

システム監査学会
第24回研究大会

GSCMS(Global Supply Chain Management System)の
事業継続監査の実施ガイドラインについて
—スーパーにおける主たる物流・資金のフロー(モデル)—

2010/06/04

リスクマネジメント研究プロジェクト

(株)NTTデータ 北條 武

0. はじめに

- 活動実績
- 前回までのまとめ
- 今年度の検討結果報告
 - ・ 社会システム全体の概念
 - ・ GSCMの対象範囲
 - ・ 総合／大手スーパーの弱点
 - ・ 階層別リスク分析の必要性
 - ・ リスクマップの作成 ーリスク評価ー
 - ・ リスク分析／評価に基づく社会システムの見直し
 - ・ 情報システムの個別部分と共通部分
 - ・ BCP/BCMIに関する作業の流れ
 - ・ BS25999-2:20007との対応関係
 - ・ GSCM監査実施のガイドライン
 - ・ 今年度の成果と次年度の予定
 - ・ (別紙) GSCMリスクチェックシートの雛形

1. H21年度活動実績(1/2)

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)

H21年度の目標:ガイドラインの作成と試行
 (注意点:BS25999との関わり)

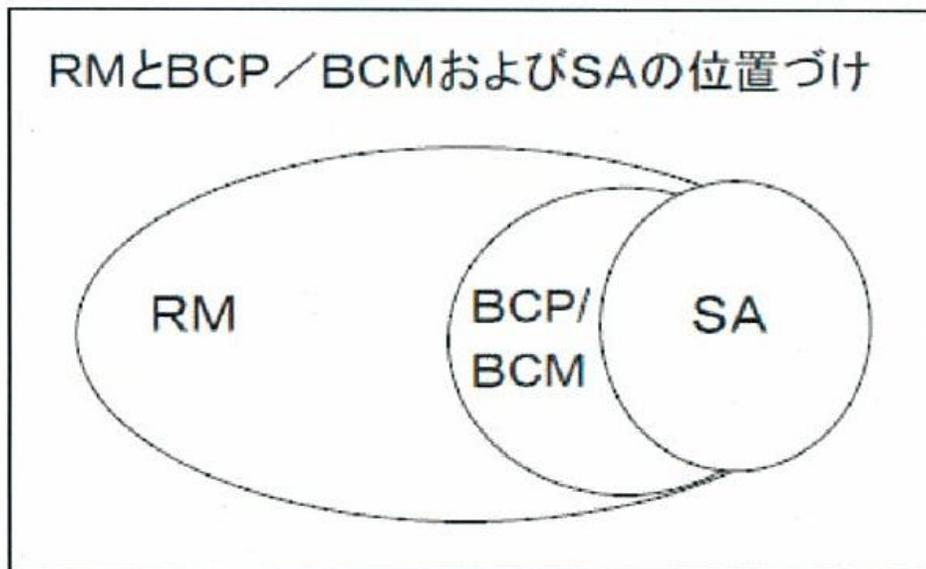
会合	日程	おもな検討内容
1回目	平成21年7月27日(月)	<ul style="list-style-type: none"> ・H21年度キックオフ ・世の中の動向確認
2回目	平成21年8月27日(木)	<ul style="list-style-type: none"> ・大手スーパーの弱点
3回目	平成21年9月24日(木)	<ul style="list-style-type: none"> ・リスクマップ ・リスクの視点 ・システムの個別部分と共通部分
4回目	平成21年10月22日(木)	<ul style="list-style-type: none"> ・BCP/BCMに関する作業の流れ ・階層別のリスク分析の必要性

1. 活動実績(2/2)

会合	日程	活動内容
5回目	平成21年12月10日(木)	・前半の整理 ・今後の予定確認
6回目	平成22年1月28日(木)	・ガイドライン作成に向けたポイントの意識合わせ
7回目	平成22年3月11日(木)	・ガイドラインの頭だしとレビュー
8回目	平成22年4月9日(金)	・発表資料レビュー①
9回目	平成22年5月18日(火)	・発表資料レビュー②

■ 前回までのまとめ

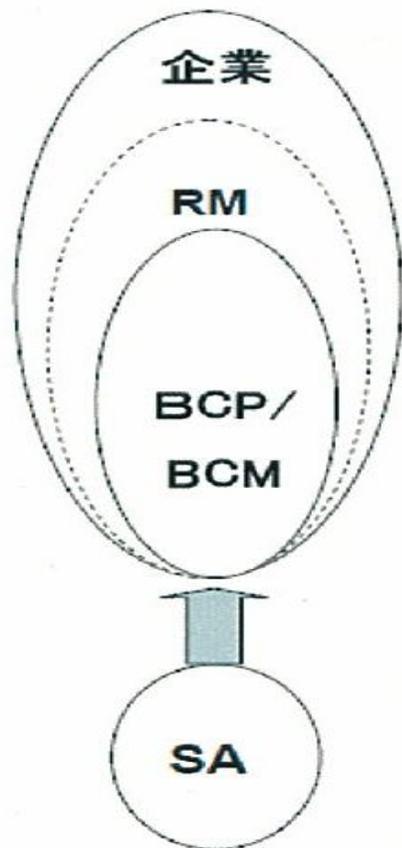
2. RM、BCP/BCMとSAの関連(主眼BCP/BCM)



BCP/BCMを主眼とした場合の関係

- ・リスクマネジメント(RM)
- ・BCP/BCM
- ・システム監査(SA)

3. RM、BCP/BCMとSAの関連(主眼SA)

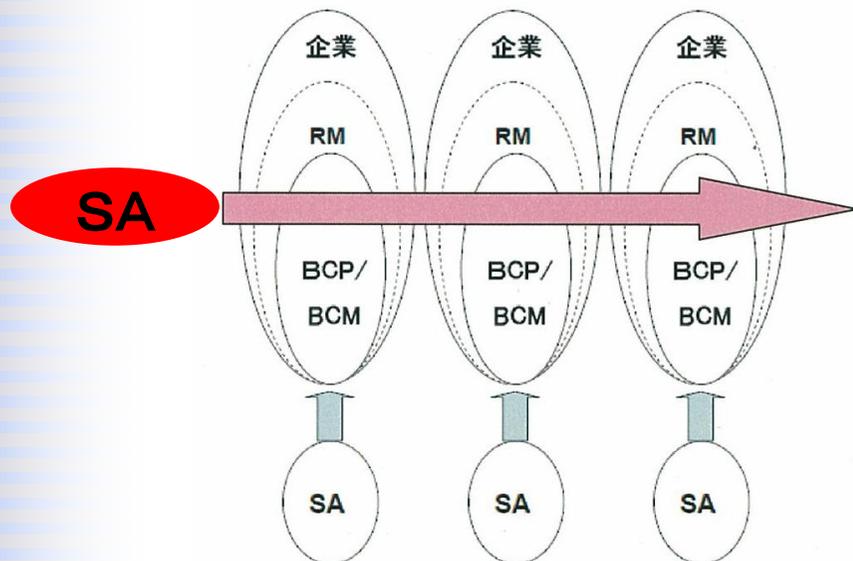
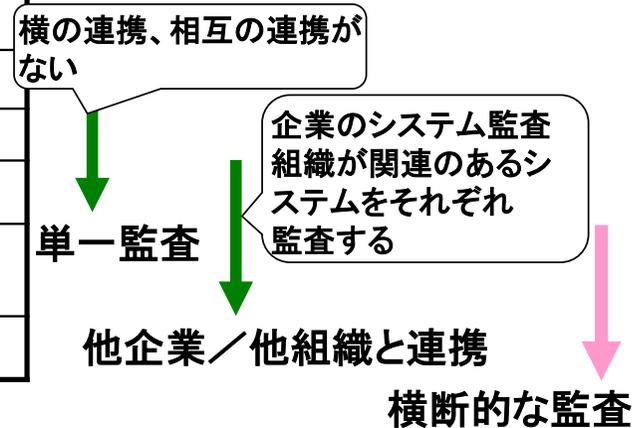


システム監査(SA)を主眼とした場合の関係

- ・リスクマネジメント(RM)
- ・BCP/BCM
- ・システム監査(SA)

4. 統合システムのSAとSCMシステムの横断SAの実施

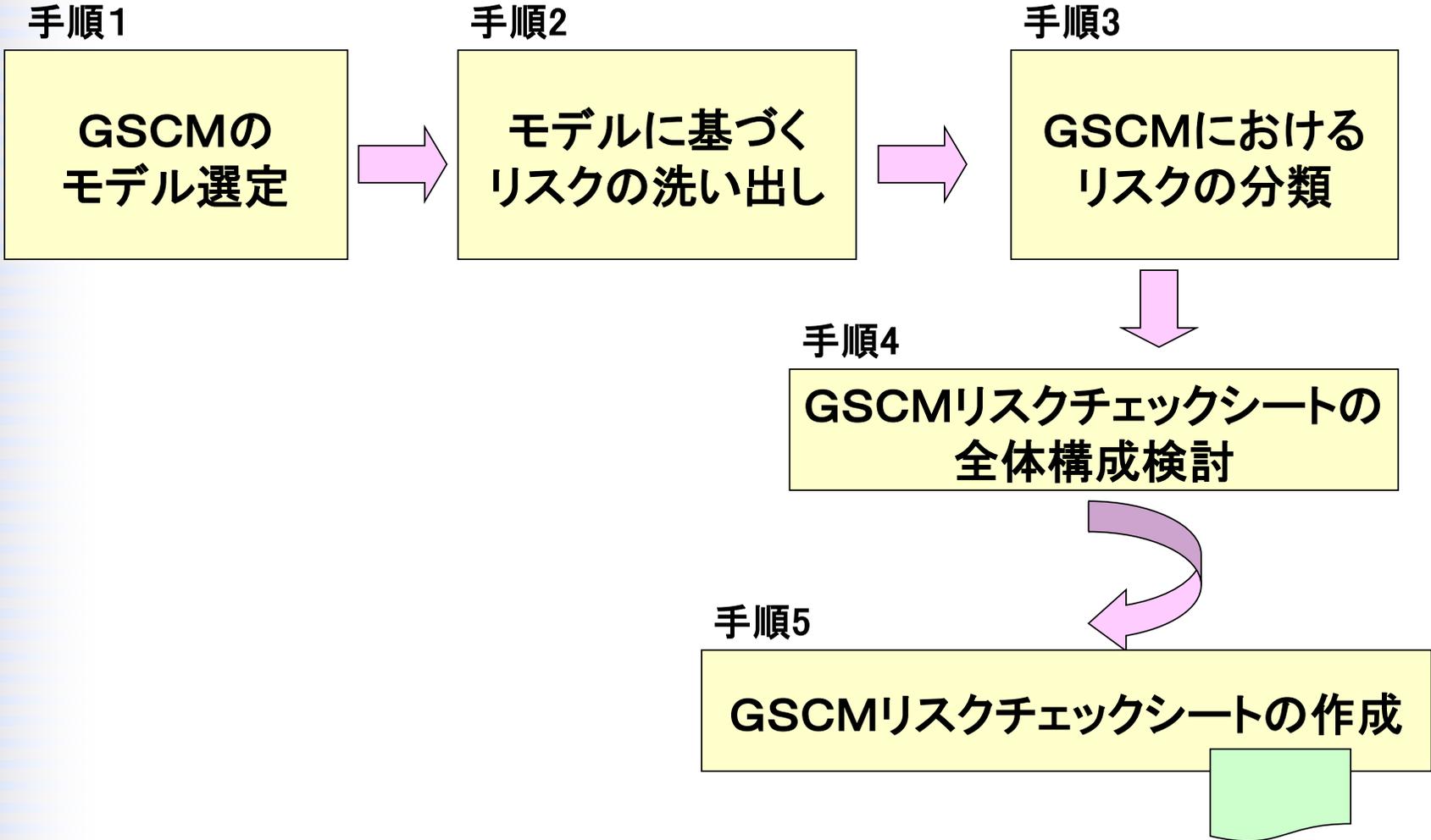
評価尺度／ 達成度	段階	概要
I	初期段階	部分的に行われている。
II	定義段階	マニュアルがあり行われている。
III	管理段階	組織化され、行われている。
IV	制御段階	定期及び不定期の訓練が行われ、且つ定量的な分析とフィードバックが行われている。
V	最適段階	マネジメントサイクル(PDCA)が確立されている。



レベルIVからVに該当

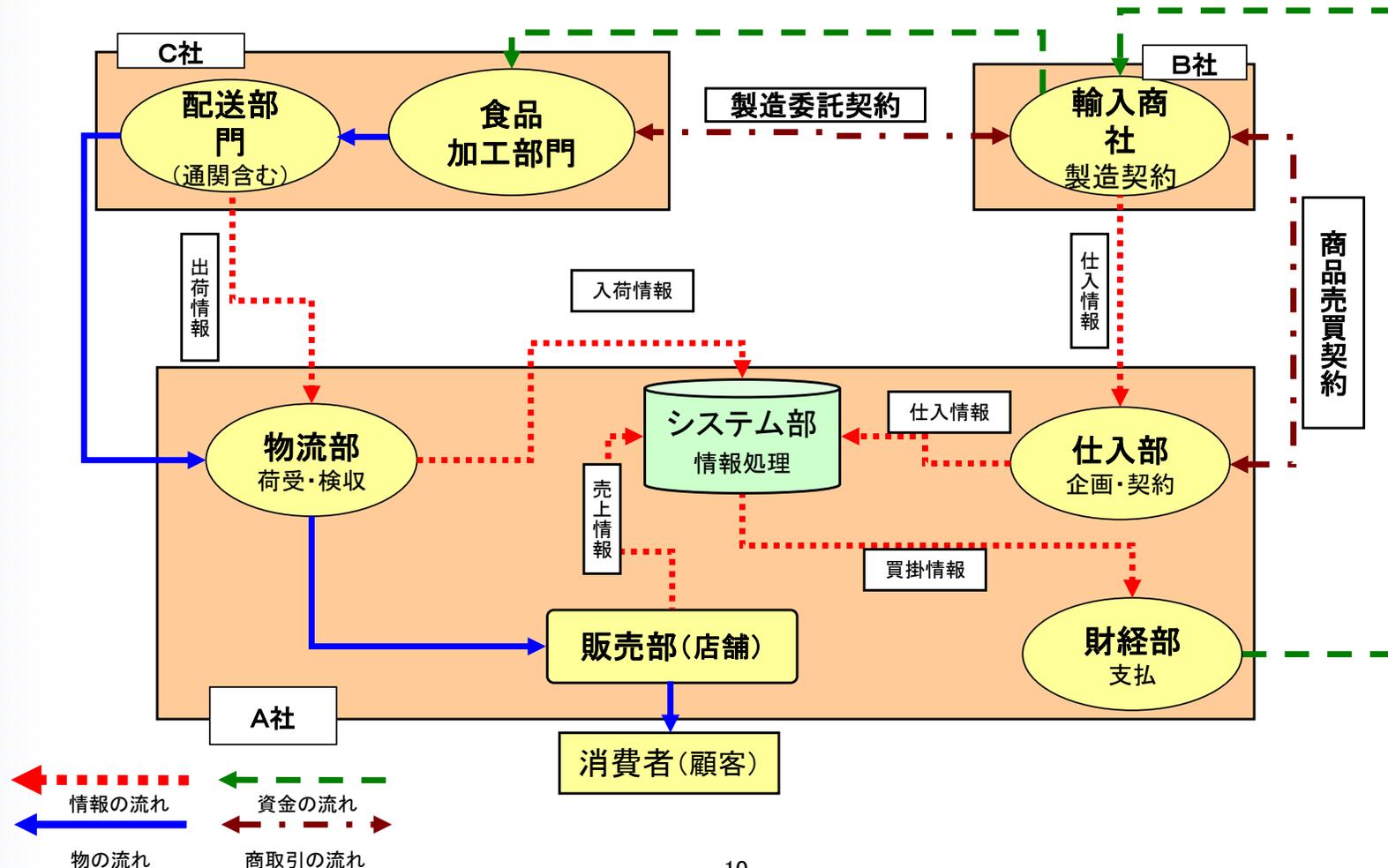
独立したシステム監査組織が横断的にチェックする

5. 昨年度の検討手順



6. 手順① GSCMモデルの選定

スーパーにおける主な物流・情報・資金のフロー(モデル)



7. 手順② 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
ファイナンス	国内外の金融危機に伴う契約先の倒産リスク(資金繰り)
ファイナンス	相手先倒産に対する財務的当てが検討されていないリスク
ファイナンス	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(情報漏えい、業務不履行etc)
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

8. 手順③④ リスク分類とリスクチェックシート全体構成の検討

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VI項 共通業務

第4項 人的資源管理

4.3教育・訓練(4項目)

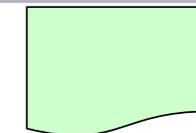
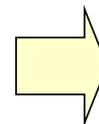
第7項 災害対策(13項目)

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

基本事項

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

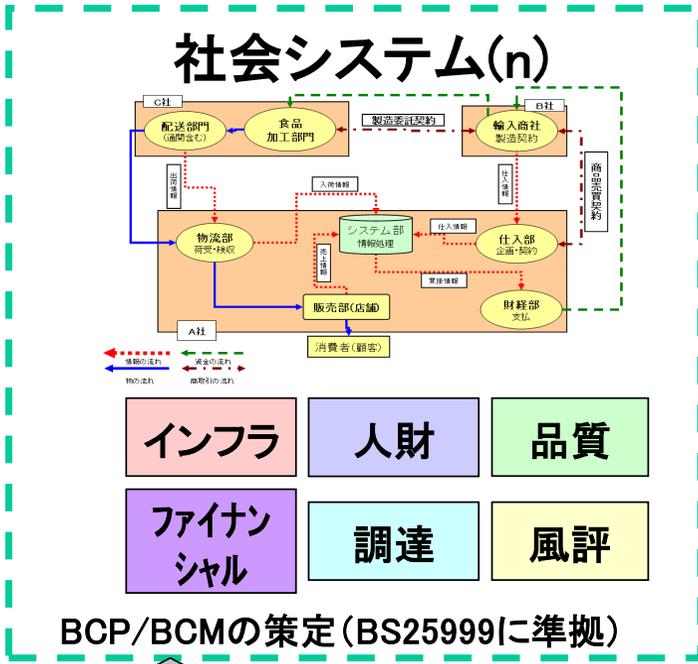
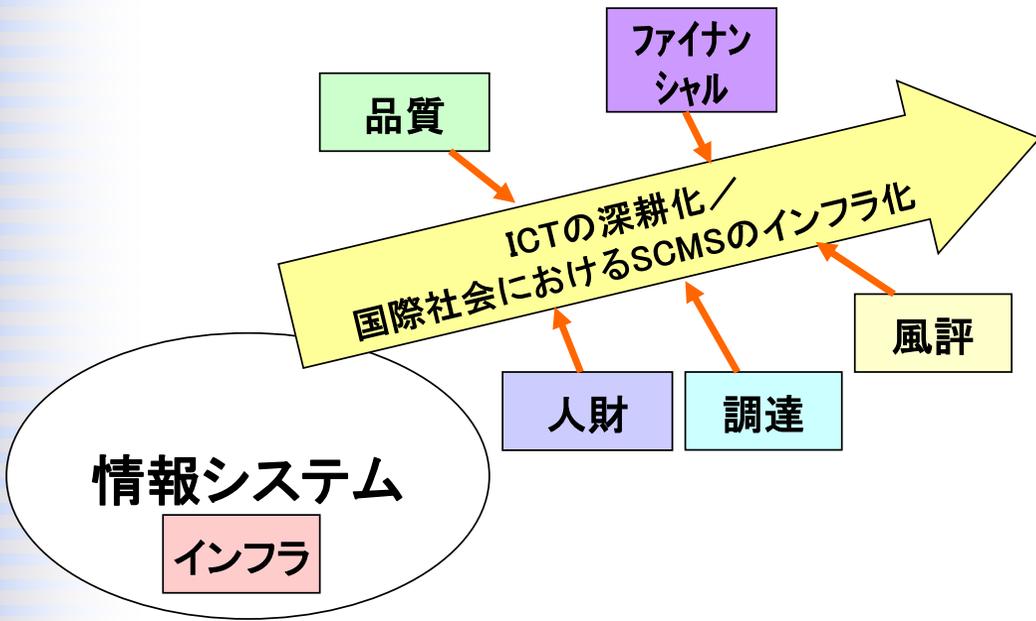
ファイナンシャル

風評

人財

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

9. (補足)情報システムの進化のシステム監査の概念図



取引先にBCP/BCMを要請するのではなく、“社会システム”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

BCP/BCMの策定 (BS25999に準拠)

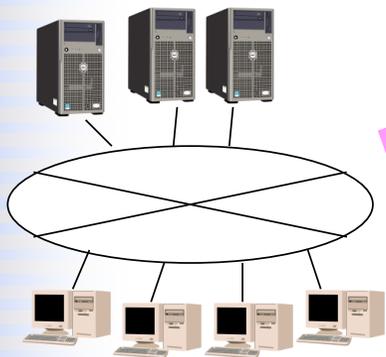
■今年度の検討結果報告

11. GSCMの対象範囲

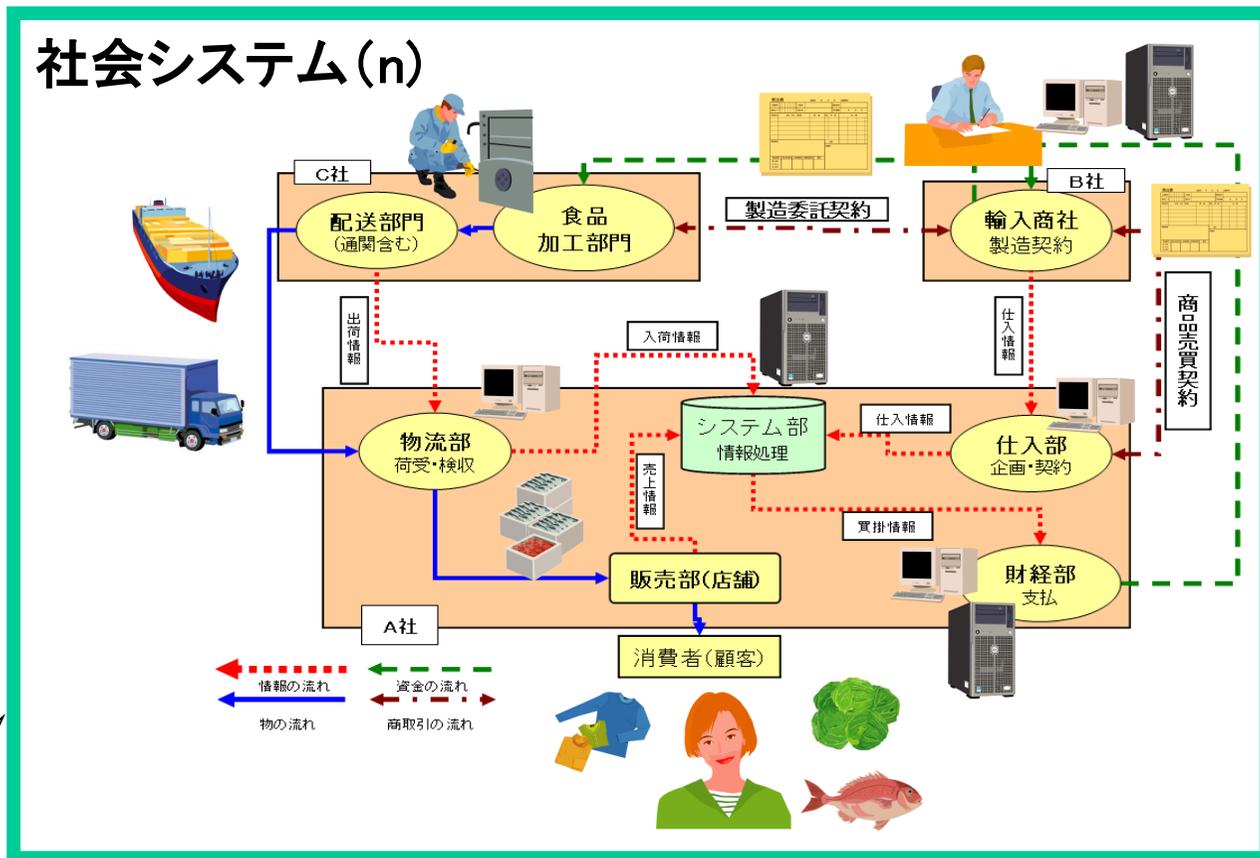
【留意点】

- ・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(n)



信頼関係の構築と維持が第一である

12. 総合／大手スーパーの弱点

総合／大手スーパー ↔ 個人商店／専門店

総合／大手スーパーの弱点：目利きがない、または継承されていない
⇒「旬」があり、「個体差」がある食品素材を扱いにくい
⇒事業継続のリスクがある

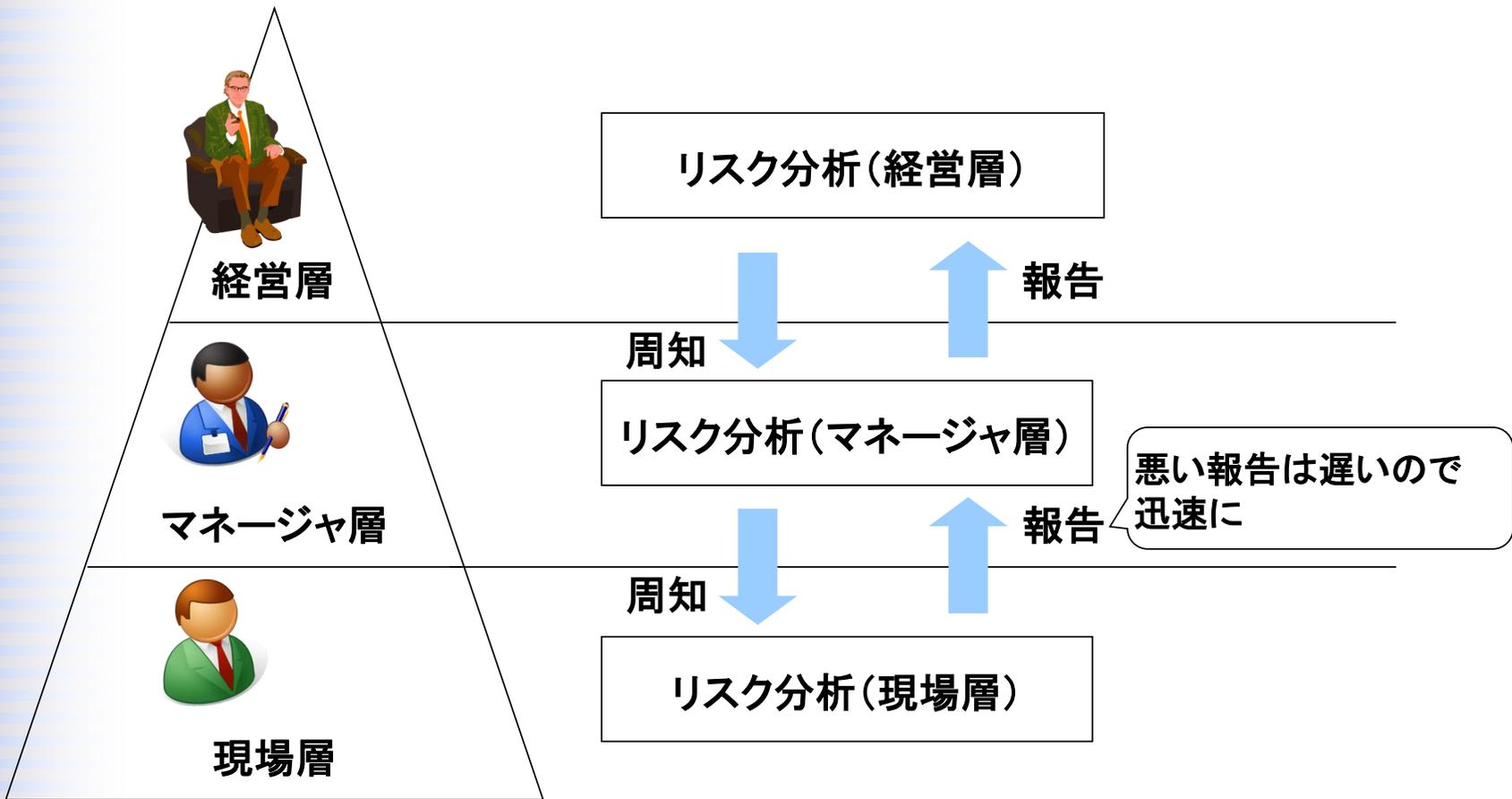
現場だけでなく、経営者も意識する必要がある

情報システムの肥大化
システム化すべきでない部分も
システム化、またはアウトソーシング

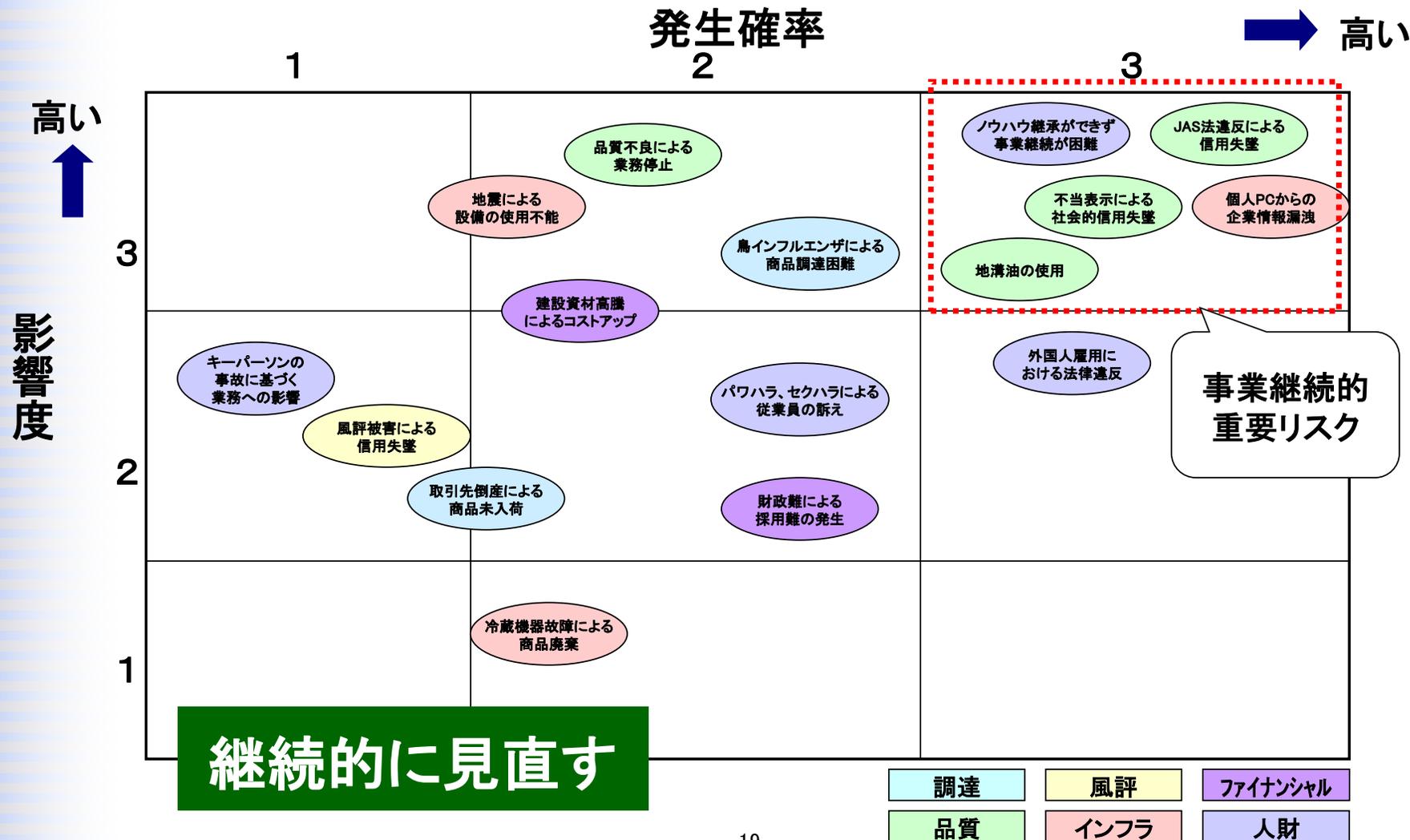
~~従業員（目利き）と顧客の
長年の信頼関係~~

従業員的能力低下

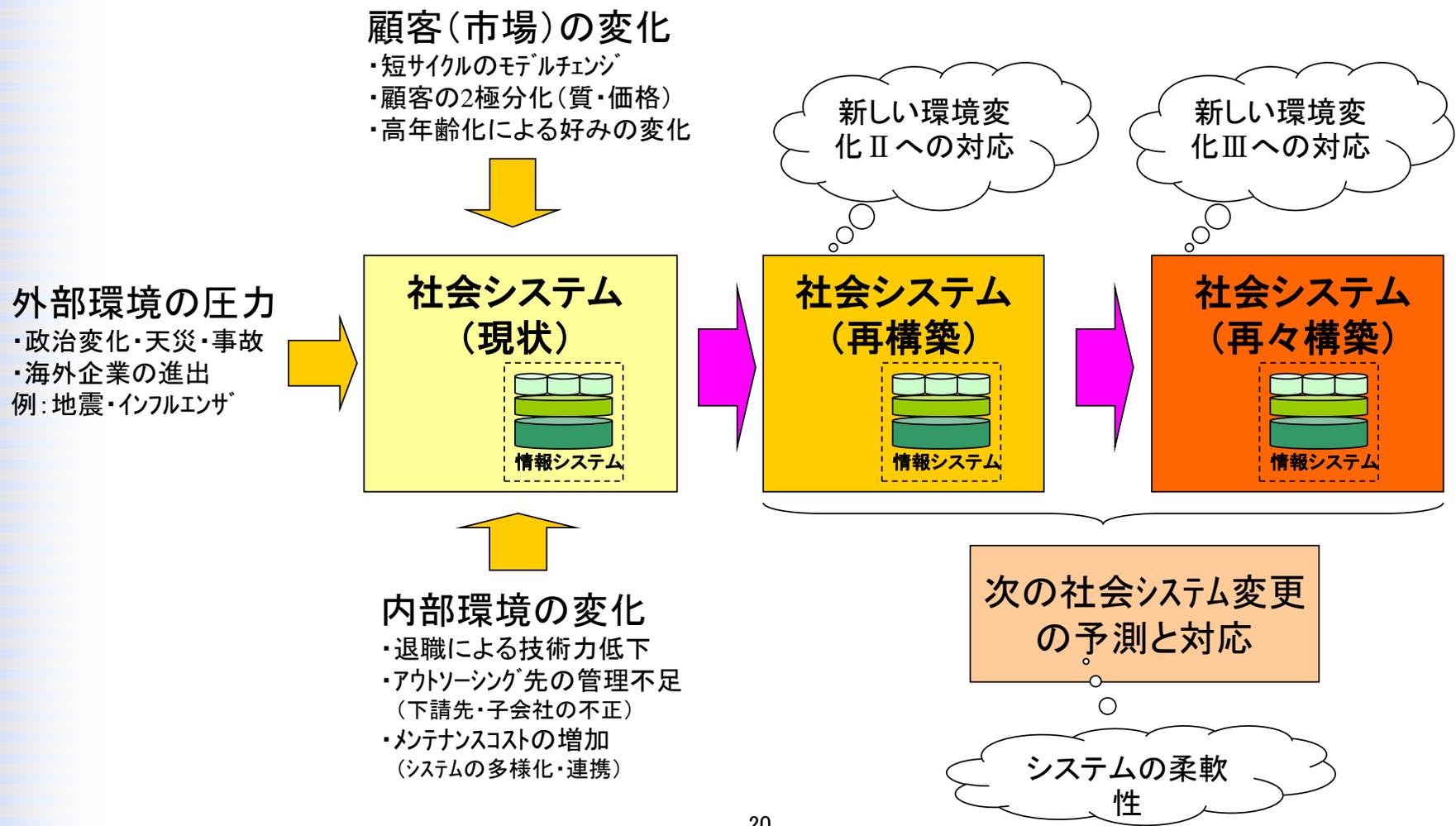
13. 階層別リスク分析の必要性



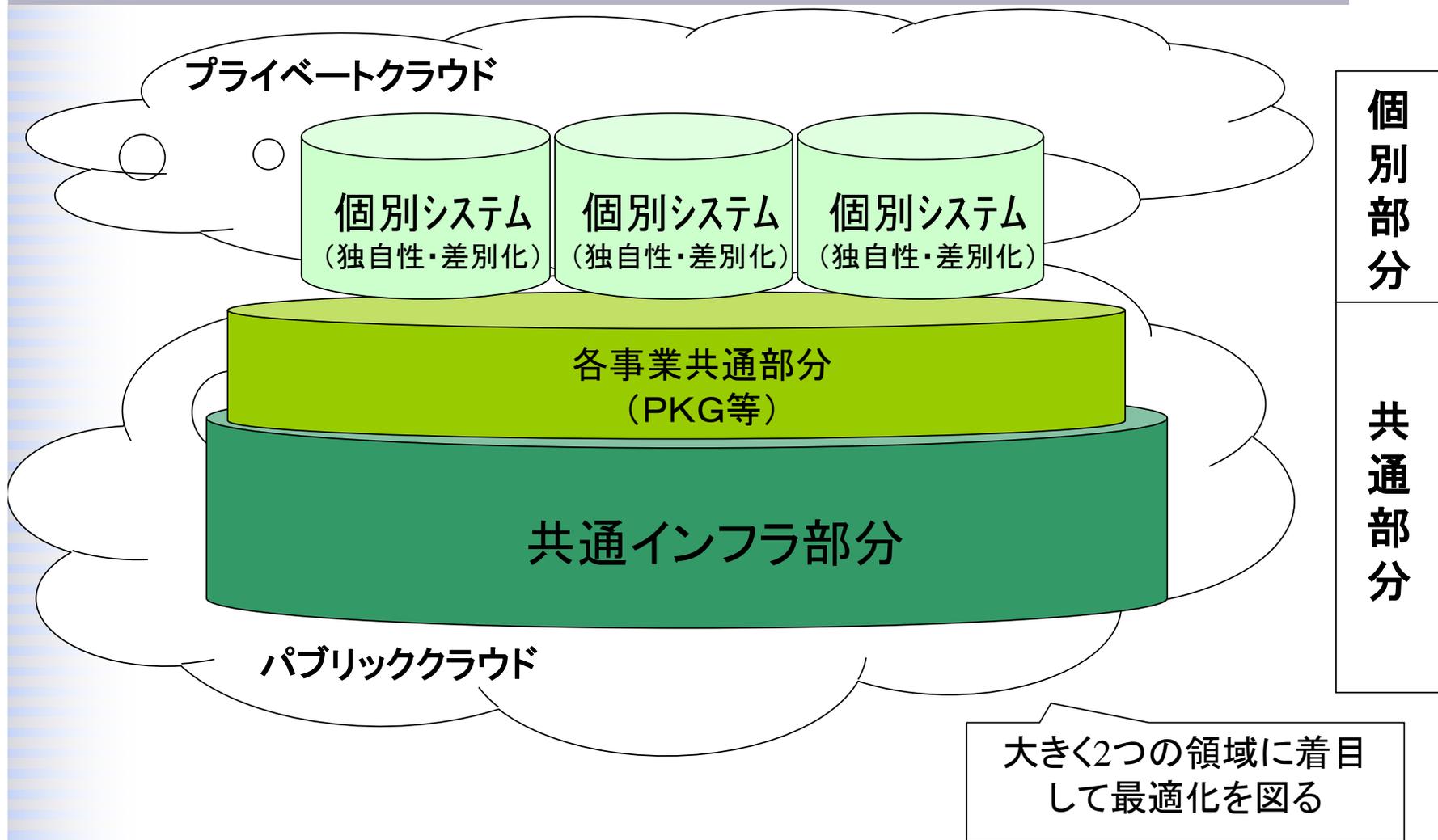
14. リスクマップの作成ーリスク評価ー



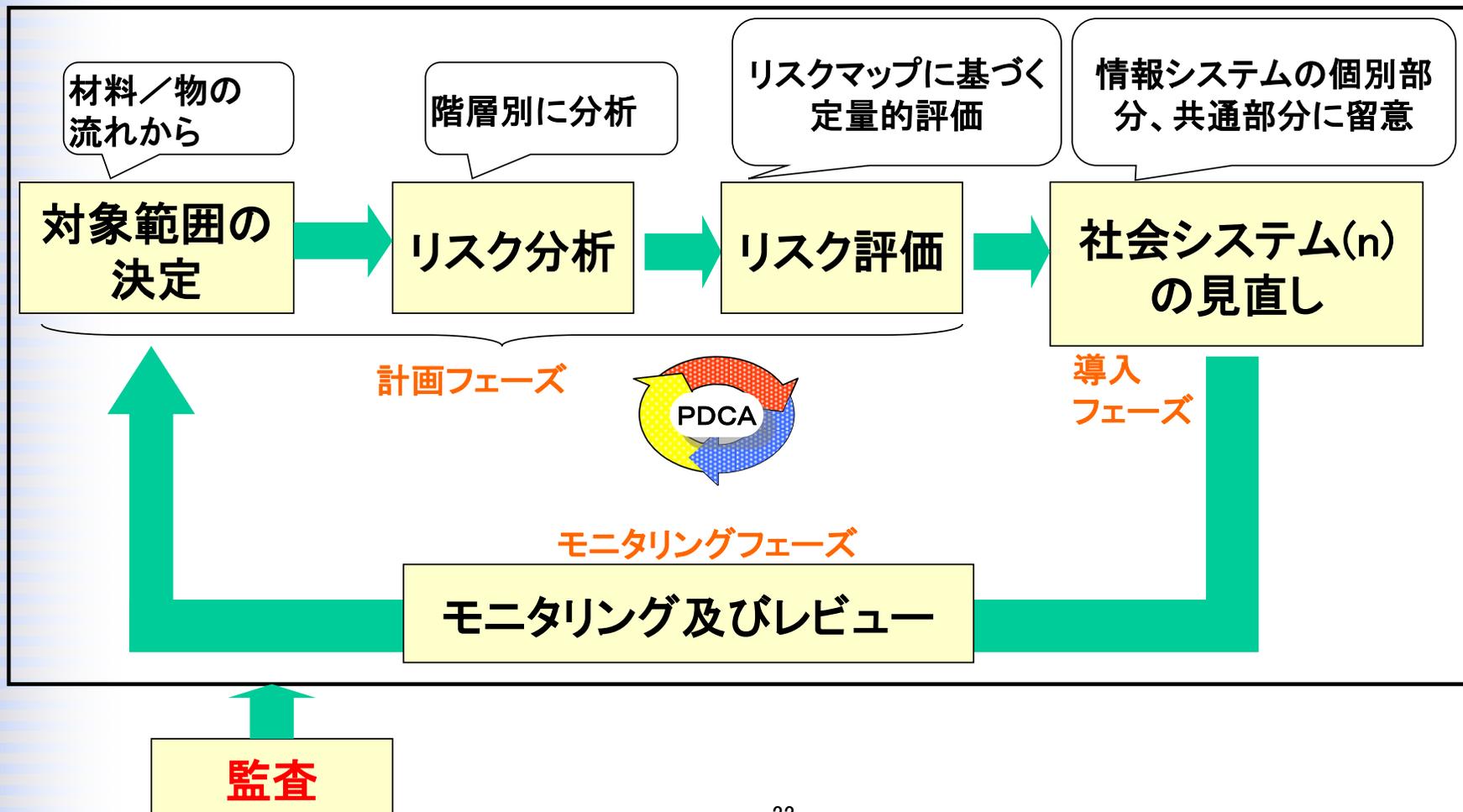
15. リスク分析／評価に基づく社会システムの見直し



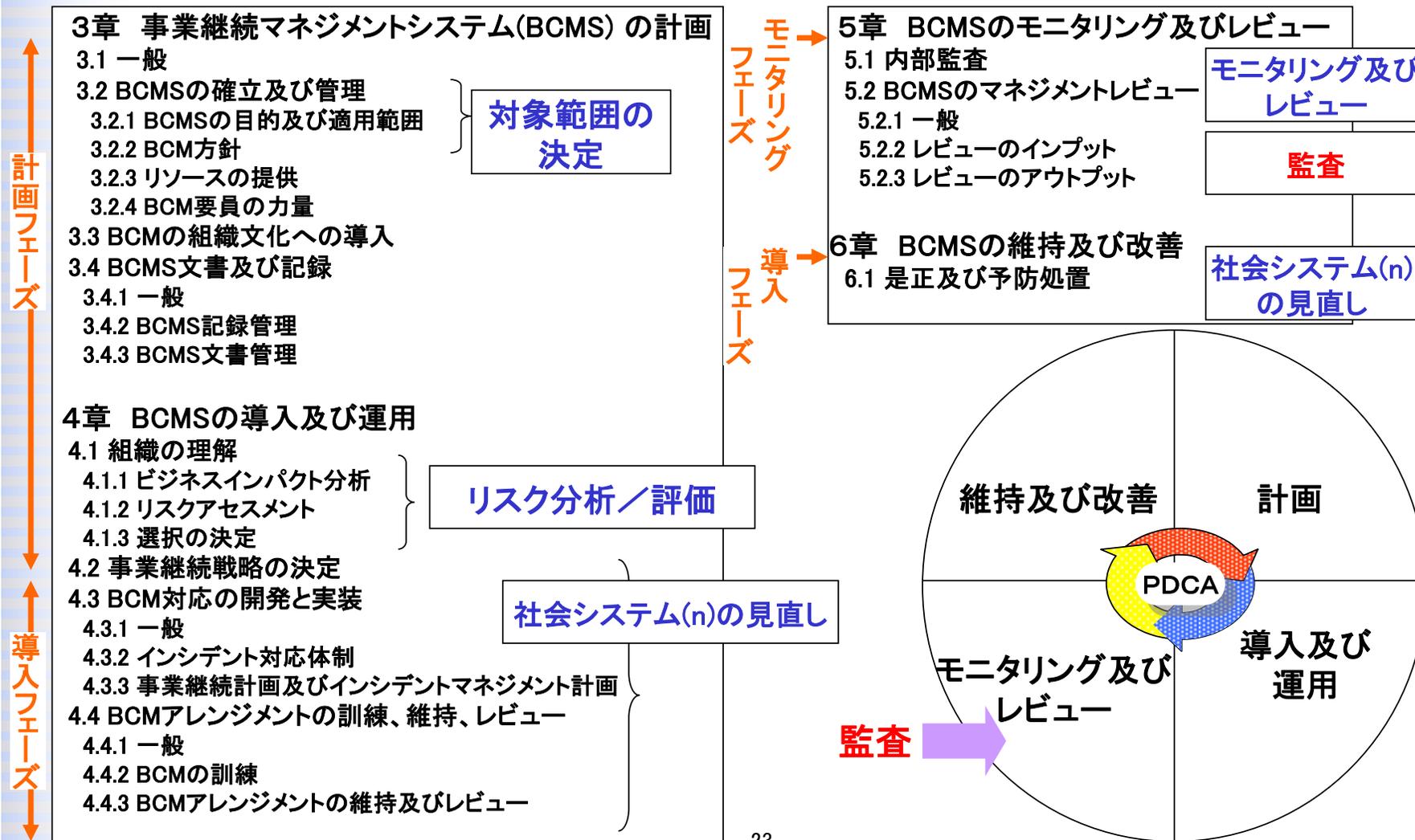
16. 情報システムの個別部分と共通部分



17. BCP/BCMに関する作業の流れ



18. BS25999-2:20007との対応関係



19. GSCM監査実施のガイドライン(1/7)

BS25999-2:20007のおもな構成要素を踏まえつつ、ガイドラインを作成

1. 監査の目的

監査対象はGSCMを構成する情報システムだけではなく、物品調達、品質確保等を含めた、**社会システムとし**、事業継続に向けた維持・改善を目的とする。

2. 経営者へのヒアリング

経営者へヒアリングを行い、**事業継続に向けた方針を確認**する。

- ・物品調達に関する方針
- ・品質に関する方針
- ・風評被害に関する方針
- ・インフラ整備に関する方針
- ・財務手当てに関する方針(収入(営業面) など)
- ・人財育成の方針(熟練者の引継ぎ、若手育成 など)

19. GSCM監査実施のガイドライン(2/7)

3. 監査チームの結成

- ・ 監査メンバ選定
 - ・ GSCMを構成する各組織から選定
 - ・ 物流業務に詳しい者、情報システムに詳しい者、経営に詳しい者等を選定(海外/現地のStaff)
- ・ 独立したシステム監査横断組織の結成(レベルⅣ～Ⅴ)

4. 監査計画の立案

- ・ 中長期計画
- ・ 年度計画

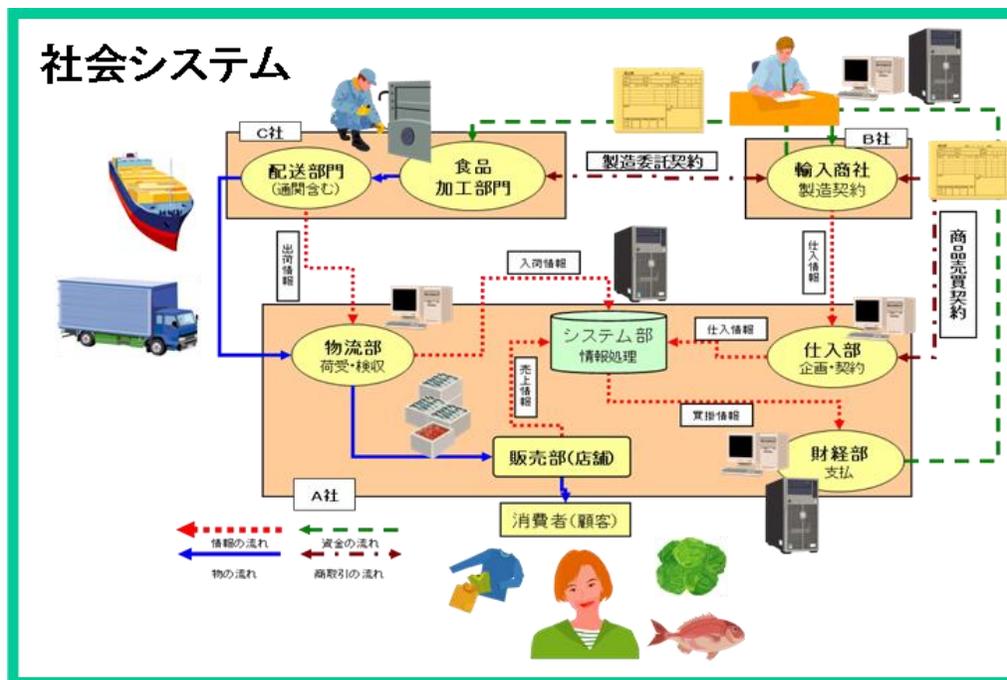
19. GSCM監査実施のガイドライン(3/7)

5. 監査実施手順

① 監査対象とするGSCM範囲の決定

範囲決定: 自責の部分(責任転嫁できない場合),
経営上のKEY-Process

例えば: PB商品における責任、下請法で保護される企業との関係



19. GSCM監査実施のガイドライン(4/7)

②. 監査ポイントの洗い出し

【留意点】

- ・自組織の弱点の洗い出し
- ・階層別のリスクの洗い出し
- ・上記、リスク分析／評価に基づいた、リスクマップの作成
- ・環境の変化に応じた、インフラ整備(情報システムの構築含む)の見直し(内外の環境の変化、BtoP、PtoP)
- ・その他留意事項
 - ・事業遂行上の要: 情流、金流、物流
 - ・発生確率: 過去発生、同業者で発生したものは確率大
例: サイコロステーキのO157、鳥インフルエンザ
 - ・1回の被害額: GSCMの上流でおこる程、被害が大きい
例: 中国倉庫の汚染物質⇒取引のある日本企業すべてに被害
店舗での事故⇒店舗全体へ被害、
部門での事故⇒部門の被害

19. GSCM監査実施のガイドライン(5/7)

③監査チェックシートの作成

②の監査ポイント、留意点に基づいて、別紙雛形シートのカスタマイズを行う。

□全体確認シート

基本事項：事業継続計画の立案、BIA

リスクマネジメント委員会における整備進捗報告

リスク評価を定期的実施(年度更新)

災害時対応計画：全員に周知徹底

例：新型インフルエンザ対応、大規模地震対応

BIA(ビジネスインパクト分析)：
組織にとって重要な業務プロセスが停止・中断した場合、
事業全体が受ける業務上および財務上の影響の度合いを
分析・評価すること。

19. GSCM監査実施のガイドライン(6/7)

□個別リスク確認シート

- **調達**: 海外・国内物流での事件や事故発生時対応、代替の調達ルート準備
- **品質**: 海外製造元・・・品質管理、検査体制
国内製造元・・・品質管理、検査体制
- **風評**: GSCM構成企業、グループ企業での風評
例: 産地偽装表示、禁止添加物使用、児童労働、不法滞在者の労働
- **インフラ**: 停電事故による冷凍庫・冷蔵庫機能停止
情報セキュリティ・・・個人情報情報の漏洩
- **ファイナンシャル**: 金融危機による契約先の倒産
例: 市場の中卸・メーカー(中小企業が中心)
- **人財**: アウトソーシング先、派遣社員との連携
技術力の継承・・・市場での買いつけ、人財育成計画の作成
コンプライアンス・・・個人情報保護等

19. GSCM監査実施のガイドライン(7/7)

6. 監査報告書の提出

監査報告書を作成し、遅滞なく監査の依頼者に提出する。

7. 監査報告に基づく改善指導(フォローアップ)

監査の結果に基づいて適切な改善指導を行う。

20. 今年度の成果と次年度の予定

昨年度までの到達点:

- ・SCMにおけるBCMSとSAのモデル化
- ・GSCMチェックリストの作成

今年度の目標:ガイドラインの作成と試行
(注意点:BS25999との関わり)



今年度の実績:ガイドラインの作成



次年度の目標:ガイドラインの評価

別紙1-1 GSCMリスクチェックシートの雛形

I. 全体確認シート *斜体、太字は前回からのおもな変更点*

分類	チェック項目	チェック欄
基本事項	社会システムに関連した事業継続の方針を策定しているか。	—
	GSCMに関わる社会システムの事業継続の対象範囲を明確にしているか。	
	GSCMに関わる社会システムの事業継続の方針を策定しているか。 <i>(物品調達、品質、風評被害対策、インフラ整備、財務手当て、人財育成)</i>	
	策定した事業継続方針は、文書化しているか。	
	策定した事業継続の方針は、経営方針との整合性が図られているか。	
	<i>自組織の弱点を洗い出し、リスク分析／評価を実施しているか。</i>	
	<i>階層別にリスク分析／評価を実施しているか。</i>	
	<i>リスク分析／評価に基づいたリスクマップを作成しているか。</i>	
	地震等のリスクが社会システムに与える影響範囲を明確にしているか。	
	社会システムの停止等により組織体が被る損失を分析しているか。	
	業務の回復許容時間及び回復優先順位を定めているか。	
	<i>リスク分析／評価に基づいて、事業継続計画、社会システムを見直しているか。</i>	
	事業継続計画は、利害関係者を含んだ組織的体制で立案しているか。	
	事業継続計画は、組織体の長が承認しているか。	

別紙1-2 GSCMリスクチェックシートの雛形

I. 全体確認シート

分類	チェック項目	チェック欄
基本事項	事業継続計画は、全員に周知しているか。(*) ・周知の方法を明確化しているか。 ・周知の時期が適切か。 ・周知されていることを確認しているか。	A社
	B社	
	C社	
	事業継続計画、 社会システム は、必要に応じて見直しているか。	—
	GSCMに関わる見直しのルールを明確にしているか。	
	見直しによる変更は、その理由を明確にしているか。	
	変更した計画を組織体の長が承認し、全員に周知しているか。 (*)	
	事業継続計画と整合をとった災害時対応計画を策定しているか。	
	災害時対応計画は組織体の長が承認しているか。 (火山噴火の影響も含む)	
	災害時対応計画の実現可能性を確認しているか。	
災害時対応計画は、全員に周知徹底しているか。 (*)		
災害時対応計画は、必要に応じて見直しているか。		
国内、関係国の法制度(知的財産など)のポイントを認識し、確認しているか。		

(*)のチェック項目：GSCMを構成する会社毎にチェックする。

別紙1-4 GSCMリスクチェックシートの雛形

事業継続計画(BCP)を策定するにあたり、次の個別リスクを確認することとする。

Ⅱ. 個別リスク確認シート

Page1

分類	チェック項目	チェック欄
調達	海外の物流に支障を来たすことがないことを社会情勢を踏まえて確認しているか。	
	国内の物流に支障を来たすことがないことを社会情勢を踏まえて確認しているか。	
	売れない商品(不振在庫)が溜まり、売れる商品(流行)を仕入ることができないなど、在庫計画を適切に見直しているか。	
	複数の調達ルートを、日常整理しているか。 (正規の調達先の不測の事態に対して、大体となる調達先を検討していること。 できれば、不測の事態に対して、その予備となる候補先と合意をしておくことが望ましい。)	
	複数の調達ルートをまたそれは定期的に見直しをしているか。	
	予備的な調達先の製造活動、経営活動を定期的に把握しているか。	
	配送するトラック、乗用車の点検を定期的実施しているか。	
	安全運転の講習会を定期的実施しているか。	

別紙1-5 GSCMリスクチェックシートの雛形

Ⅱ. 個別リスク確認シート

Page2

分類	チェック項目	チェック欄
品質	海外製造元は品質管理を計画し、実施していることを確認しているか。	
	海外製造元の検査体制を確認し、不良品の防止に努めているか。	
	海外製造元が仕様どおり作成していることを確認しているか。	
	国内製造元は品質管理を計画し、実施していることを確認しているか。	
	国内製造元の検査体制を確認し、不良品の防止に努めているか。	
	国内製造元が仕様どおり作成していることを確認しているか。	
	品質計画(目標)は、消費者(利用者)の動向、競合他社の状況を把握して決定しているか。	
	品質計画(目標)を定期的に見直しているか。	

別紙1-6 GSCMリスクチェックシートの雛形

Ⅱ. 個別リスク確認シート

Page3

分類	チェック項目	チェック欄
風評	GSCM構成企業、グループ企業、社内等との間で風評等に関する情報交換の体制を確立しているか。	
	人財育成は社員による風評リスクを考慮して計画されているか。 (*)	
	辞職・解雇・退職した人(会社に不満を持つ)からの風評リスクが発生しないような対策を講じているか。 (*)	
	マスコミ等の過剰対応による風評リスクが発生しないよう、対応組織を確立しているか。 (*)	
	マスコミ等の過剰対応による風評リスクが発生しないよう、対策を検討しているか。 (*)	
	インターネット掲示板などでの風評を定期的に確認しているか。 (*)	
	インターネット掲示板などでの風評被害に関する書き込みを発見した際は、必要な対応、処置を適切に実施しているか。 (*)	

(*)のチェック項目：GSCMを構成する会社毎にチェックする。

別紙1-7 GSCMリスクチェックシートの雛形

Ⅱ. 個別リスク確認シート

分類	チェック項目	チェック欄
インフラ	国内において関連するインフラ(電力、ガス、水道、通信、情報システムetc)の重要性を認識しているか。	
	国外において関連するインフラ(電力、ガス、水道、通信、情報システムetc)の重要性を認識しているか。	
	国内において関連するインフラ(電力、ガス、水道、通信、情報システムetc)の障害等の情報収集体制を構築しているか。	
	国外において関連するインフラ(電力、ガス、水道、通信、情報システムetc)の障害等の情報収集体制を構築しているか	
	国内において関連するインフラ(電力、ガス、水道、通信、情報システムetc)の障害発生時のGSCMの影響を調査しているか。	
	国外において関連するインフラ(電力、ガス、水道、通信、情報システムetc)の障害発生時のGSCMの影響を調査しているか。	
	障害発生時の影響調査の結果に基づく事業継続計画を策定しているか。	
	インフラ(電力、ガス、水道、通信、情報システムetc)の代替手段を講じているか。 (+)	

(+)のチェック項目 : GSCMを構成する情報システム毎にチェックする。

別紙1-8 GSCMリスクチェックシートの雛形

Ⅱ. 個別リスク確認シート

Page5

分類	チェック項目	チェック欄
インフラ	インフラ(電力、ガス、水道、通信、情報システムetc)、データのバックアップ方法並びに手順は、業務の回復目標に対応して定めているか。 (+)	
	運用の責任者は、バックアップ方法及び手順を検証しているか。 (+)	
	ユーザ及び運用の責任者は、復旧までの代替処理手続き及び体制を定め、検証しているか。 (+)	
	ユーザ及び運用の責任者は、復旧手続き及び体制を定め、検証しているか。 (+)	
	ユーザ及び運用の責任者は、復旧までの代替処理手続き及び体制を定め、検証しているか。 (+)	
	情報システムは個別部分、共通部分に着目して最適化を図っているか。 (*)	
	サイバーテロによるリスクを回避できるよう、情報セキュリティマネジメントを実施しているか。 (*)	
	情報セキュリティポリシーの見直しを定期的に行っているか。 (*)	
	情報セキュリティ規程類の見直しを定期的に行っているか。 (*)	

(*)のチェック項目：GSCMを構成する会社毎にチェックする。

(+)のチェック項目：GSCMを構成する情報システム毎にチェックする。

別紙1-9 GSCMリスクチェックシートの雛形

Ⅱ. 個別リスク確認シート

Page6

分類	チェック項目	チェック欄
ファイナンシャル	国内の金融危機に伴う契約先の倒産リスクを認識しているか。 (*)	
	国外の金融危機に伴う契約先の倒産リスクを認識しているか。 (*)	
	契約先の倒産リスクに対する対処方法を有しているか。 (*)	
	国内の物価の急激な変化に伴うコストリスクを考慮しているか。 (*)	
	国外の物価の急激な変化に伴うコストリスクを考慮しているか。 (*)	
	国内子会社におけるレガシーコスト(注)の認識はあるか。 (*)	
	国外子会社におけるレガシーコストの認識はあるか。 (*)	
	関係国の国家財政の健全性を確認しているか。	
取引の為替リスクを確認しているか。		

(*)のチェック項目：GSCMを構成する会社毎にチェックする。

(注)レガシーコスト：企業等が退職者に対して支払い続ける必要のある年金、保険等

別紙1-10 GSCMリスクチェックシートの雛形

Ⅱ. 個別リスク確認シート

分類	チェック項目	チェック欄
人財	従業員の教育訓練の方針に事業継続計画を明確にしているか。 (*)	
	従業員の教育訓練の方針に災害時対応計画を明確にしているか。 (*)	
	事業継続計画に基づいた技術力の向上、業務知識の習得を踏まえ、 人財育成を計画しているか。 (*)	
	教育訓練は人財育成計画に基づいて、定期的かつ効果的に実施しているか。	
	ノウハウの継承を実施しているか。 (*)	<div data-bbox="1004 756 1481 863" style="border: 1px solid black; background-color: #000080; color: white; padding: 5px; display: inline-block;"> 熟練者のノウハウが継承できずに事業継続できないリスクも存在する </div>
	アウトソーシング先、派遣社員含めて コンプライアンス(情報セキュリティ等) の教育を実施しているか。 (*)	
	人財育成計画は時間の経過に合わせて見直しを行っているか。 (*)	
	労務管理(児童労働等)を徹底しているか。 (*)	

(*)のチェック項目: GSCMを構成する会社毎にチェックする。

To Be Continued

Completion

Thank you for your attention.