

システム監査学会  
第23回研究大会

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)  
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)—

2009/06/12

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

## 「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: 喜入 博(KPMGビジネスアシュアランス)  
黒澤 兵夫(TAKE国際技術士研究所)  
石島 隆(法政大学)  
武田 賢二(シグマクシス)  
小倉 久宜(NTTデータフィット)  
足立 憲昭  
樽井 加奈子  
発表 : 北條 武(NTTデータ)

## 0. はじめに

### ■活動実績

#### <前回までのまとめ>

SCMにおけるBCMSとSAのモデル化

#### <今年度の検討結果報告>

### ■今年度の検討手順

### ■GSCMシステムのモデル選定

### ■モデルに基づくリスクの洗い出し

### ■GSCMにおけるリスクの分類

### ■GSCMリスクチェックシートの全体構成検討

### ■GSCMリスクチェックシートの作成

I. 全体確認シート

II. 個別リスク確認シート

# 1. 活動実績

昨年度までの到達点：SCMにおけるBCMSとSAのモデル化

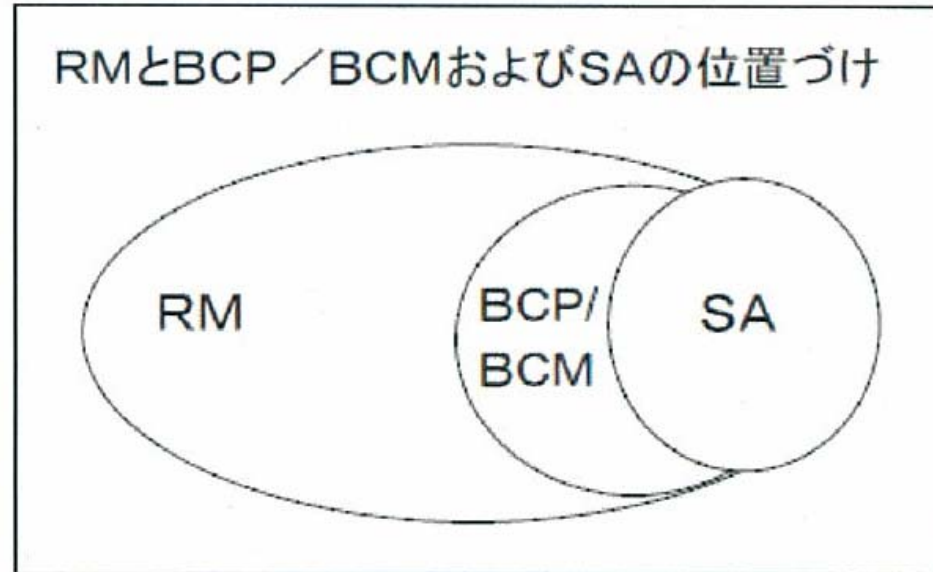
今年度の目標：①チェックリストの作成

②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             | 活動内容                                               |
|-----|----------------|----------------------------------------------------|
| 1回目 | 平成20年9月11日(木)  | 今年度のテーマ確認                                          |
| 2回目 | 平成20年10月30日(木) | SCMのBCMとリスクマネジメントについての議論                           |
| 3回目 | 平成20年12月8日(月)  | 前回はベースにしての意見交換会                                    |
| 4回目 | 平成21年1月13日(火)  | A社 GSCMシステム事例に基づくリスク分析(1)                          |
| 5回目 | 平成21年2月20日(金)  | A社 GSCMシステム事例に基づくリスク分析(2)                          |
| 6回目 | 平成21年3月17日(火)  | A社 GSCMシステム事例に基づくリスク分析(3)<br>研究大会に向けた意識合わせ(資料構成など) |
| 7回目 | 平成21年4月6日(月)   | GSCMリスクチェックシートの検討(1)                               |
| 8回目 | 平成21年4月23日(木)  | GSCMリスクチェックシートの検討(2)                               |
|     | 平成21年5月        | レビュー、校正(メール等で対応)                                   |

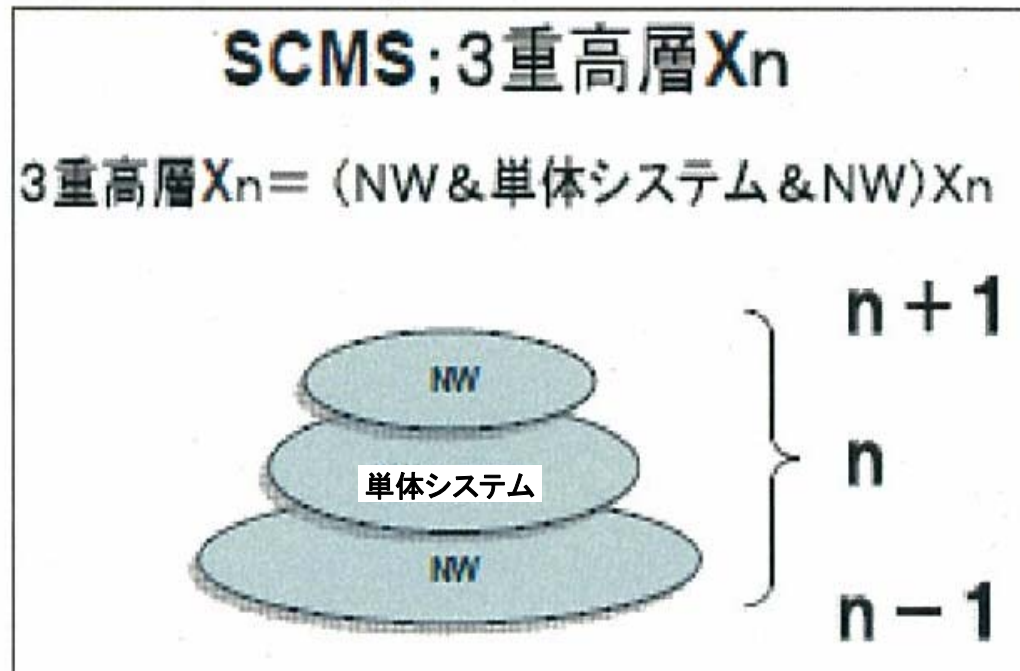
## 2. RM、BCP/BCMとSAの関連(主眼BCP/BCM)



### 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. SCMシステムのモデル

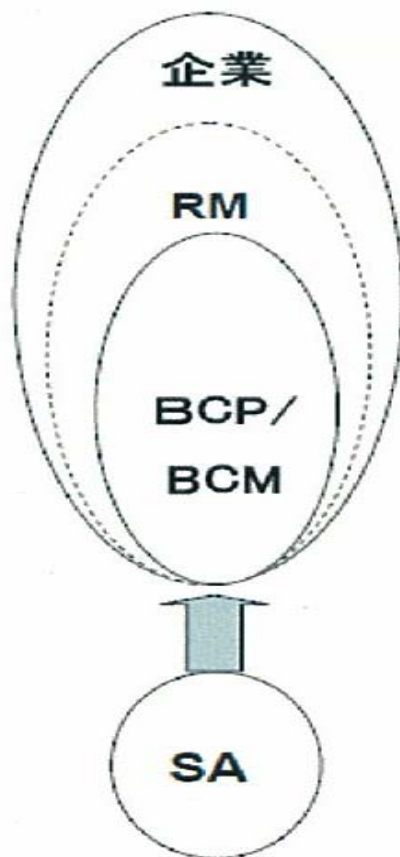


SCMのエLEMENT

NW + 単体システム + NW

SCMのエLEMENTが $n$ 個繋がっている状態

## 4. RM、BCP/BCMとSAの関連(主眼SA)



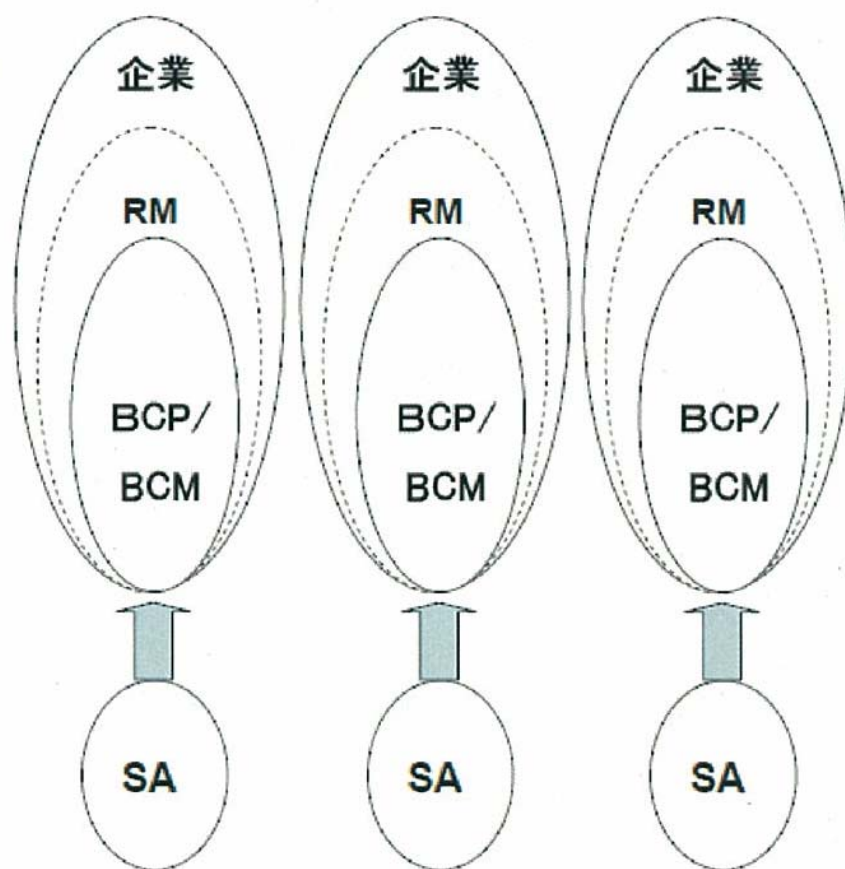
システム監査(SA)を主眼とした場合の関係

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

## 5. BCPS/BCMSの評価尺度/達成度レベル

| レベル        | 段階   | 概要                                          |
|------------|------|---------------------------------------------|
| 評価尺度／達成度 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<br>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。                   |

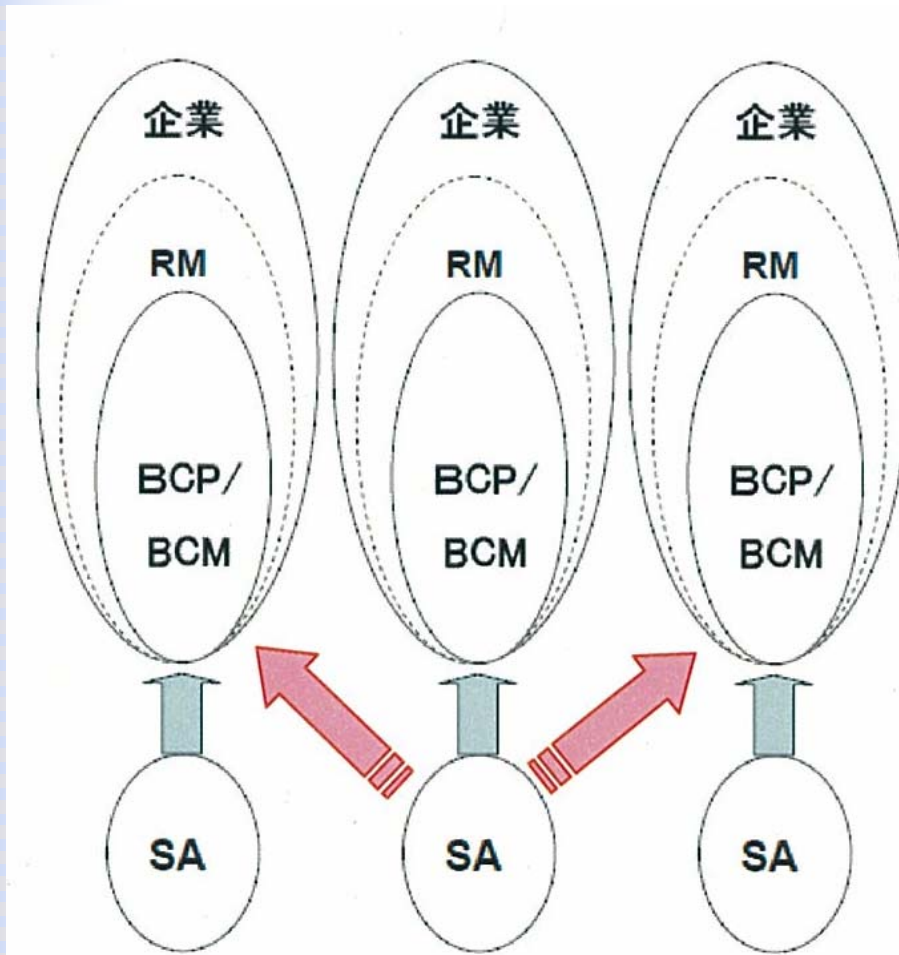
## 6. 単一ソリューションシステムの統合と単一監査



レベルⅡからⅢに該当

横の連携、相互の連携がない

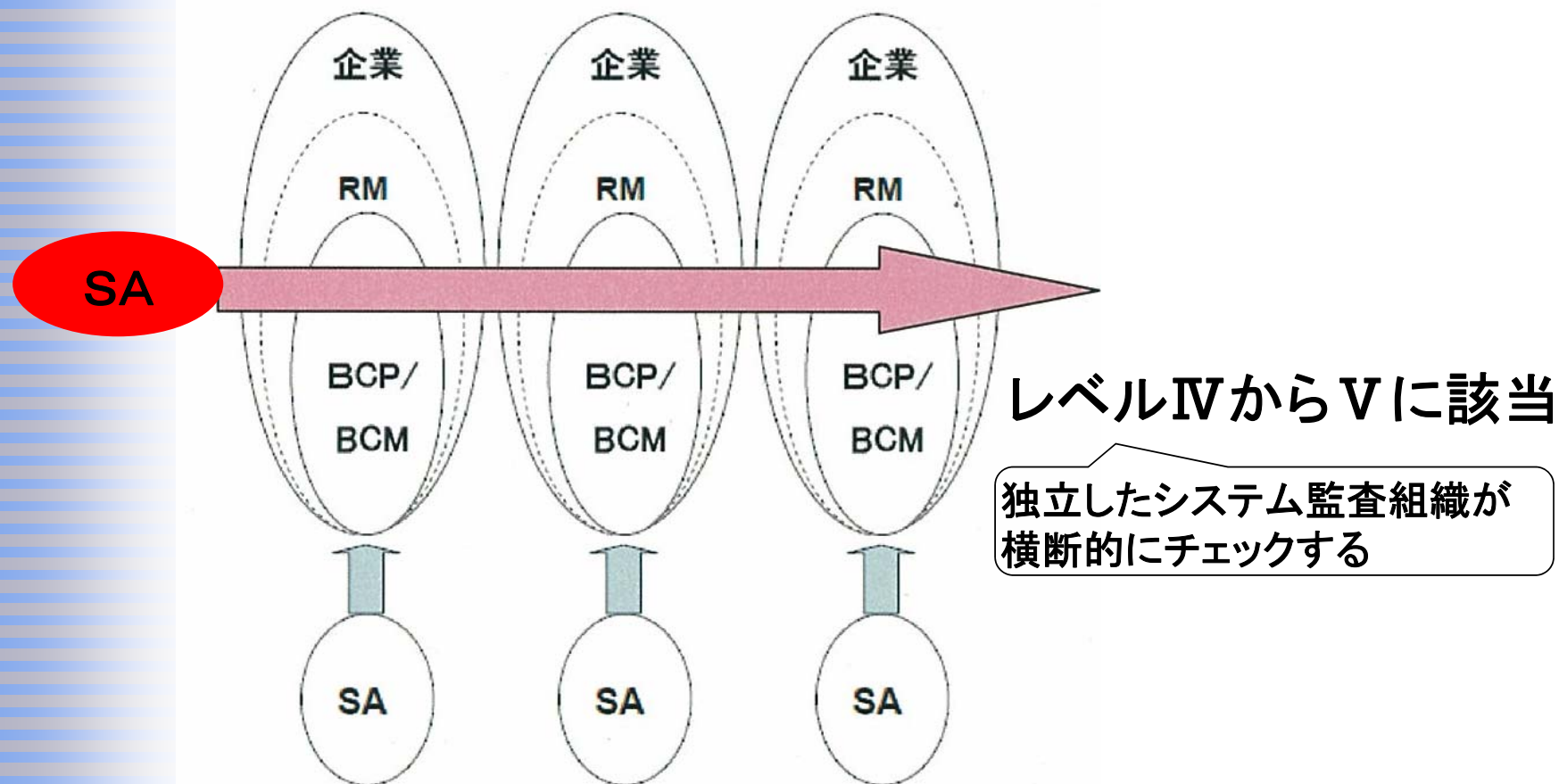
## 7. 他企業／他組織のシステムと連携したSAの実施



レベルⅢからⅣに該当

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

## 8. 統合システムのSAとSCMシステムの横断SAの実施



## 9. 今年度の検討手順

手順1

GSCMの  
モデル選定

手順2

モデルに基づく  
リスクの洗い出し

手順3

GSCMにおける  
リスクの分類

手順4

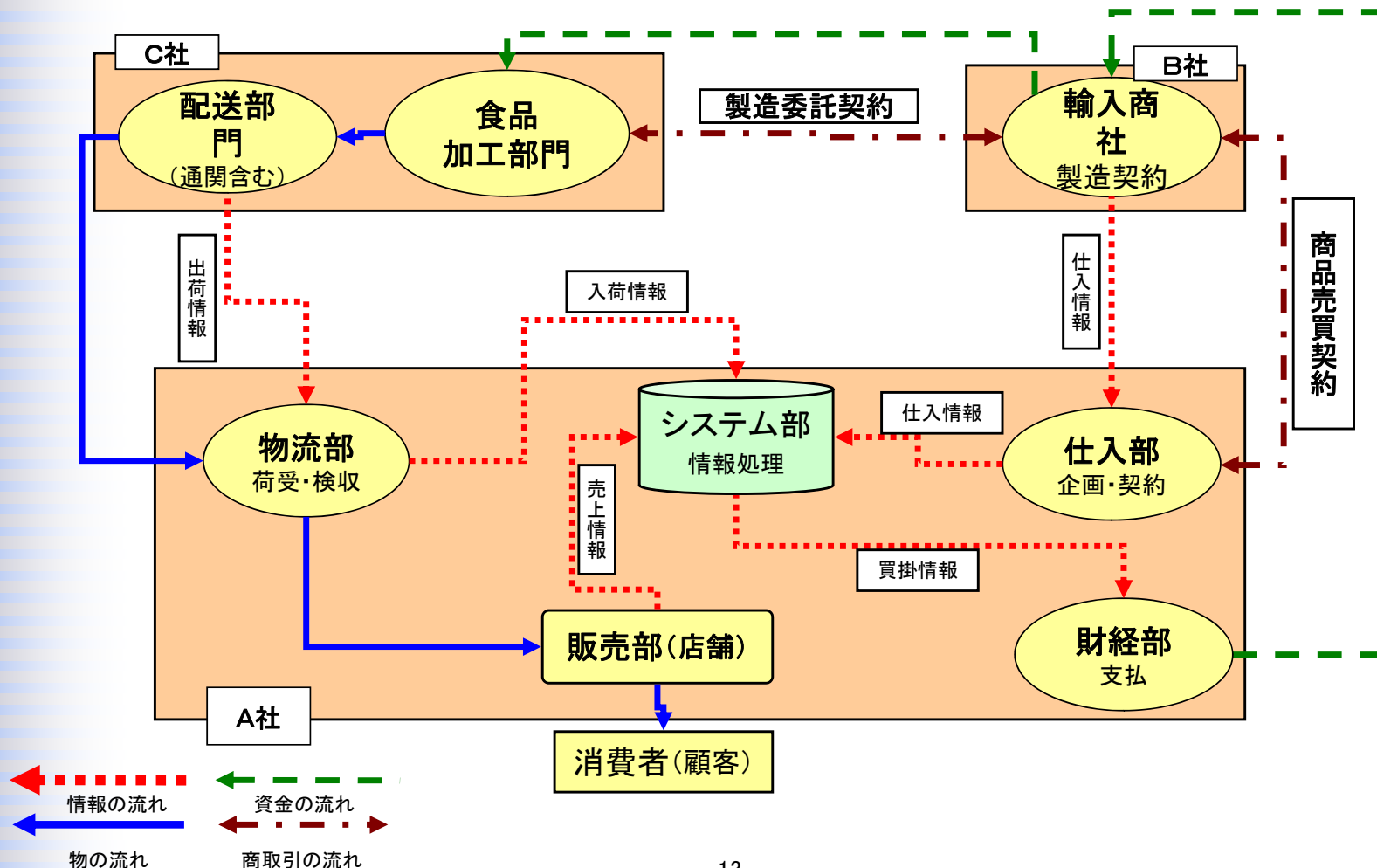
GSCMリスクチェックシートの  
全体構成検討

手順5

GSCMリスクチェックシートの作成

## 10. 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)



## 11. 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(資金繰り)              |
| ファイナシャル | 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    |

## 12. 手順③ 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Ⅴ項 事業継続計画(5項目)

第Ⅳ項 共通業務 第Ⅶ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におけるリスクの分類

調達

インフラ

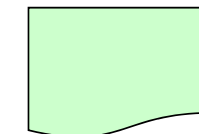
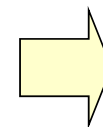
品質

ファイナンス

風評

人財

対象を“情報システム”だけでなく  
“**社会システム全体**”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

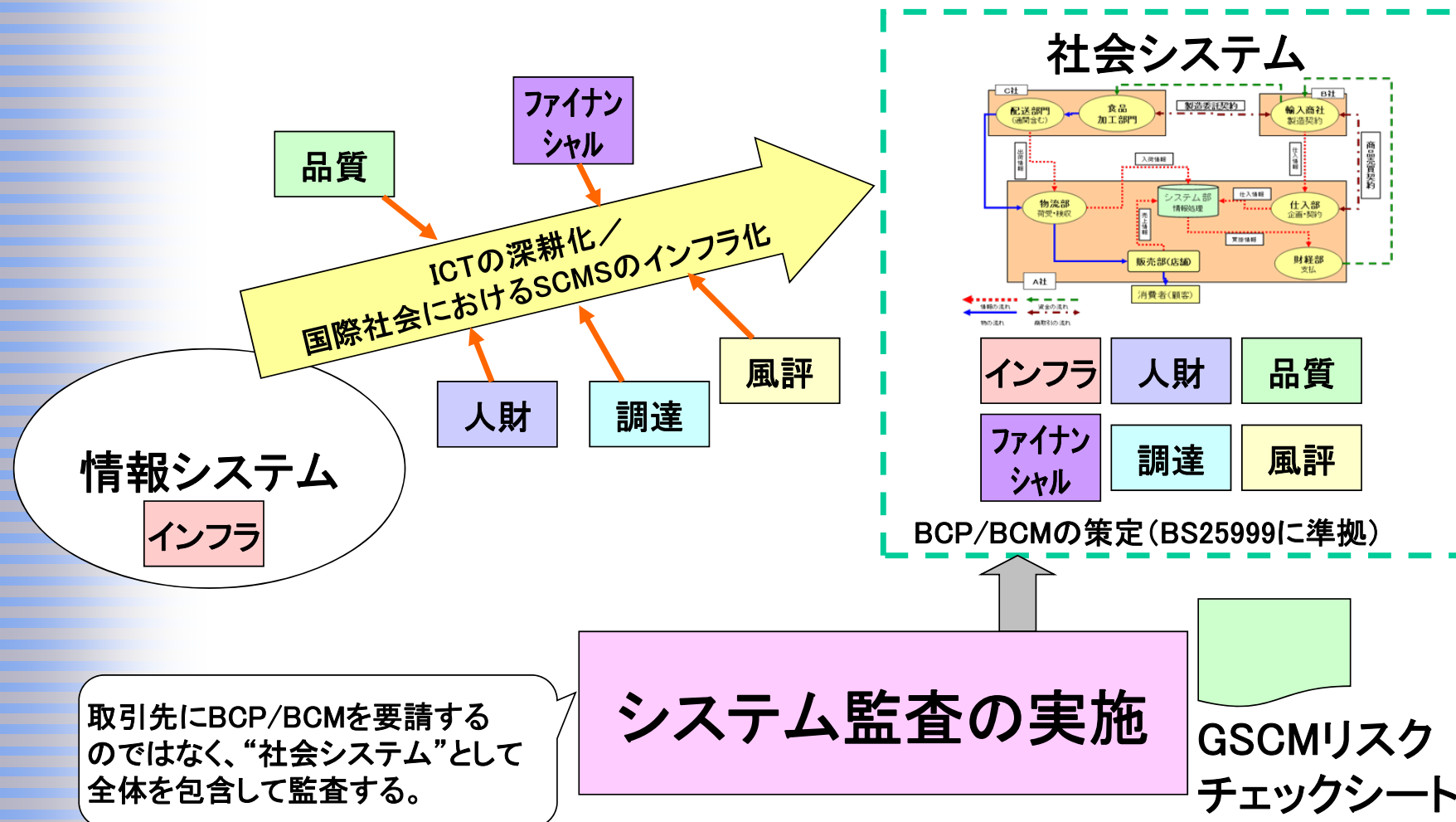
###### ③風評

###### ④インフラ

###### ⑤ファイナンス

###### ⑥人財

## 12. 手順③補足 情報システムの進化のシステム監査の概念図



## 13. 手順④ GSCMリスクチェックシート

### I. 全体確認シート

Page1

| 分類   | チェック項目                                                                           |    | チェック欄 |
|------|----------------------------------------------------------------------------------|----|-------|
| 基本事項 | 社会システム全般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。                                                  |    |       |
|      | 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。                                                  |    |       |
|      | 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。                                                           |    |       |
|      | 事業継続計画は、全員に周知しているか。(*)<br>・周知の方法を明確化しているか。<br>・周知の時期が適切か。<br>・周知されていることを確認しているか。 | A社 |       |
|      |                                                                                  | B社 |       |
|      |                                                                                  | C社 |       |

(\*)のチェック項目：GSCMを構成する会社毎にチェックする。

## 13. 手順④ GSCMリスクチェックシート

### I. 全体確認シート

Page2

| 分類   | チェック項目                                     | チェック欄 |
|------|--------------------------------------------|-------|
| 基本事項 | 事業継続計画は、必要に応じて見直しているか。                     | —     |
|      | GSCMに関わる事業継続計画の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。 (*)           |       |
|      | 地震等リスク及び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。                  |       |
|      | リスク分析の結果に基づき、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。                     |       |
|      | 災害時対応計画の実現可能性を確認しているか。                     |       |

(\*)のチェック項目：GSCMを構成する会社毎にチェックする。

## 13. 手順④ GSCMリスクチェックシート

### I. 全体確認シート

Page3

| 分類   | チェック項目                                                  | チェック欄 |
|------|---------------------------------------------------------|-------|
| 基本事項 | 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。                                 |       |
|      | 情報システム、データ及び関連設備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。 (+) | Wシステム |
|      |                                                         | Xシステム |
|      |                                                         | Yシステム |
|      |                                                         | Zシステム |
|      | 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。 (+)                  |       |

(\*)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。

## 13. 手順④ GSCMリスクチェックシート

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。<br>（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。<br>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の実施しているか。                                                                               |       |
|    | 安全運転の講習会を定期的の実施しているか。                                                                                      |       |

## 13. 手順④ GSCMリスクチェックシート

### 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。                      |       |

## 13. 手順④ GSCMリスクチェックシート

### 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(会社には不満を持つ)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。

## 13. 手順④ GSCMリスクチェックシート

### Ⅱ. 個別リスク確認シート

Page4

| 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。                     |       |

## 13. 手順④ GSCMリスクチェックシート

### 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 | サイバーテロによるリスクに対応できるような、情報セキュリティマネジメントを確立しているか。 (*) |       |
|      | 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。

## 13. 手順④ GSCMリスクチェックシート

### 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<br>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。 (*)      |       |

(\*)のチェック項目：GSCMを構成する会社毎にチェックする。

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

## 13. 手順④ GSCMリスクチェックシート

### Ⅱ. 個別リスク確認シート

Page7

| 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。 (*)           |       |
|    | アウトソーシング先、派遣社員含めて情報セキュリティなどの教育を実施しているか。 (*) |       |
|    | 労務管理(児童労働等)を徹底しているか。 (*)                    |       |
|    | 人財育成を計画しているか。 (*)                           |       |
|    | ノウハウの継承を実施しているか。 (*)                        |       |
|    | 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。 (*)            |       |

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

(\*)のチェック項目: GSCMを構成する会社毎にチェックする。

## 14. 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

今年度の目標: ①チェックリストの作成

②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: ①チェックリストの作成



次年度の目標: ②ガイドラインの作成と試行

(注意点: BS25999との関わり)

To Be Continued

---

Completion

Thank you for your attention.