事業継続計画(BCP)策定ガイドラインの概要

2005年6月

経済産業省　商務情報政策局
情報セキュリティ政策室

本ガイドラインの位置付け

- IT事故を主に想定した事業継続計画（BCP）
- BCPの構築を検討する企業にとって、考え方の理解を促すガイドラインという位置付け
- 基本的な考え方から具体的な計画の構築手順を説明
- 基本的考え方、総論、策定にあたっての検討項目、個別計画の4つの章と、参考資料から構成

事業継続計画策定ガイドラインの構成

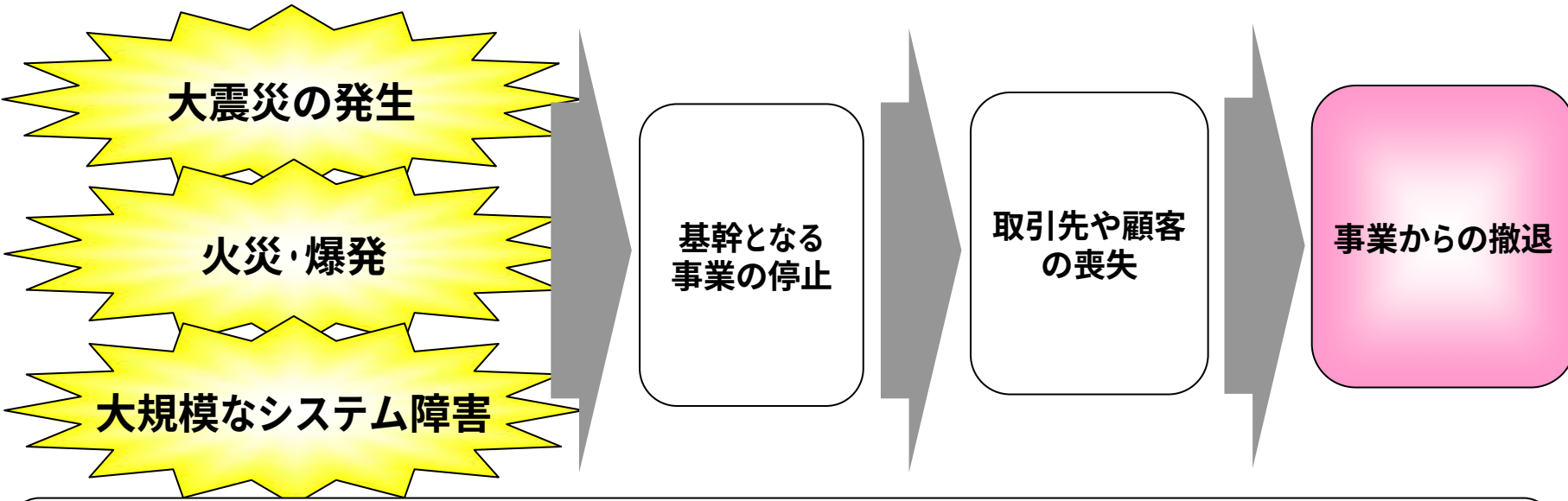
METI 経済産業省

第Ⅰ章　基本的考え方

1.1. BCP (Business Continuity Plan)の必要性
　　BCPの一般的な流れ
1.2. BCPが求められる背景
1.3. BCPの特性
1.4. 世界と日本の動向

1.1. BCPの必要性

- 地震、火災･爆発、大規模なシステム障害などが相次いでおり、その結果、基幹となる事業･業務の停止に追い込まれるケースが見られる。
- 近年発生している基幹事業の停止は、取引先や顧客の事業停止へと影響が連鎖している。
- 企業経営者は、企業存続の生命線である「事業継続」を死守するための行動計画であるＢＣＰの策定を行なわなければならない。BCMは「企業経営のあり方」そのものである。



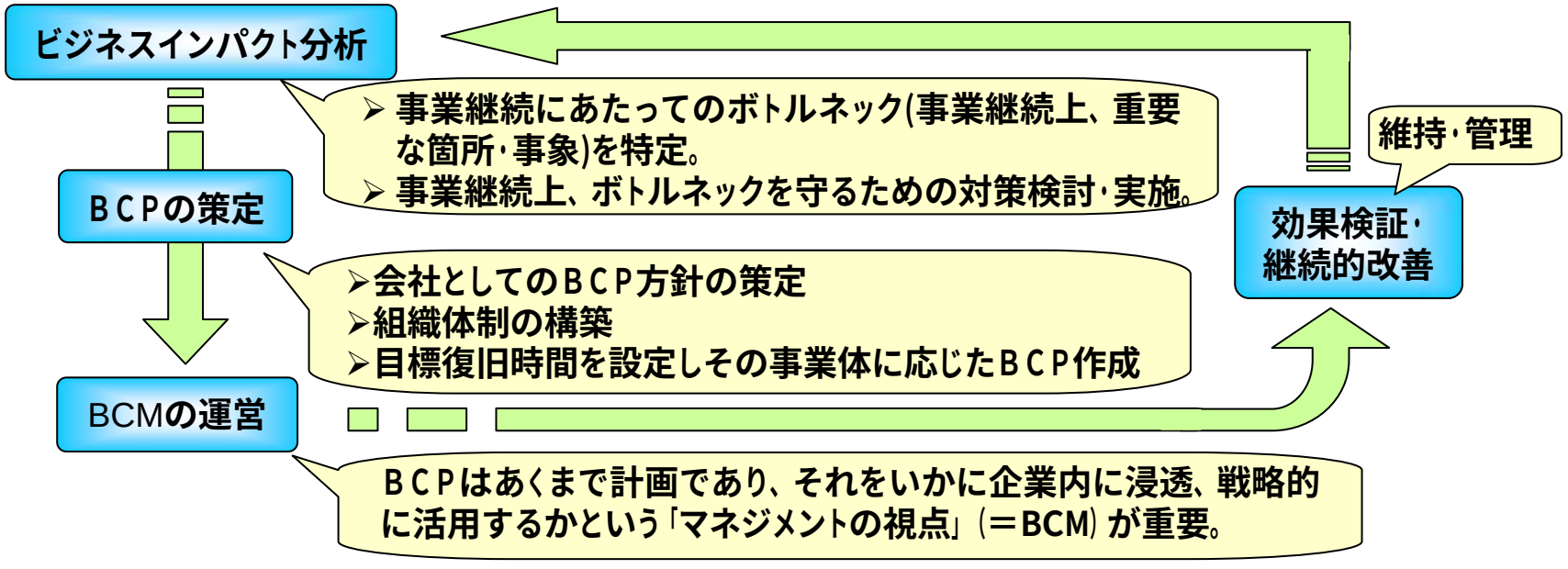
事業の継続を死守するための行動計画が不可欠！

BCPの一般的な流れ

METI 経済産業省

ＢＣＰ(Business Continuity Plan)	企業存続の生命線である「事業継続」を死守するための行動計画
ＢＣＭ (Business Continuity Management)	ＢＣＰの策定、運用、見直しまでのマネジメントシステム全体

【ＢＣＭの一般的な流れ】



1.2. BCPの求められる背景

➢ 企業の事業停止リスクは近年急激に増大している。

事業活動の変化	生産拠点･物流拠点･取引先等の集約化が、障害発生時の代替手段の確保を困難にし、結果事業の停止に追い込まれる可能性を高めている。また、サプライチェーンの発達もあり、その中のボトルネックを解消する必要がある。
情報システムへの依存増大	情報システムの停止が、事業の停止に直結するリスクになってきている。
予測困難なリスクの増大	同時多発テロ、ＳＡＲＳの蔓延のような今まで想定していないリスクが発生している。
地震等自然災害リスク	海外の企業にとって、日本の自然災害リスクは脅威に映っている。
ＢＣＰの取組みに関する情報開示	先進的な企業で、リスクの所在とその対応を積極的に開示し始めている。

1.3. BCPの特性

経営戦略としての位置付け	BCMをステークホールダーである株主や取引先へのアピールに活用。 BCMが企業間取引に必要になる時代が到来することが予想される。
経営者としてのトップマネジメント	BCMは事業継続･復旧の優先付けを行うなど、重要な経営判断。 また企業として実行性を確保することが求められる。
結果事象による対応方針の整理	ビジネスインパクト分析と最悪の想定シナリオ
BCMとリスクファイナンシング	BCM上リスクファイナンス機能も極めて重要 例) 保険、災害時発動型融資予約契約、 保険デリバティブ、リスクの証券化　など

1.4. 世界と日本の動向

- 英国･米国を中心に、ＢＣＰの世界標準化策定の動きが始まっている。
- 日本においても、内閣府中央防災会議の専門調査会にて業務継続について議論されている。

海外の動向	英国	･英国規格協会（ＢＳＩ）がＰＡＳ５６（一般仕様書）を策定
	米国	･ＮＦＰＡがＮＦＰＡ1600を発行
	シンガポール	･金融当局によるＢＣＭの強制化
日本の動向	内閣府	･中央防災会議「民間と市場の力を活かした防災力向上に関する専門調査会」で業務継続について議論
	日本銀行	･「金融機関における業務継続体制の整備について」公表

→ 世界標準化の提案を準備

第Ⅱ章　総論(フレームワーク)

2.1. BCP策定にあたっての考慮事項
2.2. 組織体制について
2.3.ビジネスインパクト分析からBCP策定までの流れ
2.4. BCPの導入と教育･訓練
2.5. BCPの維持･管理

2.1. BCP策定にあたっての考慮事項

BCP策定にあたっての考慮すべき3つのポイント

- ビジネスインパクト分析からBCP策定の対象事業･業務は原則全てであるが、**重要度･緊急度に応じて優先度付け**が必要
- リスク分析は網羅的に行う必要があるが、これに**時間をかけ過ぎてはいけない**
- BCP発動時においては、**行政の目的との整合性**が求められる場合もある

■ 対象範囲

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。

■ BCPと他規程との関係
･平時のリスク管理に関する規程類
情報セキュリティポリシー、プライバシーポリシー、コンプライアンス規程など
･有事のリスク管理に関する規程類
危機管理規程、緊急事態管理規程など

■ 遵守すべき法令･関連法規（行政の目的との整合性確認、法令違反の防止のため）
災害対策基本法、個人情報保護法、各種事業法など

2.2. 組織体制について

BCP責任者（BCマネージャー）の役割

○BCPプロジェクトの調整、組織管理

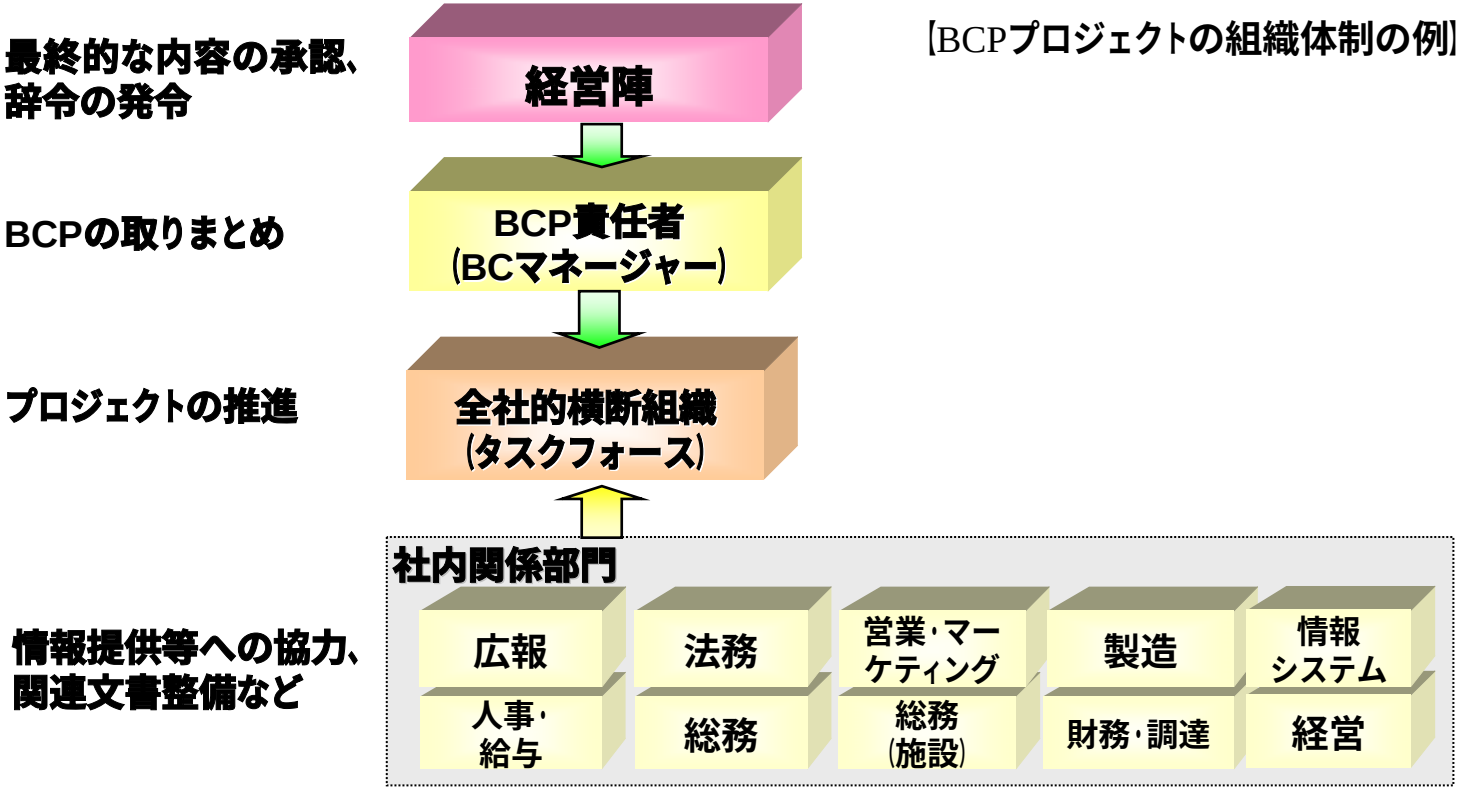
○経営陣からの支援の取り付け

○プロジェクト計画の策定と予算管理

○教育・テスト計画の策定と指導

○定期的なBCPの見直し

【BCPプロジェクトの組織体制の例】



2.3. ビジネスインパクト分析からBCP策定までの流れ

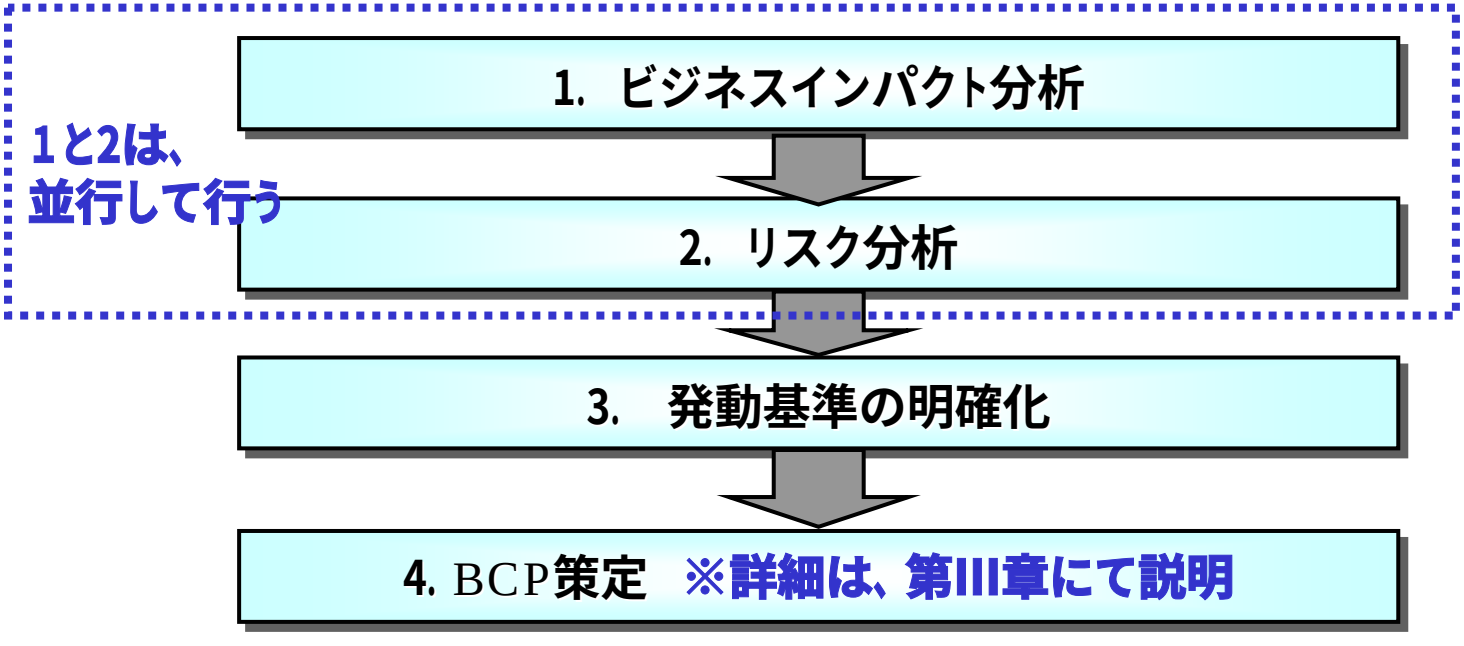
ビジネスインパクト分析の目的

○事業継続、復旧の優先順位付け

○ボトルネックの特定、事業継続のための対策立案

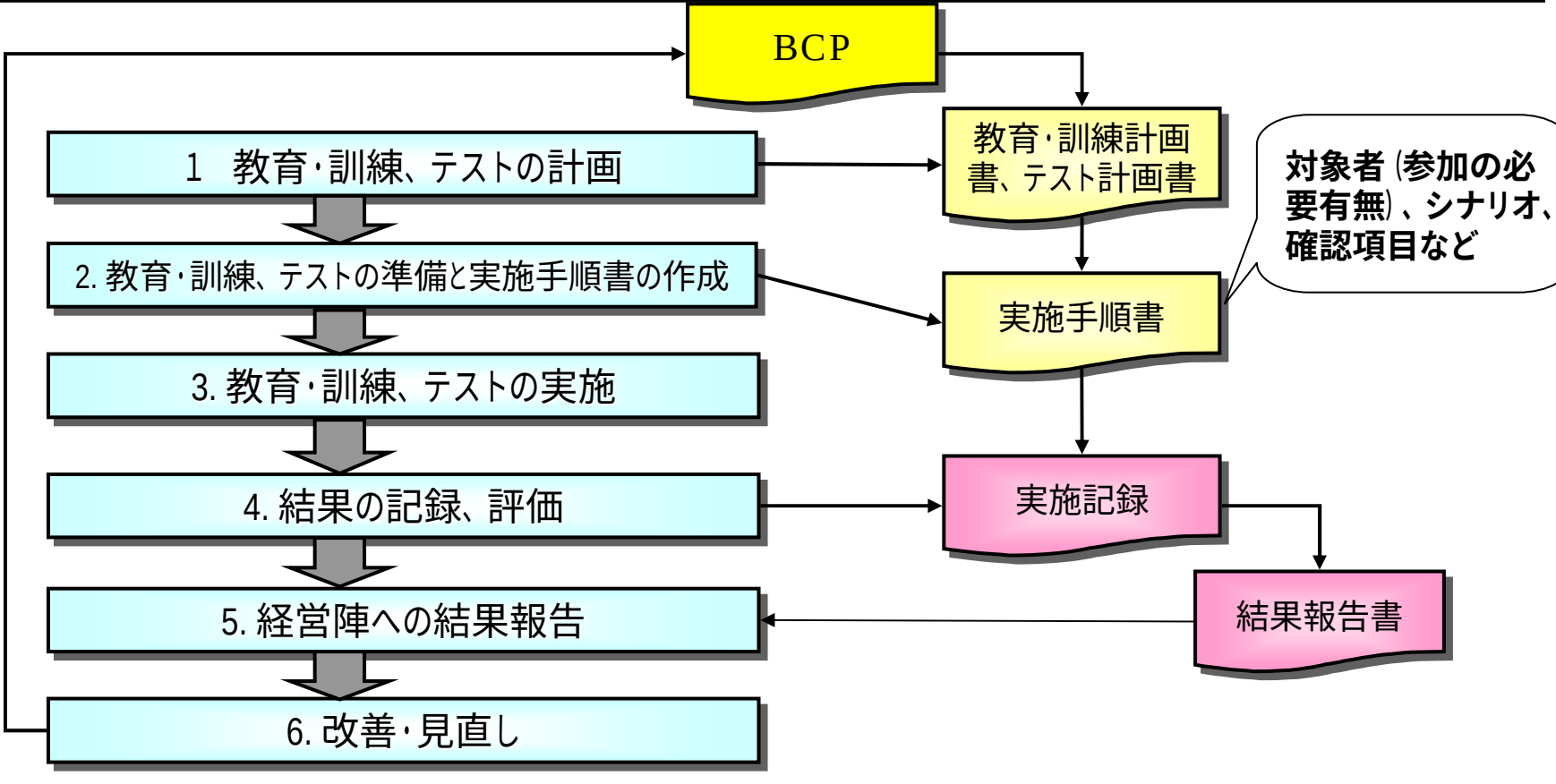
○目標復旧時間（RTO）の設定

【ビジネスインパクト分析からBCP策定までの流れ】



2.4. BCPの導入と教育・訓練

- BCPを有効に機能させるため、組織のメンバーにBCPを周知徹底し、不測の事態において確実に実行できるようにしておく必要がある。
- BCPの教育・テストは、BCPについての知識と理解を深めるために重要なものであり、計画的な実施が必要。



2.5. BCPの維持･管理

BCPの維持･管理のポイント

- 不測事態において機能するよう、日頃からBCPの周知徹底を行っておくと共に、「最新性」「正確性」を維持するための見直しや監査が重要。
- 自宅保管も含めた配付先管理も大切な維持･管理活動の一つ。

＜BCP見直しの契機の例＞

○テスト結果によるBCP自体の見直し
○定期的な見直し
○BCPの前提条件の変更による見直し
○人事異動や組織の大幅な変更による見直し
○システム構成の大幅な変更による見直し
○新たな脅威の発生（リスク環境の変化）による見直し
○監査の指摘事項による見直し
○準拠すべき法令等の改正による見直し

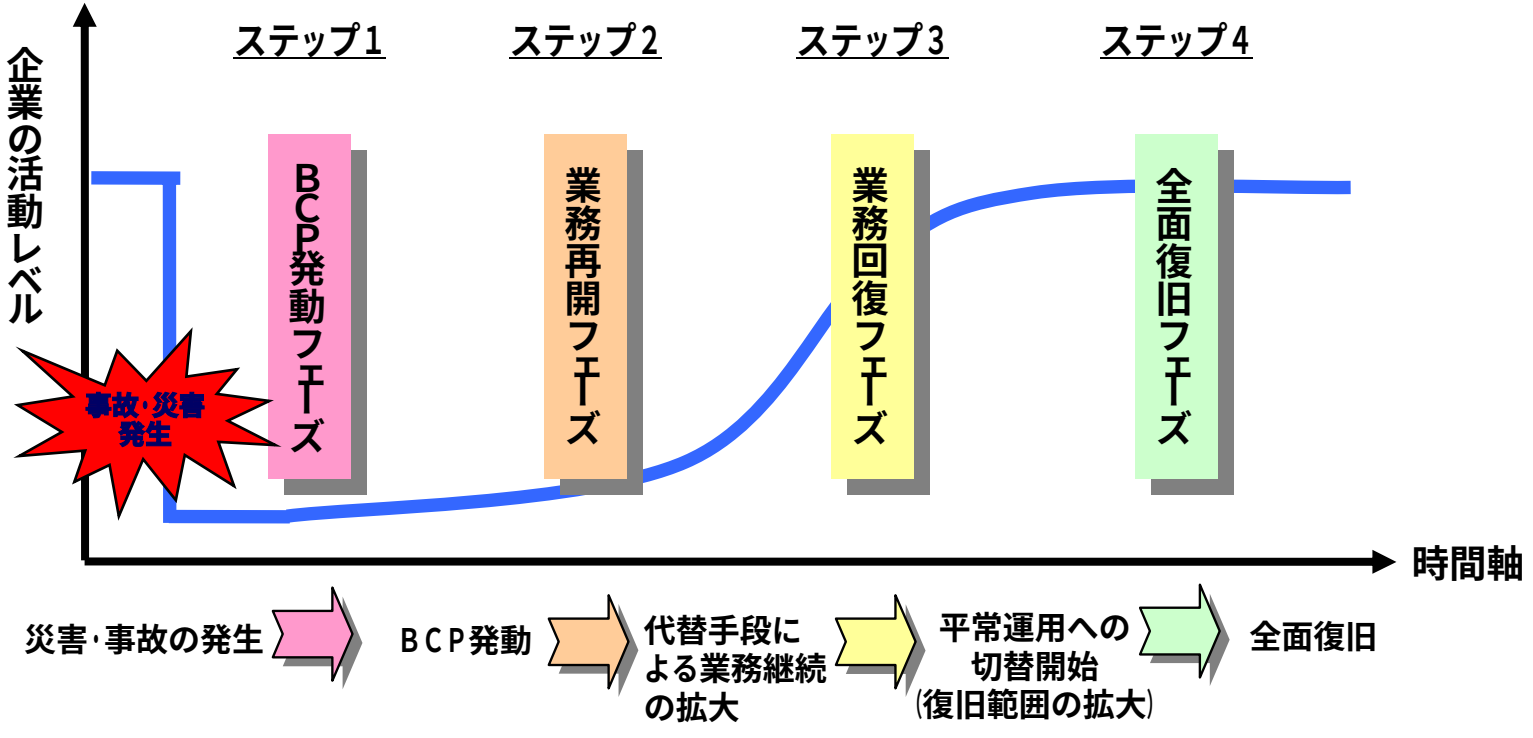
＜BCPの適切な維持･管理のための確認事項の例＞

○BCPの最新版が定められた場所（キーパーソンの自宅保管も含む）に保管されているか
○BCPテスト結果に沿って、見直しが行われているか
○緊急連絡網を含む各種リストが最新版に更新されているか
○BCPにおいて想定されている脅威等が評価され、その結果で見直しがされているか
○経営陣の承認が得られているか

第Ⅲ章　BCP策定にあたっての検討項目

3.1. 検討項目の全体像とポイント

- ＢＣＰの発動から全面回復に至るまでを、①ＢＣＰ発動時、②業務再開フェーズ、③業務回復フェーズ、④全面復旧フェーズ、の大きく4つのフェーズに分けて考える。
- 各フェーズにおいては、迅速かつ正確な情報収集、事実認識と状況判断、それに基づいた的確な意思決定、利害関係者への情報開示が等が検討のポイントとなる。

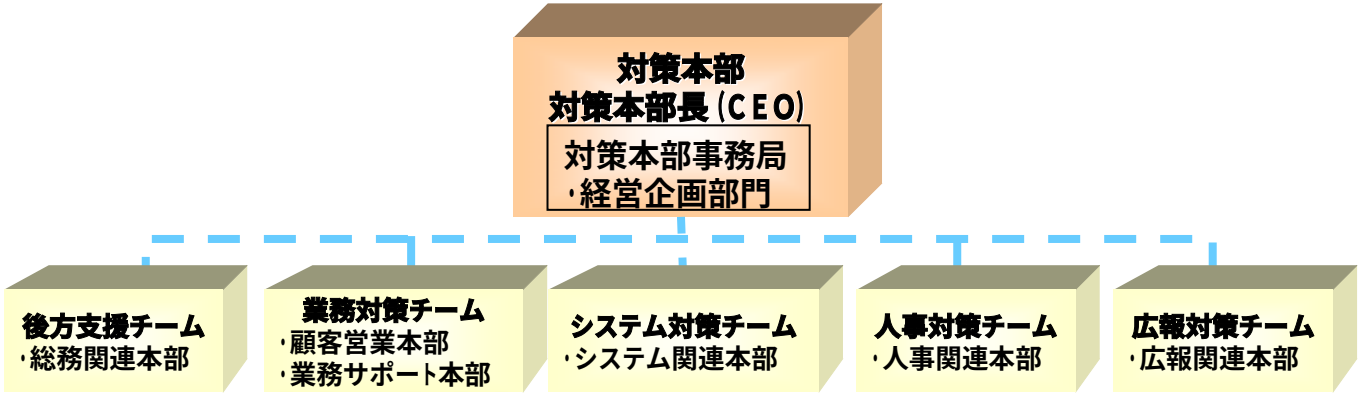


3.2. BCPの実施体制

➢ 各フェーズにおいて、経営層の的確な意思決定が求められる。緊急時の対策本部や対策チームはその意思決定をサポートするとともに、決定事項を遂行する役割を担う。

◆ 対策本部の概要（例）

・対策本部は、非常時における最高意思決定機関としてＢＣＰの指揮を行う。具体的には、ＢＣＰの各フェーズにおける意思決定、ＢＣＰに関する行動の指示、ＢＣＰの実行状況の監督等の役割を担う。



◆ 各対策チームの機能

・各対策チームは、収拾した情報や把握した状況について対策本部への報告を行い本郡の意思決定を支援するとともに、各チームが連携のうえ決定事項の遂行や現場の支援を行う。

チーム	統括部門	機能
後方支援チーム	総務関連本部	施設の復旧・保全、物資調達、物流
業務対策チーム	顧客営業本部／業務サポート本部	顧客対応、業務継続（対顧客）
システム対策チーム	システム関連本部	システム復旧・保全、業務継続（システム）
人事対策チーム	人事関連本部	安否確認、要員配置、労務
広報対応チーム	広報関連本部	社外広報・ＩＲ、社内広報

3.3. BCP発動フェーズにおける対応のポイント

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。

＜検討する項目＞

（1） 発生事象の確認及び情報伝達
（2） 安全確保、安否確認
（3） 要員の配置
（4） 被害状況の確認
（5） 業務影響の確認
（6） 基本方針の決定
（7） 対応の優先順位の決定
（8） 復旧目標の決定
（9） 初期対応の実施

3.4. 業務再開フェーズにおける対応のポイント

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。

＜検討する項目＞

（1） 人的資源の確保
（2） 代替オフィスの確保
（3） 物的資源及び物流ルートの確保
（4） 業務再開とモニタニング
（5） 施設やシステムなどの復旧作業の実施
（6） 運用上の留意事項

3.5. 業務回復フェーズにおける対応のポイント

ステップ３：ＢＣＰ発動フェーズ

- 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。

＜検討する項目＞

（1） 業務拡大範囲の見極め

（2） 確実な情報収集

（3） 業務継続の影響確認

（4） 復旧状況の確認

（5） 追加資源投入の検討、実施

（6） 更なる業務縮退の検討、実施

（7） 継続業務の拡大の検討、実施

（8） 復旧作業の実施、復旧目途の確認

（9） 全面復旧のタイミングの決定、資源再配置の計画

（10） 復旧後の制限の確認

3.6. 全面復旧フェーズにおける対応のポイント

ステップ４：ＢＣＰ発動フェーズ

- 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はらんでおり、慎重な対応が要求される。

＜検討する項目＞

(1) 代替設備･手段からの切替の判断

(2) 復旧手順の確認･全面復旧の実施

(3) 資源の再配置

(4) 業務制限への対応

(5) 総括
- －被害状況のまとめ
- －利害関係者への影響のまとめ
- －再発防止策の検討
- －BCPの見直し
- －サービスレベルアグリーメントの見直し
- －利害関係者への事後処理の実施
- －業績への影響の見極め
- －経営計画の見直し

3.7. リスクコミュニケーションの重要性

- リスクコミュニケーションとは、災害や事故が発生した（発生の可能性を検知した）場合などにおいて、情報の収集、分析、連絡、発表などを通じ、リスクに対する認識の程度を揃え、情報の共有を行うための活動のことである。
- リスクコミュニケーションの巧拙がＢＣＰ遂行の成否を分ける場合もあるので、訓練を通して周知する必要がある。

＜各フェーズにおけるリスクコミュニケーションの主な内容＞

①BCP発動フェーズ	災害や事故について、発生の事実、影響範囲、回復の見込みなどについての情報共有
②業務再開フェーズ	二次災害が発生していないか、発動したBCPが支障なく遂行できているか、顧客への影響が拡大していないか、回復見込みに遅れが生じていないかなどについての情報共有
③業務回復フェーズ	業務の再開が順調に推移しているか、代替設備･システムでの業務遂行の留意点、全面復旧の目処、などについての情報共有
④全面復旧フェーズ	全面復旧を安全に果たすための情報共有と、復旧後の業務影響を取りまとめて第三者に示すという情報収集･情報発信 対外的に発表復旧の時期、全面復旧に伴う業務遂行の留意点、今後の企業活動への影響度などについての情報共有

第Ⅳ章　個別計画（ケーススタディ）

4.1. 大規模なシステム障害への対応①
　　大規模なシステム障害への対応②
4.2. セキュリティインシデントへの対応①
　　セキュリティインシデントへの対応②
4.3. 情報漏えい、データ改ざんへの対応①
　　情報漏えい、データ改ざんへの対応②

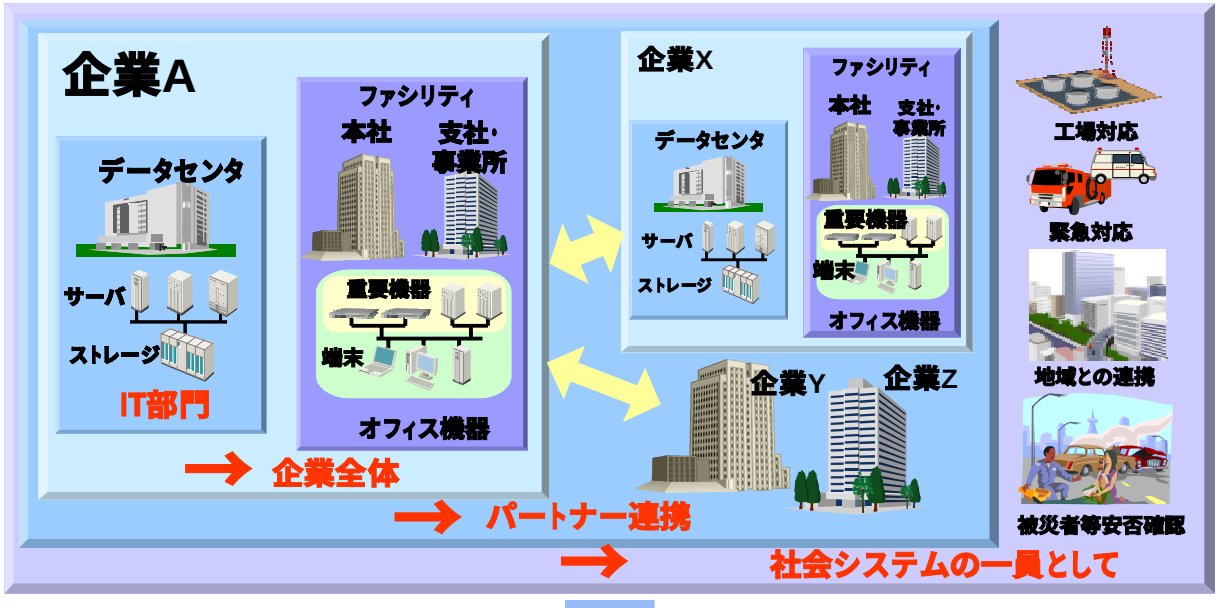
4.1. 大規模なシステム障害への対応①

METI 経済産業省

広域災害への対応で重要なポイント

- 安否確認、状況確認、指示伝達などの内部コミュニケーション、更に取引先、行政などの外部とのコミュニケーションのための通信手段の確保
- システム、データなどのバック･アップのみならず、物理的に作業を再開するワーク･エリアの確保
- 通常業務に加え生活用品や食糧などの物資を入手する物流、更に電源装置･燃料の確保

【経済活動におけるシステム間の広域相互依存】



システム間の連係･連鎖が広がり、
高信頼の広域相互依存対応が必要になっている

広域災害への対応

- 対内外通信手段の確保
- 通信手段の併用
- ワーク･エリアの確保
- 宿泊施設の確保
- 生活用品･食糧の確保
- サプライ･チェーンの維持
- 電源の確保 (UPS)
- 電源用燃料の確保

4.1. 大規模なシステム障害への対応②

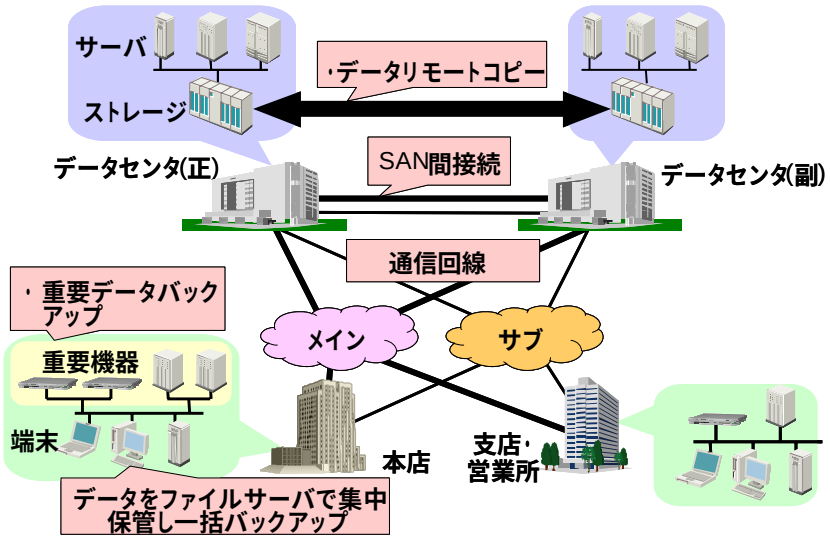
オペレーション上の課題

- オペレーションに必要な、要員・交通（通勤）手段の確保
- 事業に必要な資源の確保に関する、取引先や行政といった外部関係機関との連携・連絡
- 障害状況に係る途中経過・復旧見込みに関する自発的な情報開示（リスク・コミュニケーション）
- 業務復旧時における情報セキュリティの維持、及びオペレーション上の障害回避

技術による耐障害性の確保

- 同一ビル、付近地に加え、遠隔地への、情報・業務アプリケーションの分散配置
- 取引企業や交通機関も含めて代替システムや代替ネットワークを使用した訓練の実施

【システムの冗長化による耐障害性向上】



IT運用（技術適用）のガイドライン*

- 役割と責任体制の明確化
- システム、オペレーションの文書化と内容維持
- IT関連資産の詳細リスト作成と内容維持
- 音声・データ通信に係るネットワーク情報維持
- データ・フローとビジネス・プロセスの可視化
- ITリスク評価、リスク・マネジメント体制の導入

*Federal Financial Institution Examination Committee, IT Examination Handbookより

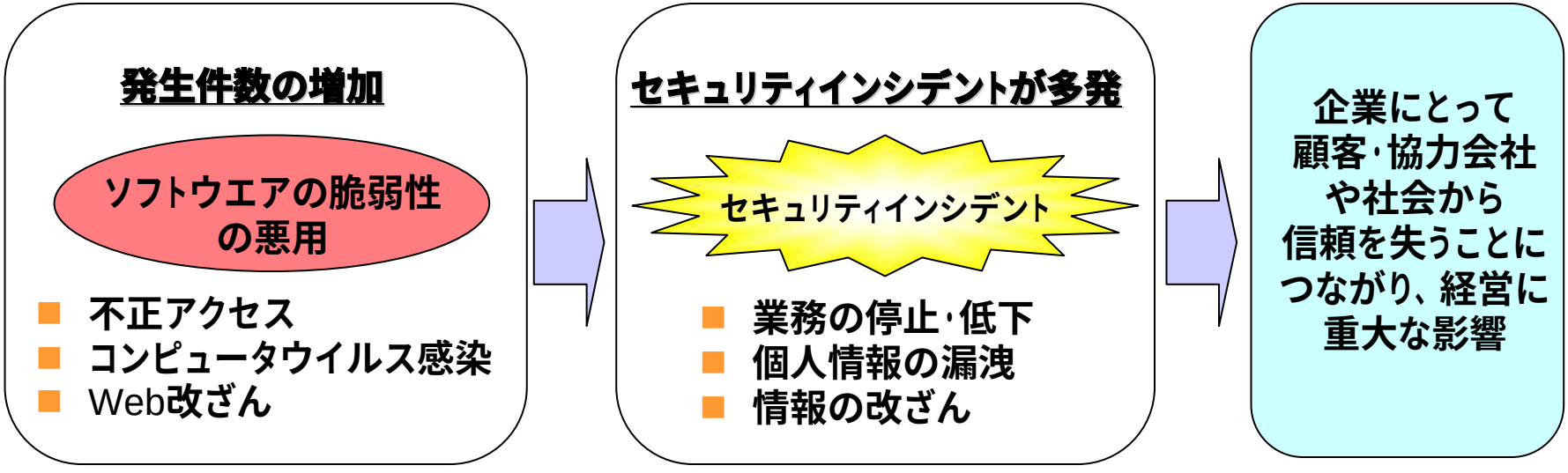
4.2. セキュリティインシデントへの対応①

セキュリティインシデントとは

- コンピュータセキュリティに関係する人為的事象であり、意図的及び偶発的なもの。またその疑いがある場合を含む。例えば、不正アクセス、ウイルスの流布、リソースの不正使用、サービスの妨害行為、データの改ざん、意図しない情報の開示や、更にそれらに至るための行為（事象）などがある。

ソフトウエアの脆弱性とは

- ソフトウエア製品、通信プロトコル、インターネットサイトなどにおいてコンピュータ不正アクセスやコンピュータウィルス等の攻撃により、その機能や性能を損なう原因となり得るセキュリティ上の欠陥のこと。



セキュリティインシデントへの対応は、24時間365日続く、見えない敵との闘い

4.2. セキュリティインシデントへの対応②

METI 経済産業省

(1) インシデント対応体制の整備と外部機関との連携活動

①社内体制整備　②外部機関との連携活動　(a) 脆弱性対策対応 (b)インシデント対応

(2) 状況把握･インシデント特定と対応

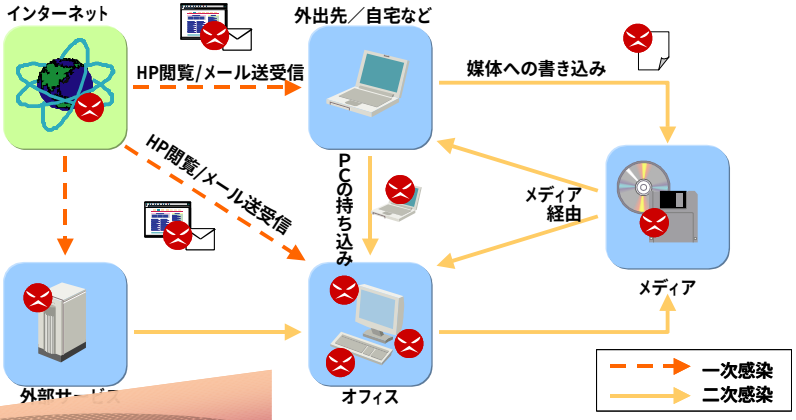
①状況把握　②インシデント特定と対応発生時　③リスクコミュニケーション

(3) 平常時の運用及び教育

①運用　②教育

ウイルス感染ルートと脆弱性

ウィルス感染経路は多岐にわたるため、トータルな対策が必要



組織に存在する脆弱性

- ●ウィルス対策ソフトの設定不備
- ●OS／ブラウザのセキュリティホール
- ●不許可（対策不備）のPC接続
- ●ファイル（メディア）の持ち込み
- ●感染拡大防止策の不備
- ●組織内のセキュリティ意識の低さ
- ●感染後の除染手順の不備

具体的運用内容：自社に適用できるものを選択

(a)インシデント発生予防（メール、web、パターンファイル更新）

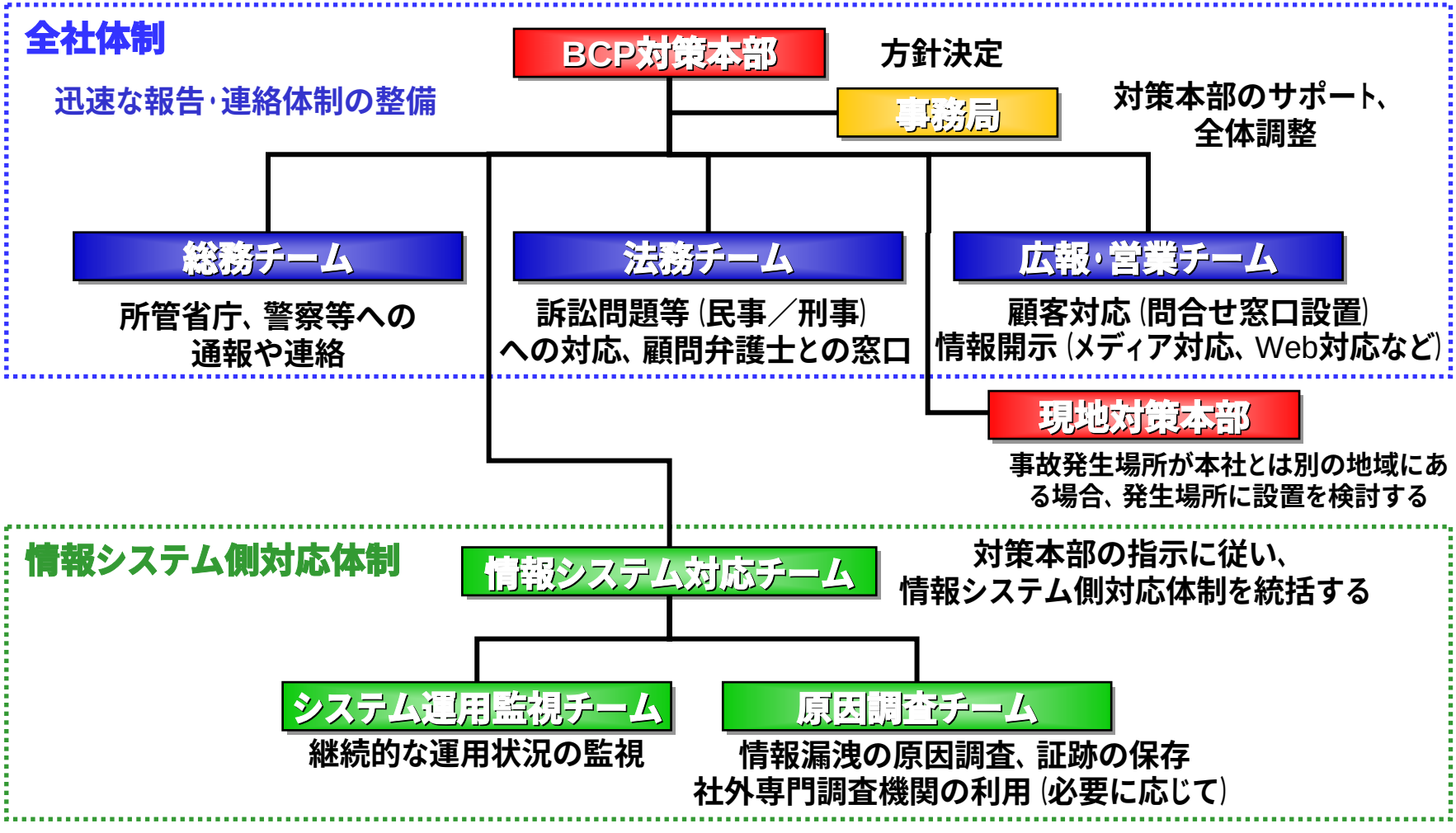
- ･ウイルスチェックサーバによるウイルス侵入防止
- ･従業員のWeb不正アクセス抑止
- ･セキュリティパッチの自動配布
- ･利用者用PCのセキュリティチェック
- ･情報漏えい防止施策（メールフィルタシステム他）
- ･セキュリティポリシーに基づく監査

(b)インシデント関連情報発信(従業員への啓発、注意喚起)

- ･脆弱性情報内容を纏め、各事業所、グループ会社へメールやwebで提供
- ･セキュリティ関連ニュースから情報収集し発信
- ･長期連休前の注意喚起を発信
- ･CERT/CCの情報を翻訳し、社内へ発信
- ･e-ラーニング等によるセキュリティ教育(定期的)実施
- ･定期的にサマリー情報を各部門、グループ会社へメール発信

4.3. 情報漏えい、データ改ざんへの対応①

- 情報漏えい事故等への対応段階において講じる措置を検討する際には、各府省庁から出されている**個人情報保護ガイドラインのフレームワークに沿って具体化**する。



4.3. 情報漏えい、データ改ざんへの対応②

リスクコミュニケーションのポイント

- 個人情報保護法では、個人情報の漏えい等の事案が発生した場合には、所管官庁への情報提供、二次被害の防止、類似事案の発生回避等の観点から、**可能な限り事実関係等を公表すること**が要請されている。

事故発覚 / 事実関係の公表 / 初期対応（レスポンス） / 再発防止に向けた対策（リカバリー）

-3～5日　0日　1ヶ月前後　3ヶ月前後

	-3～5日	0日	1ヶ月前後	3ヶ月前後
当局対応	□状況の把握・報告 □捜査への協力 □必要書類・資料の準備		□調査結果、再発防止策の報告	□決算発表、株主総会、アナリスト説明会の準備
マスコミ対応	□取材・会見対応準備 □プレス・リリース原稿・Q&Aの作成	□報道モニタ(論調分析)	□調査結果・再発防止策の公表	
取引先・顧客対応	□問い合わせ窓口設置 □HPに事実関係を公表 □お詫び広告	□HPに継続的に情報を開示 □問合せ対応	□HPに調査結果・再発 防止策の公表	
社内対応	□対策本部設置 □原因究明	□ リカバリー・プランの策定	□再発防止策の策定 □一斉点検 □社内教育	□事故対応の反省 □再発防止策の実行