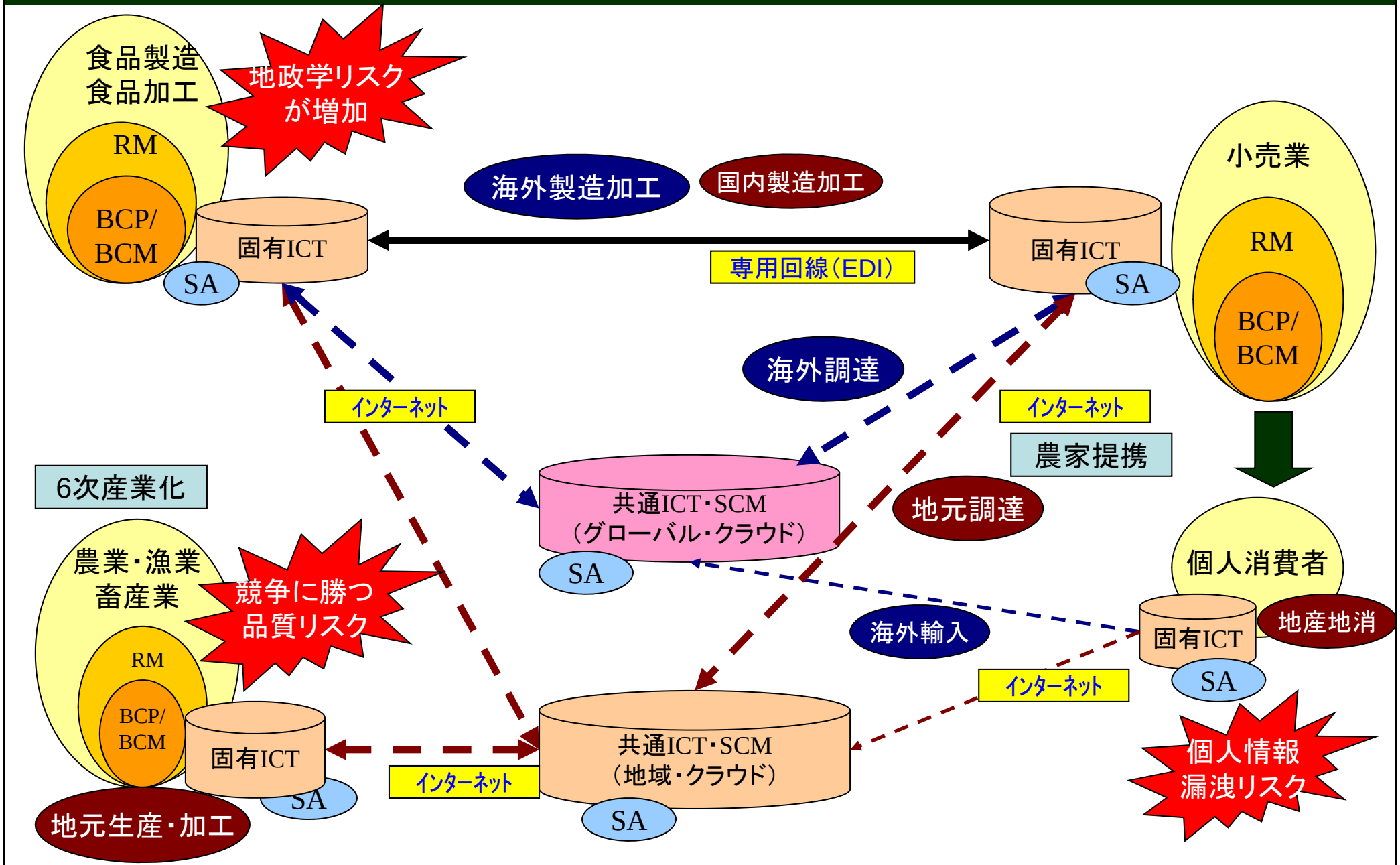


2-9.リスク評価ー（サプライチェーン　Ⅳ）

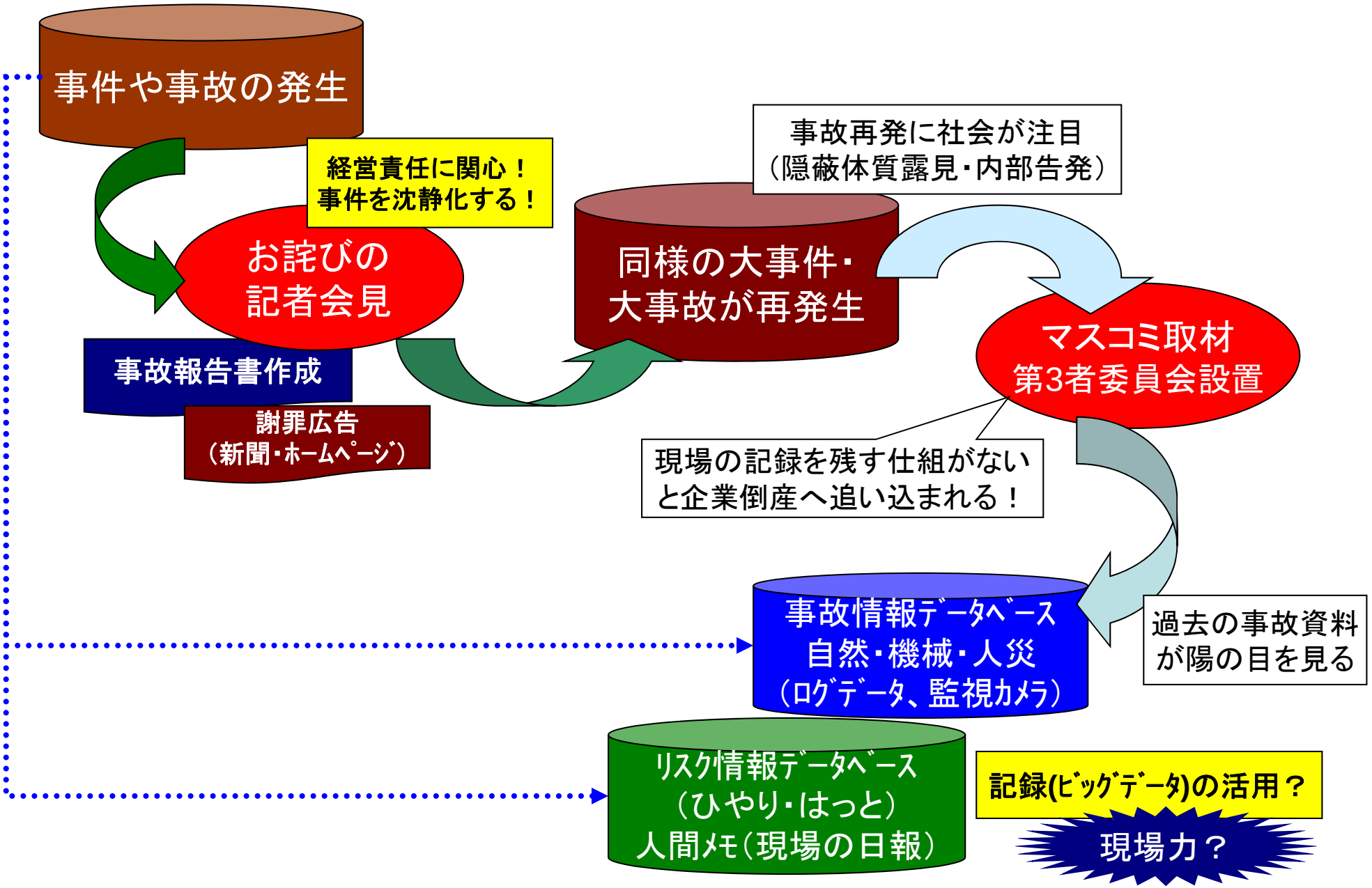


継続的に見直す

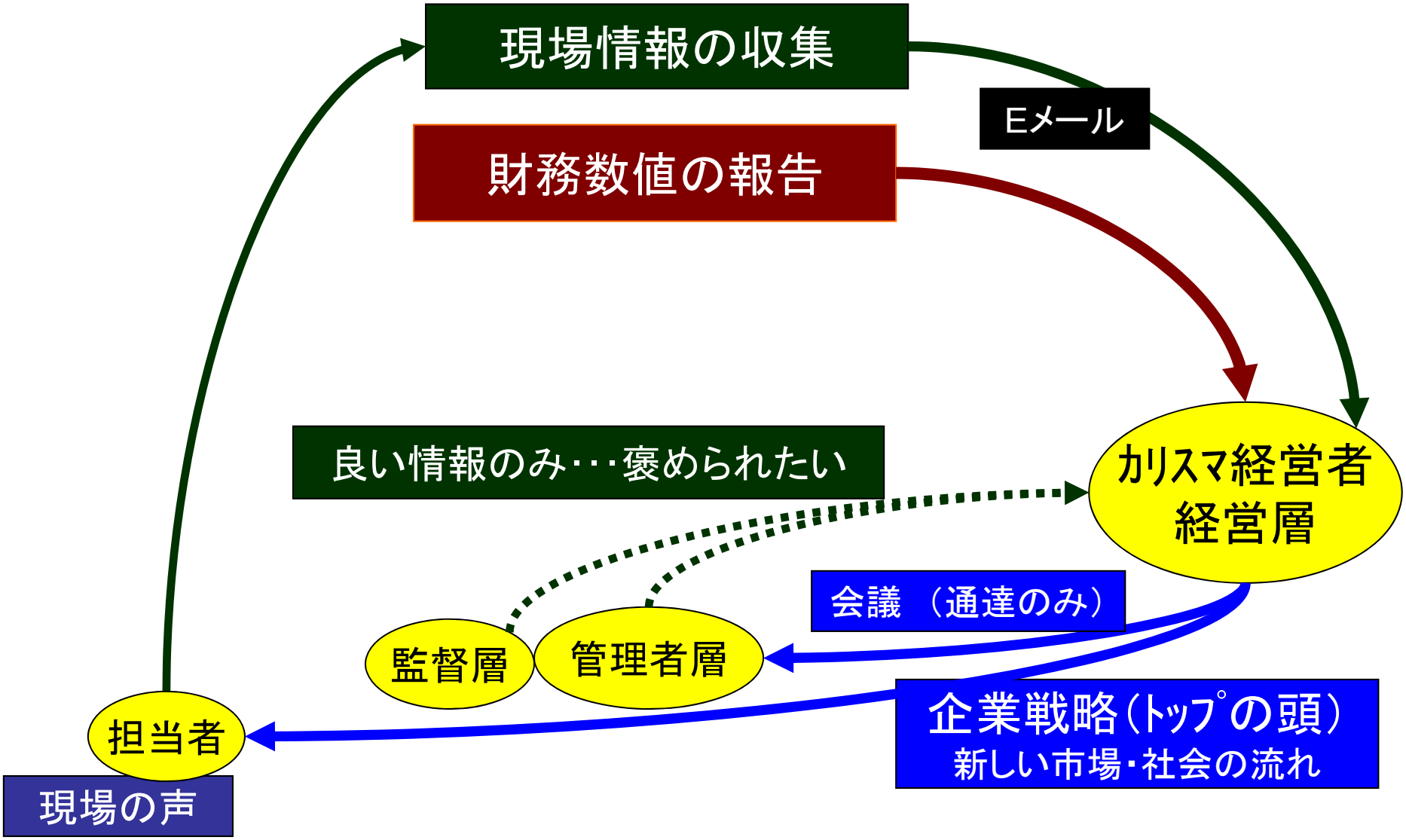
2-10.サプライチェーンの発展過程　V（将来イメージ）



3-1.繰り返される事件・事故・・・データベースが活かされない



3-2.中小小売業の情報の流れ（レベルⅠのイメージ）



3-3.中小小売業のリスクマネジメント成熟度（仮想モデル）

各階層が経営戦略系・
コントロール系・オペレーション系
にアクセスできる体制

【レベル5】社会的責任（SR）
SCMとして一体でRM実現
従業員が自律的にRMを実施
社会の中に未然防止が定着

【レベル4】 フィードバック（PDCA）
情報共有化による迅速な対応
（事件・事故、失敗情報含む）
定量・定性分析とマネジメントレビュー

機密性

【レベル3】 組織的な対応A
取締役会へ報告⇒責任体制
※縦型命令組織（一方通行）

横展開シフト！

可用性

【レベル3】 組織的な対応B
経営陣（情報開示）、現場と対話
※参画型組織、個人の知恵

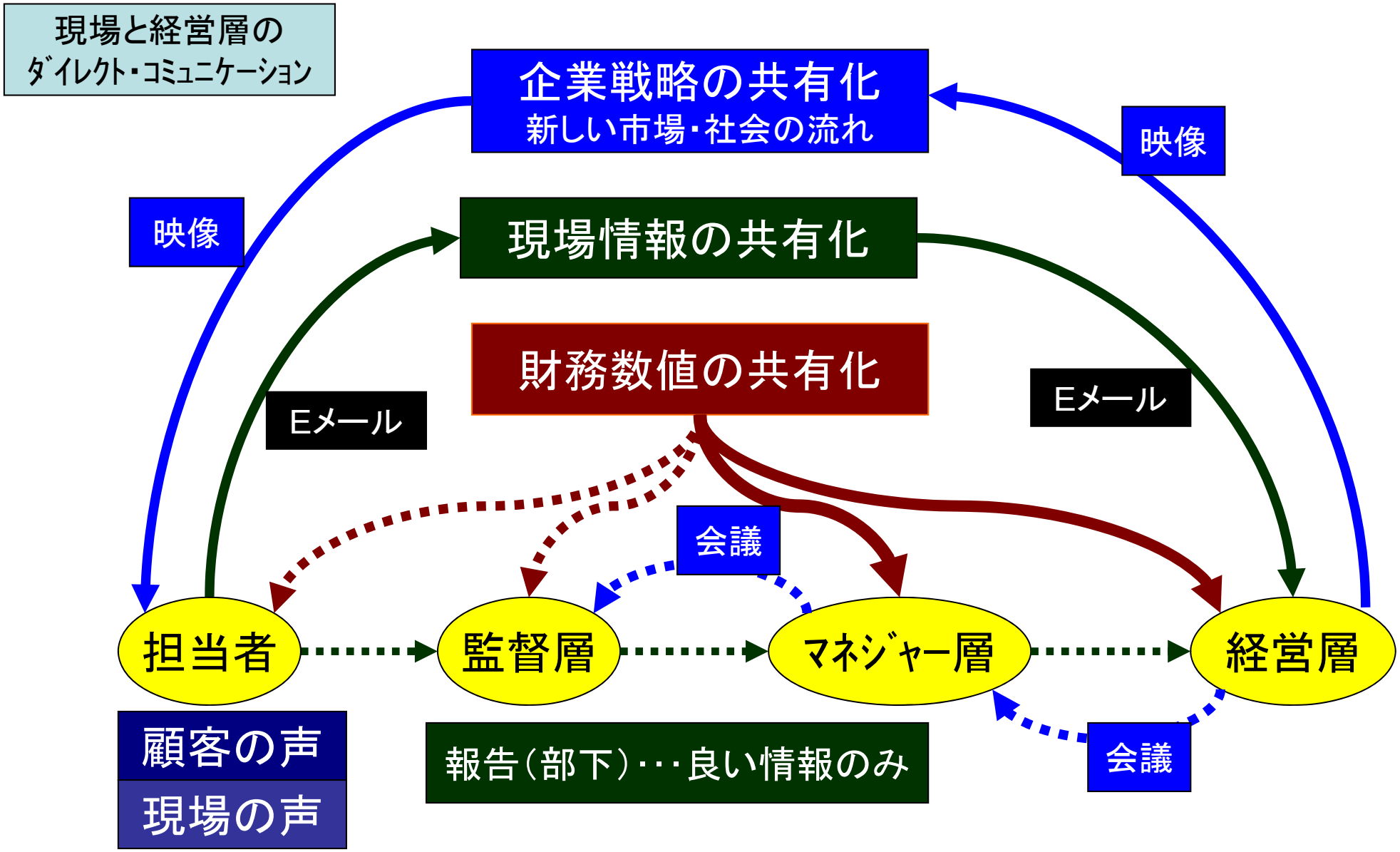
【再構築】創造的な破壊（改革）
全従業員の意識変革（文化の変化）
多様な人材の登用（ダイバーシティ）

【レベル2】 定義されている
関連部署が対応に当たる
部門のリスク意識にばらつき

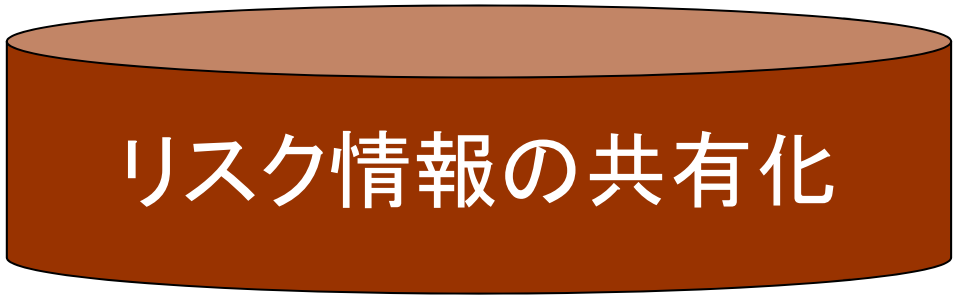
完全性

【レベル1】 組織未対応
ベテラン従業員の倫理感に依存
暗黙知（見える化がない）

3-4.中小小売業における情報の流れ（レベルⅢのイメージ）



3-5.なぜ、事故報告が再発防止に繋がらない？



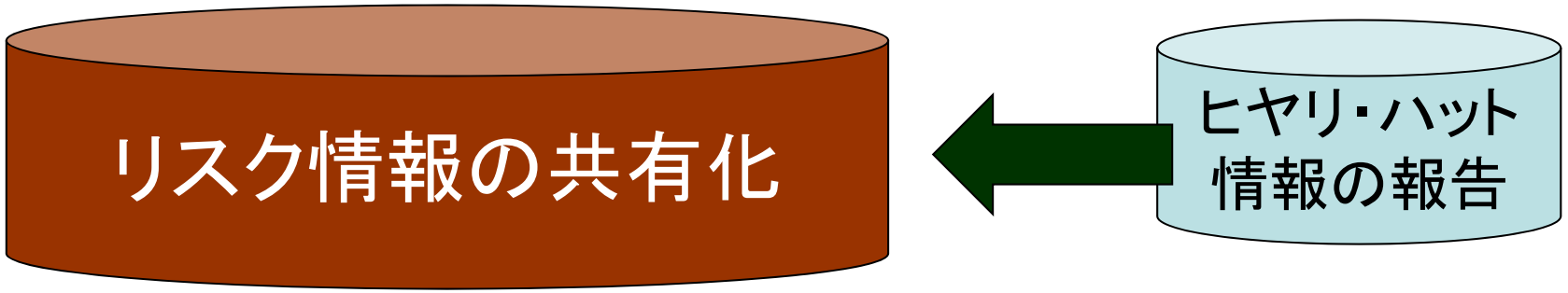
反対意見を記録する！

1.第三者委員会の必要性・・・内部監査・外部監査
　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・・・不利な情報
　「真のリスク情報（失敗・事故）」

3.多くの業界・学会・官公庁が合同で取組み
　知恵を集める、資源を有効に使える

3-6.なぜ、真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

事件の真相が闇に消されてしまう

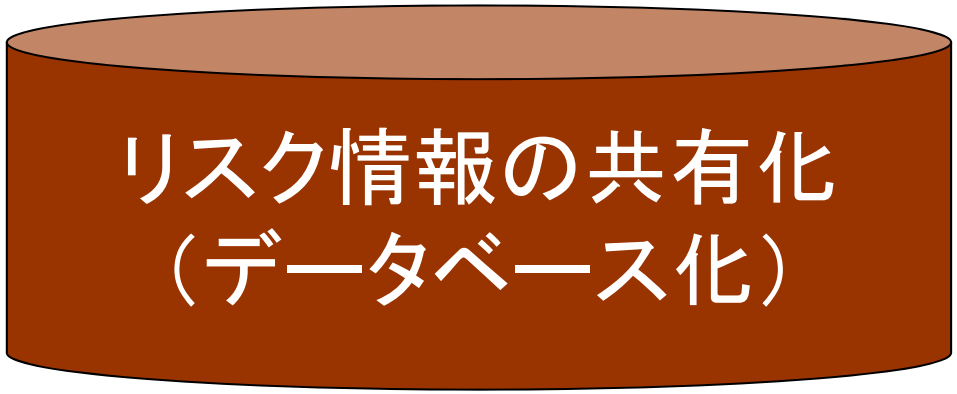
関係者が保身に走り、無関係を装う

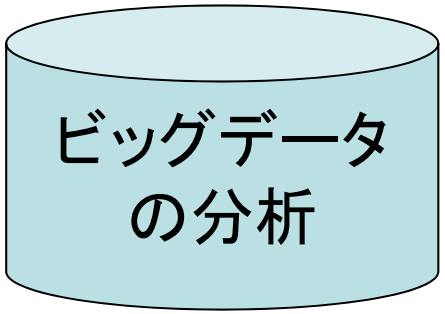
※告発すれば、マイナス評価

2.組織的不正・・・カビが蔓延る（組織全体）

個人的不正・・・虫がつく（取り除ける）

3-7.不正情報やリスク情報

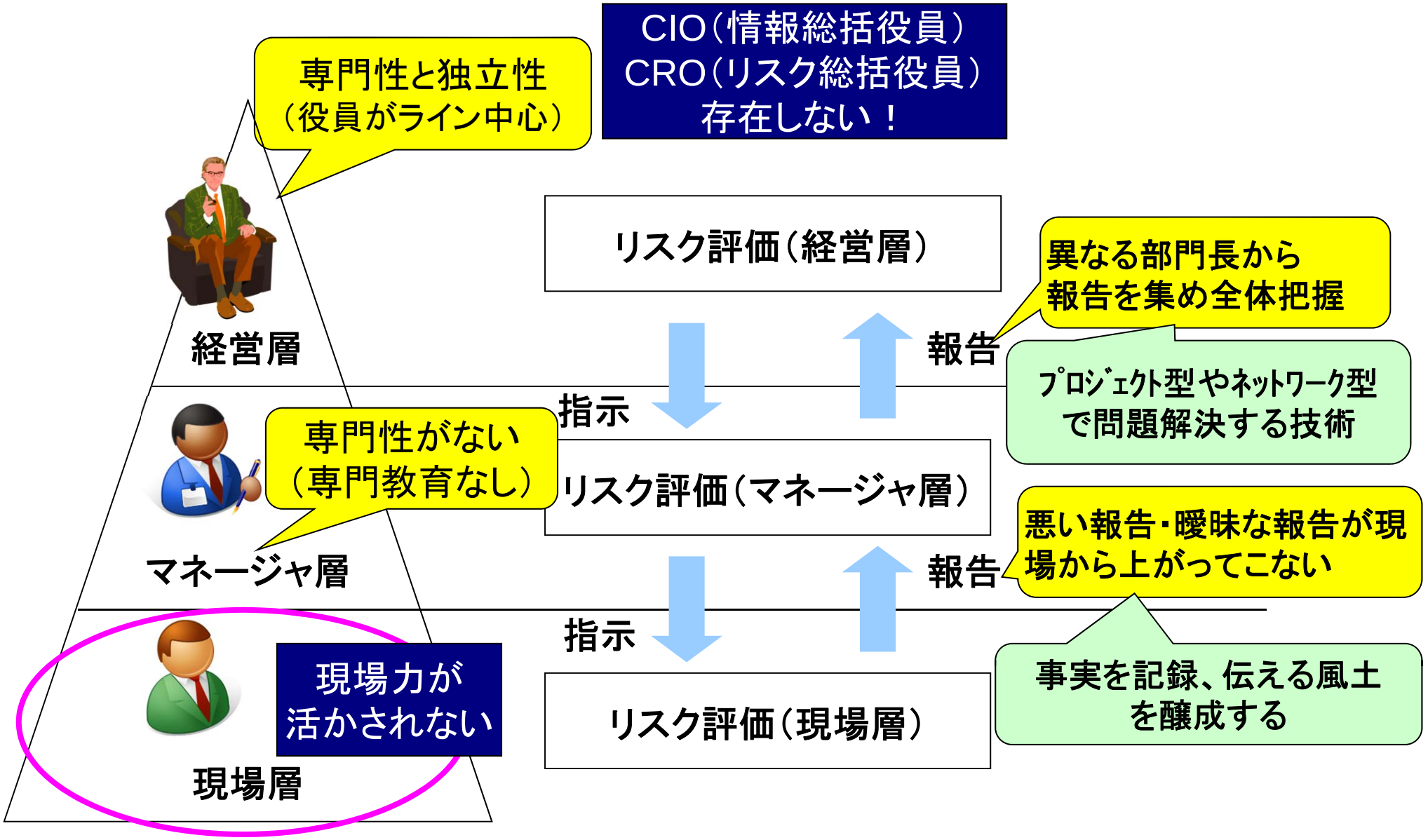




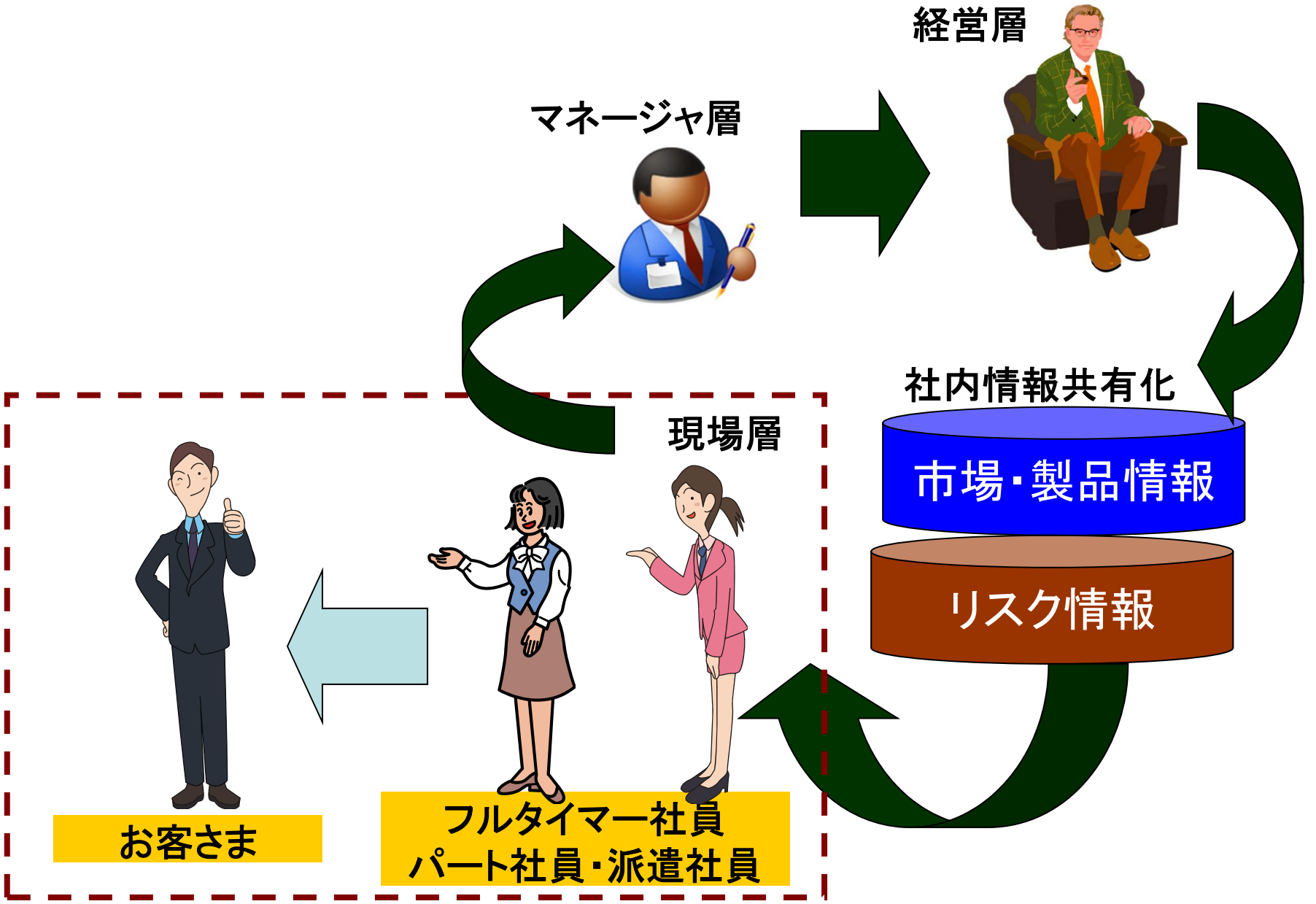
1.役員（トップ）が持つ情報価値⇒報告が上がらない
　企業の不正情報は、現場とネットで洩れる
2.「高収益企業」と「一生働きたい企業」の違い
　継続的に変革し、自己実現ができる会社
3.同質的な情報源から多様性な情報源の確保へ
　異業者の経験から真の解決糸口が生まれる

ブラック企業
（社会批判）

4-1. 階層別リスクマネジメントの必要性



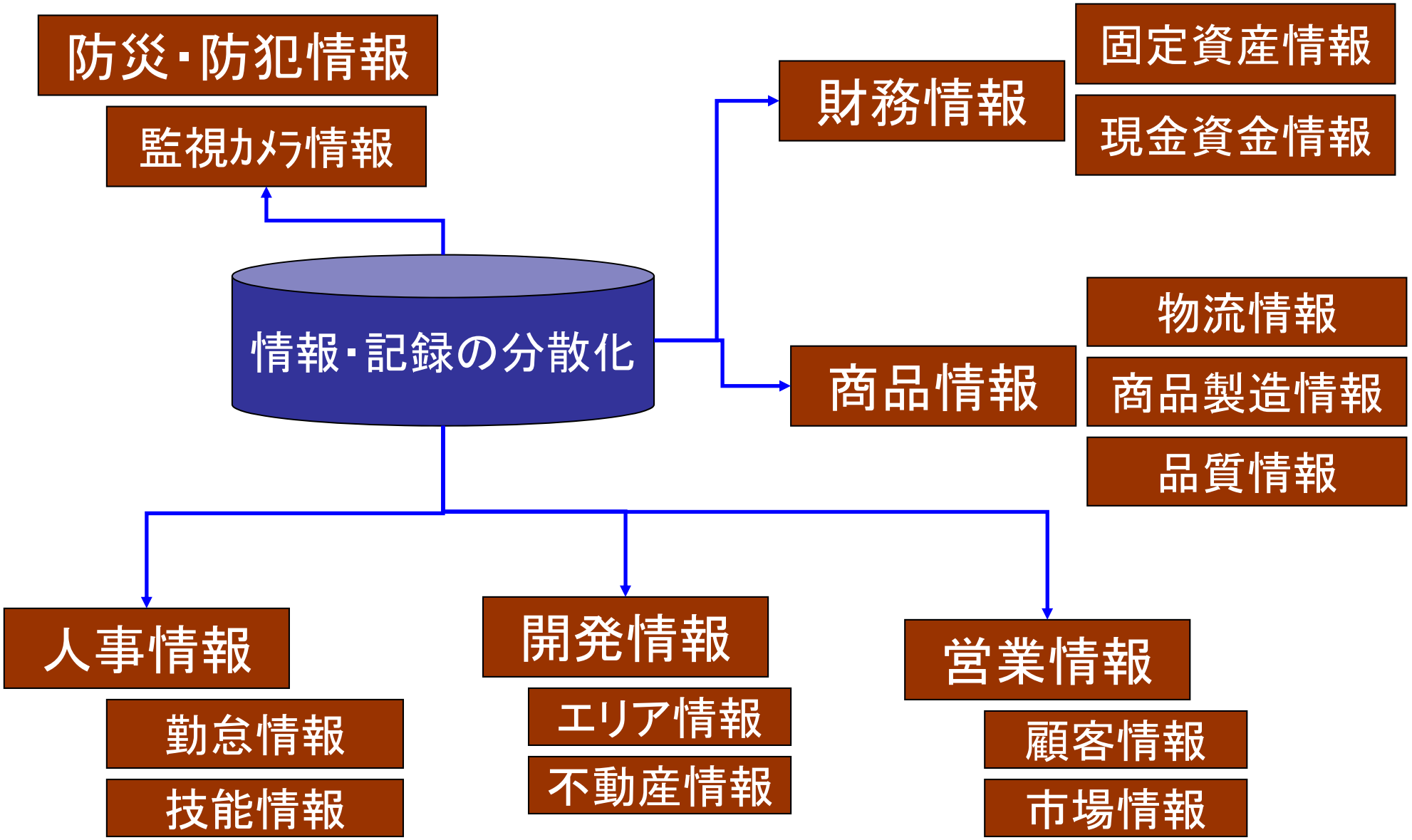
4-2. 階層別リスクマネジメントの変化



4-3.急激な社会変化への適応（グローカルの進展）

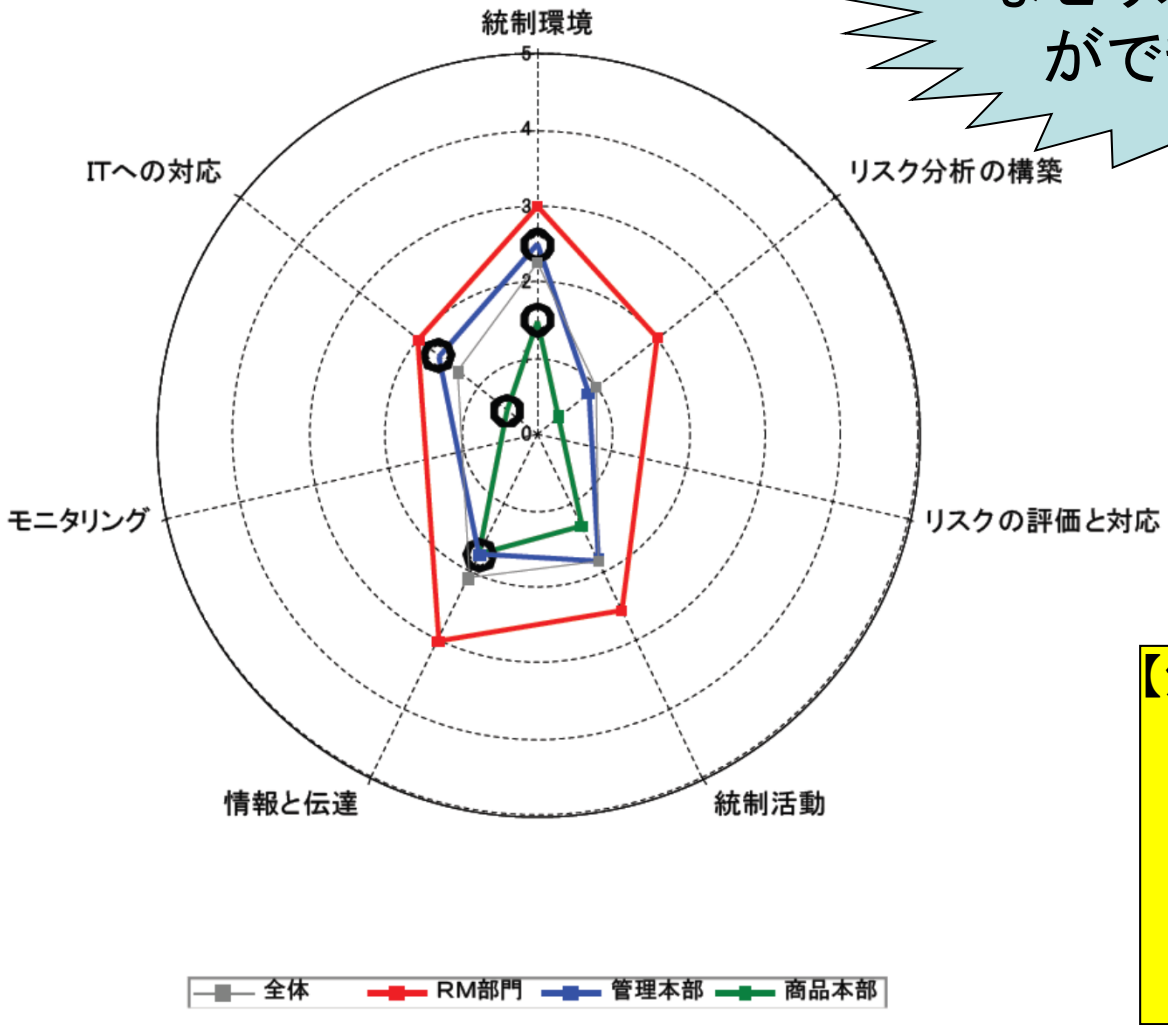
1.小売業が地元支援（ローカルニーズ）へ対応
　ネットスーパー、御用聞きの復活
2.買物頻度の増加（毎日）とコミュニケーションの場を求める⇒半径200m～500mの商圏
3.単身世帯の急増による少量パック（使いきり）
4.健康志向（無添加、有機農法、地産地消）

4-4.中小小売業に関連する情報



5-1.評価レーダーチャート・・・内部統制（2011年）

会社全体



疑問

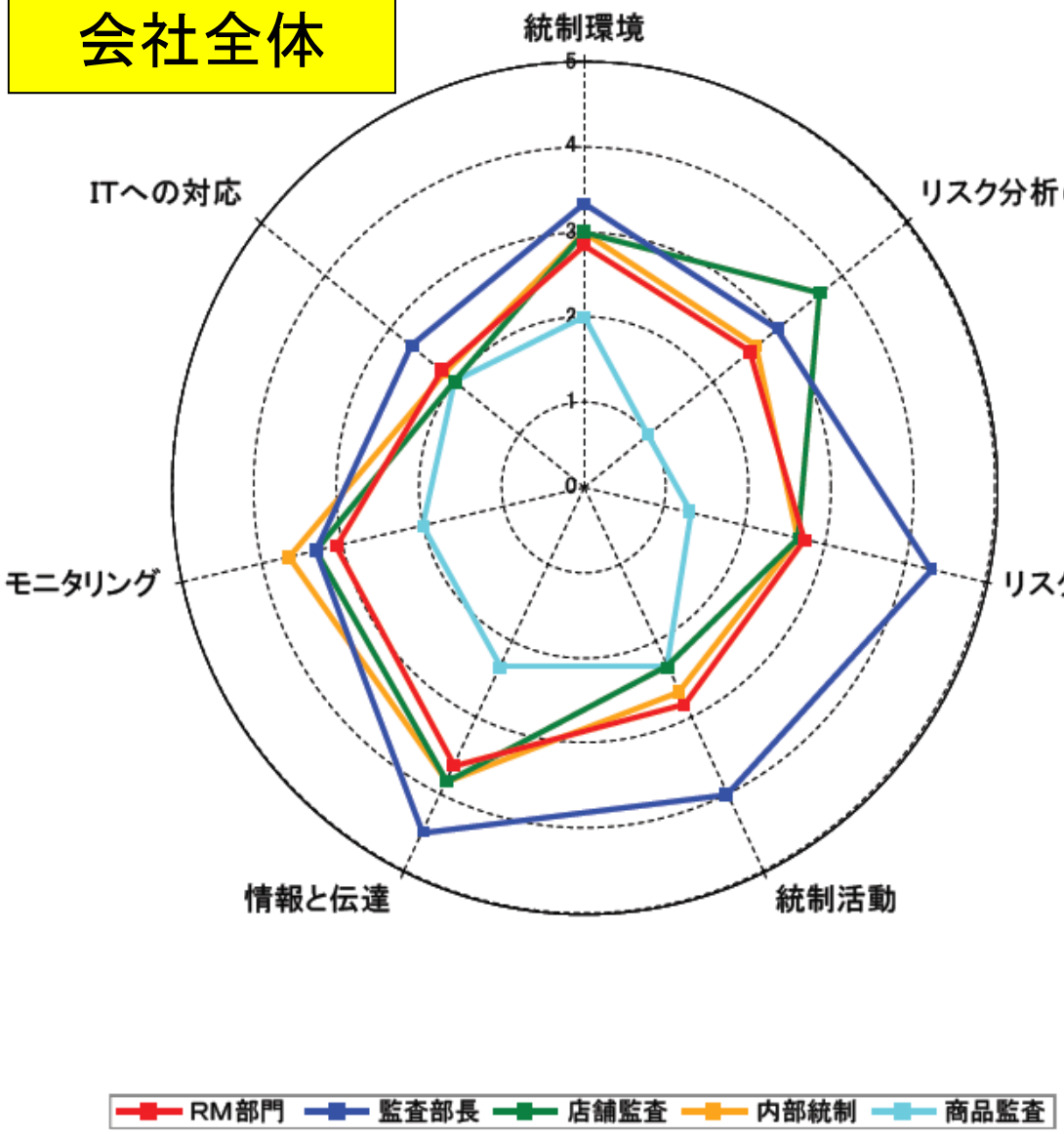
なぜリスク分析や評価ができないのか？

表面的な理解
納得していない

【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
- 仕入部門の評価が低いのは教育機会が少ない
- 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

5-2.評価レーダーチャート・・・内部統制（2013年）

会社全体



前進！
内部統制評価がスタートして4年目

RM部門が評価して報告

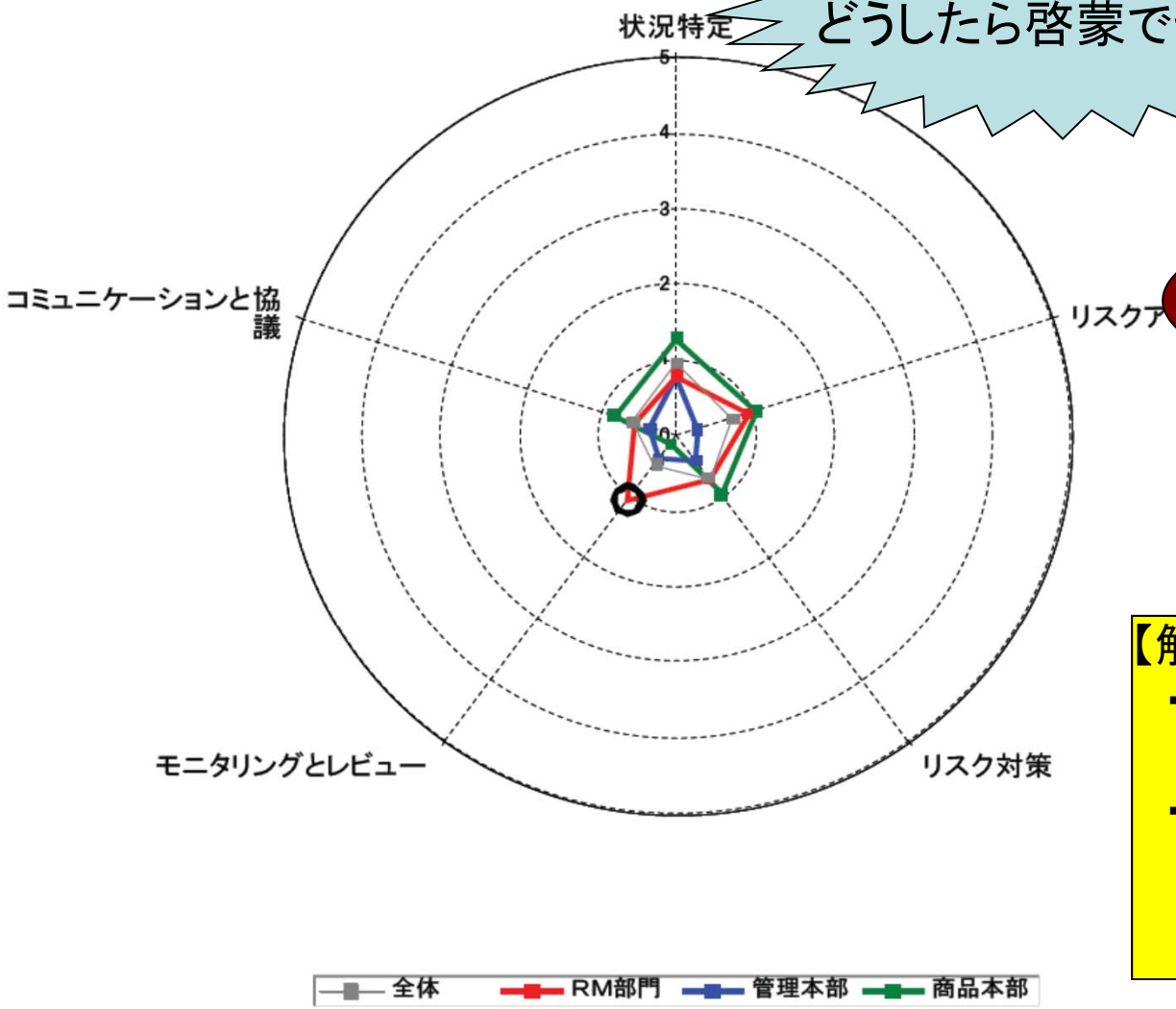
【解説】 クィックスタート版
- リスク分析、リスク評価が進んだ
- 情報と伝達⇒コミュニケーションが良くなってきた
- 全体としてレベル3.0となっている
  ITへの対応が遅れている。

5-3.評価レーダーチャート・・・事業継続（2011年）

会社全体

疑問
事業継続の考え方を
どうしたら啓蒙できる？

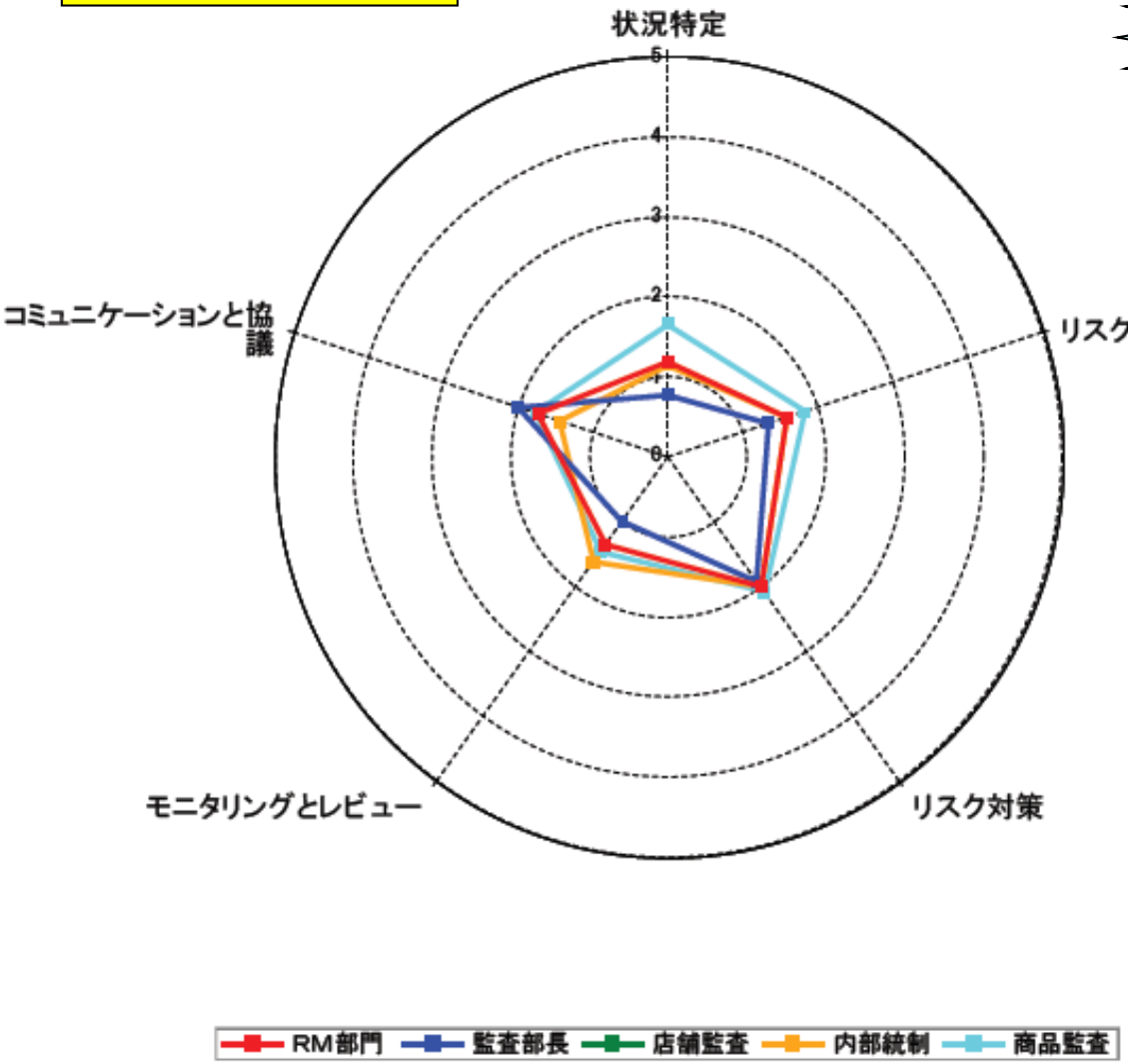
リスク情報の共有化
リスク・コミュニケーション構築



【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。

5-4.評価レーダーチャート・・・事業継続（2013年）

会社全体



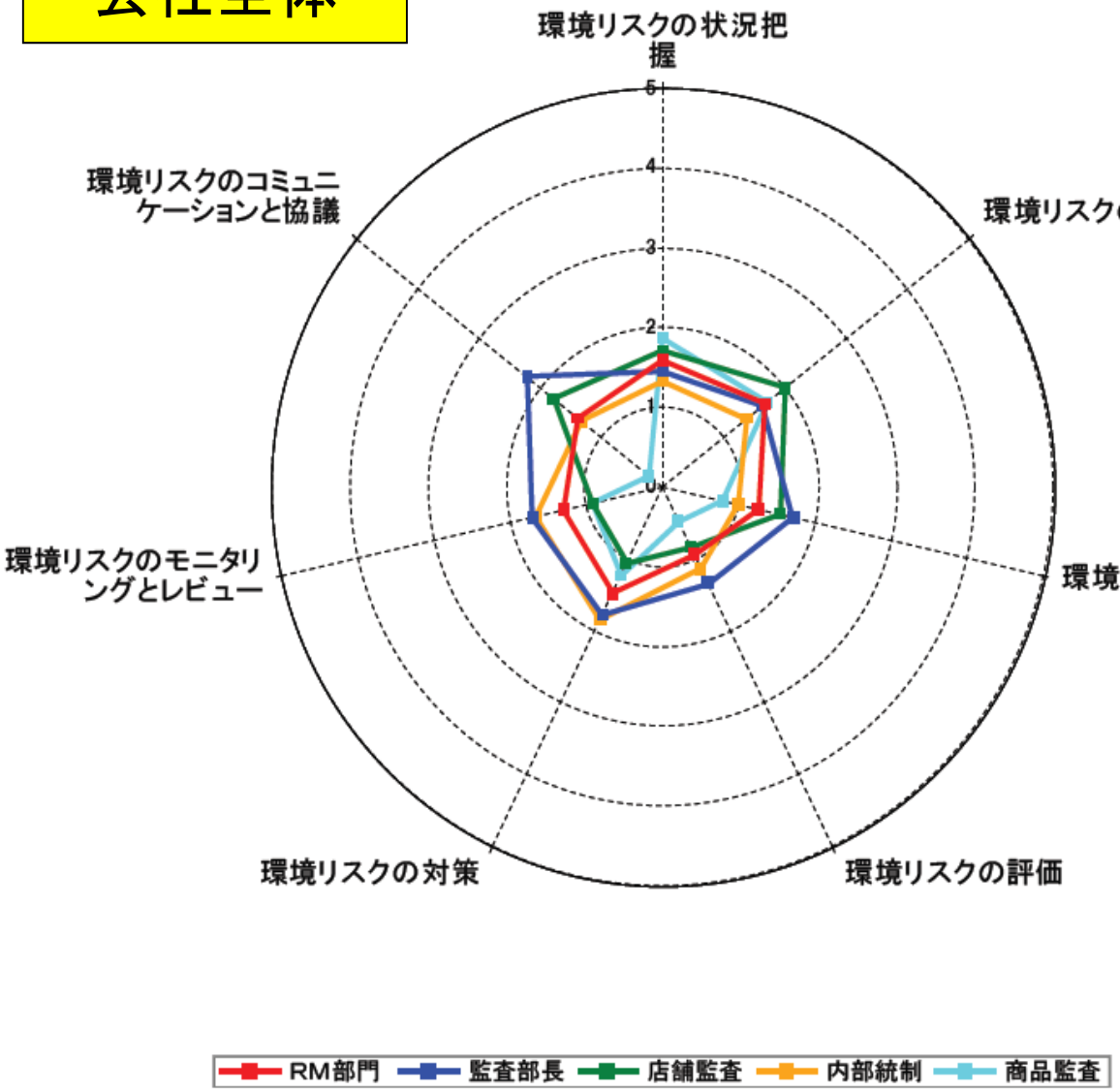
少し前進
リスク・マネジメントの意識と部門でのリスク評価

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

5-5.評価レーダーチャート・・・環境（2013年）

会社全体



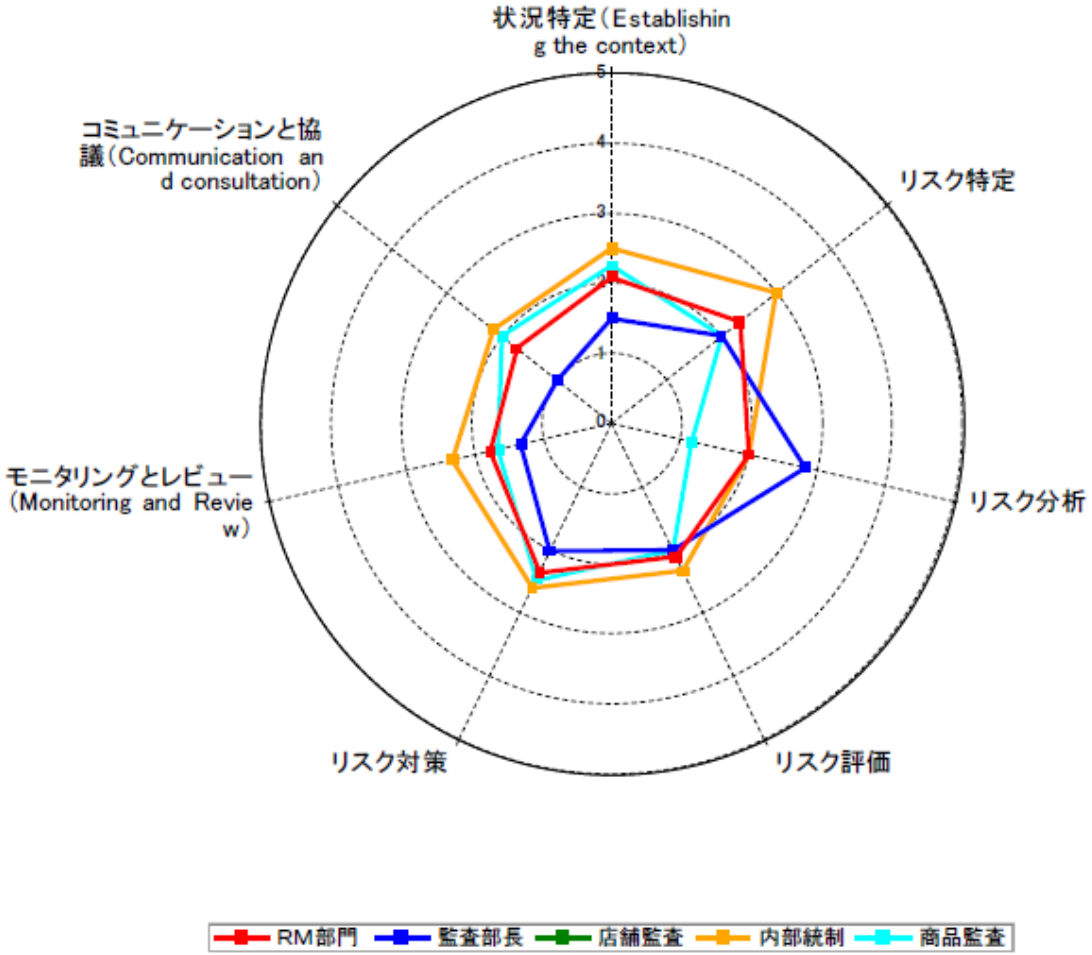
一部の人が頑張る
環境MSの導入準備
これから！

RM部門が
体制構築中

【解説】 クィックスタート版
・一部の人が頑張って準備している
・リスクの特定・分析・評価がされていない⇒まず評価してみたい
・全体としてレベル1.5となっている
まだまだ認知されていない

5-6.評価レーダーチャート・・・情報セキュリティ（2013年）

会社全体



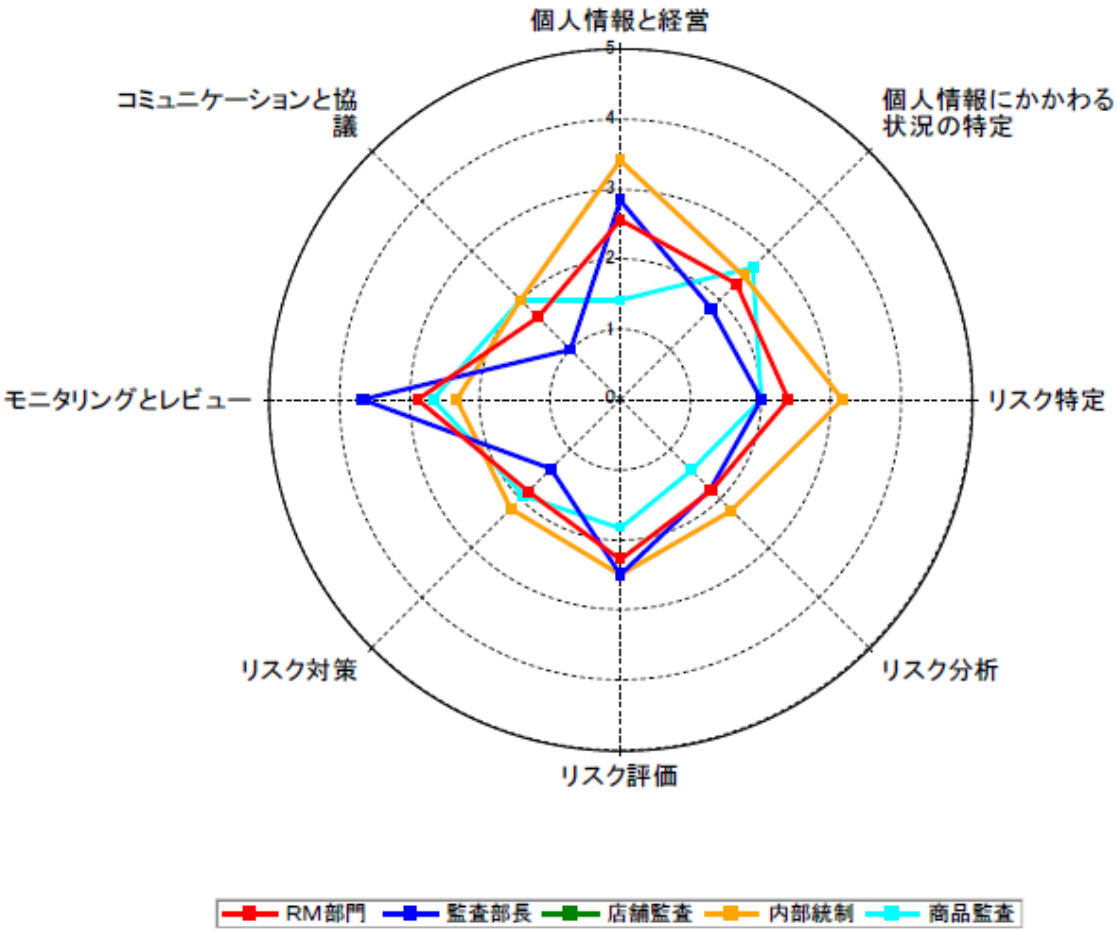
一部の人が頑張る
情報セキュリティの理解
これから！

RM部門が
体制構築中

【解説】 クィックスタート版
- 一部の人が頑張って準備している
- リスクの評価、コミュニケーションがされていない⇒まず評価してみたい
- 全体としてレベル2.0となっている
  まだまだ認知されていない

5-7.評価レーダーチャート・・・個人情報保護（2013年）

会社全体



進んだ！
監査指摘で現場に
変化が出ている！

RM部門が
全社啓蒙中

【解説】 クィックスタート版
- ガイドブックで啓蒙している
- リスクの特定・モニタリングがされてきた⇒コミュニケーションが弱い
- 全体としてレベル2.5となっている
  PDCAを回して浸透させたい

5-8.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

5-8.リスクマネジメントシステムの成熟度モデルの考え方

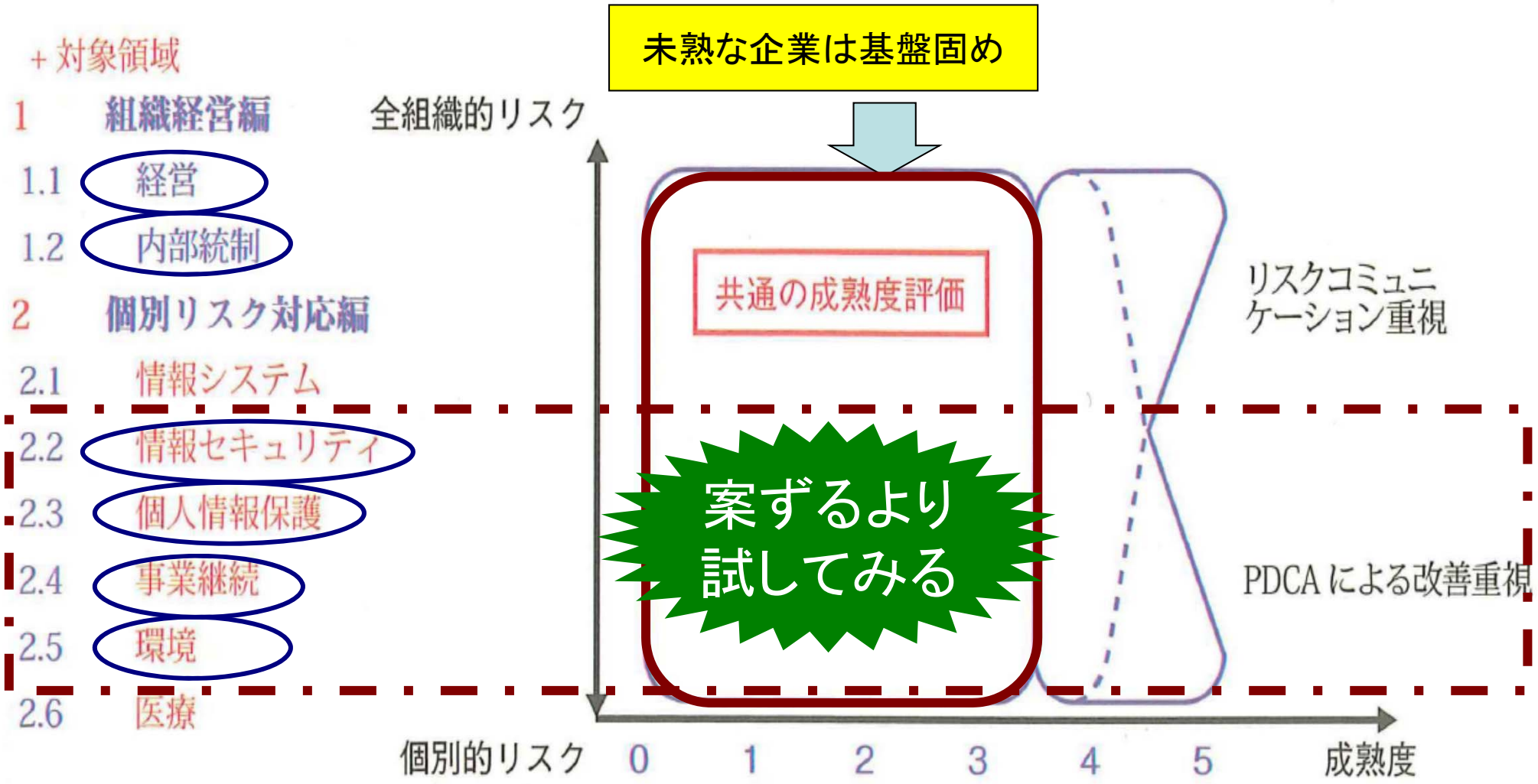


図 1-3.　リスクマネジメントの対象領域と成熟度の定義

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

5-9.仮説事例・・・個人情報保護による評価

個人情報保護の成熟度モデル

評価レベル		摘要例
0	未認識・未対応	・個人情報保護について知らない。 ・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	・コールセンターでは、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、規程どう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。

リスク社会で勝ち抜くためのリスクマネジメント−JRMS2010−より

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

5-10. 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

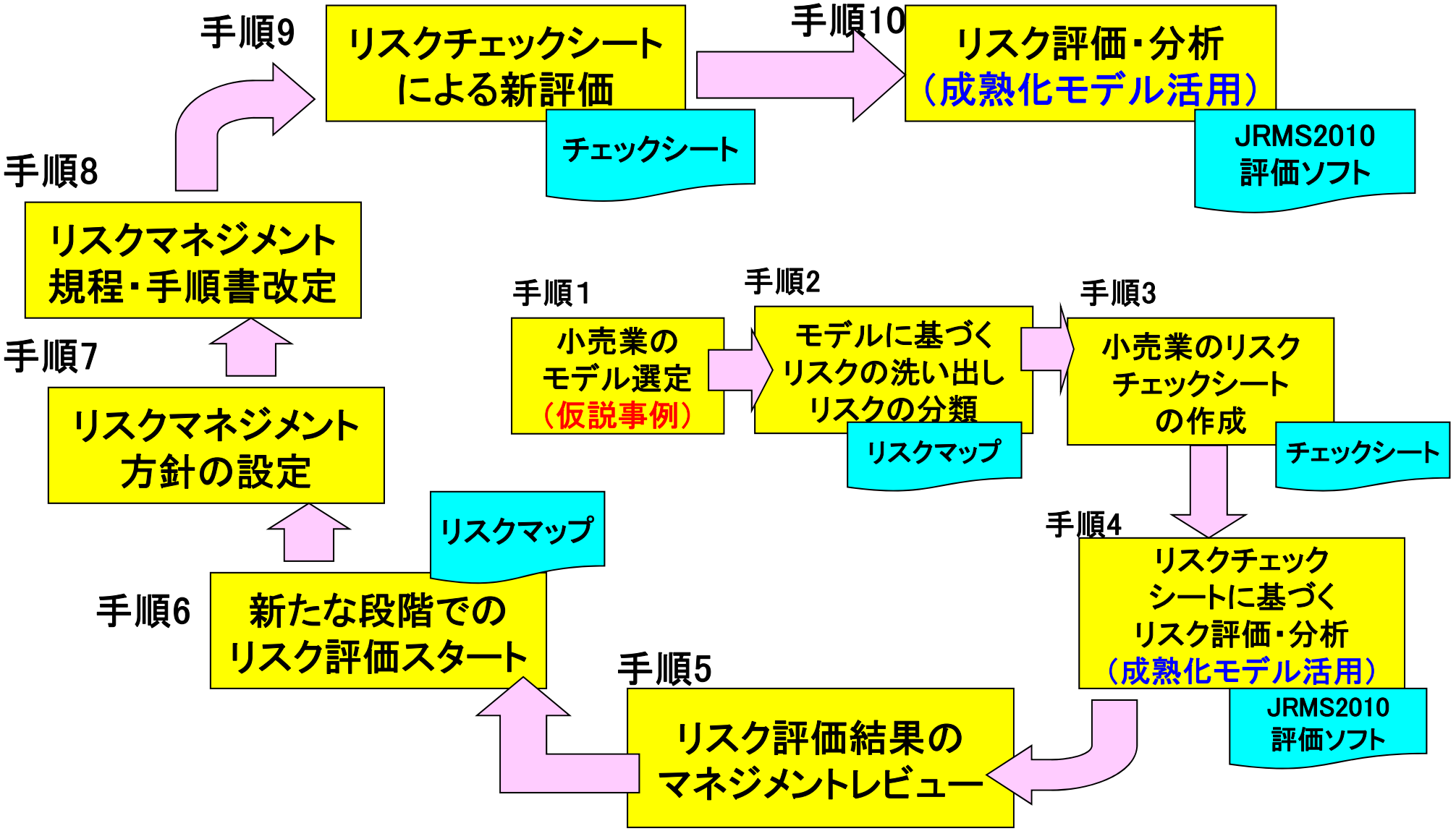
成熟度の評価レベル		定　義	摘要例
0	未認識・未対応	対象のリスクに対して、インシデントの発生まで何の対応もしていない。	・対象のリスクに対する認識もリスクを管理する認識もなく、対応方法について知識を持っている要員もいない。 ・インシデントの発生により、最大限の被害を受ける。
1	個人ごとによる対応	対象のリスクに対して個人的な対応を実施している。	・対象のリスクに対する認識や対応方法は、個人に依存している。 ・発生した個別のインシデントに対し、各個人が個人的な対応を行う。 ・インシデントの発生による被害は、誰が対応したかにより、大きく異なる。
2	部門ごとによる対応	対象のリスクに対する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。

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

5-11.小売業のリスク評価の流れ（評価⇒2年目）



5-12.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
（事業継続マネジメント）

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
（クライシスマネジメント）

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）

5-13.成熟度モデルを活用して良かったこと

“大きな壁も「現場の理解」が突破する”
現場にノウハウが落ちている（情報交換）

“事業継続における復旧方法は規模に関係なく”
コミュニケーション（絆）と日常訓練（PDCAサイクル）

成熟度レベルの階段を一歩ずつ登り続ける！
あせらずにマネジメントシステムを築いていく

ご静聴ありがとうございました。