

セキュリティとガバナンス

令和2年11月15日 上村章文

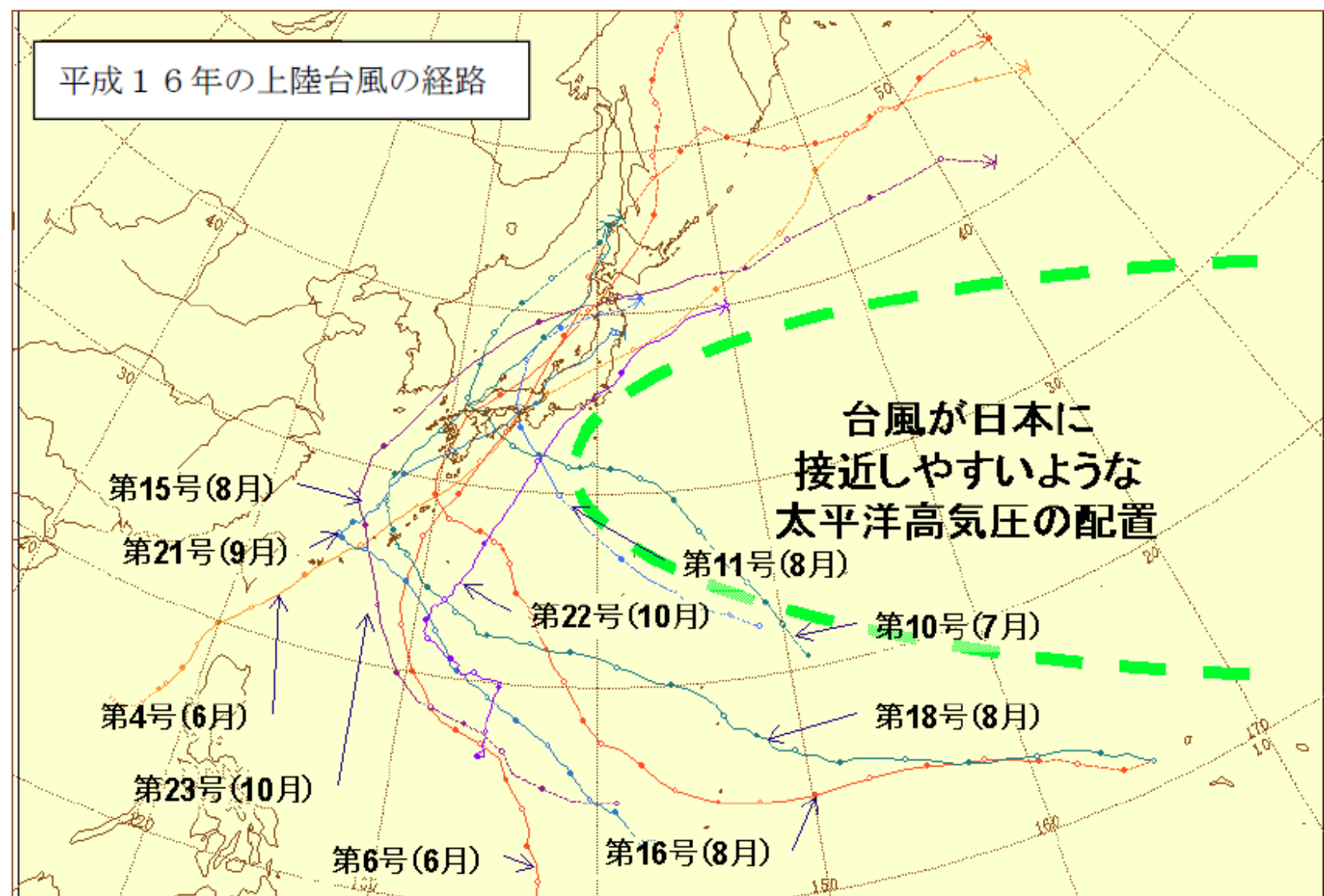
危機管理の本質とガバナンス

はじめにー平成16年から17年の危機管
理をふりかえって

頻発した危機管理に関する事態 4

- 新潟・福島豪雨、福井豪雨(H16. 7)
- 10個の台風の上陸(H16. 6~10)
- 台風23号(H16. 10、非常災害対策本部)
- 新潟県中越地震(H16. 10、非常災害対策本部)
- 各地で高潮被害が発生
- 福岡県西方沖地震(H17. 3)
- JR福知山線脱線事故(H17. 5)
- 千葉県北西部を震源とする地震(H17. 7)

平成16年の上陸台風の経路



その後の危機管理に関する事態 6

- 東日本大震災(H23. 3)
- 台風12号(H23. 9)
- 豪雪(H26. 2)
- 8月豪雨・広島市の土砂災害(H26. 8)
- 御岳山噴火(H26. 9)
- 熊本地震(H28. 4)
- 7月豪雨(H30. 7)
- 台風19号(R1. 10)
- 7月豪雨(R2. 7)

災害の教訓により対応した事項

7

- 避難報告等の判断・伝達マニュアル作成ガイドライン
- 災害時要援護者の避難支援ガイドライン
- 大規模災害発生時における国の被災地応急支援のあり方検討
- 防災に関する標準テキスト作成

1. 危機管理の本質

危機の発生という平常時と極めて異なる状況
の中で、損失を最小限にするために、いかに
適切なマネジメントを行うかということ

危機の特殊性

○突発性

○巨大性

○緊急性

○深刻性

危機の特性

- 突発性＝予測不可能な事態
- 巨大性＝大量資源投入の必要性
- 緊急性＝緊急対処の必要性
- 深刻性＝組織の存続に重大な影響

危機の種類と特性

	突発性	巨大性	緊急性	深刻性
大規模地震	◎	○～◎	◎	◎
大津波	○～◎	○～◎	◎	◎
洪水	△～○	○	◎	△～○
土砂災害	○	△	◎	△～○
高潮	△	△～○	○	△～○
火山噴火	△	△～◎	○～◎	◎
航空機事故	◎	△～○	◎	◎
列車事故	◎	△～○	◎	○～◎
林野火災	◎	△～○	○	△～○
原子力事故	◎	△～◎	◎	◎
テロ	◎	△～◎	◎	◎
鳥インフルエンザ・口蹄疫	○～◎	△～○	◎	△～○
新型インフルエンザ(H5N1)	△～◎	◎	◎	◎
新型コロナウイルス (COVID19)	△～◎	◎	◎	◎
法令遵守違反	△～○	△	△～○	△～◎
サイバーインシデント	△～◎	△～◎	○～◎	△～◎

危機管理の類型

- 組織自体が危機の発生の原因となるもの
- 外部からの要因により組織に危機が発生する場合
- 組織がその業務として他者の危機について対応する場合

2. 危機に強い組織づくり

危機管理の基本原則

- 初動時における対応が極めて重要であること
- 限られた情報の中で、①将来発生が予想される状況を推測しながら、②組織全体で危機に関する情報を共有し、適切かつ迅速な対応をとること

日本型組織の留意事項

- 危機管理には、調整型の時間のかかるボトムアップ方式ではなく、トップダウンによる迅速な意思決定が不可欠
- 調整型の時間のかかるボトムアップ方式ではなく、トップダウンによる迅速な意思決定が不可欠

危機管理は

最終的にはトップの判断力
とリーダーシップの問題

危機管理におけるトップの心得

- 危機発生に際し、将来発生するであろう状況を予測・推測し、先回りの対応を図る。
(シミュレーションの習慣を身につける)
- それぞれの危機のもつ性格、危機管理上の特性を理解(危機に関する基礎知識の習得)
- 前例にとらわれずに、状況を把握、分析し、迅速な対策を意思決定

危機管理におけるマネジメント能力

■ 危機管理に関する多様な知識

災害等の危機に関する知識の習得

事態対処に関する制度などの知識の習得

■ 意思決定能力

発生した事態に対して最適な判断を下す能力

ワークショップ・図上訓練

コントローラーからプレイヤーに対する状況付与

■ イマジネーション能力

今後起こることが予想される事態を想像する能力

危機管理の体制整備

- 危機管理組織・スタッフの配置
- 人材育成・訓練の実施
- 情報伝達・情報共有の仕組みづくり
情報システム・情報通信インフラ
- 危機管理センターの整備

オーランド市(フロリダ州)危機管理センター



オーランド市(フロリダ州)危機管理センター 22



マネジメントとの本質

保有する資源(人、モノ、金、情報＝経営資源)を活用して、組織目的を最大限に実現する。

3. 危機管理のオペレーション

- 危機発生時において経営資源(人、モノ)をいかに集中的に投入し、生命、財産の損失を軽減するか
- 危機発生時に意思決定を躊躇しないように、危機の特性に応じて危機発生時に対処すべき組織体制や調査分析、意思決定の手順、情報伝達などについて、予め計画を策定

新潟県中越地震

26

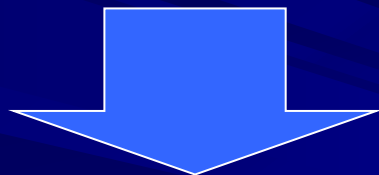
	新潟県中越地震 2004.10.23 05.56 pm	阪神・淡路大震災 1995.1.17 05.46 am
地震	マグニチュード 6.8 深さ 13km	マグニチュード 7.3 深さ 16km
死者・行方不明者	68	6,436
負傷者	4,805	約44,000
避難者	約103,000	約317,000
損壊家屋 (全壊)	約107,000 (約 2,800)	約513,000 (約 105,000)
火災	9	285

中山間地域の
孤立集落の発生

大都市地域の
経済的大損失

緊急事態に対する対応と 被災地の支援

Quake



30 分

➤ 災害対策要員のポケベルによる首相官邸の
危機管理センターへの緊急参集要請

➤ 防災担当大臣の指揮の下に局長級幹部で構
成される緊急参集チーム会議の開催

◆ 緊急の情報分析



地震直後の記者会見

災害応急対策

➤ 情報先遣チームを現地に派遣

➤ 捜索・救援部隊を動員

◆ 警察、消防、自衛隊

3 時間



➤ 全面的な捜索・救助活動

➤ 全国規模の緊急支援

◆ 緊急医療支援

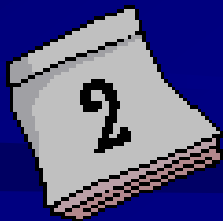
◆ 水と食糧

◆ 毛布と衣服

◆ 地すべりなど二次災害の防止

◆ インフラ及びライフラインの応急復旧

24 時間



情報先遣チームを地震発生当日に派遣²⁹



➤8省庁の11人の構成員

➤地震発生から3時間後に
東京を出発

➤自衛隊のヘリコプターを利用



地震による被害の状況

30





防災担当大臣を団長とする政府調査団が 2004年10月24日に現地調査

32



知事との意見交換



市長との意見交換



防災担当大臣を本部長とする 非常災害対策本部の設置

33



➤ 21省庁の局長等が出席する本部会議

➤ 21回にわたる会議

➤ 現地支援対策室とのテレビ会議

➤ 被災地のニーズに即応するため省
庁横断的に設置された12のプロ
ジェクトチーム



○ 新潟県中越地震の際の12のプロジェクトチーム 34

- ① 下水道・トイレ
- ② 物流
- ③ 災害廃棄物
- ④ 避難者・被災者の生活の質的向上
- ⑤ 住宅
- ⑥ 医療・健康管理
- ⑦ 災害時要援護者
- ⑧ 地場産業・中小企業・農林水産業
- ⑨ 積雪・寒冷対策
- ⑩ ボランティア
- ⑪ 公共インフラ
- ⑫ 山古志村

搜索と救助 / 避難

2,700人以上の救出

地震発生後5日目に東京消防庁のハイパーレスキュー隊により救出された幼児



負傷者の救助活動



山古志村全村民の救助・避難

緊急援助物資の輸送

24日, 25日に330,000食以上

毛布23,000枚以上



ボランティア活動

ボランティアの総数:50,000人以上



山のように積まれた、
救援物資の配送を円
滑かつ適切に行うため
には、物流の専門家
のボランティアの助け
が必要

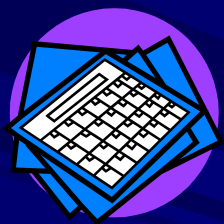


災害ボランティアセンターによるボランティア
の活動の連絡調整



ボランティア活動

応急対策から復旧・復興への移行の段階



1-3 週間

余震

10月27日 マグニチュード 6.1
11月8日 マグニチュード 5.9

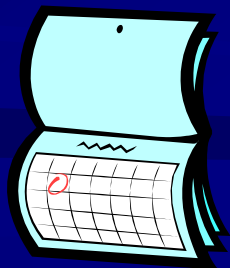
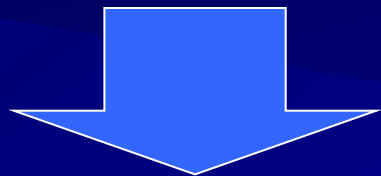
➤ 避難者の生活の質的向上

- ◆ 温かく多様な食事
- ◆ 入浴サービス
- ◆ PTSDに対する心のケア
- ◆ 高齢者や障害者の旅館への避難

➤ インフラとライフラインの完全復旧

➤ 復旧・復興段階への円滑な移行

- ◆ 住まいの確保
- ◆ 冬や雪への備え
- ◆ 地域経済の復興
- ◆ 孤立・荒廃した地域の支援



1ヶ月後

全村避難の山古志村に対する支援 39



全村を襲った地すべり

岩石、土砂により堰き止め
られた芋川



美しく活力のあるコミュニティの 復旧・復興を目指して

40



事業継続計画(BCP)

1. 事業継続計画(BCP)の意義とBCM

危機管理計画

1. 危機事象の発生を抑止
2. 危機事象による影響を抑止
3. 危機発生による影響からの回復

■ 企業の事業継続計画は主として2及び3を想定したもの

BCP とコンティンジェンシープラン (Contingency Plan : CP、緊急時対応計画)

BCP は事業の継続性の観点から事項、手順、体制、資源等の計画を具体化したもの

CPは緊急事態発生直後の行動を中心とした計画

BCPは事前にビジネスプロセスの脆弱性を分析(ビジネスインパクト分析)した上で、それに基づいた計画を実施することに特徴

BCPに初動対応としてのCPを包含して策定

事業継続計画

- 事業継続計画(BCP: Business Cintunuity Plan)とは、災害等の危機発生時において企業等の組織が様々な業務阻害要因のなかで障害を克服し、その本来の業務を継続するための方針、体制、手順等を示した計画

事業継続計画(BCP)の意義

- 災害等の危機発生時に経営資源が毀損するなかで、可能な限り組織の業務を継続し、早期に通常業務の実施体制を回復するためには、危機事態発生時の対応について詳細に定めたBCPの策定、周知等が必要
- BCPの策定は取引先等関係者との間の安定的な経済活動を継続するうえで重要な要素、企業価値の向上につながり、企業マネジメント、企業の社会的責任(CSR)として重要である。

BCPの求められる背景

47

1. 集約化とサプライチェーン

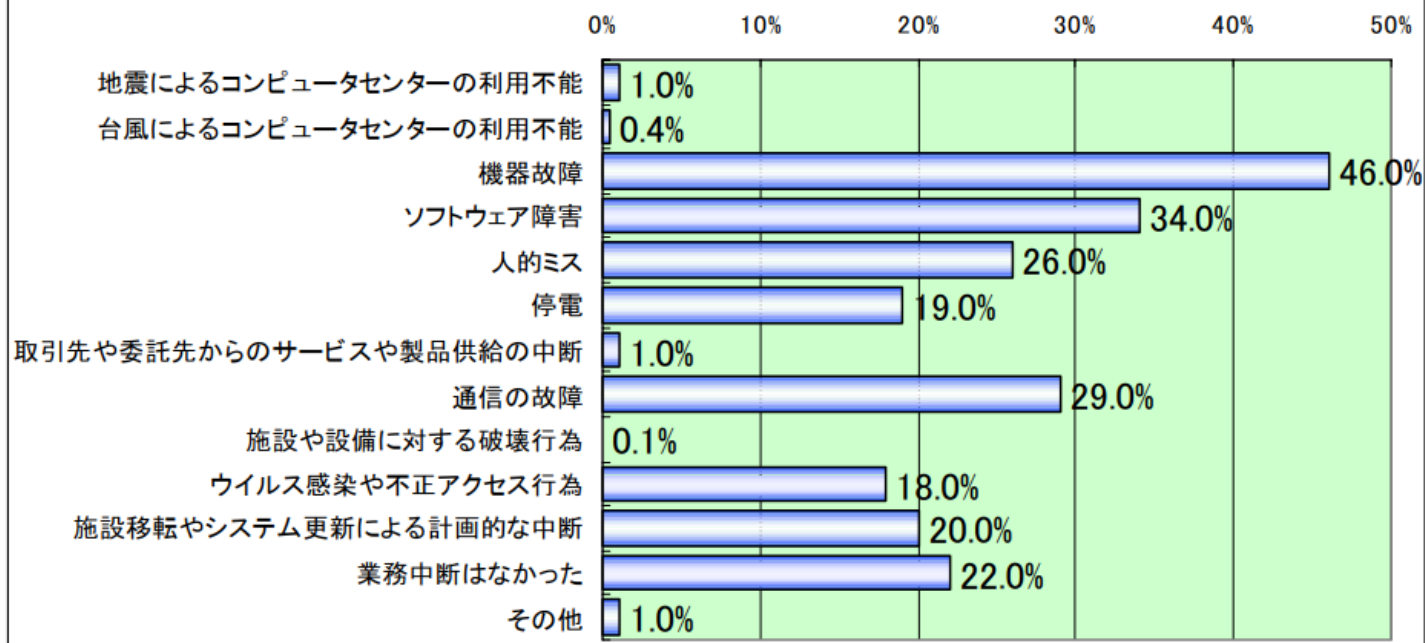
- コスト削減を行うため、生産拠点や物流拠点、取引先を集約化
- 拠点や取引先に障害が発生した場合、代替拠点や取引先の手配を困難にし、基幹事業の停止に直結する確率が格段に増加
- サプライチェーンを構成する一企業にボトルネックがあれば、構成企業全体に影響を与える

2. 情報システムへの依存増大

- 金融サービスや通信サービスを提供する企業だけでなく、在庫管理や受発注管理、顧客管理等、ほとんどすべての企業の事業は情報システムやネットワークの稼動を前提に構築
- ビジネスの中断の原因には情報システムの障害によるケースが非常に目立つ
- 情報システム障害にBCPがない場合、事業存続に大きな影響

【図表 2 業務中断の原因】(KPMG ビジネスアシュアランス ビジネス継続マネジメントサーベイ 2002)

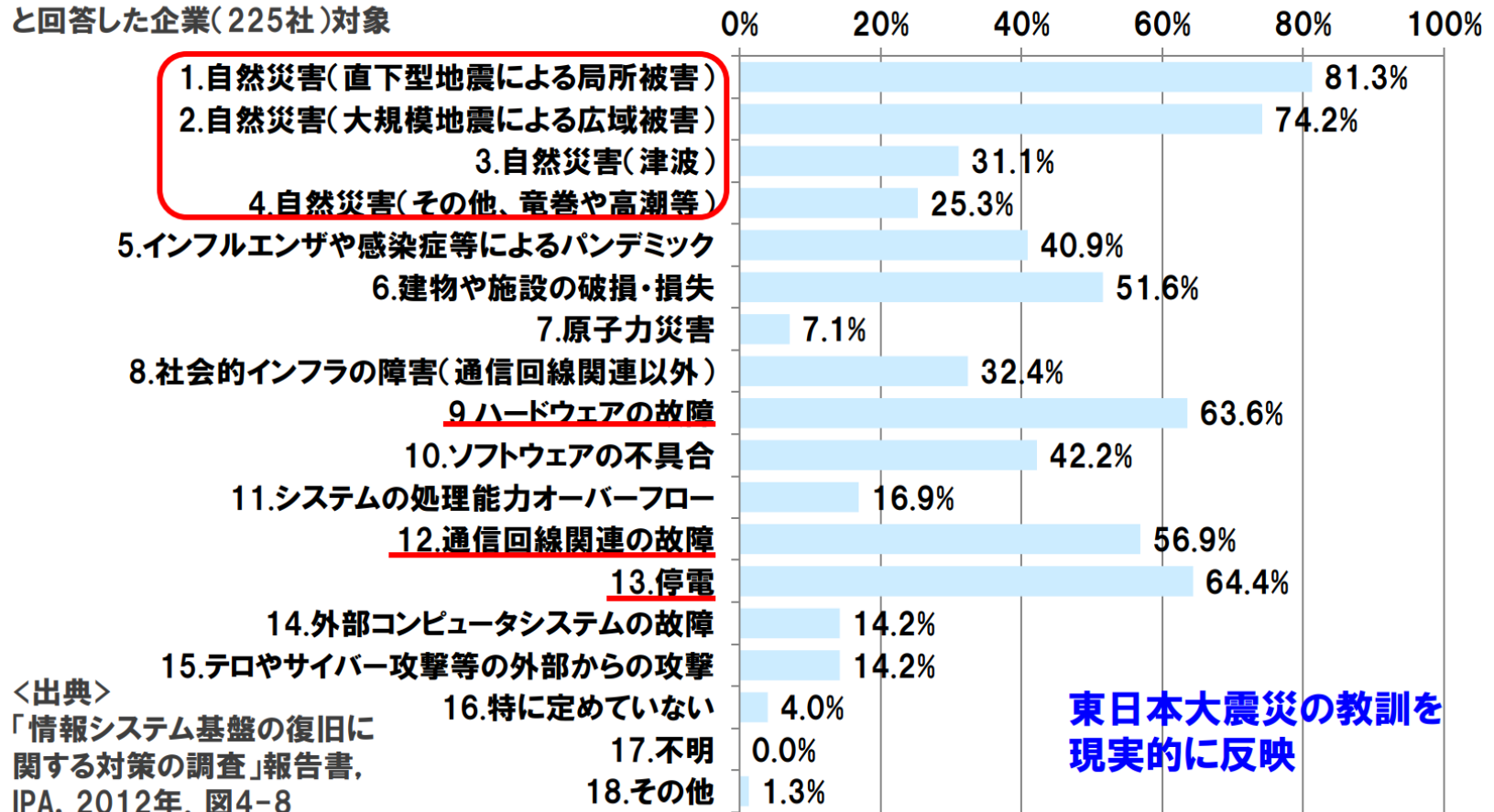
【質問】「貴社において過去一年間に下記のうち、どの原因による業務中断を経験しましたか(複数選択可)」



ITサービス継続計画策定時に想定するリスク

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

IT-BCPを「策定済み」または「未策定(検討中)」
と回答した企業(225社)対象



東日本大震災の教訓を
現実的に反映

<出典>

「情報システム基盤の復旧に
関する対策の調査」報告書,
IPA, 2012年. 図4-8

事業継続計画の内容

■ 緊急参集

緊急参集要員(緊急参集チーム)と集合場所の指定

■ 安否確認、被災状況の調査

社員、施設、公共インフラ等の利用可能な経営資源の把握

■ 優先順位の決定と優先業務の開始

企業価値最大化のため、利用可能な資源により優先して継続する業務を決定、実施可能な業務を再開

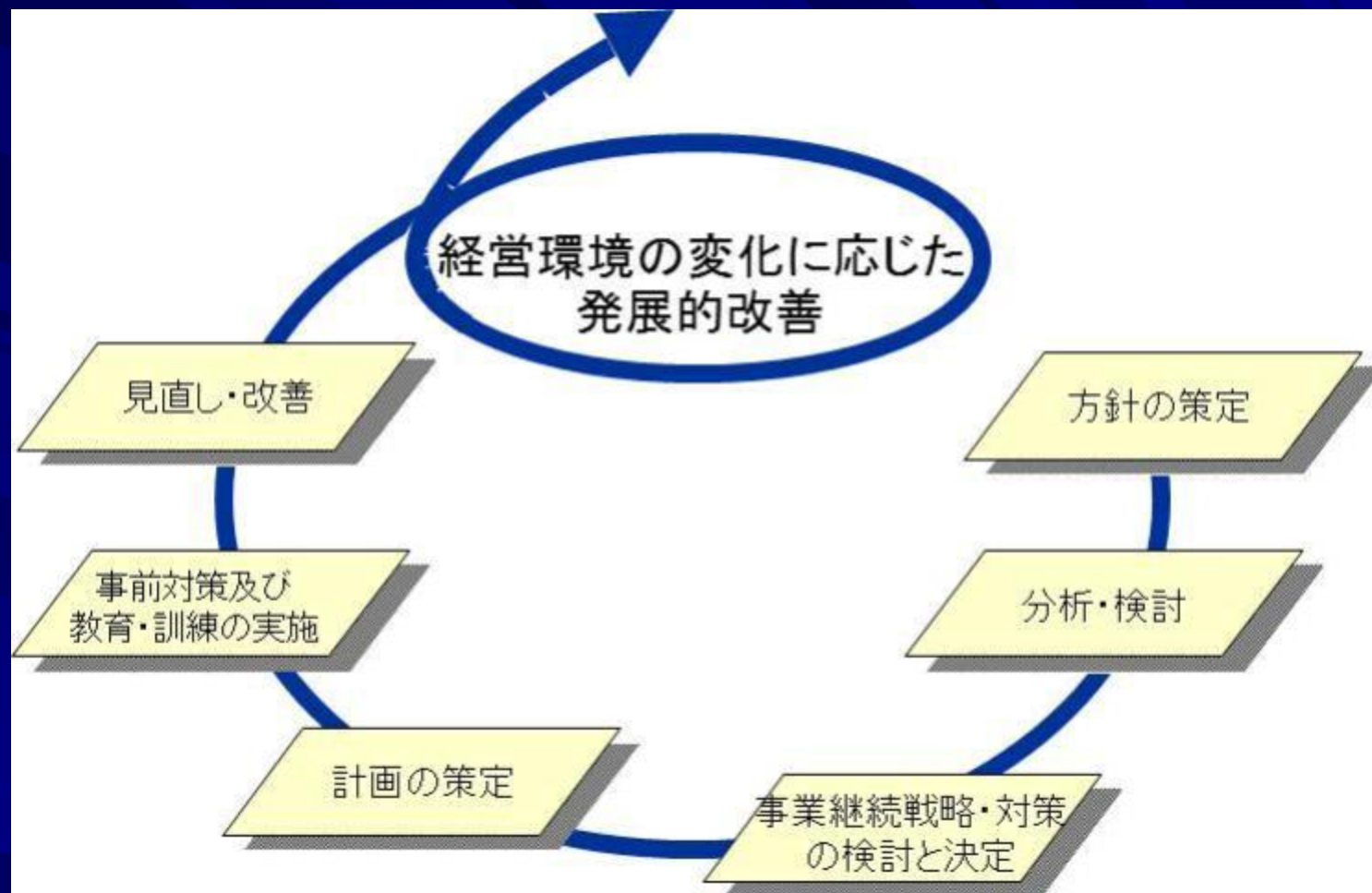
■ 復旧計画の策定

施設、設備の復旧計画を策定、実施により順次業務を再開

事業継続マネジメント (Business Continuity Management、BCM)

- BCP策定や維持・更新
- 事業継続を実現するための予算・資源の確保
- 事前対策の実施
- 取組を浸透させるための教育・訓練の実施
- 点検、継続的な改善

など平常時からのマネジメント活動

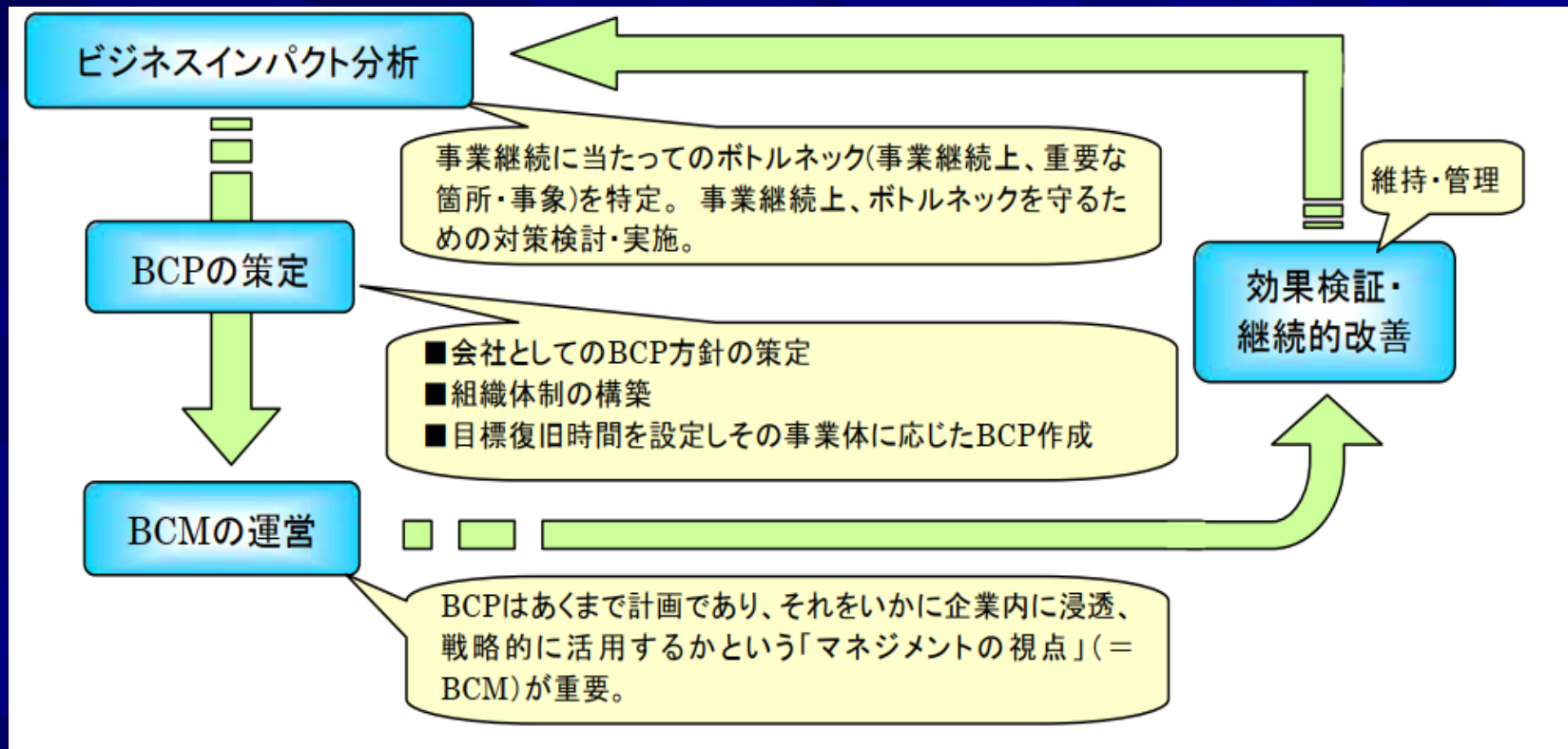


BCMの重要ポイント

- 不測の事態において事業を継続する仕組
- 社内のBCP及びBCMに関する意識の浸透
- 事業継続の仕組及び能力を評価・改善する仕組

BCM構築の一般的な流れ

(経済産業省報告書)



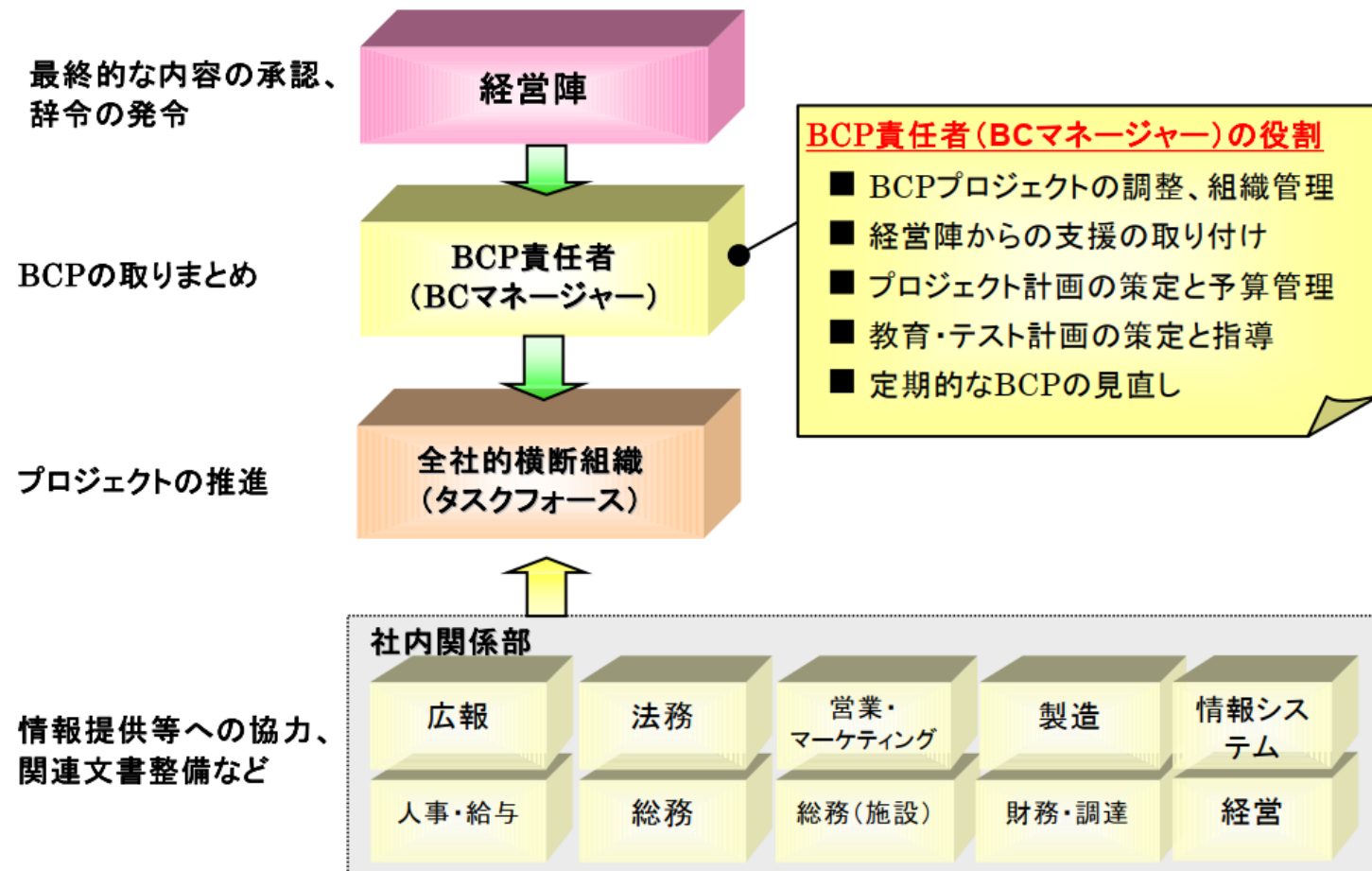
BCPの対象範囲

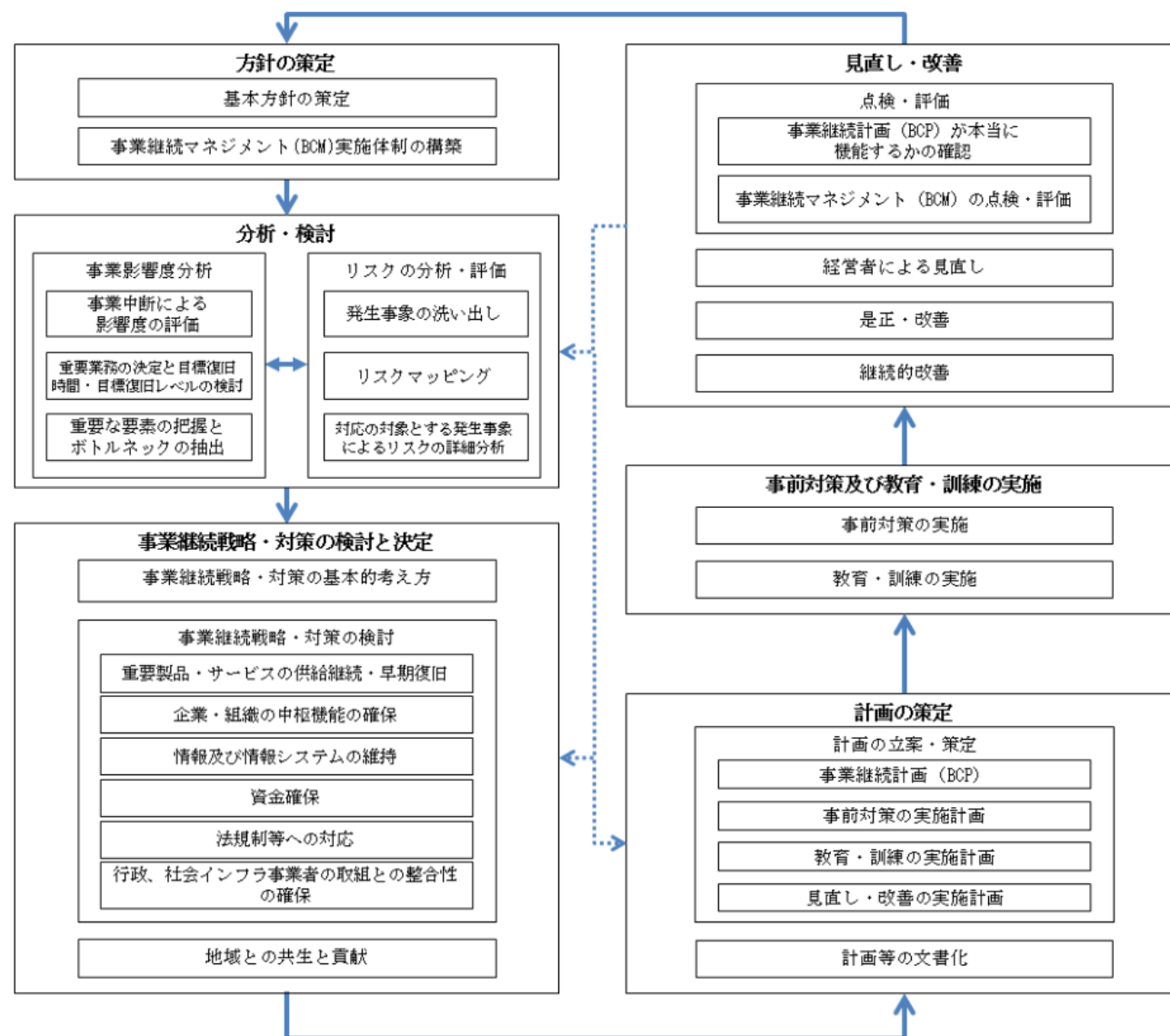
- 対象範囲は原則として、全ての事業・業務、施設、人員
- 組織によっては、対象範囲を基幹事業・業務に特定したり、優先度に応じて復旧させる施設(設備)を限定したりする場合も考えられる。
- BCPにおいても、対象とする業務、対象施設、対象となる人員を定義することは必要。段階的にその範囲を拡大していくことも考慮。

BCPの対象範囲の例

対象範囲	記述の例
対象事業・業務	全ての事業・業務、基幹事業・業務など。
対象施設	対象施設が被災した場合に、事業・業務の継続が困難となる可能性のある本社・他の拠点ならびにコンピュータセンターとする。
対象となる人員	対象施設に常勤の正社員、契約社員、派遣社員ならびに協力会社社員等。 その他、対象施設に来訪している顧客等については、必要に応じて対象に準じた扱いをする。

BCP プロジェクトの組織体制の例



図 1.5-1 事業継続マネジメント(BCM)の各プロセス¹⁸

2. 事業継続計画の分析・検討

ステップ1 事業影響度分析(Business Impact Analysis、BIA)

組織における重要な事業・業務(基幹事業・業務)・プロセス、それに関連するリソースを特定、事業継続に及ぼす影響の分析を行う。

- 事業継続・普及の優先順位付け
 - 特定した事業・業務やそれに関連するリソースのうち、その影響度を総合的に勘案したうえで、事業継続及び早期の事業再開の観点から、それぞれに優先順位をつける。
 - ボトルネックの特定
 - 事態から想定されるシナリオのうち最悪のシナリオ・事態を設定、優先して検討
 - 事業を継続する上でのボトルネックとなるリソースの喪失を特定
 - 目標普及時間の設定
 - 目標復旧時間(RTO)
- 事業・業務の中断が発生した場合、事業に重大な影響を及ぼさないうちに事業活動を復旧・再開させるための目標時間を設定する

事業中断による影響度を評価する観点(例)

- 利益、売上、マーケットシェアへの影響
- 資金繰りへの影響
- 顧客の事業継続の可否など顧客への影響、さらに、顧客との取引維持の可能性への影響
- 従業員の雇用・福祉への影響
- 法令・条例や契約、サービスレベルアグリーメント(SLA)等に違反した場合の影響
- 自社の社会的な信用への影響
- 社会的・地域的な影響(社会機能維持など)

優先的に継続・復旧すべき重要業務を絞り込む

影響度評価の結果

業務ごとに

- 時間の許容限界(停止・低下時間)
 - レベルの許容限界
- の推定

事業影響度の時系列分析から推定

どれくらいの時間で復旧させるか＝
「目標復旧時間(Recovery Time Objective、RTO)」

どの水準まで復旧させるか＝
「目標復旧レベル」(Recovery Level Objective、RLO)」
の設定

許容限界より早い・高いレベルで設定

業務間の優先順位の設定

重要な要素の把握とボトルネックの抽出

それぞれの重要業務の実施に不可欠となる重要な要素(経営資源)を把握

全てを漏れなく洗い出す

当該重要業務の復旧、復旧レベルの向上に不可欠な要素「**ボトルネック**」として特定



重要な要素の中で、必要とされている量の確保が可能となるまでの時間をより早めない限り、当該重要業務の復旧をさらに早めたり、復旧レベルを上げたりすることができないもの

事業を構成する業務・工程・部門、事務所・工場等の拠点、物流、キーパーソン、データ、システム、資金など

ビジネスインパクト分析のイメージ

【図表4 ビジネスインパクト分析結果のイメージ】

[illegible]

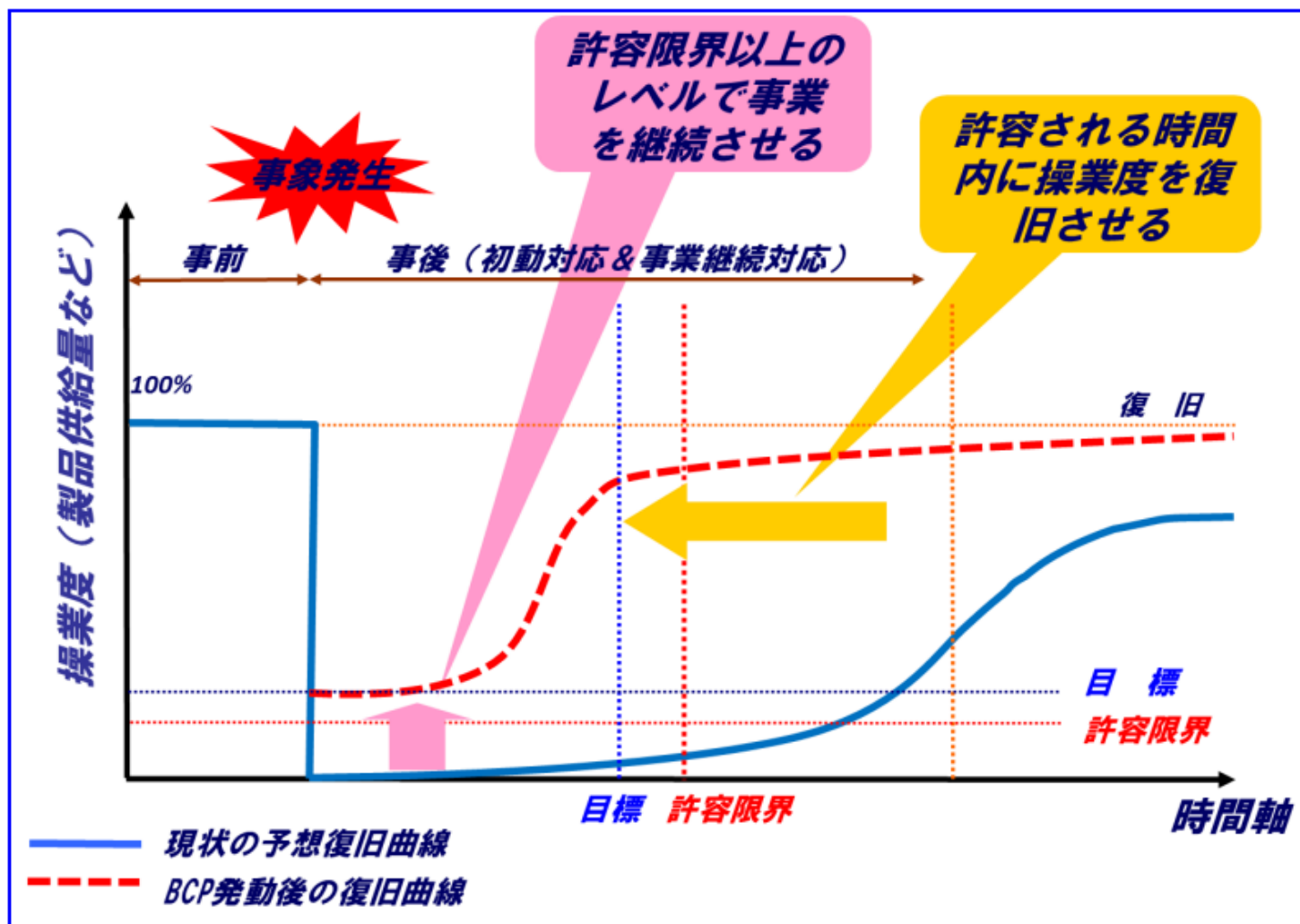
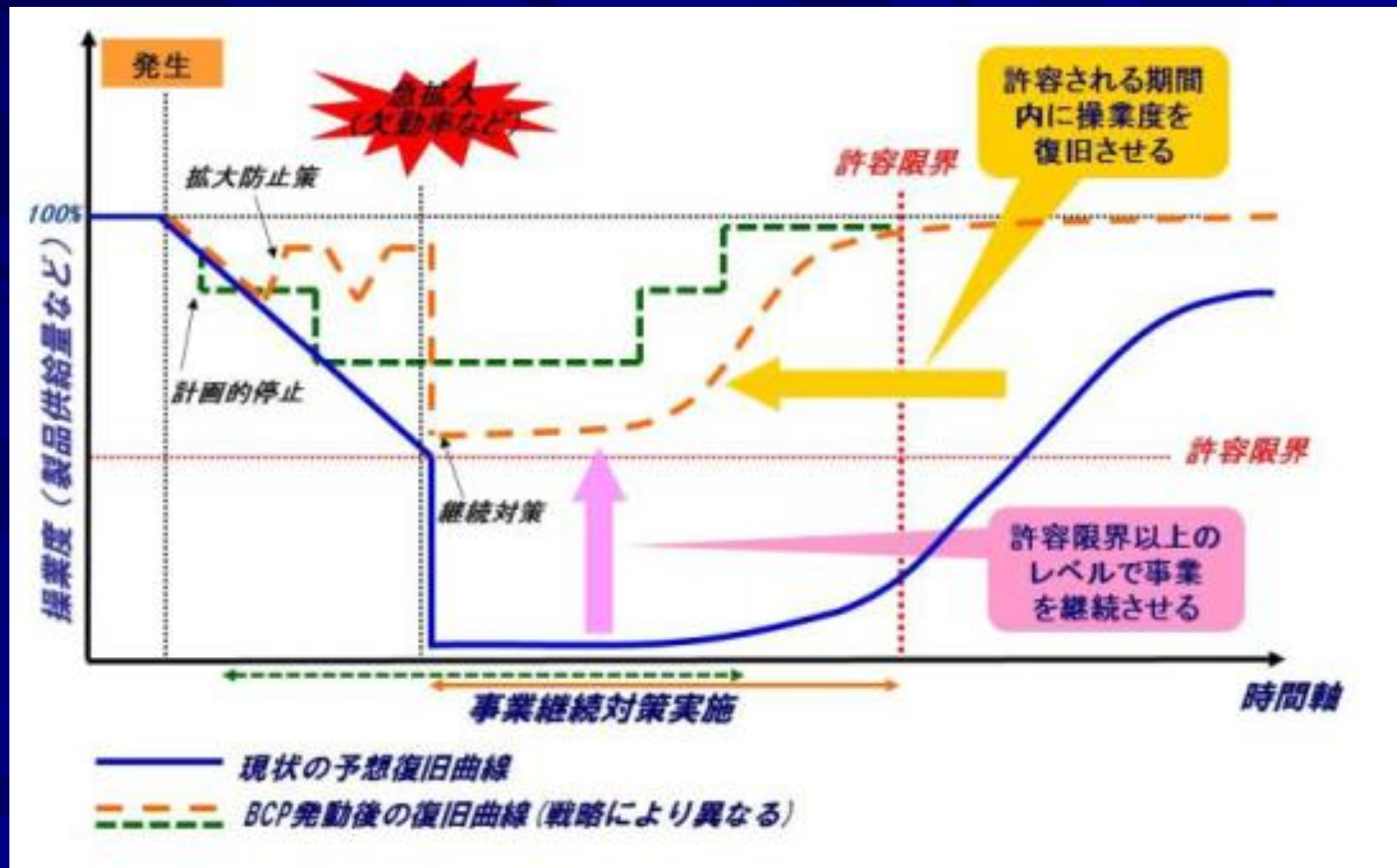


図 1.1-1 事業継続計画（BCP）の概念^{7, 8}

感染症に関するイメージ図



ステップ2: リスクの分析・評価(リスクアセスメント)

① 発生事象の洗い出し

自社の事業の中断を引き起こす可能性がある発生事象を洗い出す。極力発生し得る全てのものを考慮する。

② リスクマッピング ①で洗い出された発生事象について、発生の可能性及び発生した場合の影響度について定量的・定性的に評価し、優先的に対応すべき発生事象の種類を特定し、順位付けする。

③ 対応の対象とする発生事象によるリスクの詳細分析

②で優先的に対応すべきと特定した発生事象により生じるリスクについて、自社の各経営資源や調達先、インフラ、ライフライン、顧客等にもたらす被害等を想定する。

リスクの詳細分析は**事業影響度分析**で選定した**重要業務**に対して行うのが通常

具体的には、

①特定した発生事象によって、当該重要業務について把握した重要な要素が、現状(すなわち、対策の実施前)において、どのような被害を受けるかを検討

②その重要な要素を確保するために現状で要する時間を推定

③その重要業務が現状ではいつまでに復旧できるか(=現状で可能な復旧時間RTO)

どのぐらいの業務水準で継続・復旧できるか(=現状で可能な復旧レベルRPO)

を推定するという手順が一般的

3. 事業継続戦略・対策の検討と決定

事業継続戦略・対策の検討

企業・組織が検討すべき事業継続戦略を検討する観点として

- ① 重要製品・サービスの供給継続・早期復旧
- ② 企業・組織の中核機能の確保が特に重要。

さらに、次の観点も重要。

- ③ 情報及び情報システムの維持
- ④ 資金確保
- ⑤ 法規制等への対応
- ⑥ 行政・社会インフラ事業者の取組との整合性の確保

1. 重要製品・サービスの供給継続・早期復旧

(1) 業務拠点に関する戦略・対策

- 拠点（本社、支店、支社、工場等）の建物や設備の被害抑止・軽減
- 拠点の自社内での多重化・分散化
- 他社との提携（OEM、アウトソーシング、相互支援協定の締結等）
- 在宅勤務、サテライトオフィスでの勤務

(2) 調達・供給の観点での戦略・対策

- 適正在庫の見直しや在庫場所の分散化による供給継続
- 調達先の複数化や代替調達先の確保
- 供給先・調達先との連携
- 代替調達の簡素化（汎用部品の使用など設計仕様における考慮等）

(3) 要員確保の観点での戦略・対策

- 重要業務の継続に不可欠な要員に対する代替要員の事前育成・確保
- 応援者受け入れ（受援）体制・手順の構築、応援者と可能な範囲で手順等の共通化
- 調達先や連携先におけるBCM 支援のための人員の確保

2. 企業・組織の中核機能の確保

本社が被災した場合の対策

- 本社の建物・施設に対して想定する発生事象(インシデント)からの被害を軽減する対策を講じることは、最も基本的な戦略
- 従業員等の生命・身体を守る観点からも重要
- 同時に被災しない拠点を代替拠点として確保

さらに

- 企業・組織の中核機能である経営者を含む対策本部、財務、経理、人事、広報等の各部署にが機能するために不可欠な要員、設備等の経営資源の確保が必須
- 緊急参集及び迅速な意思決定を行える体制や指揮命令系統の確保を行うとともに、特に通信手段、電力等の設備、ライフライン確保の対策が必要。

情報発信

- 復旧可能性の情報発信が重要
- 取引先、顧客、従業員、株主、地域住民、政府・自治体などへの情報発信や情報共有を行うための自社内における体制の整備、連絡先情報の保持、情報発信の手段確保

事業継続戦略における検討の視点



重要業務に不可欠な要素、特にボトルネックとなる要素をいかに確保するかを検討

2つの観点から様々な選択肢を検討する

現地復旧戦略
＝被害からどのように防御・軽減・復旧するか



最も事業継続しやすい

拠点代替戦略
＝どのように代わりを確保するか



幅広い発生事象に共通した
対応策として有効性が高い

平常時のコスト・採算性
多重化の困難性

3. 情報及び情報システムの維持

- 重要業務の継続には、自社における重要な情報及び情報システムを被災時でも使用できることが不可欠
- 重要な情報についてはバックアップを確保し、同じ発生事象（インシデント）で同時に被災しない場所に保存
- 重要な情報システムには、必要であればバックアップシステムも求められ、電源確保や回線の二重化を確保する

4 資金確保（リスクファイナンス）

- 資金繰り（キャッシュフロー）の悪化を防ぐため、企業・組織自身が、日頃から危機的事象に対応するための最低限の手元資金を確保
- 保険、共済、デリバティブ、災害時融資予約、災害時ローン、事前対策に活用できる融資（BCM格付融資、BCPの支援ローン等）等の調査検討

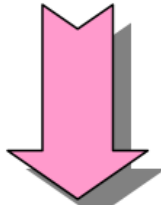
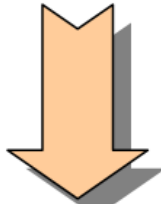
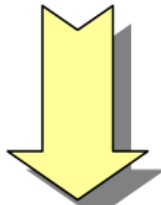
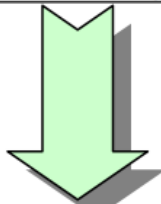
5 法規制等への対応

- 想定する発生事象（インシデント）により企業・組織が被害を受けたとしても、法令や条例による規制その他の規定は遵守
- 関係する政府・自治体の機関に要請して、緊急時の緩和措置等について検討

6 行政、社会インフラ事業者の取組との整合性の確保

- 自らのBCP・BCMを、政府・自治体、指定公共機関等の社会インフラ事業者のBCP・BCM、防災業務計画、地域防災計画等と整合性を持たせるよう努める
- 政府・自治体や社会インフラ事業者の側も、地域における企業・組織のBCP・BCMを意識し、それを考慮した計画となるように努力すべき

4. 事業継続計画の策定

災害・事故の発生BCP発動代替手段による
業務継続の拡大平常運用への切替え開始
(復旧範囲の拡大)全面復旧ステップ1:BCP発動フェーズ

- 災害や事故の発生(或いは発生の可能性)を検知してから、初期対応を実施し、BCP発動に至るまでのフェーズ。
- 発生事象の確認、対策本部の速やかな立ち上げ、確実な情報収集、BCP基本方針の決定がポイント。

ステップ2:業務再開フェーズ

- BCPを発動してから、バックアップサイト・手作業などの代替手段により業務を再開し、軌道に乗せるまでフェーズ。
- 代替手段への確実な切り替え、復旧作業の推進、要員などの経営資源のシフト、BCP遂行状況の確認、BCP基本方針の見直しがポイント。
- 最も緊急度の高い業務(基幹業務)の再開。

ステップ3:業務回復フェーズ

- 最も緊急度の高い業務や機能が再開された後、さらに業務の範囲を拡大するフェーズ。
- 代替設備や代替手段を継続する中での業務範囲の拡大となるため、現場の混乱に配慮した慎重な判断がポイント。

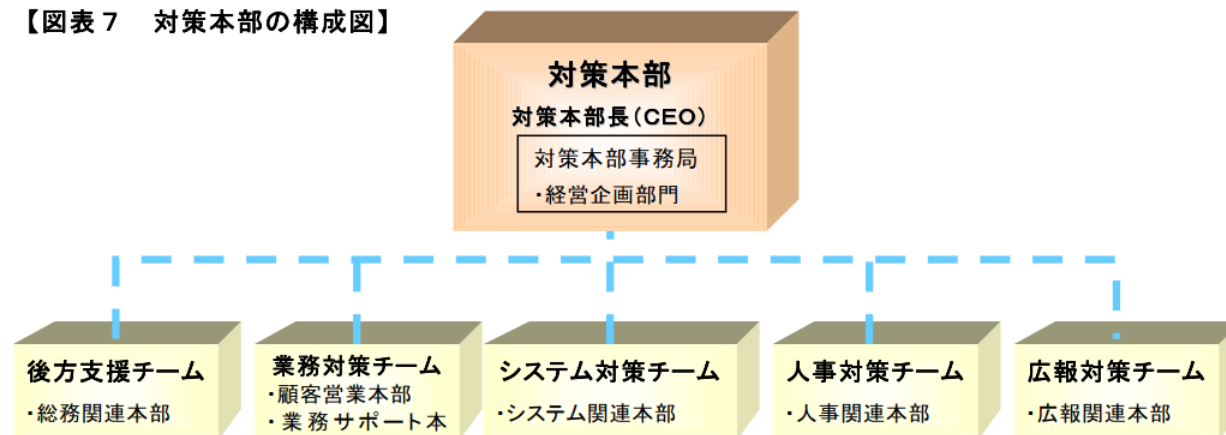
ステップ4:全面復旧フェーズ

- 代替設備・手段から平常運用へ切り替えるフェーズ。
- 全面復旧の判断や手続きのミスが新たな業務中断を引き起こすリスクを是らんでおり、慎重な対応が要求される。

緊急時の体制

- 不測の事態に対応するべく、事業継続のための緊急的な体制を定め、関係者の役割・責任、指揮命令系統を明確に定め、その責任者は、経営者CEOが担う。
- 権限委譲や、代行者及び代行順位も定める。
- 緊急時には非日常的な様々な業務が発生するため、全社の各部門を横断した、事業継続のための特別な体制を作ること検討。
- 災害時の初動対応や二次災害の防止など、各担当業務、部署や班ごとの責任者、要員配置、役割分担・責任、体制などを定めることも必要

【図表 7 対策本部の構成図】



＜対策本部設置基準の例＞

- 東海地震に関する注意情報（あるいは予知情報、警戒宣言など）の発表
- 本店、主要拠点、システムセンターの設置地域における震度〇以上の地震発生
- 緊急度レベル〇の障害が発生し、回復の見込みがない
- 大規模な情報漏えい事故の発生、もしくはその恐れを検知
- 大規模なシステム統合・更改の〇日前

実施主体	実施事項	
	項目	詳細
対策本部(本社及び各拠点)	参集及び対策部の立ち上げ・指揮命令系統の確立	<ul style="list-style-type: none"> ● あらかじめ定められた参集基準に基づき、参集対象者は所定の場所への参集 ● 参集後における、対策本部の迅速な立ち上げ ● 参集場所が利用できない場合は、代替拠点へ参集
	建物、設備、従業員等経営資源の被害状況の確認	<ul style="list-style-type: none"> ● 建物、構築物、設備、作業現場等の被害確認 ● 従業員等の安否確認を実施、結果を集約
	顧客・従業員の安全確保及び物資配給	<ul style="list-style-type: none"> ● 避難が必要な場合、顧客・従業員の避難誘導 ● 水・非常用食料等の必要な物資を配給(備蓄の活用、必要に応じ追加調達) ● 必要な場合、安全な帰宅方法の指示
	二次災害の防止	<ul style="list-style-type: none"> ● 落下防止、火災の防止(ガス栓の遮断・確認等、必要なら一部電源の遮断を含む)、薬液漏洩防止、危険区域の立入禁止など、安全対策の実施 ● 危険が周辺に及ぶ可能性のある場合、住民への危険周知や避難要請、行政当局への連絡
	自社の状況についての情報発信	<ul style="list-style-type: none"> ● 連絡手段の確保 ● 社内の被害状況等の情報集約 ● 社内外の必要な相手先に対し、自社の状況についての情報発信(連絡先一覧による)
	事業継続計画(BCP)の発動	<ul style="list-style-type: none"> ● 初動が落ち着いた後、然るべき権限者は、あらかじめ定められた基準に基づき、事業継続計画(BCP)発動の可否を判断し、発動となった場合、事業継続体制へ移行
	対応の記録	<ul style="list-style-type: none"> ● 実施した対応や、発生した問題点等の記録

実施主体	実施事項	
	項目	詳細
各従業員	自身及び周囲の安全確保	身の安全を確保した後、初期消火、周囲のケガ人や閉じ込め者の救出（救出用資材を活用） 必要な場合には避難
	自身の安否についての報告	定められる方法に基づき、自身及び家族の安否の報告

実施主体	実施事項	
	項目	詳細
対策本部・事業継続組織 (本社及び重要業務の拠点)	自社の事業継続に対して、求められている事項の確認、調整	<ul style="list-style-type: none"> ● 重要な製品・サービスの供給先や関係当局との連絡、WEBサイトによる通達や告示の閲覧等により情報収集 ● 自社の事業継続に対して、求められている事項の確認、必要に応じて相手方と調整
	現拠点、代替拠点での事業継続の能力・可能性の確認	<ul style="list-style-type: none"> ● 自社の経営資源の被災状況、調達先やサプライチェーンの状況等、必要資源の確保可能性の確認 ● 情報のバックアップ、バックアップシステムの保存、稼働の状況の確認 ● 復旧資材の必要性・入手可能性の把握 ● 必要なら、被災拠点に先遣隊や調査隊の派遣 ● 現拠点での復旧可能性や復旧可能時間の見積もり ● 代替拠点や OEM その他の提携先の状況確認 ● 必要なら、代替拠点での業務立ち上げ時間等の見積もり
	実施する戦略や対策の決定	<ul style="list-style-type: none"> ● 実施する復旧、代替等の戦略を決定(現地復旧、代替拠点活用、OEM等の提携先活用等) ● 基本方針、目標、対策の優先順位を決定 ● 戦略に基づき実施する主要な対策の決定
	業務の継続・再開	<ul style="list-style-type: none"> ● 業務の継続・再開に向けた各対策を実施(現拠点の復旧手順、代替拠点の立ち上げ手順、バックアップシステム立ち上げ手順等を活用) ● 重要業務に係る主体との連絡調整 ● 対策実施状況の進捗管理及び追加指示 ● 臨時予算の確保 ● 業務の継続・再開・復旧の状況把握
	自社の状況についての情報発信	<ul style="list-style-type: none"> ● 対外的に発信すべき情報の集約・判断 ● 取引先、消費者、従業員、株主、地域住民、地方公共団体などに対して、自社の事業継続の状況について情報発信
	平常時の体制への帰	<ul style="list-style-type: none"> ● 臨時あるいは当面の業務実施の方法・体制を平常時の方法・体制に復帰
	対応の記録	<ul style="list-style-type: none"> ● 実施した対応や、発生した問題点等の記録

5. 教育・訓練の実施

BCMを実効性のあるものとするには、経営者をはじめ役員・従業員に事業継続の重要性を共通の認識として持たせ、その内容を**社内**に「**風土**」や「**文化**」として**定着させる**ことが重要、継続的な教育・訓練の実施が不可欠

訓練の目的

- 対象者が知識として既に知っていること(バックアップシステムの稼動方法、安否確認等)を実際に体験させることで、身体感覚で覚えさせること
- 手順化できない事項(経営者の判断が必要な事項、想定外への対応等)について、適切な判断・意思決定ができるようにする能力を鍛えること
- BCP やマニュアルの検証(これらの弱点や問題点等の洗い出し)をすること

など

教育・訓練の実施方法の例

	概要	実施方法(例)
教育	1. 基礎知識の提供	● 事業継続の概念や必要性、想定する発生事象(インシデント)の概要など 講義、eラーニング等による
	2. 自社のBCMの周知	● 講義、ワークショップ、eラーニング等による
	3. 最新動向の把握	● 専門文献や記事の購読 ● 外部セミナー、専門講座、ワークショップ等への参加等による
訓練	4. 代替要員の事前育成・確保	● クロストレーニング: 欠勤者が出た場合にその重要業務の代替を可能とするため、他の重要業務の担当者とお互いに相手方の業務を訓練する
	5. BCP、マニュアル	● 内容確認(ウォークスルー): BCP やマニュアルに基づき、役割分担、手順、代替先への移動 ● 確認等を机上訓練などにより行う
	6. 手順書、マニュアルの習熟	● 反復訓練(ドリル): 重要な動作等を繰り返して行うことで身に付ける実働訓練で、避難訓練、消防訓練、バックアップシステム稼動訓練、対策本部設営訓練などがある

	概要	実施方法(例)
訓練	7. 事業継続能力の確認・向上、及び意思決定のための訓練	<ul style="list-style-type: none">● 以下のような様々な訓練の要素を適宜組み合わせ、実効性の高い訓練を実施する● 災害模擬演習(モックディザスター): 模擬的に緊急時を想定した状況下において判断・対応を体験する● 状況想定訓練(シミュレーション): 緊急時に発生する様々な状況を想定し、実際に対応できるかを確認する● 役割演技法訓練(ロールプレイング): 緊急時に状況が変化する中で、それぞれが各役割に応じた対応や意思決定を模擬的に行う● さらには、発展的な訓練として以下のような訓練がある● 総合演習(フルスケールエクササイズ): 机上訓練と実働訓練を組み合わせ、模擬負傷者の救護・搬送、代替場所への移動、目標復旧時間内での業務再開など、対応力を確認する。限りなく現実に近い状況を想定し、実際に活用する環境等で実施する● 業界・市場をあげた連携訓練: 同業他社や他業界、複数の取引先なども含めて行う

6. 点検・評価

事業継続計画(BCP)が本当に機能するかの確認

策定したBCPによって重要業務が目標復旧時間や目標復旧レベルを本当に達成できるかを確認

様々な要因に対して、BCM が合致しているか、必要な変更が行われているかの視点からも点検・評価

BCMの拡充における観点での点検・評価

監査の活用によるBCMの点検・評価

- 事前対策、訓練、点検等がスケジュール通り実施されているか、予算は適切に執行されているか
- 事業継続戦略・対策は有効か、費用対効果は妥当か
- 教育・訓練は目標を達成しているか
- 業界基準やベストプラクティス等と比較して重大なギャップはないか
- 自社の事業継続能力が向上しているか

7. 情報システムにおけるBCP

情報システムにおけるBCPの対象

脅威		リスク発生事象	特性	対策
大規模災害	地震、水害、津波 等自然災害 火災、事故災害	建物、設備、機器、ネットワーク、 要員など資源が被災し、情報処理 施設での情報システムの提供が 長期間できない状態	可用性	設備や機器、システムの冗長化 BCPの策定・運用 危機管理体制の整備 訓練の実施
大規模システム障害	ハードウェア障害 ネットワーク障害 重大なソフトウェア障害	設備、機器等のハードウェアの 故障やネットワークの寸断、ソフト ウェアの障害が発生し、情報シ ステムの提供が長期間できない 状態	可用性	
その他の情報セキュリティ脅威	不正アクセス、操作ミス等による個人 情報、企業情報等情報漏洩、 情報改ざん、滅失、ソフトウェア障害	情報漏洩によるユーザー被害の 発生、信用の失墜、知的資産の 喪失などの状況が発生 業務遂行上の障害の発生 情報システムの停止	機密性 完全性 可用性	アクセス制限 認証システム強化 ソフトウェア開発時の品質管理・更新 IPS/IDS 監視による事象発見の迅速化 教育の実施 ISMS認証

目標復旧時間(RTO)の設定

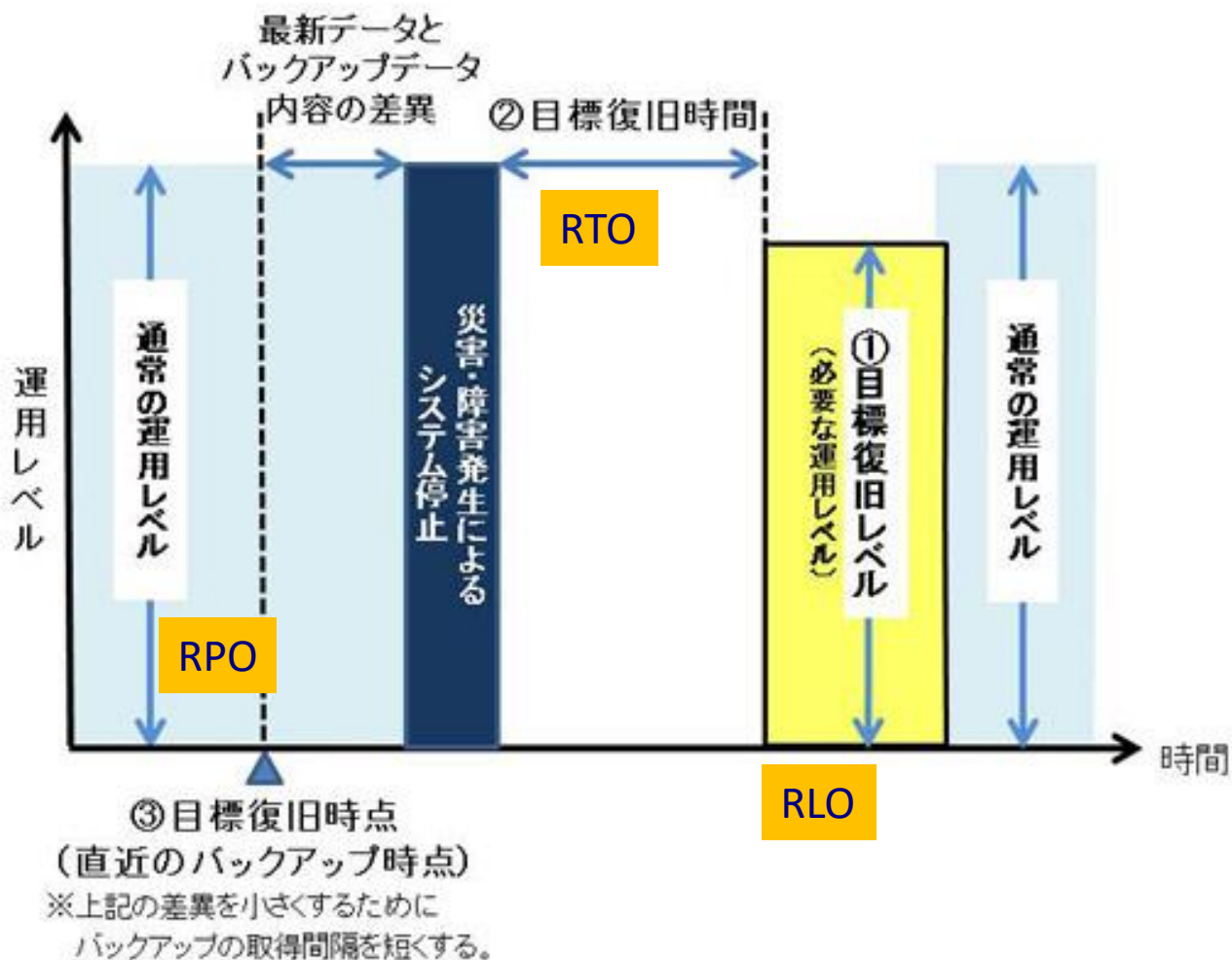
- 事業・業務の中断が発生した場合に、事業に重大な影響を及ぼさないうちに事業活動を復旧・再開させるための目標時間
- ビジネスインパクト分析における主な成果物
- 事業・業務と、それに関連するリソースを特定した上で、影響度を分析する。加えて、顧客からの要請、社会的要請、さらには関係当局からの要請など影響度を総合的に勘案した上で設定。
- IT 部門においては、データ・システムの喪失をどれだけ許容できるかを示す**目標復旧ポイント(RPO; Recovery Point Objective)**を設定し、これに応じたバックアップシステムを構築することが重要

情報システムに対するBCPの3種の復旧目標

情報セキュリティにおけるBCPでは情報システムに対する復旧の優先度を決め、次の3種の復旧目標を決定

(1) 目標復旧レベル(RLO)	目標とする復旧の業務範囲、処理能力の程度等
(2) 目標復旧時間(RTO)	目標復旧レベルまでの復旧に要する時間
(3) 目標復旧時点(RPO)	目標とする復旧の時点(直近のバックアップ時点)

事業継続計画（BCP）と復旧目標（IPA資料）



高回復力システム基盤のパターン(モデルシステム)(IPA資料)

			モデルシステム			
			1	2	3	4
モデル システムの特徴	① システム基盤の強度		低	中	高	高
	② 復旧時間	障害時	1～3日	2時間以内	2時間以内	2時間以内
		災害時	1～6ヶ月	1～6ヶ月	1～7日	2時間以内
	③ 投資規模		低	中	高	高
モデル システムの 主要要件	① バックアップ保有形態、 取得間隔		非同期 月次	非同期 週次	非同期 数回/日	非同期 数回/時
	② 機器などの冗長化		なし	あり	あり	あり
	③ バックアップサイト		なし	なし	あり	あり (ホット スタンバイ)

目標復旧時間(RTO)・目標復旧ポイント(RPO)の例

情報サービス産業などではシステムダウン等の復旧時間は短い場合が多い。

(例) インターネット通販

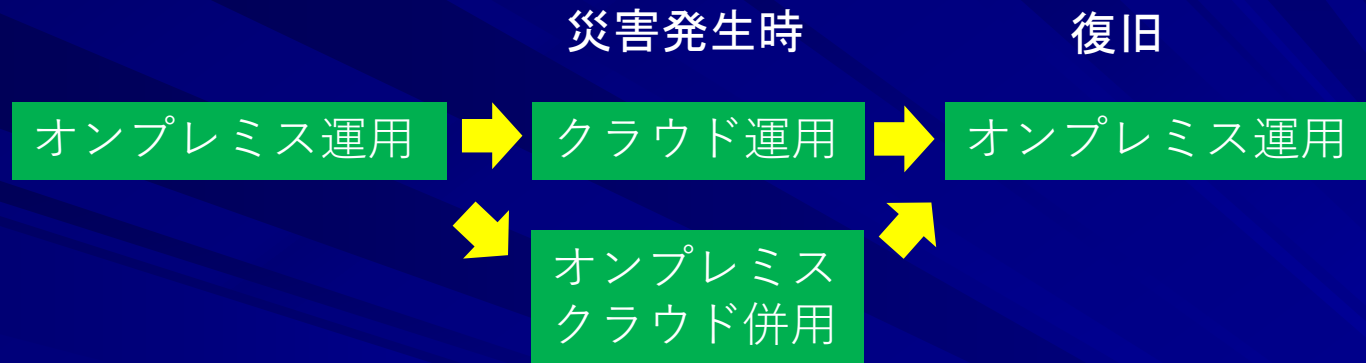
緊急事態が発生した場合、基本的には 1 時間以内の全面復旧を目標とします。ただし、事態が深刻で、サービスの維持が困難な状況に陥った場合には、可能な限り迅速にバックアップサイトに切り替えるとともに、メインシステムの復旧作業を実施します。バックアップサイトへの移行に伴う各種データの受け渡しや保全については、事業継続計画に則って正確かつ迅速に行います。

ディザスタ・リカバリ (Disaster Recovery:DR) : 災害復旧

DRシステムの構築はBCPにおいてシステムの早期復旧を図るうえで重要

	データ送付形態	特徴	コスト	スピード
データバックアップ	テープ媒体送付	バックアップのみでは、リアルタイムなデータの更新が難しいため、障害時や誤操作などによるデータの消去や破損への対応が十分にできない(非同期)	低	低
	オンライン(データセンター)		中	中
		データを自動的にリアルタイムでバックアップシステムへ複製する方法(同期)	高	高
レプリケーション	オンライン	ハードウェアを含め同じシステム環境を2組あらかじめ用意 実稼働、待機用を同時運用、常にデータの同期を行っているため、障害が発生すると短時間に、待機用に制御が切り替わり、システムを続行	高	高
クラウド活用		導入の簡便さ、コスト削減、人手不足対策	低～中	中～高

DRへのクラウドの活用



情報漏洩のリスクやネットワークの安定性に対する不安



コスト(運用, 移行)、セキュリティ、信頼性、提供機等
魅力を備えた、信頼性の高いシステムを選ぶことが重要

ビジネス環境、技術の進展等を考慮し検討

BCP とサービスレベルアグリーメント (SLA)

SLA(Service Level Agreement):

製品・サービスの提供者が、利用者にサービスの品質を保証する制度
(契約)

- 情報システムの構築、運用や保守、データ保存などを外部に委託している事業者がBCP を策定し、「目標復旧時間」を定める場合は、外部のサービス事業者とサービス内容について協議しなければならない。
- SLA の項目の一つとして、障害などが発生した場合に備えて、どの程度システム停止が許容できるのかを取り決め、そのレベルを保証するために二重化等の措置を取る。
- IT 関係であれば、レスポンスタイム、セキュリティレベル、保守体制、緊急時体制、許容停止時間、料金体系などの項目について規定し、サービス提供側はそのサービスレベルを保証

情報セキュリティガバナンス総論

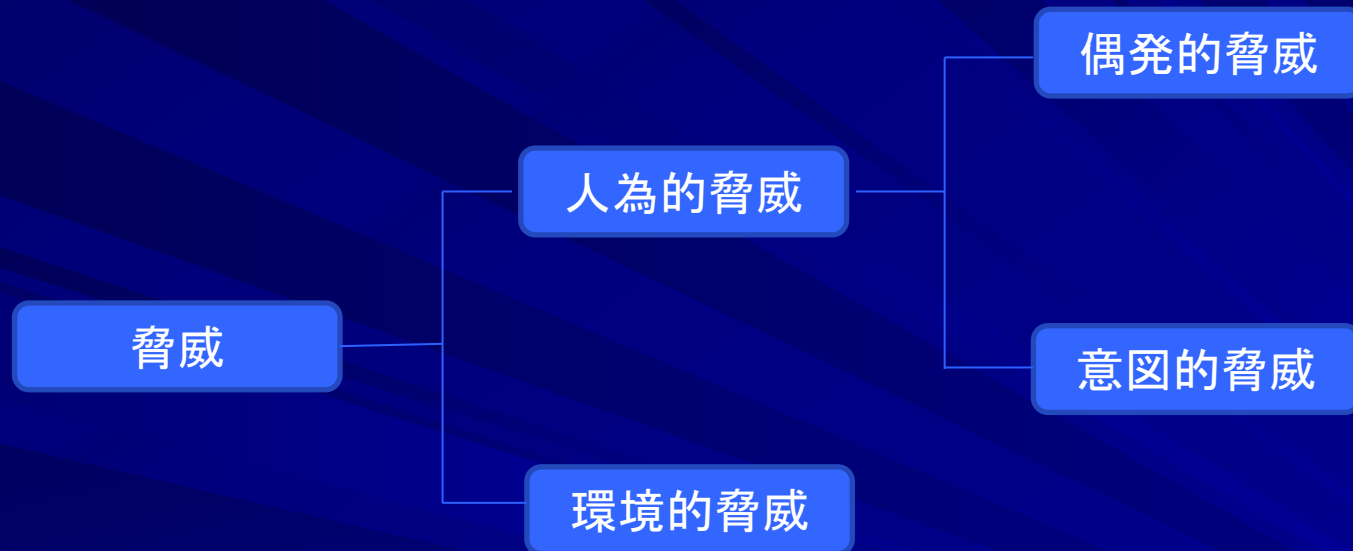
1. 情報セキュリティガバナンス

情報セキュリティ	
情報の機密性、完全性及び可用性の維持	
機密性	情報にアクセスすることを認められた者だけが、情報にアクセスできる 状態を確保すること
完全性	情報が破壊、改ざん又は消去されていない状態を確保すること
可用性	情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保すること

情報セキュリティにおける脅威と対策(IPA資料より)

確保すべきもの	脅威	技術的対策	管理的対策
機密性	不正アクセス 情報漏洩 盗聴 プライバシー侵害 コンピュータウイルス	暗号化(暗号技術) 認証技術 アクセス管理技術 アクセス制御技術 ウイルス検出/除去技術	セキュリティポリシー (周知徹底・教育) 利用者管理 入退室管理 秘密保持契約 情報収集 (脆弱性情報 新技術情報 攻略方法 標準・法規) 情報のバックアップ 運用体制 (修正プログラム適用 パターンファイル更新 バックアップ計画) 教育 脆弱性検査 セキュリティ監査 緊急時対応計画 コンプライアンス 見直し
完全性	不正アクセス 改ざん、変更 破壊、削除 操作ミス コンピュータウイルス	電子署名 改ざん検出技術 改ざん防止技術 ウイルス検出/除去技術	
可用性	不正アクセス DoS攻撃 地震 火災 ハードウェア障害 誤作動、 コンピュータウイルス	認証 二重化、負荷分散 アクセス制御技術 ウイルス検出/除去技術 QoS技術	

脅威 (threat) とは、「システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因」



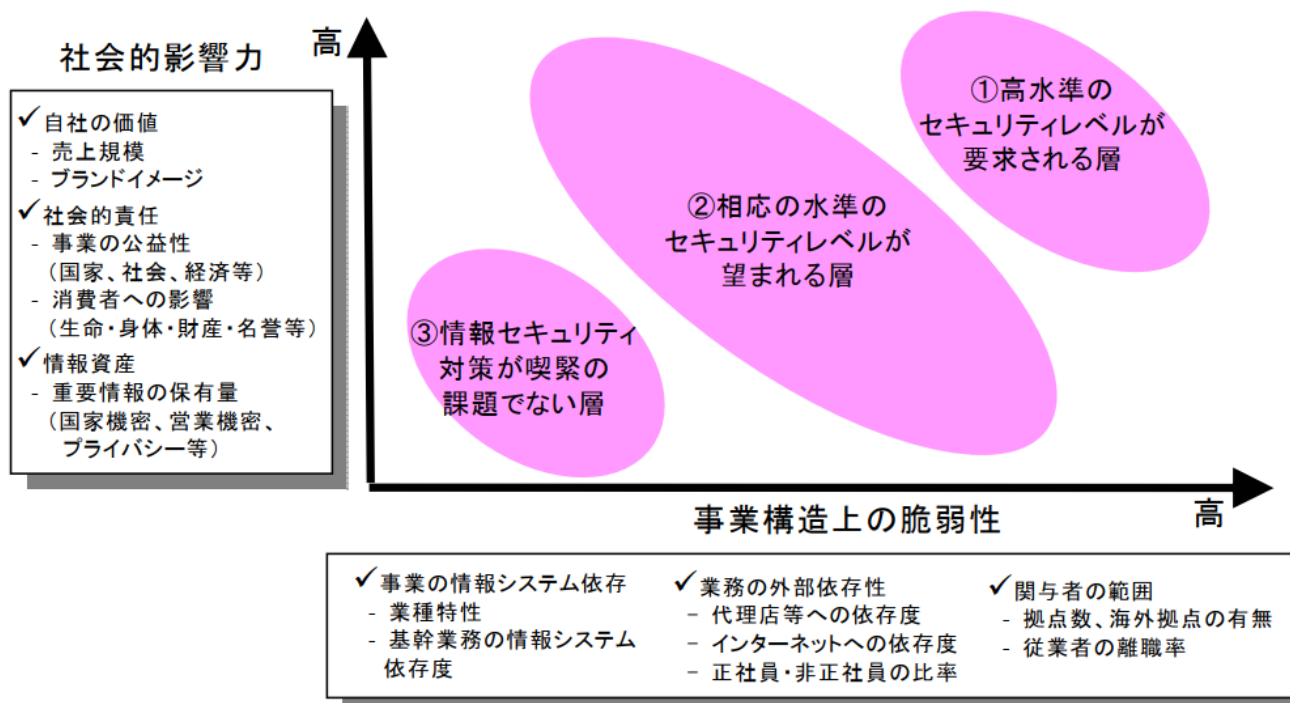
脆弱性 (vulnerability) とは、一つ以上の脅威によって付け込まれる可能性のある資産または管理策の弱点

リスクレベル＝資産価値 × 脅威 × 脆弱性

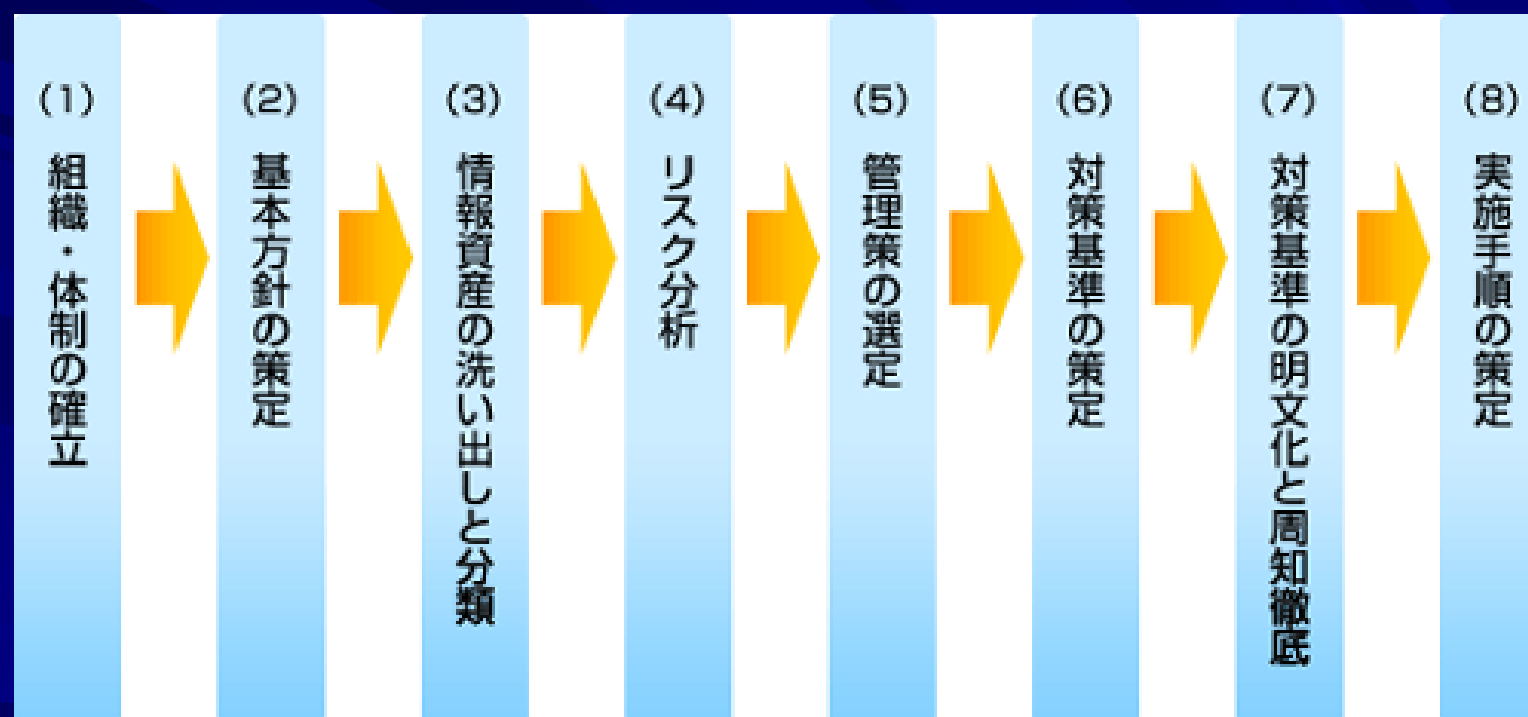
脅威の種類

	意図的脅威	偶発的脅威
外的脅威	サイバー攻撃 不正アクセス 盗難	自然災害 事故
内的脅威	内部者によるサイ バー犯罪 情報漏洩	システム障害 機器故障 誤送信 PC・メモリー等持ち出 し紛失

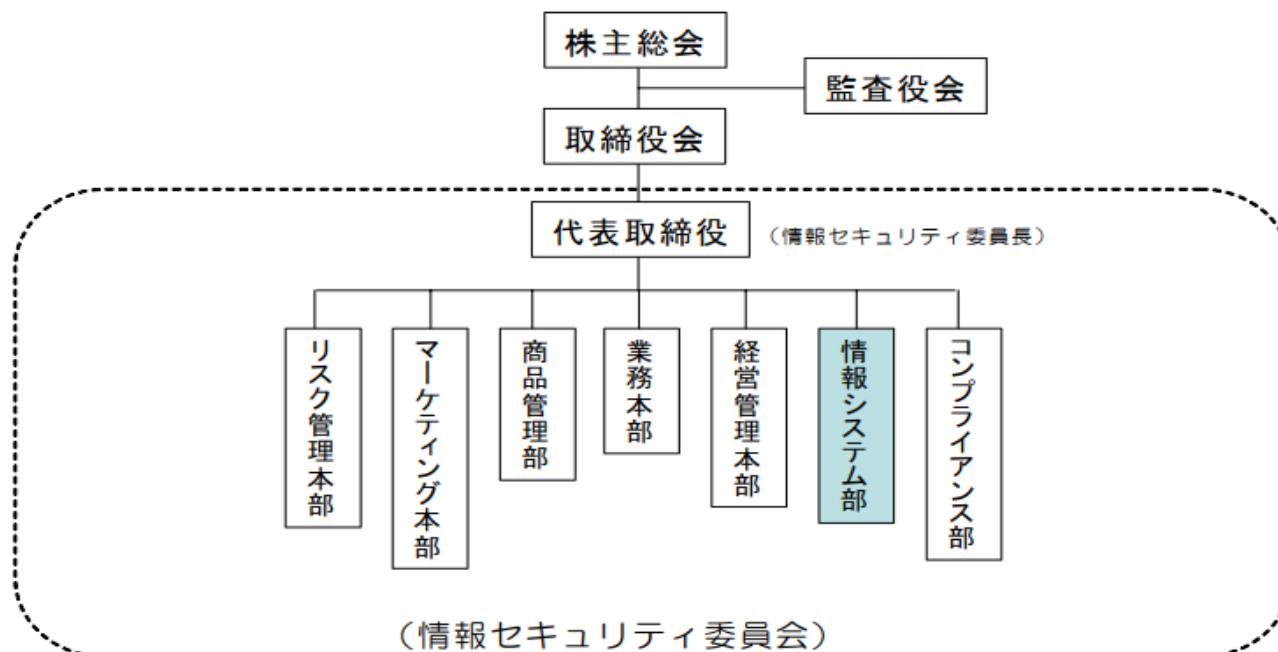
図 3-2 要求される情報セキュリティの水準に基づく分類



情報セキュリティポリシーの策定の流れ

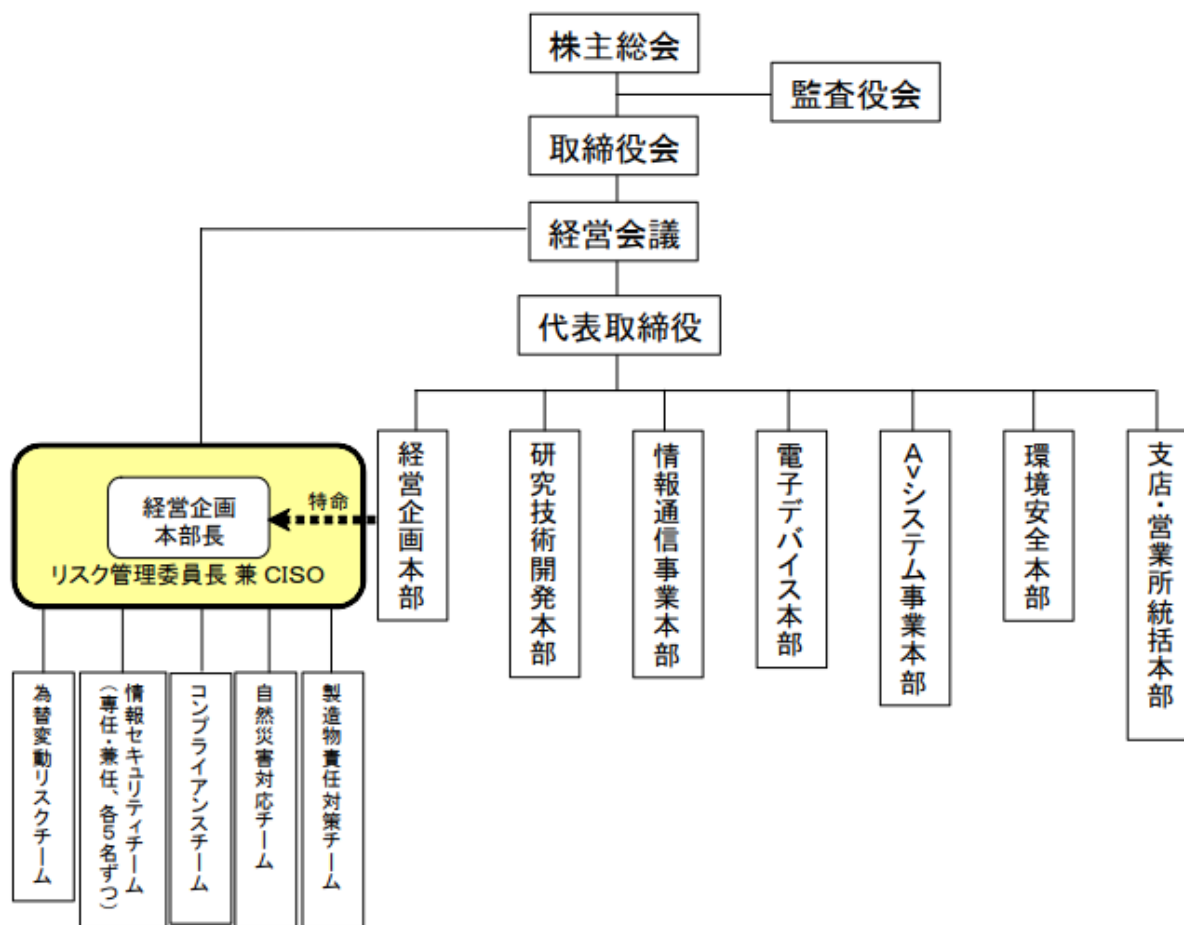


情報セキュリティ管理体制の例(インターネット通販)



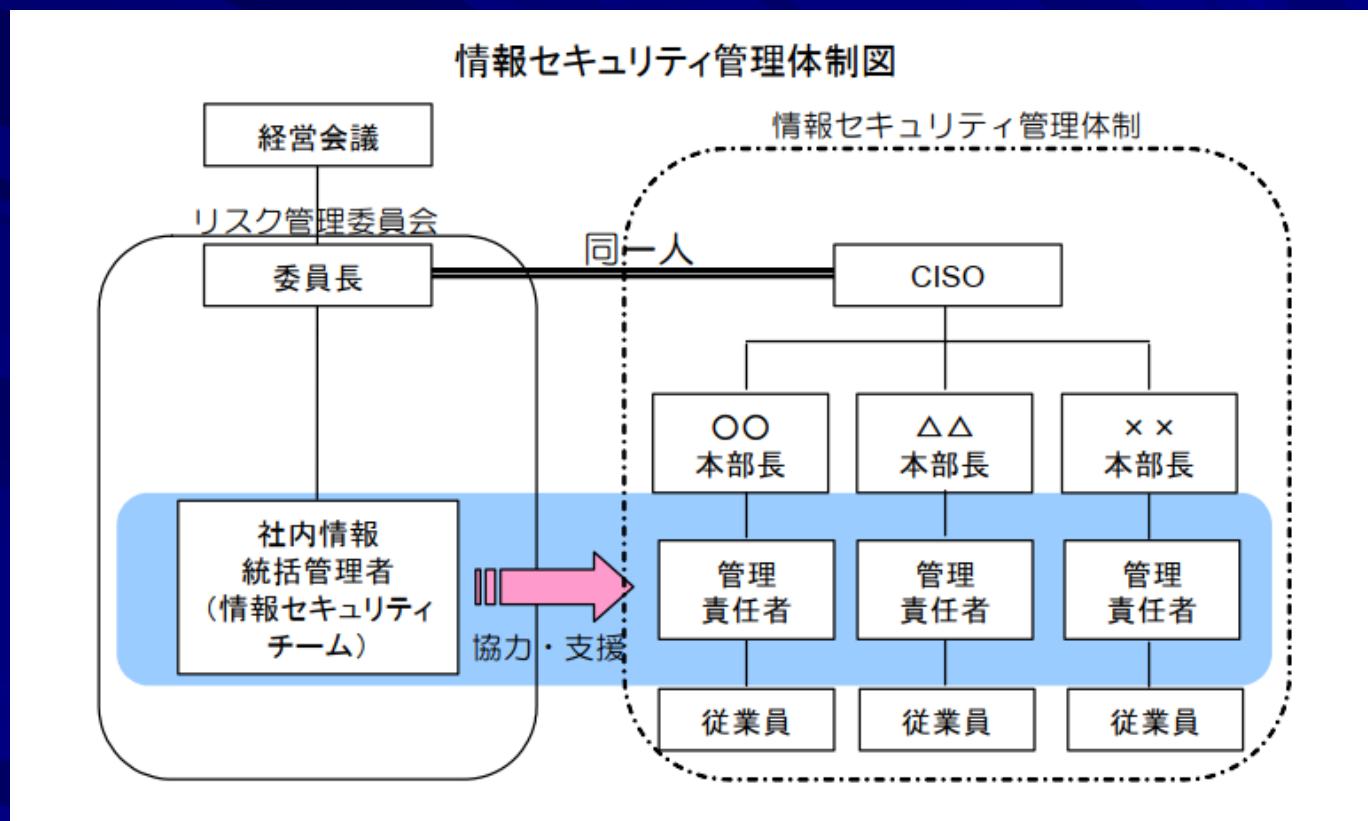
※本委員会の事務局は情報システム部が担当し、各部間の連携を図る。また、個人情報最高責任者(CPO)を2名おく。
(顧客情報担当CPO:業務本部長、社員情報担当CPO:経営管理本部長)

情報セキュリティ管理体制(大手家電メーカー)



(リスク管理委員会の構成チーム)

情報セキュリティ管理体制(大手家電メーカー)



CISO

CISO (Chief Information Security Officer) 最高情報セキュリティ責任者

経営層やそれに近い職位の強いリーダーシップが必要
業務アプリケーションの利用や各種情報を扱う社内のユーザー部門の協力が不可欠

部署間をつなぐための役割を担い、セキュリティ対策の取り組みを全社的に広げることがCISOの重要な業務

従来はCIO (Chief Information Officer) がセキュリティ領域の責任者

CIOとは別にCISOを置くことが必須になりつつある

CSIRT

Computer Security Incident Response Team コンピューター・セキュリティ・インシデント・チームの略、シーサート

サイバー攻撃など自社のセキュリティ上の問題が発生した場合、調査を行い、原因解析や必要に応じてダメージの局所化やシステムの回復、再発の防止などを担当する組織。

社内のセキュリティ研修やセキュリティ施策の検討・実施を行う。

情報システム部門の直下に置かれるほか、経営層の直下に置かれる場合もある。

SOC

Security Operation Center(セキュリティ・オペレーション・センター)の略

セキュリティ監視を行う拠点

サイバー攻撃の検出や分析を的確なアドバイスを提供する役割を持つ
部門や専門組織

24時間365日企業へ向けたサイバー攻撃を監視する組織

高い専門性が要求され、かつ24時間365日の監視が必要であることから、外部に委託されるケースが多い

