事業継続の１０のポイント

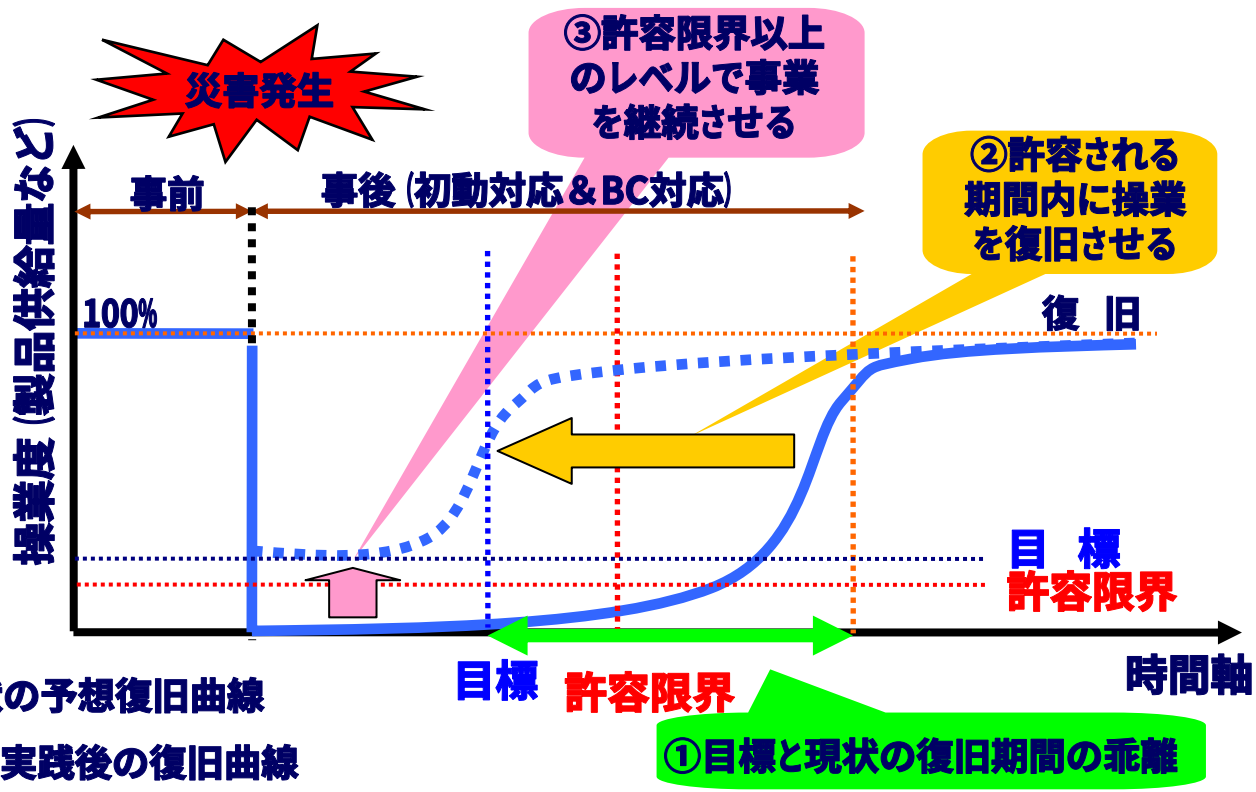
2006年3月23日

東京海上日動リスクコンサルティング株式会社
情報グループ
グループリーダー　　指田　朝久

事業継続の概念

不測の事態（危機・災害）などの発生により事業リソース（社員・施設・機器など）が損傷を受け、通常の事業活動が中断した場合に、残存する能力で優先すべき業務を継続させ、**許容限界以上のサービスレベルを保ち、かつ許容される期間内に復旧できるように**、前もって代替リソースの準備を行ったり、災害発生時の対応方法や組織を規定したりするもの。

概念図



情報セキュリティ管理に求められる事業継続計画

1. 情報セキュリティマネジメントシステム（ISMS）の中で事業継続管理が求められている。（11．事業継続管理）
   1．管理手続き
   2．影響度分析
   3．計画の作成および実施
   4．計画作成のための枠組み
   5．試験、維持及び評価、維持および再評価
2. 目的；事業活動の中断に対処するとともに、重大な障害または災害の影響から重要な業務手続きを保護するため
3. 対象とするリスク；災害及びセキュリティ障害（例；自然災害、事故、IT障害、装置の故障、悪意による行為の結果）

TOKIO MARINE NICHIDO

情報セキュリティ管理の事業継続計画と全社レベルの事業継続計画の整合性

1. 情報セキュリティマネジメントシステム（ISMS）では、重要な情報と情報システムを対象として適用範囲を選定する。

2. 全社を対象としたBCPでは、情報システムのバックアップを重要な対策に位置づけている。

3. 企業や組織の多くでこれらの対象は一致する。しかし、金融やプロバイダーなど情報システムが重要な要素となる業種がある一方、製造業などにおいては情報システムの停止よりも製造装置などの破損のほうがより深刻な影響を与えることから、全社的には優先度が下がることがある。

4. 企業自身をよく知ることが重要

TOKIO MARINE NICHIDO

経済産業省と内閣府のガイドラインの特徴

- **経済産業省の事業継続ガイドライン（２００５年３月）**

  情報システムを対象としたガイドラインで、大規模なシステム障害、セキュリティインシデント、情報漏洩、データ改竄などが発生した場合のケーススタディなどを取り上げている。

  また、事件事故発生後の取り組み方について４段階に時間を区分し具体的な行動指針を解説している。

- **内閣府の事業継続ガイドライン（２００５年８月）**

  一般的な企業の包括的な指針であり、すべてのリスクに対応できる枠組みを提示している。まず代表的なリスクである地震を考慮して対応し、継続的改善を行いながら対象とするリスクを拡大することを推奨している。

TOKIO MARINE NICHIDO

内閣官房「第1次情報セキュリティ基本計画」の特徴

- **内閣官房の第1次情報セキュリティ基本計画「セキュア・ジャパン」の実現に向けて（2006年2月）**

「セキュア・ジャパン」実現に向けて、重要インフラ（＊）の情報セキュリティ対策については、

「重要インフラは、文字通り国民生活・社会経済活動の基盤であり、あらゆる脅威からその安定的供給を確保することが最優先の課題である。・・・(中略)・・・・重要インフラの情報セキュリティ水準の向上とIT障害への対応能力の強化(未然防止、被害拡大防止・迅速な復旧、再発防止)の両面で、各事業分野や重要インフラ事業者等の特質を踏まえながら、従来の縦割り型の施策実施体制だけでなく、分野横断的な取り組みを含め新たな官民の連携体制を再構築していく必要がある。」と記されている。

- **（＊）重要インフラ10分野**

情報通信、金融、航空、鉄道、電力、ガス、
政府・行政サービス、医療、水道、物流

従来の防災対策との関係

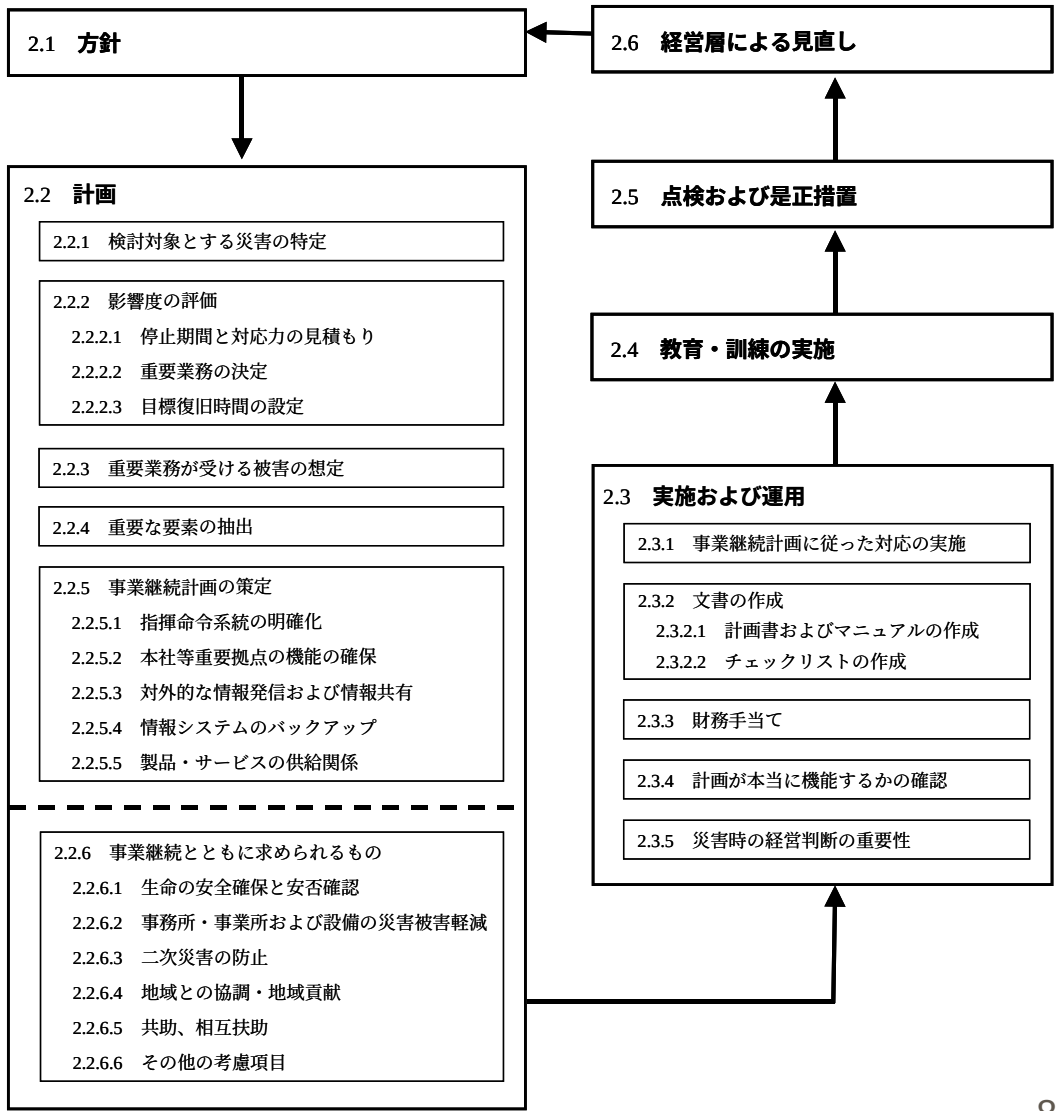
	従来の防災対策	事業継続計画
主な着眼点	◆ 人命安全、建物等の資産保全	◆ 優先業務の継続（対象品目の供給継続）
対策の内容 ①減災 mitigation ②準備 preparedness ③対応 response ④復旧 recovery	① 耐震・耐火・消火設備導入、転倒防止等 ② 災害対応体制、備蓄、安否確認システム、防災訓練等 ③ 被害状況把握、避難・救助、二次災害防止等 ④ 建物・設備の復旧等	左記①～④に加え、以下を追加 0 **優先業務の特定、目標復旧時間・レベル設定など** ① 事業継続に必要な要素の保全等 ② 事業継続体制、事業継続に必要な要素の確保（要員を含めた資源の二重化）、代替手段、事業継続手順、事業継続訓練など ③ ＢＣＰ発動（施設・システム要員の代替手段による業務・運用）など ④ 通常業務・運用への切り替えなど
対策の策定単位	◆ **本社・拠点・工場・組織毎の対策でも可**	◆ **優先業務の系・サプライチェーン（上流工程～下流工程まで）ごとの対策**
総コスト・コスト賦課の考え方（例）	◆ 総コストは企業の規模（資産・従業員）に略比例 ◆ 全社共通管理費としての位置付け、部門の規模に応じて賦課	◆ 総コストは優先業務の規模と対策レベル（目標復旧時間の程度など）による ◆ 事業を維持するための営業費用として賦課
評価	◆ 労働安全的、人道的な観点からの評価	◆ ビジネス上（顧客からの期待・ステークホルダーへの説明責任）の観点からの評価 ⇒災害対策投資の最適化（コアビジネスを守る） ⇒サービスレベルやビジネスプロセスの最適化

TOKIO MARINE NICHIDO

内閣府「事業継続ガイドライン」

ガイドラインの構成

事業継続の取組みの流れ



注) 国際標準規格との整合性も考慮している

事業継続戦略の１０ポイント

1　方針の策定

2　戦略/計画の策定

- 災害の特定
- ビジネスインパクト分析
- 重要業務の選定
- 復旧目標の設定
- 被害想定
- 具体的な事業継続計画の策定

3　事業継続のための対策

- 具体的対策の実施
  - 指揮命令系統の明確化
  - 本社等重要拠点機能の確保
  - 対外的な情報発信、情報共有
  - 情報システムのバックアップ
  - 製品･サービスの供給
- マニュアル･チェックリストの作成
- 財務的手当

4　教育･訓練

5　点検･見直し

Point1 方針策定のポイント
（BCPの目的･体制構築）

Point2 重要業務の選定のポイント

Point3 ﾋﾞｼﾞﾈｽｲﾝﾊﾟｸﾄ分析と目標復旧時間（RTO）のポイント

Point4 被害想定のポイント

Point5 計画策定のポイント

Point6 指揮･命令系統のポイント

Point7 対応情報開示のポイント

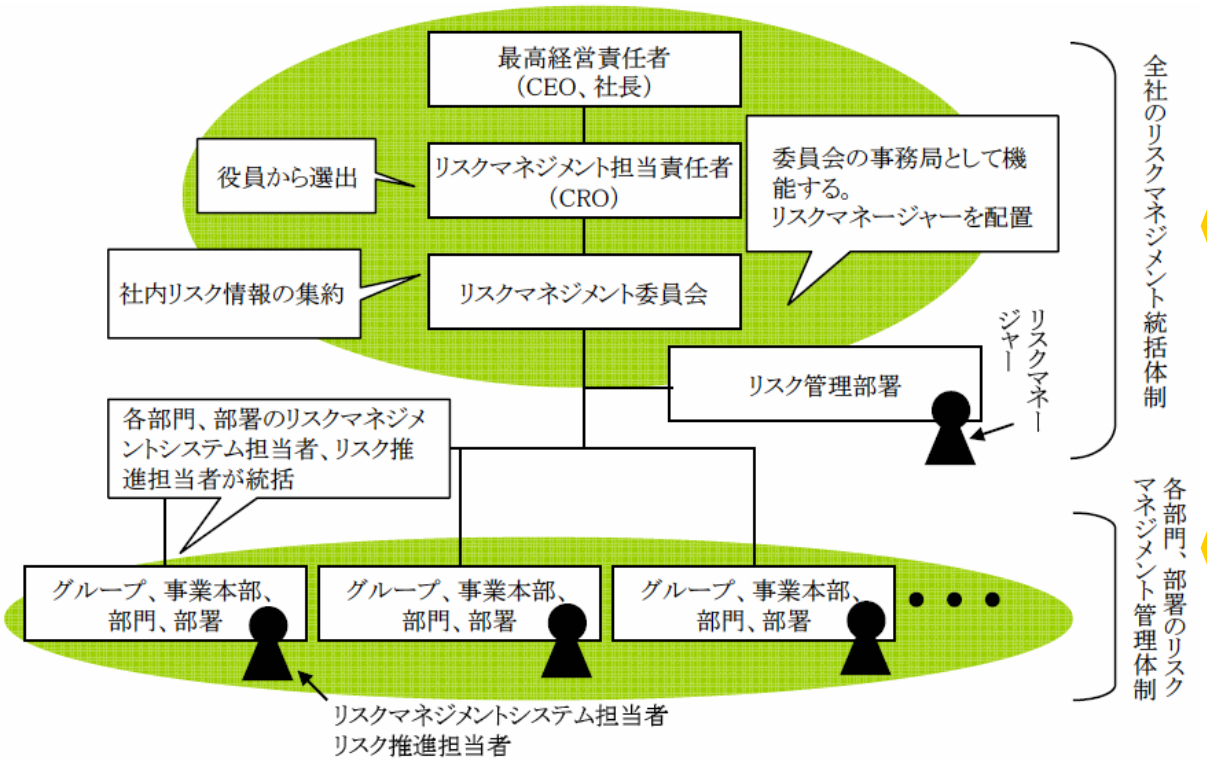
Point8 文書（ﾏﾆｭｱﾙ/ﾁｪｯｸﾘｽﾄ）化のポイント

Point9　BCP教育･訓練のポイント

Point10 継続的改善のためのポイント
（他のリスクへの応用）

Point 1　方針策定のポイント（BCPの目的・体制構築）

・経営トップの承認と支援が最も重要
・BCP策定チーム（事務局）の編成（企業規模・組織体制により異なる）
・経営トップと各事業部・カンパニーとの橋渡し役
　（欧米では、“BCC（Business Continuity Coordinator）”という職業）



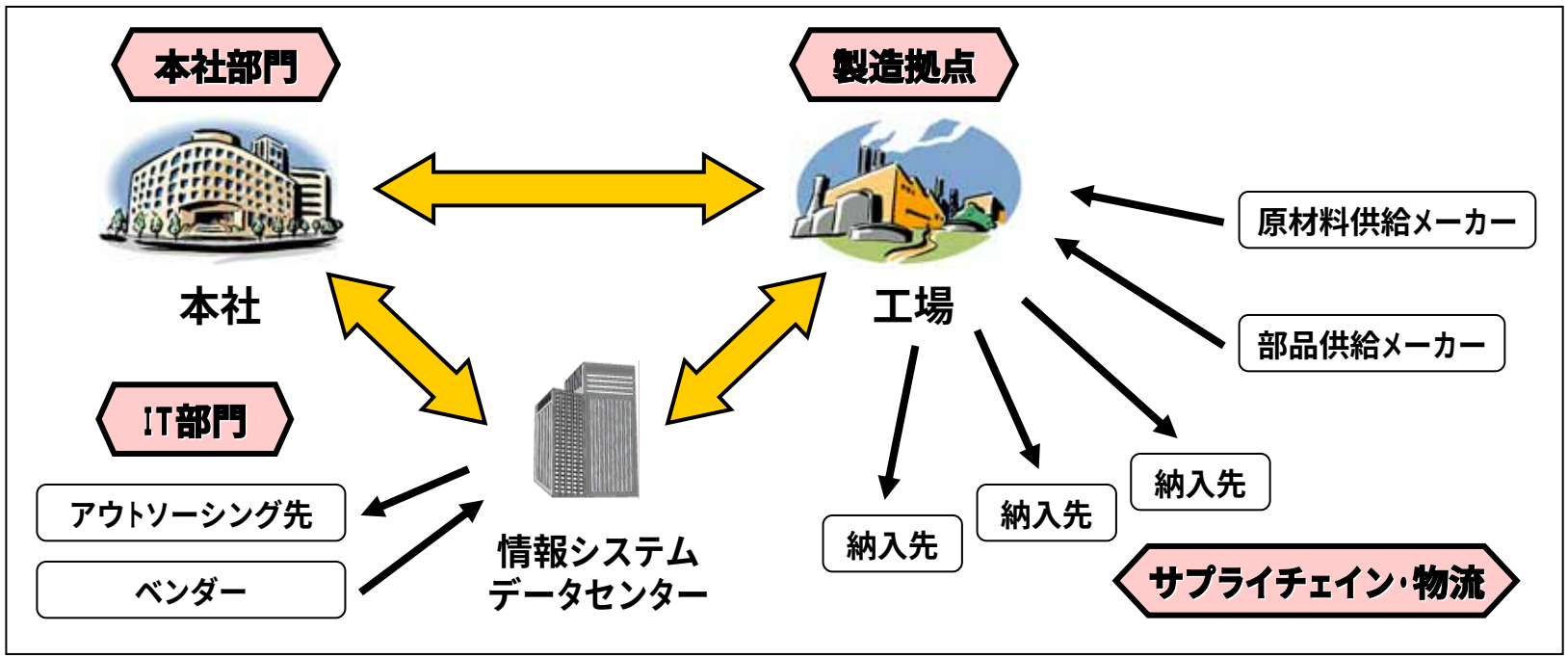
・リスク分析
・ビジネスインパクト分析
・対策・戦略立案
・教育・訓練計画
・・・

BCPチーム（事務局）
BCプランナー・コーディネーター
外部機関（コンサルティング会社）

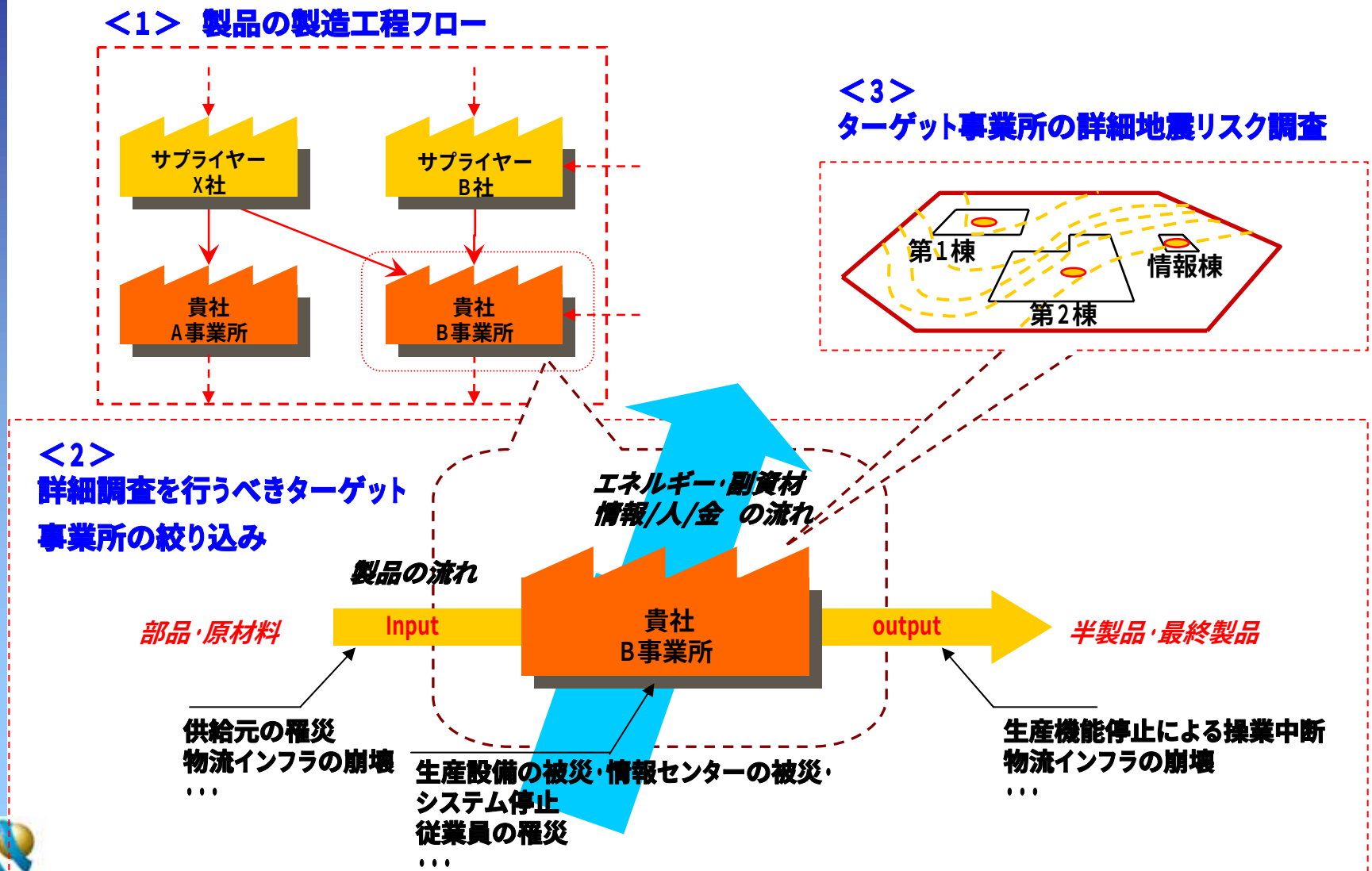
↑一般的な事業リスクマネジメント体制
「先進企業から学ぶ事業リスクマネジメント実践テキスト　経産省」より引用

Point 2　重要業務の選定のポイント

重要な事業・品目に着目してサプライチェーンを整理し、
●本社中枢機能　●IT・データセンター　●物流拠点
●製造拠点　●原材料・部品サプライヤー・外注先
のそれぞれが被災するケースについて、リスクの発生確率と影響度、同時被災の可能性等を考慮すること。ただし、現実的に取り組みやすい機能・部署から始めることも一案。



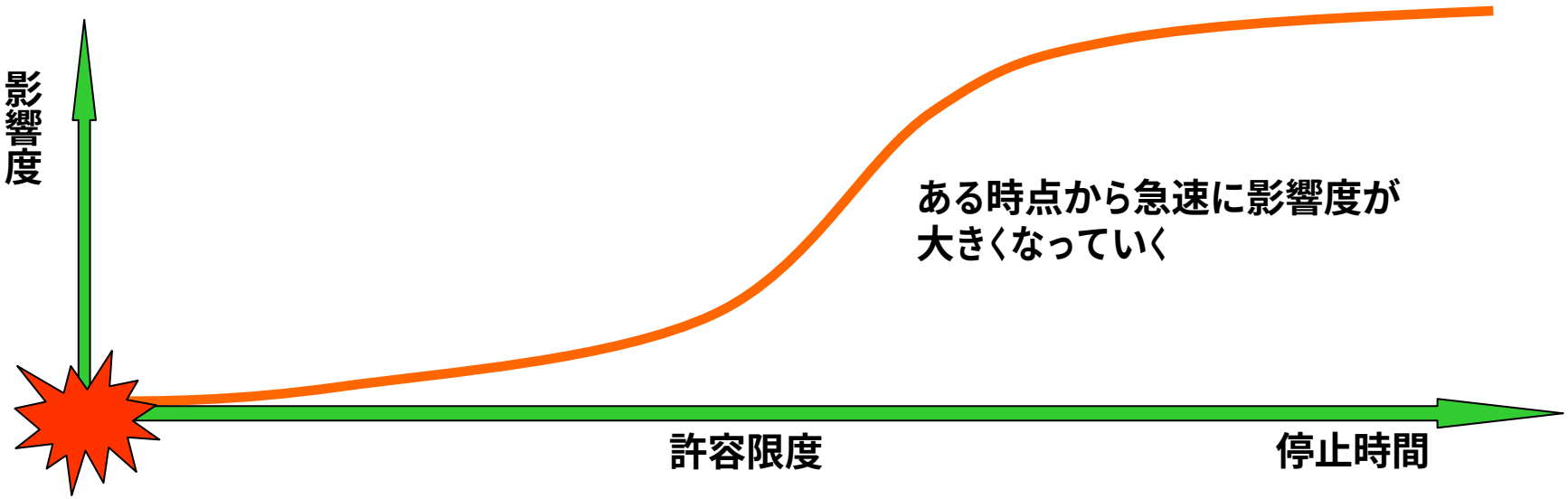
Point 2（続き） 系（ビジネスフロー）の分析・ボトルネックの洗い出しの進め方



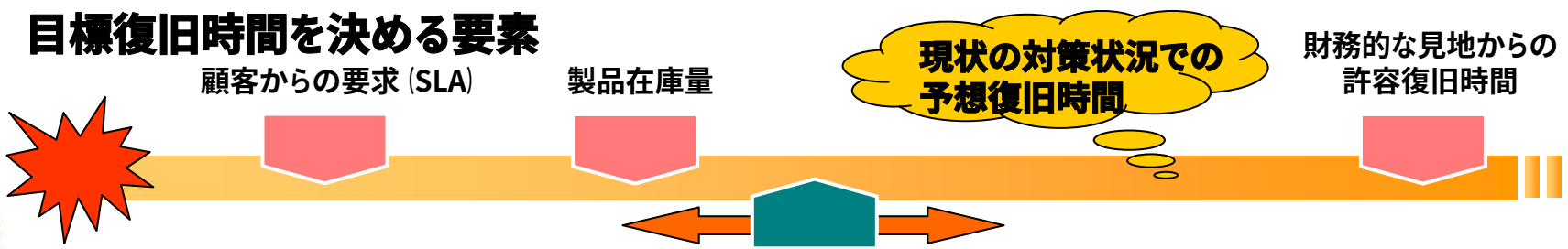
Point 3　ﾋﾞｼﾞﾈｽｲﾝﾊﾟｸﾄ分析と目標復旧時間（RTO）のポイント

・目標復旧時間（RTO；Recovery Time Objective）は、企業への財務的な影響に加えて、製品在庫量、顧客・取引先を含む全ステークホルダーへの影響、シェアやブランドイメージへの影響、CSR（企業の社会的責任）の見地から総合的に検討する。

・ただし、被害想定結果を踏まえて、無理のない目標値を決めることが重要。



目標復旧時間を決める要素



SLA ；Service Level Agreement

Point 4　被害想定のポイント

なぜ被害想定が必要か

- リソース減の状況を可視化し、被害の様相のイメージを共有する。
- 対策の投資を見合うものにする。
- シナリオを明確化し、机上訓練を有効なものにする。
- 残存リスクを明確にする。

- 業務内容に即したシナリオを想定する。
- 標準的なシナリオ、対処可能な最悪のシナリオなどを用意する。
- まずラフなシナリオを作成し、対応策を検討してみる。

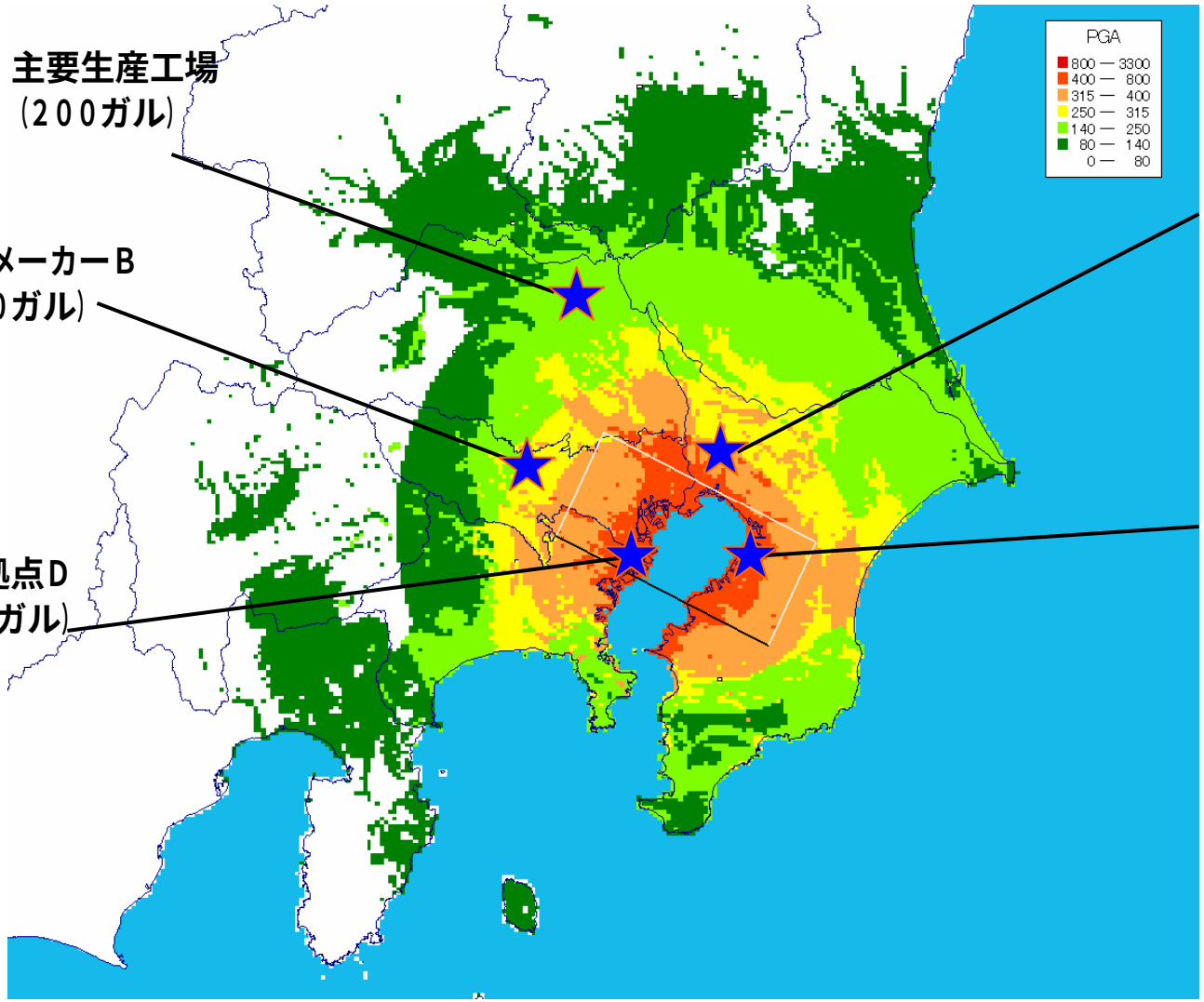
★順次シナリオを詳細化することも現実的。

★機能の停止を想定する。

実際に対策を立てる場合は、機能を停止させるリスク源毎の対策も合わせて検討する事が一般的。
ひとつのリスク源から検討を開始して（例えば地震）継続的改善の過程で追加していく。

TOKIO MARINE NICHIDO

Point 4（続き） サプライチェーンを考慮した地震リスク評価例



主要生産工場
（２００ガル）

部品メーカーＢ
（３００ガル）

物流拠点Ｄ
（５００ガル）

外部委託先メーカーＣ
（４００ガル）

原材料メーカーＡ
（６００ガル）

上記：ＴＲＣ－ＲＡＭＳシステムによる出力例
首都圏直下型地震（東京湾北部地震）（地表面加速度）

過小評価されやすい業務（工場の例）

外部委託している業務 - ユーティリティー(排水処理、水供給など)

メーカー委託している保守部品供給

海外から調達した機器･機械など – コミュニケーション不足

試運転･調整運転期間や、必要とする要員数など

主要プロセスの評価は十分だが、その周辺が見落とされやすい

TOKIO MARINE NICHIDO

Point 5　計画策定のポイント

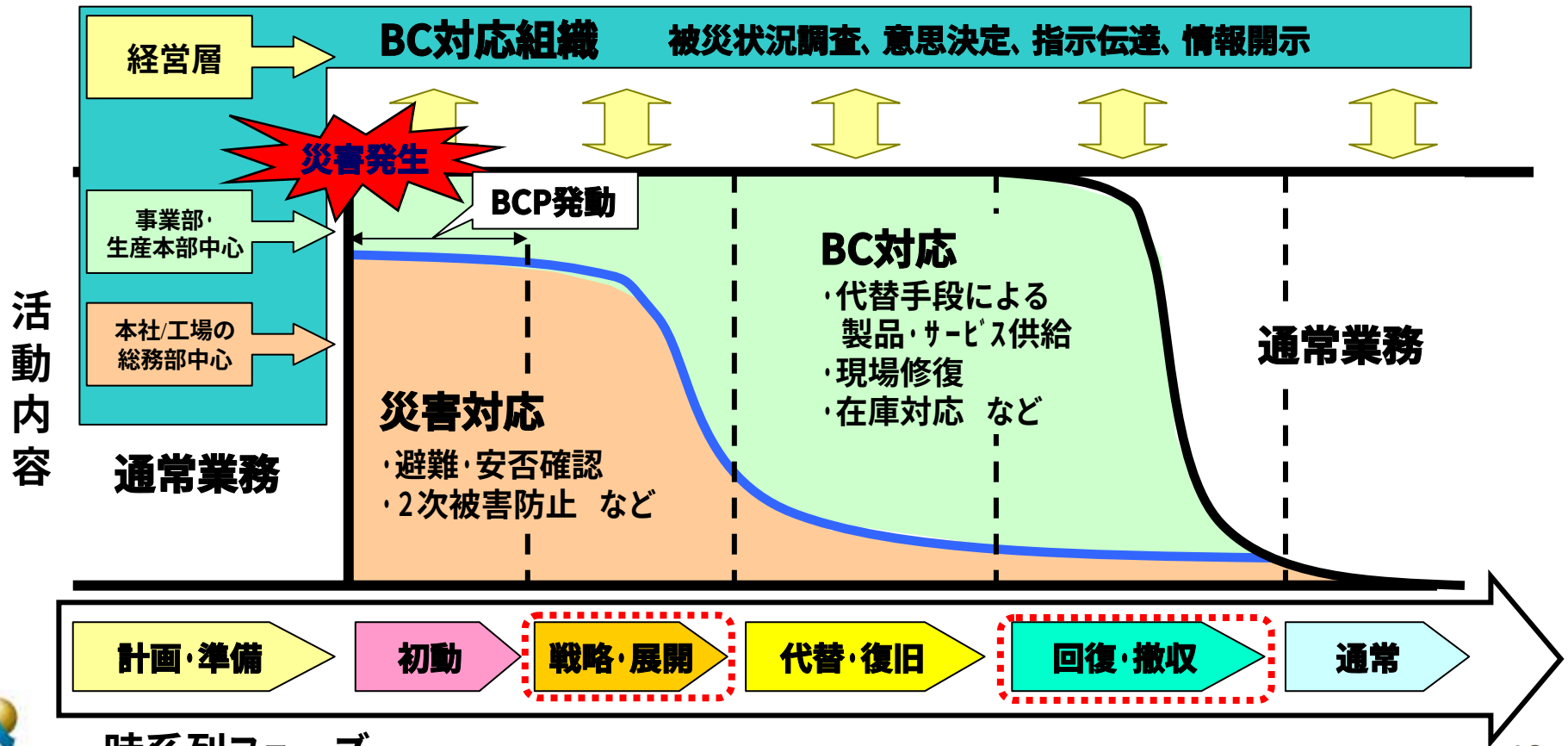
重要なことは、大災害に見舞われても、事業を継続させ、製品を供給しつづけること（市場本位・顧客満足・ブランドの維持）。

- 手段は耐震対策などのハード対策だけではない。
- 緊急代替生産、外部委託、現場修復、在庫などのオプションの組み合わせも考えられる。
- 未だ日本企業の大半で十分に検討されていない被災後に迅速かつ円滑に行動できる組織体制（ソフト面）を構築する。

TOKIO MARINE NICHIDO

Point 6　指揮･命令系統のポイント

･時系列で活動内容やその担い手が異なる。
･「戦略･展開」「回復･撤収」フェーズへの移行を考える必要がある。
　⇒検討されていないことが多い。
･全体のグランドデザインが重要となる。



Point 7　災害対応に関する情報開示のポイント

ステークホルダーへ対応に関する情報の開示を行う必要がある。

（ステークホルダー：顧客、取引先、株主、従業員、関連会社、自治体、地域市民など）

- **事前に幅広く対応を周知させる。**
  - ホームページ、店頭掲示、訪問による説明等
- **業務を継続する場合の条件の提示。**
- **業務を継続できない場合の状況説明。**

Point 8　文書（マニュアル/チェックリスト）化のポイント

作成時の留意事項

・既存のマニュアル類の活用　⇒事業継続計画に合わせた見直し

・チェックリストの作成　⇒非常時における具体的な実施事項を短時間に漏れなく確認するため（詳細なマニュアルを読む余裕がない）

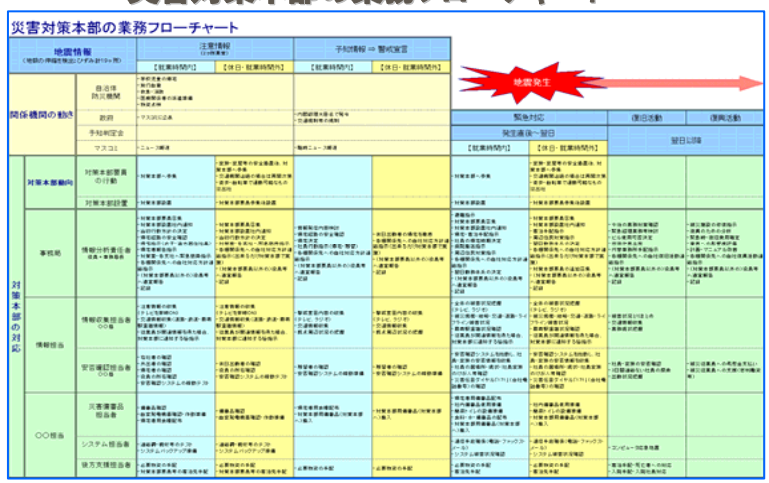
・平時業務の明確化　⇒取組みを形骸化させない工夫

＜事業継続計画＞

①本計画の性格・・・背景、当社の特性、計画の位置付け
②本計画の目的・目標・・・基本的な考え方、目的、目標
③被害想定・・・被害想定の根拠、被害の種類・内容
④災害時の対応体制・・・災害対策組織、体制移行・復帰条件、継続業務及び業務実施方法の決定
⑤情報連絡手段・ルート
⑥災害時の社員行動基準
⑦平時の準備業務
⑧平常業務への復旧要領
⑨本計画の維持管理
⑩その他様式類　・・・関係機関連絡先、報告シート、備品リスト　等

＜マニュアル・チェックリスト＞

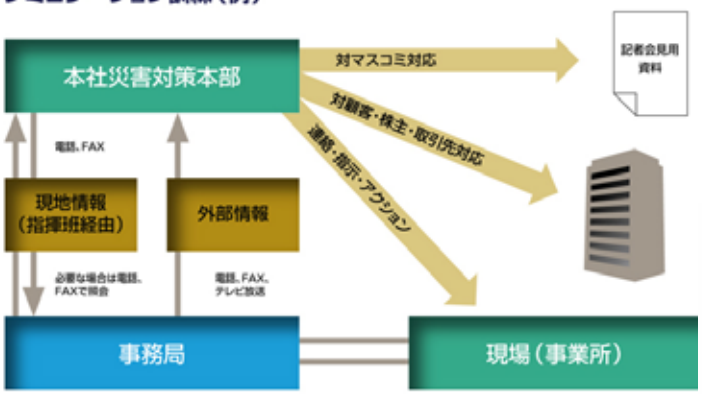
災害対策本部の業務フローチャート



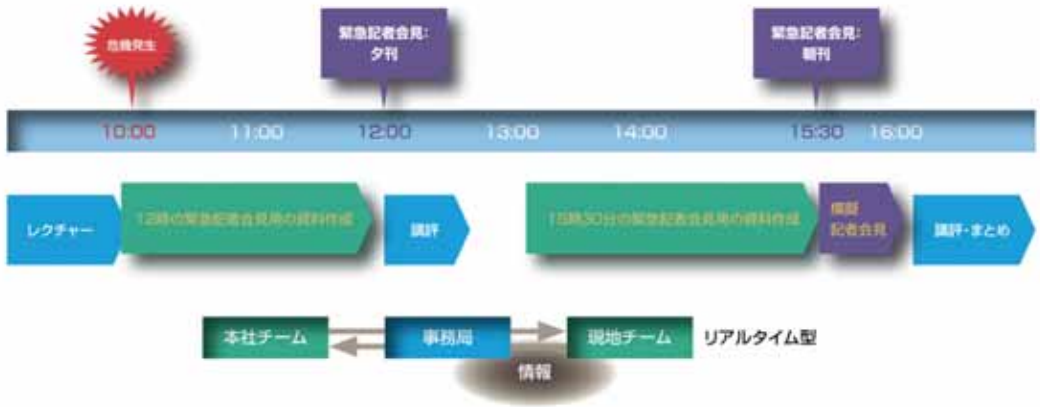
Point 9　BCP教育・訓練のポイント

・実際に危機対応を行う要員の育成と危機時の実践対応能力の向上を図ることが重要。
　⇒役割/立場により、その内容は異なる。
・危機的状況を模擬体験することにより、初動および実施業務の重要性を認識する。
・現状の問題点・課題を洗い出し、ﾏﾆｭｱﾙ、ﾁｪｯｸﾘｽﾄ、連絡網などの改善に活用する。

シミュレーション訓練（例）



広報対応訓練（例）



Point 9(続き)　BCP教育･訓練のポイント

対策本部要員育成　机上訓練

◎事業継続の重要性を認識し、カルチャーとして定着させることが重要。
◎災害対応はすべて応用問題。計画をたたき台に臨機応変に判断し、
　対応できることが重要。
◎経営者および対策本部の要員に対してケーススタディ訓練を実施。
　･シナリオおよびケーススタディによる机上訓練
　･災害対応を時系列でシミュレーションするリアルタイム訓練

危機広報訓練　記者会見訓練

◎対外的な情報発信および情報共有の重要性
◎記者会見の前にまず情報収集機能の強化
◎記者会見訓練の実施
　･プレスリリースの作成支援･添削
　･スポークスパーソンのステートメント作成
　･記者会見Ｑ＆Ａの作成
　･スポークスパーソンの記者会見訓練
◎ＷＥＢ、営業社員による説明も含めた情報発信戦略の構築。

TOKIO MARINE NICHIDO

Point 10　継続的改善のためのポイント（他のリスクへの応用）

・リスクによって、企業への影響が異なる（グループ化）。
・対策実施時には、他のリスクとの整合性を図る必要性が有る。
（整合性を考慮する例：環境リスク対応における屋外危険物配管の二重管化
⇒メンテナンス・漏洩の知覚に支障）

・**広範囲かつ同時被災**の可能性があるリスク
⇒地震・風水害など

・**局所的に壊滅的**な破壊を及ぼす可能性があるリスク
⇒火災・テロなど

・条件によっては資産の**修復が可能**なリスク
⇒地震・火災による煙・腐食性ガス汚損

・物的資産（施設）を破壊せずに**オペレーションを停止**させるリスク
⇒システムダウン、SARS・炭疽菌、風評など

・サプライチェーンや同業他社の**影響**によるリスク
⇒委託先の被災、市場の閉鎖など

企業を取り巻くリスク

事業継続計画構築のポイント（まとめ）

- **事業継続の構築は経営者の責務**
  - 継続する事業・業務・製品などの選択
  - 経営資源（人材、予算、時間）の投入
- **本社機構、製造・サービス拠点、ITの総合的取り組み**
- **できるところから着手し知恵を絞る**
  - 既存の危機管理体制、工場などの防災体制の活用
  - 「あらゆるリスク」という言葉に惑わされない
- **継続的改善**
  - 文書（マニュアル）策定で50%、教育訓練で50%
  - 解散が前提のプロジェクトチームとはせず、ノウハウの蓄積ができる体制を構築
- **情報開示と連携**
  - 有事に強い企業であることを株主、顧客、取引先、従業員、市民、自治体などに情報開示、アピール
  - サプライチェーンや地域との連携
- **重要インフラは国民生活・社会経済活動の基盤**
  - IT障害の発生を限りなくゼロに
  - 情報共有・分析機能の整備、分野横断的な演習、相互依存性解析の実施

TOKIO MARINE NICHIDO

東京海上日動の地震災害を想定した事業継続計画

- **基本方針の策定**
  - 人命第一
  - 業務継続方針
- **重要業務の選定**
  - 重要業務
    - 非被災地の業務の継続
    - 被災地の地震保険の支払業務
- **業務フローの分析**
  - 被害想定
    - 首都圏直下型地震の発生に伴う、本店、ITセンターの同時被災を想定（最悪のケース）
    - 本店は1ヶ月のビル機能停止を想定
  - 重要要素（ボトルネック）の特定
    - 情報システムのバックアップ
    - バックアップ業務（保険金支払い/契約内容照会システムの手作業化）

TOKIO MARINE NICHIDO

東京海上日動の地震災害を想定した事業継続計画（続き）

- **対策検討**
  - **対応策**
    - 安否確認システムの導入
    - バックアップシステムの見直し、手作業マニュアルの整備
    - 本店災害対策本部設置場所の機能改善/備品確保
    - 本店代替場所の準備（首都圏：6箇所、エリア分散）
    - 代行順位、指揮命令系統の確立
- **文書の作成**
  - **役割/階層毎にマニュアル・チェックリスト化**
    - コアメンバーマニュアル
    - 支店マニュアル
    - ポケットマニュアル（全員配布）
- **具体的対策の実施、BCPの定着化（教育・訓練）**
  - **役割/階層毎の教育訓練の実施**
    - 年1回社長以下役員に机上訓練（92年～）
    - 年1回対策本部会議室設営訓練（96年～）
    - 支店訓練、コアメンバー向け机上訓練など
    - バックアップシステム立ち上げ訓練（月1回）
  - **災害対策監査の実施**

東京海上日動リスクコンサルティングは、
貴社のＢＣＰ策定をご支援させていただきます。

TRCのサービスメニューについては、ウェブサイトでもご案内しております。刊行物のご案内や研究員レポートも掲載しておりますので、是非ご参照下さい。

http://www.tokiorisk.co.jp

TOKIO MARINE NICHIDO