日本システム監査人協会近畿支部　第165回定例研究会

「事業継続計画（BCP）の概要とIT－BCPについて」

2017年3月17日

野原英則

第1部　事業継続計画（BCP）概論

事業継続の取り組みが高まる社会的背景

1995年　兵庫県南部地震（M7.3）（1月）

2000年　鳥取県西部地震（M7.3）（10月）

2001年　米国同時多発テロ（9月）

リーマンブラザーズ
バックアップDCによる事業継続

2003年　日本政府、SARS流行のため香港、広東省への渡航延期勧告（4月）
宮城県沖地震（M7.1）（5月）
十勝沖地震（M8.0）（9月）

2009年　新型インフルエンザ流行（H1N1）

2011年　東日本大震災発生　　サプライチェーンの供給問題(ダイヤモンド構造)
原発停止による電力不足、タイの洪水発生

2014年　御嶽山噴火

2015年　鬼怒川決壊

2016年　熊本地震

鳥取地震

様々な災害が発生し、企業の事業継続力が問われる時代となってきた。

事業継続計画（Business Continuity　Plan：BCP）とは

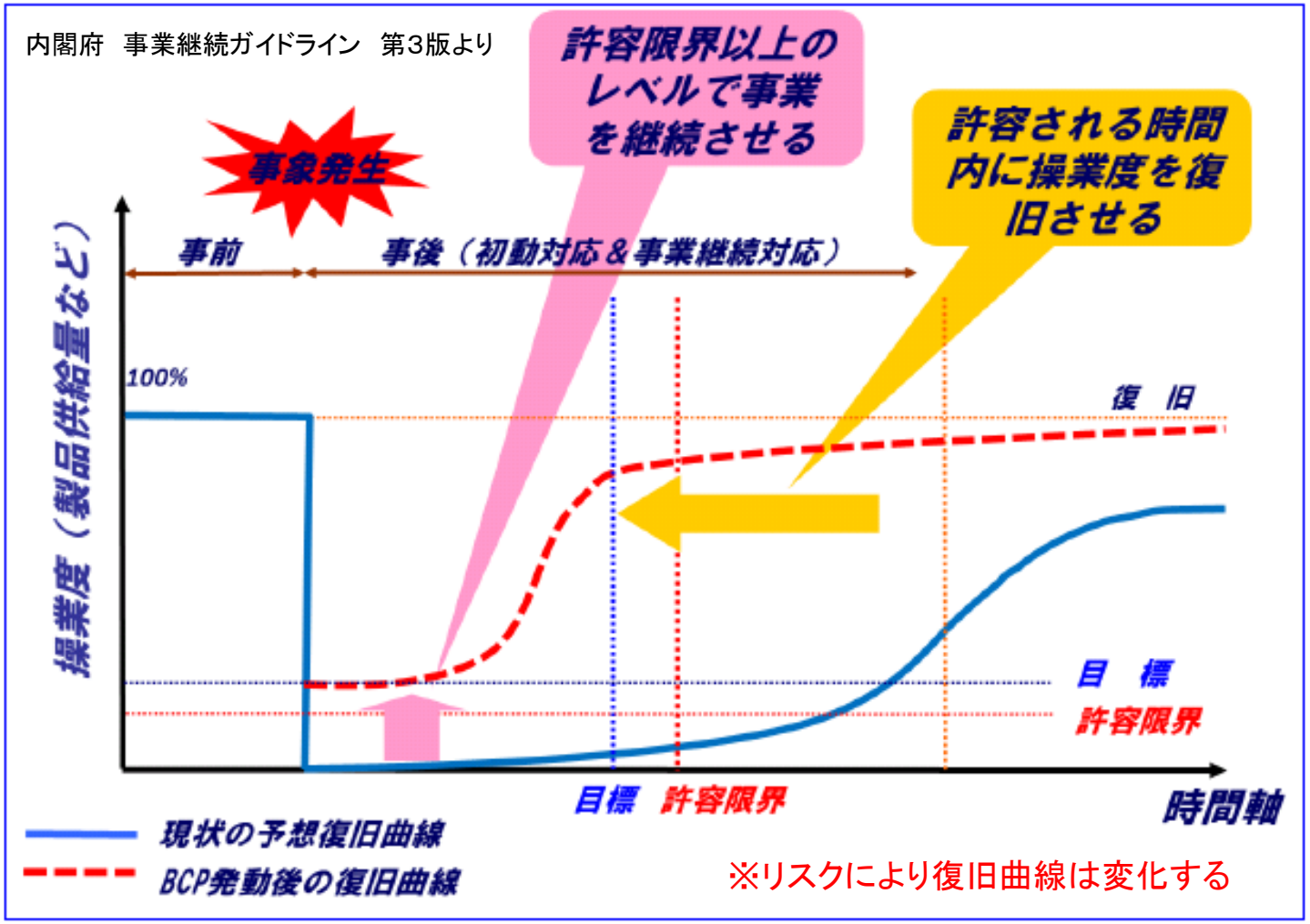
■内閣府　事業継続ガイドライン　第3版より

大地震等の自然災害、感染症のまん延、テロ等の事件、大事故、サプライチェーン（供給網）の途絶、突発的な経営環境の変化など不測の事態が発生しても、重要な事業を中断させない、または中断しても可能な限り短い期間で復旧させるための方針、体制、手順等を示した計画のことを事業継続計画（Business Continuity Plan：BCP）と呼ぶ。

■ISO：22301より

事業の業務の中断・阻害に対応し、事業を復旧し、再開し、あらかじめ定められたレベルに回復するように組織を導く、文書化された手順

目標復旧期間と復旧レベルの概念



いかに短時間で、目標のレベルまで復旧し、製品・サービスを供給できるか。事前にできる事は、実施、決定しておくことが重要。

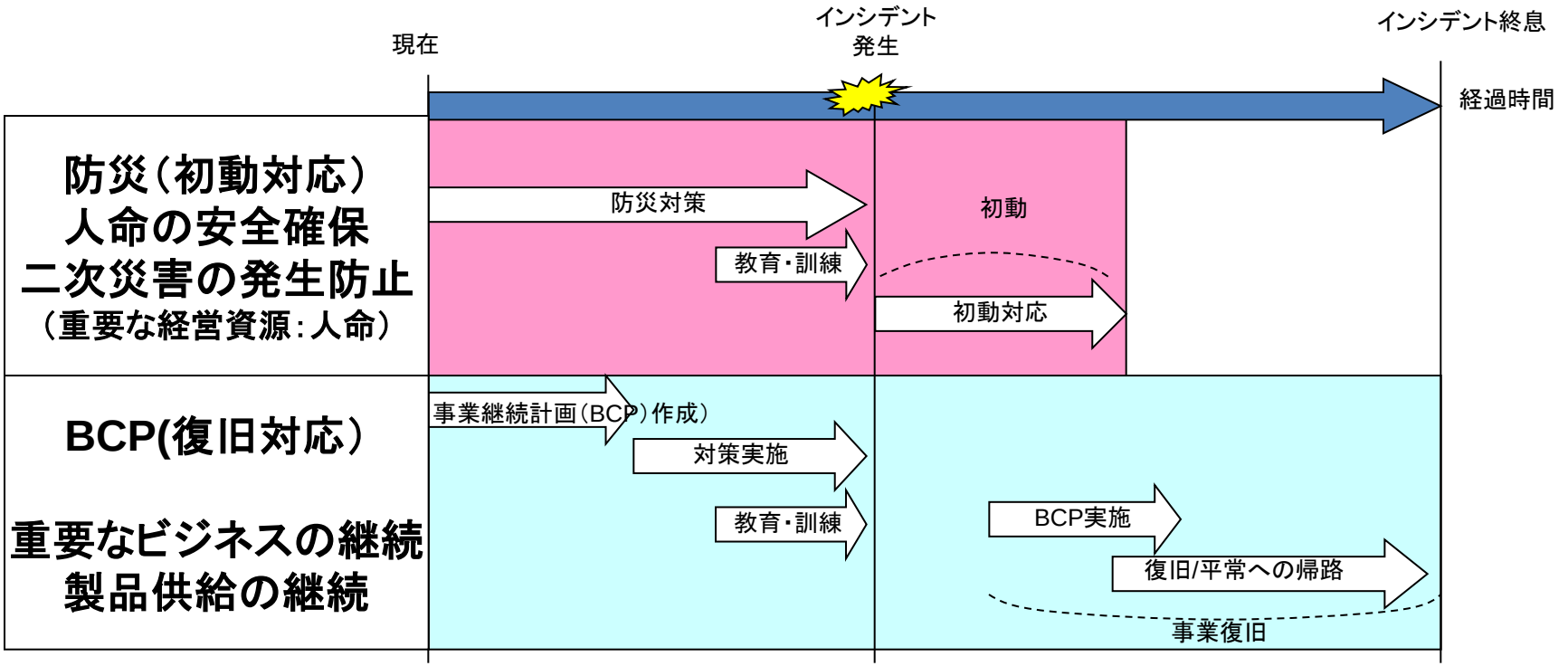
リスクマップに見る傾向と対策

BCM NAVI http://www.newton-consulting.co.jp/bcmnavi/glossary/risk_map.htm より

BCPは対象のリスクは、可能性の低減を考えることは困難。また、そもそも発生頻度が少ないため、対策にかかるコストが効果として表れにくい。いつ起こるかわからないリスクに対して、どの程度コストをかけるかは、経営者による経営判断が必要。

防災とBCPの関係

防災（初動対応）とBCP（復旧対応）の役割



防災は人命の安全確保、二次災害の発生防止を重視。BCPは、事業継続に必要な経営資源（**人、モノ、金、情報**）をいかに復旧確保し、製品、サービスの供給を継続するかということを重視。

※初動（防災）から事業復旧（広義のBCP）、初動（防災）を除く事業復旧（狭義のBCP ）

日本におけるBCPに関連する主なガイドライン

－　全業種向けのガイドライン等　－

■リスクを限定しない、事業継続全般に関するガイドライン等

（内閣府）
「事業継続ガイドライン 第三版」
http://www.bousai.go.jp/kyoiku/kigyou/keizoku/pdf/guideline03.pdf

（経済産業省）
「事業継続計画策定ガイドライン（企業における情報セキュリティガバナンスのあり方に関する研究会報告書・参考資料6）」
http://www.bousai.go.jp/kyoiku/kigyou/keizoku/pdf/sec_gov-report.pdf

「ITサービス継続ガイドライン」
http://www.bousai.go.jp/kyoiku/kigyou/keizoku/pdf/itsc_gl.pdf

（中小企業庁）
「中小企業BCP策定運用指針　～緊急事態を生き抜くために～ 」
http://www.chusho.meti.go.jp/bcp/

日本におけるBCPに関連する主なガイドライン

－　全業種向けのガイドライン等　－

■個別リスクに関するガイドライン等

・突発的に被害が発生するリスク（地震、水害、テロなど）に関するガイドライン
（日本経団連）
「大規模災害への対応における官民連携の強化に向けて」
http://www.keidanren.or.jp/policy/2016/028.html

・段階的かつ長期間に渡り被害が継続するリスク
（厚生労働省）
「新型インフルエンザ対策ガイドライン」
http://www.mhlw.go.jp/bunya/kenkou/kekkaku-kansenshou04/09.html

※個別業種向けのガイドライン等は
http://www.bousai.go.jp/kyoiku/kigyou/keizoku/sk.html　をご参照ください。

日本国内におけるBCPの策定状況

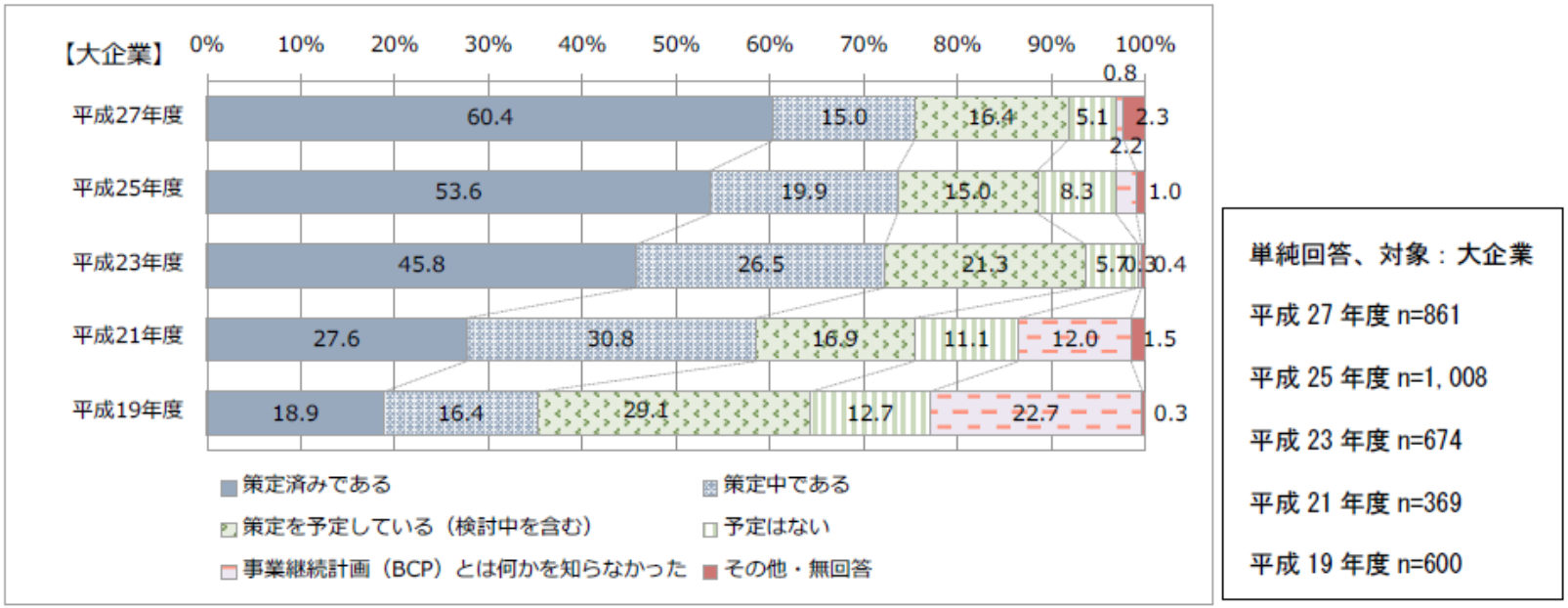
内閣府　平成27年度 企業の事業継続及び防災の取組に関する実態調査　より

平成26年6月3日に閣議決定された「国土強靱化基本計画」では、企業連携型BCP/BCMの構築促進等が盛り込まれている。また、平成26年6月3日に国土強靱化推進本部決定が決定した、「国土強靱化アクションプラン2014」では、起きてはならない最悪の事態の例として、サプライチェーンの寸断等による企業の国際競争力低下が例示されており、サプライチェーンを確保するための企業ごと・企業連携型BCPの策定が求められており、平成32年までの目標として、大企業はほぼ100%、中堅企業は50%の策定割合の指標が決められている。

日本国内におけるBCPの策定状況

内閣府　平成27年度 企業の事業継続及び防災の取組に関する実態調査　より

【大企業】

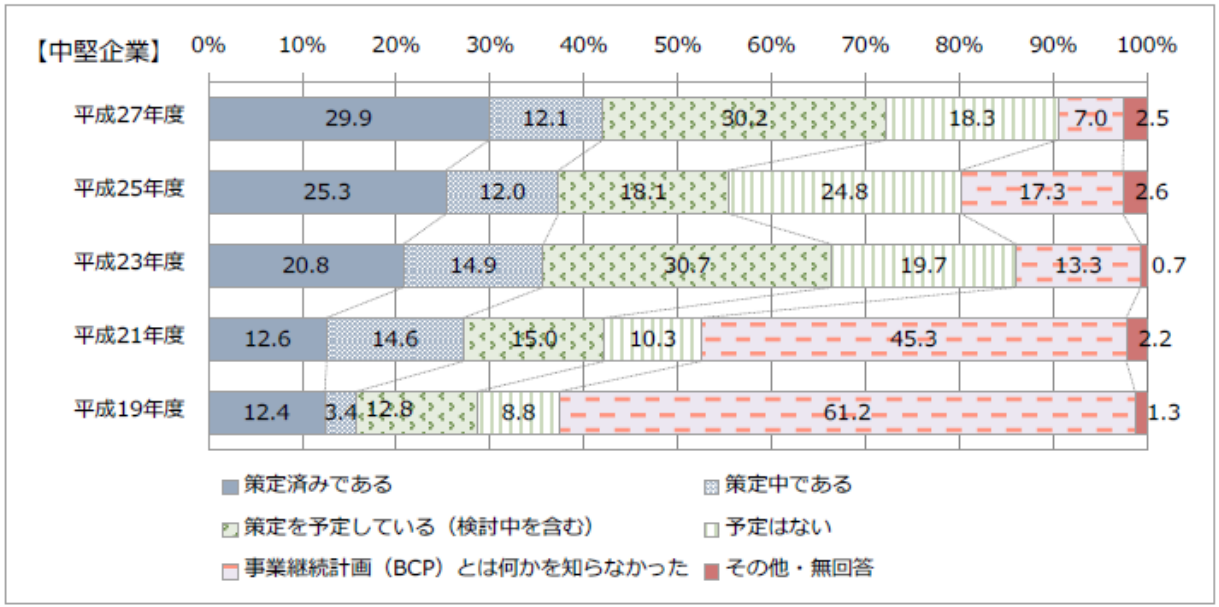


事業継続計画（BCP）の策定状況については、大企業では60.4%が「策定済み」と回答しており（平成25年度比6.8ポイント増）、初めて6割を超えた。これに「策定中」（15.0%）を加えると、8割近くとなっている。
なお、大企業でBCP策定の「予定をしている」という回答が16.4%（平成25年度比1.4ポイント増）となったほか、「予定はない」という回答が5.1%（平成25年度比3.2ポイント減）、BCPを「知らなかった」という回答が0.8%（同1.4ポイント減）となった。
以上のことから、大企業を中心に、BCPの策定は進んできている状況と言える。

日本国内におけるBCPの策定状況

内閣府　平成27年度 企業の事業継続及び防災の取組に関する実態調査　より

【中堅企業】



中堅企業では、29.9%が「策定済み」と回答している（平成25年度比4.6ポイント増）。これに「策定中」（12.1%）を加えると4割強となっている。
なお、中堅企業でBCP策定の「予定をしている」という回答が30.2%（平成25年度比12.1ポイント増）となったほか、「予定はない」という回答が18.3%（平成25年度比6.5ポイント減）、BCPを「知らなかった」という回答が7.0%（同10.3ポイント減）となった。以上のことから、大企業同様、BCPの策定は進んできている状況と言える。

世界におけるBCPの動き

ー　BCPに関連する規格　ー

■ANSI/NFPA1600（米国）
ANSI（米国規格協会）とNFPA（米国防火協会）が1993年策定。
NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs 2007 Edition
（政府・企業・NGO・一般市民などを対象。地方自治体を中心に実績。）

■BS25999（英国）
BSI（英国規格協会）が2006年策定。
・BS-25999-2（要求事項）⇒ISO22301の原型

その他、韓国、シンガポール、オーストラリア、カナダ他

■国際標準（ISO）：ISO22301
ISO/TC223（社会セキュリティ）　⇒　ISO/TC292（セキュリティ）へ統合

世界におけるBCPの動き

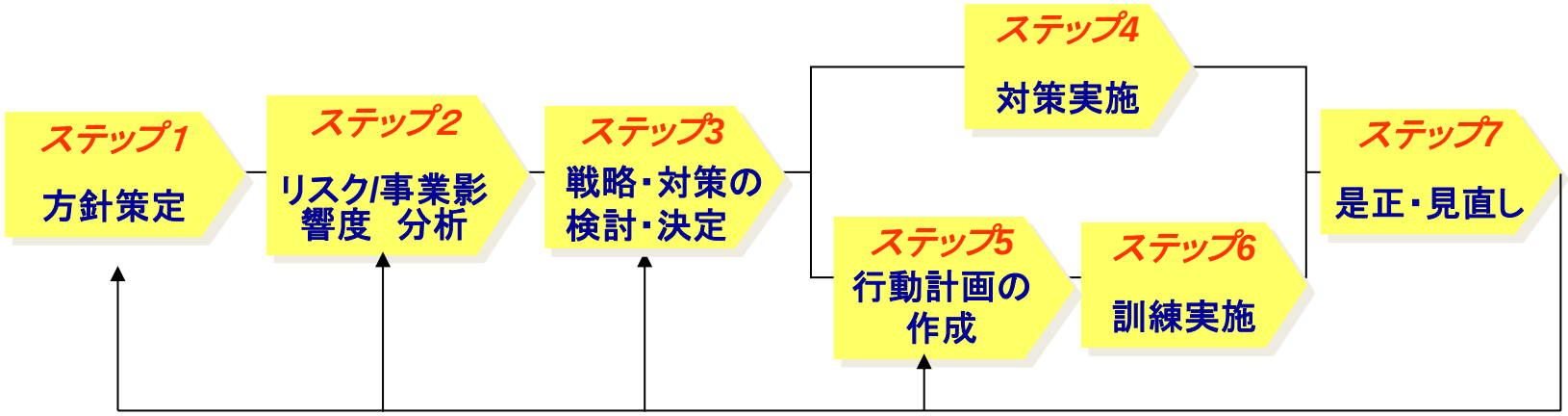
ー　BCPに関連する推進団体　ー

（米国）
DRII（Disaster Recovery Institute　International）
https://drii.org/

（英国）
BCI（The Business Continuity Institute）
http://www.thebci.org/

（日本）
特定非営利活動法人　事業継続推進機構（BCAO）
http://www.bcao.org/

BCP策定の活動ステップ（例）



ステップ１　方針策定
　　基本方針、リーダーシップ、対象範囲、体制の確立
ステップ２　リスク/事業影響度　分析
　　災害の特定、事業への影響を確認、目標復旧期間・目標復旧レベルの決定
　　重要な経営資源の抽出、影響を受ける経営資源の特定、財務状況
ステップ３　事業継続戦略・対策の検討、決定
　　影響を受ける経営資源に対して、対策に関する方針を事業継続戦略として
　　位置づけ、被害軽減策、早期復旧策、代替策を検討、決定、実施する。
ステップ４　対策実施
ステップ５　タイムラインの作成　－　重要経営資源を意識した行動計画　－
ステップ６　訓練実施　－　タイムラインを使用した訓練　－
ステップ７　是正、見直し

BCP策定の活動ステップ（例）

ステップ１　方針策定

■基本方針、リーダーシップ、対象範囲、体制の確立

（１）基本方針

　BCP策定に当たり、経営者はまず自社の事業及び自社を取り巻く環境を改めてよく理解し、自社が果たすべき責任や、自社の経営方針や事業戦略に照らし合わせ、社内外のステークホルダーからの要求に基づき、自社の事業継続に対する考え方を示す基本方針を策定する必要がある。

（２）リーダーシップ

　事業継続の目的やBCPの活動で達成すべき目標を決定し、取締役会または経営会議の決議を経ることにより、経営の一環として活動を推進することが重要である。

（３）対象範囲

　BCP策定の対象とする事業の種類や事業所の範囲などを明確にする。

BCP策定の活動ステップ（例）

ステップ１　方針策定

■基本方針、リーダーシップ、対象範囲、体制の確立

（４）体制の確立

**　経営者は、BCP策定に当たり、リスク/事業影響度　分析、対策の検討・決定・実施、訓練の実施等、BCP活動に必要な全社的な体制を構築する必要がある。**
なお、BCPを策定した後も、実効性のあるBCPを維持するため、見直し・改善を継続的に行うことができる体制が必要である。

BCP策定の活動ステップ（例）

ステップ２　リスク/事業影響度　分析

■リスク/事業影響度　分析の考え方

限られた経営資源の中で、製品・サービスを供給するためには、取捨選択が必要。効率的に資源配分を行うためのリスク/事業影響度　分析を行う

（１）災害の特定、

BCPの取り組みを行う組織のリスクを洗い出し、どのリスクを対象にするか決定する。
発生確率や影響度を見て決定。
・自然災害　地域の防災計画、防災マップを見て選択
・感染症
・IT関連事故（機器障害、情報漏えい、不正アクセス）

（２）事業への影響を確認

事業継続すべき重要事業（業務）を選定し、優先度を決定する。
・人命の安全確保や、社会インフラにかかわる事業（業務）
・市場占有率が高い製品を供給する事業
・重要なステークホルダー（利害関係者）に関連する事業
・主たる売上を確保する事業

BCP策定の活動ステップ（例）

ステップ２　リスク/事業影響度　分析

（３）目標復旧期間（Recovery Time Objective ：RTO）の決定

いつまでに、製品の生産が再開できるか、もしくは製品・サービスの供給が再開させるか目標とする時間、期間を決定する。

（４）目標復旧レベル（Recovery Level Objective ：RLO）の決定

目標とする時間、期間までに復旧する製品・サービスの供給量（レベル）を決定する。

※システム障害は目標復旧ポイント（Recovery Point Objective ：RPO）の設定を行う。損壊・紛失したデータを復旧させる際に、もどの時点（どれくらいの古さ；世代）のデータを復旧しなければならないのか、目標とするリカバリポイントを決定する。

BCP策定の活動ステップ（例）

ステップ２　リスク/事業影響度　分析

（５）重要な経営資源の抽出

選定した重要業務に必要な重要経営資源を選定する。

５M＋1E ＋１Ｉ の視点で分析

・材料、部品（Material）　・・・金型、冶工具、消耗工具、器具、備品、 原材料、副資材、金具、仕掛り在庫、保守・サービス業務、加工委託先

・設備、機械（Machine）　・・・ユーティリティ、装置・プラント、作業場、設備、機械
ITハードウェア（PC、サーバ、ネットワーク機器）

・作業者（Man)　　・・・労働力、資格、スキル

・作業方法（Method）　・・・生産・作業方法/手順

・検査、測定（Measurement）・・・検査方法/手順

・環境（Environment）　・・・建屋、作業場、拠点、クリーンルーム

・情報（Information ,System）・・・　技術系（CAD,CAM,研究/試験データ）、
設備系（エンベデットシステムマイクロプログラム）
管理系（勘定系、人事、給与、メール等）
PC　OS、DB、OLTP、ネットワークOS、
各種設定情報

BCP策定の活動ステップ（例）

ステップ２　リスク/事業影響度　分析

（６）影響を受ける経営資源の特定

選定した重要経営資源が、想定したリスクが発現した際に受ける影響を見積もる。

（７）財務状況

現在の経営状況で、どこまでの事業中断が許されるのか自組織の財務状況（資金繰り）を分析し、事業の許容停止時間を見積もる。

また、対策に投資可能な金額を把握する。

分析時点の対策状況で重要な経営資源が、復旧までに必要とする時間を推測し、目標した期間とレベルに対して、不足する場合は対策検討のステップへ。

BCP策定の活動ステップ（例）

ステップ３　事業継続戦略・対策の検討、決定

■事業継続戦略の考え方

（１）複数の組織に共通する対策

（２）複数の経営資源に共通する対策

（３）複数の製品に共通した完成品在庫による供給

（４）代替拠点による製品、サービスの供給

（５）競合他社による製品、サービスの供給

対策を考える中で戦略が決まる場合もある

BCP策定の活動ステップ（例）

ステップ３　事業継続戦略・対策の検討、決定

■重要な経営資源に対する対策の考え方（3段回で考える・・・バトルボックス）

（1）被害を最小化するための対策
- **・地震による直接的な影響**
  - **設備のずれ（移動）、転倒・・・耐震固定**
  - **部材の落下、漏えい**
- **・地震による間接的な影響（交通マヒ、物流停止、サプライチェーン中断）**
  - **部材在庫の確保。代替物流ルートの確保。**

（2）被災したとしても早期に復旧するための対策

再調達をいかに早くするか、復旧をいかに早くするか
- **・設備の故障・・・予備部品の確保。修理業者の手配。**
- **・部材の調達・・・複数購買、部材在庫の確保。**
- **・人材の確保・・・多能工化、復旧時の行動計画作成**

（3）復旧するまでの代替策

完成品在庫、代替生産（委託含む）立ち上げ

戦略があればその戦略に沿って、対策を検討および決定、実施する

BCP策定の活動ステップ（例）

ステップ３　事業継続戦略・対策の検討、決定

選定したリスクに応じて、リスクが発現した際に、重要な経営資源が受ける影響を確認。
事前の計画を策定し、必要であれば対策を実施する。　以下は事前災害、感染症の例。

		地震	水害	風害	火山噴火	感染症
受ける影響（直接）		揺れ	水ぬれ、流出	風で飛ばされる、物が飛んでくる	風、空振、噴石、火山灰、土石流、火砕サージ	症状により異なる
影響を受ける経営資源（間接被害も含む）		人、物（設備・部材）、金、情報				人 一部部材
対策	(1)被害を最小化するための対策	・耐震固定 ・免震、制震 ・耐震補強	・防水 ・耐水化	・防風 ・耐風化	・防熱 ・防風 ・防塵	・感染予防対策
	(2)被災したとしても早期に復旧するための対策	・補修部品の確保（リスクによって故障する部位）				マスク、タミフル等、薬剤の確保
		・代替人員の確保、多能工化				
		・サプライヤーや復旧業者との復旧時の取決め				
		・代替サプライヤー、部材在庫の確保				
	(3)復旧するまでの代替策	・完成品在庫による供給継続				
		・他工場での代替生産（関連会社、協力会社、同業他社も含む）				

対策の「(1)被害を最小化するための対策」は、リスクによって異なるが、(2)、(3)については、リスクが異なってもほぼ同じ対応になる。地震を対象としたBCPでも、他のリスクに対して、かなりの部分が応用可能である。

BCP策定の活動ステップ（例）

ステップ４　対策実施

■対策実施の考え方

（１）高額な対策費用で一度に実施できない対策は複数年かけて実施してもよい。

（２）高額な対策費用がかかる場合は、リスクを許容する選択肢もありうる。

（３）保険等の活用も検討する。

（４）BCPの対策にためだけに投資するのはもったいない。設備更新等と合わせて
効率的に対策を検討する。

（５）長期目標と短期目標を設定し、定期的に対策の完了時期を見直す。

BCP策定の活動ステップ（例）
ステップ５　タイムラインの作成
－　重要経営資源を意識した行動計画　－

■タイムラインの考え方

　災害時に各BCP取り組み組織の行動（対応）を組織全体として機能させるには、各組織間でお互いの行動を理解し合い、各部門が連携の取れた対応を行う必要がある。そのためには、時間の流れを共有して、まず自組織の災害時の行動を明確にする事が大切である。

BCP策定の活動ステップ（例）
ステップ５　タイムラインの作成
－　重要経営資源を意識した行動計画　－

（１）縦軸　　初動から復旧までの時間の流れ（タイムライン）を記載

（初動）　・・・行っている事業の内容にかかわらず統一した行動が必要。

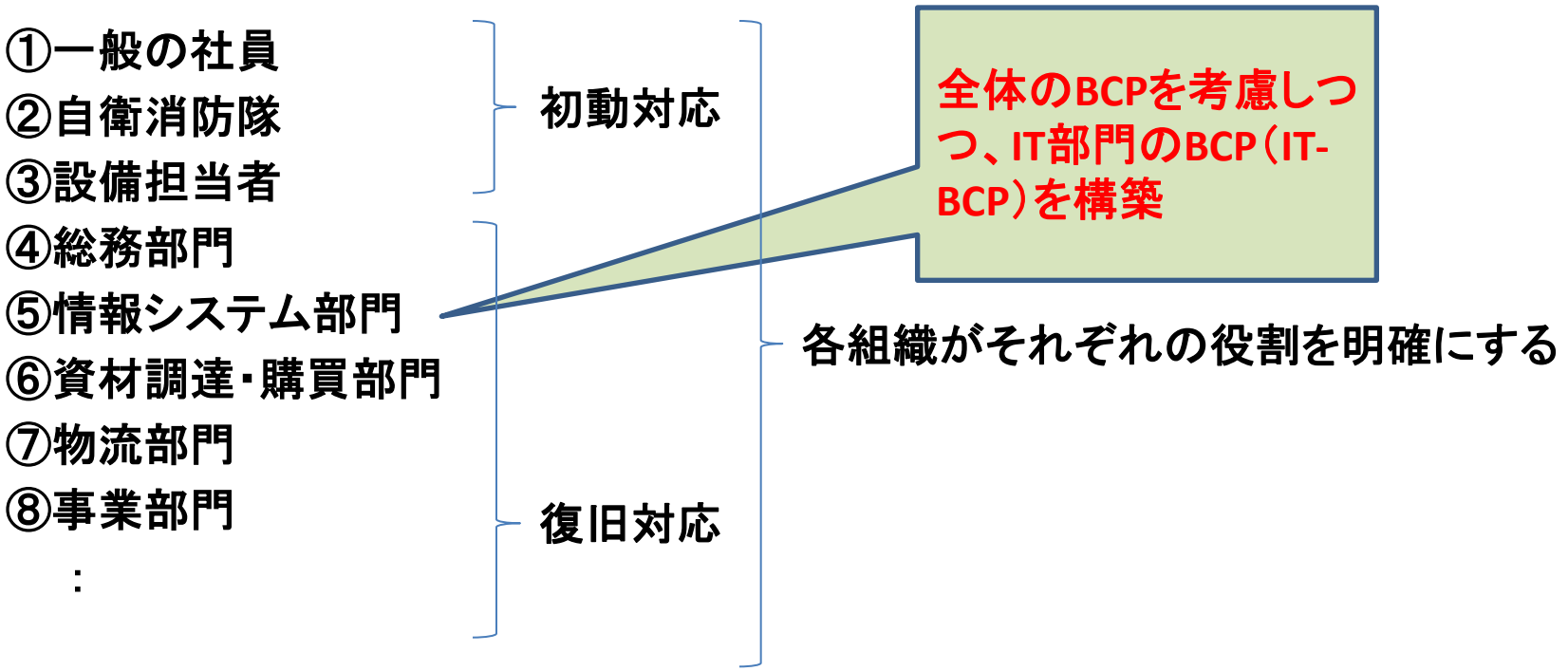
①一時避難
②二次災害防止
③周囲の状況確認と報告
④屋外避難
⑤帰宅指示

（復旧）　・・・行っている事業（重要な経営資源）の内容に合わせ行動を記載。

⑥地震BCP発動
⑦復旧準備
⑧復旧作業
⑨生産再開

BCP策定の活動ステップ（例）
ステップ５　タイムラインの作成
－　重要経営資源を意識した行動計画　－

（２）横軸　時間の流れ（タイムライン）に合わせ、各組織の役割を記載



BCP策定の活動ステップ（例）

ステップ６　訓練実施

－　タイムラインを使用した訓練　－

■訓練実施の考え方

　災害時に各組織の行動（対応）を組織全体として機能させるには、自部門の行動計画を各組織と共有し、各組織間でお互いの行動を理解する必要がある。
　また、訓練を通して、自組織の行動計画に反映すべき内容がないか、また自組織で解決できない課題を共有して、各ステップへの是正事項を洗い出す。

※自部門の復旧対応が、他部門の復旧の妨げになることがある。全体で調整し、
　全体を俯瞰した事業復旧が望まれる。

BCP策定の活動ステップ（例）

ステップ6　訓練実施

■訓練実施の考え方

　災害時に各BCP取り組み組織の行動（対応）を組織全体として機能させるには、策定したBCPが有効に機能するか、訓練を通じて確認する必要がある。

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

①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

②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

③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

BCP策定の活動ステップ（例）

ステップ6　訓練実施

日本ではあまり実施されてはいないが、さらには、発展的な訓練として以下のような訓練がある。

＜発展的な訓練の例＞

① 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

②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

BCP策定の活動ステップ（例）

ステップ7　是正・見直し

■是正・見直しの考え方

　対策状況や訓練状況から、早急に是正改善をしなければならない事項がないか確認する。特定組織の改善事項なのか、他組織に共有すべき改善事項なのかを判断し、他組織に共有すべき改善事項あれば、組織全体に是正を促す。
時間的に余裕のある改善事項は、翌年の活動に含める事も可能。
（あくまでも経営判断として。）
また、直近におこったインシデントの対応記録や経営環境の変化についても見直しの材料とする。

経営者のレビューにより活動の評価を実施し、
次期の活動計画に改善点を反映する。

IT-BCPを策定する上で関連する国際規格

ISO20001：
　ITサービスマネジメントシステム（ITSMS）に関する国際規格

ISO20002：
　ITサービスマネジメントについての実践規範

ISO/IEC27001：
　情報セキュリティマネジメントシステム（ISMS）に関する国際規格

ISO/IEC27002：
　情報技術 — セキュリティ技術 — 情報セキュリティマネジメントについての
　実践規範

ISO/IEC27017:
　ISO/IEC27001やISO/IEC27002に示されている詳細管理策を、
　クラウドサービスにおけるセキュリティ対策という観点で補完

IT-BCPを策定する上で関連する国際規格

ISO27031:
IT-BCPの国際ガイドラインでIT-BCPの策定・維持管理に必要な活動やテクニックについて解説。但し、この規格内ではIT-BCPという表現ではなくIRBC（ICT readiness for business continuity ）という用語で表現されている。

ISO31000：
リスクマネジメント手法のガイドライン
組織体のどのレベル・規模であっても適用可能な「リスクマネジメントの考え方」を説明

COSO ERM
リスクマネジメント手法のガイドライン
事業体全体としてのリスク管理を目的としている

日本におけるIT-BCP等に関連する主なガイドライン

（経済産業省）
「IT サービス継続ガイドライン 」
http://www.meti.go.jp/policy/netsecurity/downloadfiles/itsc_gl.pdf

「サイバーセキュリティ経営ガイドライン」
http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf

（内閣官房情報セキュリティセンター）
「中央省庁における情報システム運用継続計画ガイドライン」
http://www.nisc.go.jp/active/general/pdf/itbcp1-1_2.pdf
「IT-BCP 策定モデル」
http://www.nisc.go.jp/active/general/pdf/IT-BCP.pdf

（サイバーセキュリティ戦略本部）
「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」
http://www.nisc.go.jp/active/infra/pdf/shishin4.pdf

第２部　「中央省庁における情報システム運用継続計画ガイドライン」をもとにIT-BCPを考える

中央省庁における情報システム運用継続計画ガイドラインとは

■中央省庁における情報システム運用継続計画ガイドライン

http://www.nisc.go.jp/active/general/pdf/itbcp1-1_2.pdf

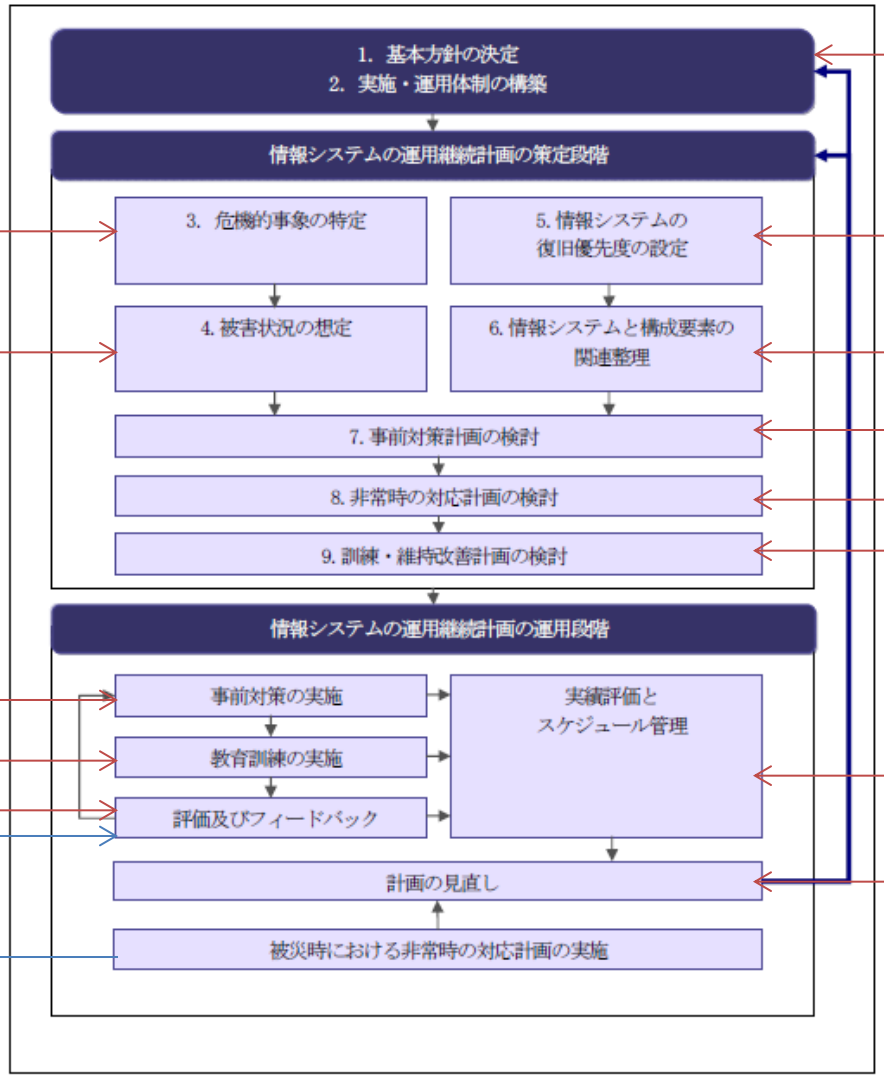
中央省庁業務継続ガイドラインにおける情報システムの検討部分をより詳細化もの

＜構成＞
・策定手引書
・雛型及び雛型の別紙

＜対象＞
中央省庁の情報システム担当者

＜内容＞
「情報システム運用継続計画」（以下、IT-BCP）を策定し、計画を運用（計画の実施及び継続的維持改善）するための手引書

IT-BCP の策定と運用の流れ



方針・体制の確立

RA

BIA

BIA

BIA

戦略・対策

戦略・対策

教育・訓練

戦略・対策

教育・訓練

評価

評価

是正・見直し

（加筆）

※実施した計画は評価、フィードバックが必要

図 1.2-1 情報システム運用継続計画策定・運用の流れ

「中央省庁における情報システム運用継続計画ガイドライン」 P.6

IT-BCP の策定内容

表 1.2-1 検討作業の概要

	検討作業名		検討作業の概要
1	基本方針の決定		情報システム運用継続計画策定の対象範囲を定める。検討に当たり関係者間で共有すべき基本方針を定める。
2	実施・運用体制の構築		情報システム運用継続計画の策定・運用に係る推進体制を構築する。
3	危機的事象の特定		情報システム運用継続計画の対象とする情報システムの継続を脅かす危機的事象を調査・検討し、特定する。
4	被害状況の想定		対象とする危機的事象が発生した場合に想定される情報システムの被害状況を想定する。
5	情報システムの復旧優先度の設定		
	①	優先業務と情報システムの関連整理	非常時優先業務を確認した上で、対象の情報システムと両者の関連性を整理する。
	②	情報システムの復旧優先度の設定	業務の目標復旧時間と、情報システム停止時の代替手段を踏まえ、情報システムの復旧優先度を設定する。
6	情報システム運用継続に必要な構成要素の整理		
	①	情報システムを支える構成要素の明確化	非常時に必要な情報システムの構成要素（システム、データ、サーバ、要員等）を整理する。
	②	構成要素ごとの目標対策レベルの設定	情報システムの構成要素ごとに、情報システムの復旧優先度に応じた目標対策レベルを設定する。
7	事前対策計画の検討		
	①	現状対策レベルの確認と脆弱性の評価	情報システムの構成要素ごとに、現状の対策レベルを評価し、情報システムの脆弱性を整理する。
	②	事前対策の実施計画の作成	脆弱性と目標対策レベルを踏まえ、情報システムの継続能力を強化する「事前対策計画」を作成する。
8	非常時の対応計画の検討		
	①	非常時体制の構築	非常時に情報システムを早期に復旧させるために必要となる情報システム部局の体制・役割を決定する。
	②	非常時における対応手順の作成	情報システムを復旧させる具体的な対応方法を手順書として整理する。
9	訓練・維持改善計画の検討		
	①	教育訓練計画の検討	事前対策や非常時の対応計画の実効性を高めるための「教育訓練計画」を作成する。
	②	維持改善計画の検討	情報システム運用継続計画を定期的に見直すための「維持改善計画」を作成する。

今回の記載番号	検討作業名	
1	基本方針の決定	
2	実施・運用体制の構築	
3	危機的事象の特定	
4	情報システムの優先度の決定	
	4．1	優先業務と情報システムの関連整理
	4．2	情報システムの復旧優先度の設定
5	被害の想定	
	5．1	情報システムを支える構成要素の明確化
	5．2	選定した重要な経営資源が受ける影響の見積もり
6	現状対策レベルの確認と脆弱性の評価	
7	構成要素ごとの目標対策レベルの設定 復旧戦略の策定	
8	事前対策計画の検討	
9	非常時の対応計画の検討	
	9．1	非常時体制の構築
	9．2	非常時における対応手順の作成
10	教育訓練計画・維持改善計画の検討	
	10．1	教育訓練計画の検討
	10．2	維持改善計画の検討

「中央省庁における情報システム運用継続計画ガイドライン」 P.7

1．基本方針の決定

■検討内容と留意事項

IT-BCP策定の対象範囲を定め、優先すべき復旧すべき重要システム等、
関係者間で合意すべき基本方針について定め、合意形成する。

①業務システムだけでなく、業務システムを支える共通情報インフラも対象範囲
から漏れないようにする。

・メールシステム、DNS、認証サーバ、LAN、WAN等

②新規業務システム導入時の運用設計からIT-BCPを検討事項に含め、導入時
より必要な対策を実施する

２．実施・運用体制の構築

■検討内容と留意事項

「1 基本方針の決定」で定めたIT-BCPの策定の対象範囲を踏まえつつ、必要な担当者を定める。また、関係者間（ステークホルダー）との連携体制を構築する。

①業務システムを中心にステークホルダーである関係部門（他の情報システム部門や購買部門、経理部門、営業部門、総務部門等）を明確にする。

② IT-BCPの策定・運用に必要な要員を定め、その要員の役割を明確にする。他部門の要員が、 IT-BCPの策定・運用の検討に加わる場合、指示命令系統の調整等、関係者との連携方法を調整する。

③①の関係部門が立案した業務継続計画との整合性を考慮する。

④機密性と可用性の整合性を考慮し、緊急時の例外運用をどこまで認めるか事前に調整する。

３．想定する危機的事象の特定

■検討内容と留意事項

IT-BCPの対象とする危機的事象を決定する。関連部門の業務継続計画で対象とした危機的事象だけでなく、情報システム特有の危機的事象も考慮する。

①発生の確率と業務への影響を考慮し、対象とする危機的事象を決定する。
情報システム特有の危機的事象および、関係部門が立案した業務継続計画の危機的事象に対応できるよう検討する。

情報システム特有の危機的事象　機器の故障、ウイルス感染、不正アクセス等

②初めから全ての危機的事象について、検討することは時間、費用の面で難しいため、まずは地震等の発生確率は低いものの、業務への影響が大きい危機的事象から優先順位をつけて取り組む。

４．情報システムの復旧優先度の設定

４．１　優先業務と情報システムの関連整理

■検討内容と留意事項

既存の業務継続計画に定められる非常時優先業務を確認し、対象システムとの関連性を整理する。

①業務継続計画に定められた非常時優先業務を洗い出す。
　平常時の重要業務と異なる場合があるため注意が必要。また、非常時優先業務を支える共通業務があれば、それも対象に含める。
　洗い出した非常時優先業務は、最終的に関係者で合意形成を行うこと。

②業務継続計画に定められた非常時優先業務を支える業務システムを洗い出す。
　洗い出す業務システムは、業務側で意識されている情報システム単位とする。
　業務システムを支える共通（基盤系）システムがあればそれも、業務システムの前提のシステムとして関連性をまとめ、対象に含める。

４．情報システムの復旧優先度の設定

４．２　情報システムの復旧優先度の設定

■検討内容と留意事項

「4.1 優先業務と情報システムの関連整理」で洗い出した情報システムに対して、それぞれ目標復旧時間（IT-RTO） を設定する。

①業務の目標復旧時間の確認と情報システムに求められるIT-RTOの設定
「 4.1 優先業務と情報システムの関連整理」で整理した各非常時優先業務の目標復旧時間を確認する。かりに、その業務が情報システムを使わない手段で業務継続できるのであれば、いつまで、もしくはどれくらいの処理量まで、情報システムを使わない手段で対応可能か関係者に確認し、IT-RTO を設定

②IT-RTOが短ければ短いほど対策にかかる費用は高額になる。予め、業務側へ説明し、情報システムを使わない手段で業務継続できる方法も検討すること。

③複数の非常時優先業務で使用される業務システムは、最もRTOが短い非常時優先業務に合わせたIT-RTO を設定する。

④共通（基盤系）システムは、非常時優先業務で使用される業務システムのIT-RTOと同じ、もしくはそれより短い復旧が要求されることを留意すること。

4. 情報システムの復旧優先度の設定

4. 2 情報システムの復旧優先度の設定

⑤システム復旧優先度のグループ分け

IT-RTO の設定結果より、最終的に情報システムをIT-RTO の時間帯により、層別し、復旧の優先度を決定する。
復旧優先度ごとに層別することにより、情報システム全体を俯瞰し、検討の抜けや漏れ、優先順位の整合性に問題がないかを確認する

「情報システムの復旧優先度ランク」

復旧優先度ランク	情報システムに求められる目標復旧時間
S	0～3時間以内に復旧が必要な情報システム
A	3時間から1日以内に復旧が必要な情報システム
B	1日から3日以内に復旧が必要な情報システム
C	3日から1週間以内に復旧が必要な情報システム
D	1 週間から2週間以内に復旧が必要な情報システム
E	2週間を超える停止が許容できる情報システム

⑥復旧優先度の高い情報システムは出来るだけ数を絞り込むこと。

災害発生直後は、人命の安全確保、二次災害の防止等、対応する人員も限定されるため、復旧すべき業務システムは極力、限定する。

４．情報システムの復旧優先度の設定

４．２　情報システムの復旧優先度の設定

⑦情報システムの優先順位は検討メンバーで、優先度の仮説を立てたうえで、関係者へ確認し、合意を得る。

⑧担当者の変更や定期的な見直しの際に、情報システムの優先を設定した根拠を明確にしておく。

５．被害状況の想定

５．１　情報システムを支える構成要素の明確化

■検討内容と留意事項

危機的事象が発生した際に重要な情報システムに係る重要な経営資源を明らかにする。情報システムに係る重要な経営資源を5M＋1E ＋1Ｉ の視点で選定する。

重要な経営資源の種類	具体的な資源の例
設備、機械（Machine）	ITハードウェア（PC、サーバ、ネットワーク機器、外付けHDD、光学ドライブ、プリンタ）
資材品・サービス（Material）	保守・サービス業務、外部ベンダー
作業者(Man)	オペレータ、データ入力者
作業方法（Method）	業務データ処理方法/手順
検査、測定(Measurement)	検査、測定方法/手順
環境（Environment）	拠点、建屋、フロア、電気、ガス、燃料、水、通信（音声、データ）、交通機関
情報（Information ,System）	技術系（CAD,CAM,研究/試験データ）、設備系（エンベデットシステム、マイクロプログラム）、業務系（生産管理、人事給与、財務会計等）、OS、DB、OLTP、メール、Web、CAD、各種設定情報

5. 被害状況の想定

5．2　選定した重要な経営資源が受ける影響度の把握

■検討内容と留意事項

危機的事象が発生した際に重要な情報システムに係る重要な経営資源への被害状況を想定する。

具体的な資源の例	地震によって受ける影響
ITハードウェア	ラックの転倒や机から落下して、HDD、マザーボード、電源等が破損し動かなくなる。
保守・ｻｰﾋﾞｽ業務、外部ﾍﾞﾝﾀﾞｰ	保守業者が手配できない。外部委託したクラウドサービスが利用できなくなる
オペレータ、データ入力者	オペレータ、データ入力者もしくはその家族が被災し、出社できなくなる。
業務データ処理方法/手順	通常の業務データ処理方法/手順で運用ができなくなる。
検査、測定方法/手順	検査、測定方法/手順
・拠点、建屋、フロア、 ・電気 ・ガス、燃料 ・水 ・通信（音声、データ） ・交通機関	拠点、建屋、フロアが使えなくなる。 電気を使用したITハードウェア、空調設備が使用できなくなる。 ガス、燃料を使用した発電機が使用できなくなる。 水を使用した水冷のメインフレーム、空調設備が使用できなくなる。 携帯電話や内線や外線電話が使えない。他拠点、社外とのデータ交換、外部からの情報収集が出来ない。 交通機関の停止により、社員が帰宅や出社ができない。
技術系、設備系、業務系、OS、 DB、OLTP、メール、Web、CAD、 各種設定情報	HDDの故障によりデータが利用できなくなる。

５．被害状況の想定

５．２　選定した重要な経営資源が受ける影響度の把握

①細かすぎる被害想定は避ける。被害状況は、正確に詳しく予測することは不可能である。また、軽すぎる被害状況を想定すると、本来必要な事項の検討に抜けが出る恐れがある。起こりうる状況を鑑み、ある程度、重大な被害(再調達や再作成になるくらいの被害)を受けることを前提とした被害状況を想定することが望ましい。

６．現状対策レベルの確認と脆弱性の評価

■検討内容と留意事項

現時点での情報システム環境の対策状況を確認し、「５．２　選定した重要な経営資源が受ける影響度の把握」で確認した影響に対して、どこまで耐えうるか、現状の情報システム環境を継続するための課題（脆弱性）を評価する。

①現状対策レベルの確認と脆弱性評価
情報システムごとに、IT-RTOを達成できる対策レベルあるのか評価する。該当する情報システムが複数の設備機器で構成されており、設備機器毎に現状対策レベルが異なる場合は、最も対策レベルが低い設備機器の対策レベルを、当該情報システムの現状対策レベルとし、そのレベルがIT-RTOを達成できる対策レベルに達していない場合は、その設備機器が当該情報システムの脆弱点となる。

６．現状対策レベルの確認と脆弱性の評価

②最低限、脆弱性を評価すべき事項

　情報システムの復旧継続を困難とさせる以下の重大な脆弱性については最低限評価しておく必要がある。

・危機事象発生時の対応体制及び連絡方法の整備状況
・同一拠点内でのハードウェアへの対策状況
・重要なデータ（システム領域／データ領域）のバックアップ状況
・ハードウェアやソフトウェアの再調達が困難になる可能性の有無の把握

③脆弱性の評価の結果、IT-RTOを達成できると判断した情報システムは追加の対策は不要とする。

④計画的に事前対策を行い、最も対策レベルが低い設備機器の対策レベルが、IT-RTOを達成できるレベルになった場合は、情報システムを構成する他の設備機器の対策レベルが、IT-RTOを達成できるレベルになっているか再評価を行う。

7．構成要素ごとの目標対策レベルの設定 復旧戦略の策定

■検討内容と留意事項

情報システムをIT-RTO 内に復旧させるために、復旧対策の計画立案に際して、対策全体にかかわる方針（戦略）を作成する。
また復旧優先度に対応して必要となる構成要素毎の対策の目標（以下、目標対策レベルと言う）を設定し、重要な経営資源に対して対策計画の立案、実行管理するための基準を作成する。

＜方針、基準の例＞

- 現状の拠点が被災した場合、同時被災しない拠点への移設
- 目標復旧期間が１週間の設備は、災害対策が考慮されたデータセンターへ移設する。
- 復旧の余裕が１か月以上あるシステムは、バックアップメディアが、確実に被災しない対策がされていれば同一拠点に保管することも対策として認める。

7. 構成要素ごとの目標対策レベルの設定 復旧戦略の策定

① 「情報システムを支える構成要素の明確化」で定めた構成要素ごとに復旧優先度レベルに応じた目標対策レベルを整理する。

これにより、IT-RTOを達成するために必要な対策の目標（ゴール）が設定され、現状の情報システム環境を踏まえた状況との乖離及び今後実施すべき対策を明確化することができる。

＜目標復旧レベル設定の例＞

現状の拠点と同時被災しない場所にバックアップシステムを確保することを基本方針とする対策レベル （ハードウェアの例）

情報システムの復旧優先度	対策目標（例）	対策レベル
S	ホットスタンバイ用ハードウェアの確保 ・専用の代替機を、現在の拠点と同時被災しない拠点に設置する。被災時は代替機に切り替えることで、バックアップシステムによる復旧を行う。※1	4
A B	ウォームスタンバイ用ハードウェアの確保 ・他システムと共有の代替機を、現在の拠点と同時被災しない拠点に設置する。被災時には専用の代替機として利用することにより、バックアップシステムによる復旧を行う。※1	3
C D	コールドスタンバイ用ハードウェアの確保 ・現在の拠点と同時被災しない拠点にOS、アプリケーションをインストールしていない状態の予備機を準備する。※1	2
E	遠隔地にバックアップ用ハードウェア準備なし（被災拠点での復旧） ・販売が終了しており、再調達できないハードウェアを利用しないようにしておく。 ・ハードウェアの損壊時に修理部品や代替機を入手できるよう、保守契約を締結する。 ・耐震性が確保されたサーバルーム内に設置するとともに、冗長化構成をとることで、被災時にシステムが停止する可能性を低減させる。	1

データセンタへの移設を基本方針とする対策レベル（ハードウェアの例）

情報システムの復旧優先度	対策目標（例）	対策レベル
S A B C	データセンタへの移設 ・首都直下型地震発生時にも情報システムへの被害が極小化される堅牢なデータセンタへ移設する。	2
D	データセンタへの移設なし ・販売が終了しており、再調達できないハードウェアを利用しないようにしておく。 ・ハードウェアの損壊時に修理部品や代替機を入手できるよう、保守契約を締結する。 ・現在の拠点の情報システムのハードウェアに耐震措置や免震措置を実施するとともに、冗長化構成をとることで、被災時に損壊する可能性を低減させる。	1
E		

※1 現在の拠点の情報システムのハードウェアについては、耐震性が確保されたサーバルーム内に設置するとともに、冗長化構成をとることで、被災時にシステムが停止する可能性を低減させることを前提とする。

7．構成要素ごとの目標対策レベルの設定 復旧戦略の策定

② 目標対策レベルは、目標復旧時間を満たすための視点で作成すること。
ここで設定する目標対策レベルは、あくまでも目標復旧時間を満たすために必要な望ましい対策手段である。
現状の情報システム環境や予算からみた場合、短期間で対策を完了することは難しい場合がある。しかしながら、システムの再構築や機器の更新時等、中長期的視点に立ち、継続的維持改善することで、目標レベルを達成できるように管理することが重要である。

８．事前対策計画の検討

■検討内容と留意事項

① 目標対策レベルと現状対策レベルのギャップ を解消し目標対策レベルに近づけるための方策をシステムごとに検討し、事前対策計画を作成する。
事前対策計画の作成に当たっては、現状の情報システム環境や予算等を考慮し、必要に応じて幾つかのステップに区切り、段階的に継続能力を強化する計画としてもよい。目標対策レベルどおりの対策を実施することを終ステップに置き、その前には幾つか現実的に取り組める対策群を対策ステップとしてまとめる。また、計画的に復旧優先度の高い情報システムから順次対策を実施する。ステップを区切る際は、各ステップでどのような脆弱性を解決できるか（期待効果）を整理する。
また、ステップを実施しても残存する脆弱性（残存リスク）を整理する。これらとともに、概算費用も考慮し、それぞれのステップの実施計画を作成する。

② 事前対策計画の具体化として各ステップの実施計画に基づき、「情報システムを支える構成要素の明確化」で定めた構成要素ごとに、事前対策の実施内容を具体化する。実際に事前対策を実施する際には、立案した情報システム運用継続計画を確認し、仕様書に必要な条件を盛り込むこと。

８．事前対策計画の検討

③ 予算等の関係から、目標として定めた対策をすぐに実施することが難しい場合には、「優先的に取り組むべき対策一覧（首都直下型地震）」に示すような対策を優先して実施することが望ましい。
この他、非常時にシステムを利用するためには、利用者側のクライアント端末に対しても対策を行う必要がある。
首都直下型地震に対してはパソコンに耐震固定を施す等、必要な対策に取り組むことが望ましい。またイントラネットに接続するクライアント端末は、非常時においてもセキュリティ要求事項を極力満たすようにしておく必要がある。
セキュリティ要求事項を満たした端末を早急に用意できるように、セキュリティ用のアプリケーションのインストール媒体や他の端末からのセキュリティ機能をコピーできる仕組み等を、予め用意することが望ましい。
また、必要に応じ、非常時のセキュリティレベルの低下をどこまで許容するか関係者と事前調整しておくことが望ましい。

8. 事前対策計画の検討

「優先的に取り組むべき対策一覧（首都直下型地震）」

構成要素		実施内容	対策例
施設	＜建屋＞	重要システムの設置されている建屋の耐震性能を確保すること。	・耐震性能の高い拠点への移設、代替環境の構築
	＜電源＞	非常時のシステム運用に必要な自家発電能力を確保すること。	・自家発電を管理する部局との間で、システム運用に割り当てられる自家発電能力を確認の上、必要な発電能力を確保
		システムの電源に対する必要な措置をとること。	・自家発電装置への切り替えに備えた、無停電電源装置（UPS）の準備 ・無停電電源装置（UPS）の定期的な確認
	＜空調＞	システム運用用の空調が非常時にも稼働するよう考慮すること。	・空調の非常用電源との接続
		空調本体の落下等、二次被害を低減するための対策を実施すること。	・空調本体の構造躯体に対する固定措置
	＜セキュリティ＞	非常時における不正な機器の接続防止やその前提となるマシン室等への入退室管理について適切なセキュリティ確保の対策を実施すること。	・情報セキュリティに係る府省庁の基準の改訂（非常時の対応を検討する）

8. 事前対策計画の検討

「優先的に取り組むべき対策一覧（首都直下型地震）」

構成要素	実施内容	対策例
ネットワーク	府省庁内LANを早期に復旧できる対策を実施すること。	・各種ネットワーク設定ファイルの定期的なバックア ップ ・耐火性・耐震性のある保管庫への定期的保管や同時被災しない拠点への外部保管 ・ルータやハブ等の予備品確保 ・障害発見を迅速に行うためのネットワーク障害監視の仕組みを導入
	被災時にLAN切断の可能性を低減させる対策を実施すること。	・LANの冗長化 ・冗長化したLANの経路考慮（東回りと西回りでLANを敷設する等）
	被災時にLANが不通になる可能 性を低減させる対策を実施すること。	・無線LANの活用
	拠点間をつなぐアクセス回線やバックボーンの停止する可能性を下げる対策を実施すること。	・アクセス回線の冗長化 ・キャリアの分散
周辺機器	周辺機器の被害を低減させる対策を実施すること。	・転倒防止措置の実施
	情報漏えいの可能性を低減させる対策を実施すること。	・データの暗号化 ・廃棄時の適切な処理

8. 事前対策計画の検討

「優先的に取り組むべき対策一覧（首都直下型地震）」

構成要素	実施内容	対策例
ハードウェア	再調達が不可能、もしくは長期間を要するハードウェアを確認し、必要な対策に取り組むこと。	・旧システム入替の検討 ・ハードウェアを利用するシステムや業務について、同様のサービスを提供できる企業・団体へのアウトソーシングや、非常時のみ業務を委託する事前契約
	地震発生時もハードウェアへの被害を最小限に抑える対策を実施すること。	・サーバラックの耐震補強 ・免震措置
システム領域／データ領域	データ消失を回避するための対策を実施すること。	・バックアップの取得 ・耐火性・耐震性のある保管庫への定期的保管や同時被災しない拠点への外部保管
	バックアップの適切な頻度を検討すること。	・各データの更新頻度に応じた現状のバックアップ頻度の適正化
	バックアップのリカバリテストを実施すること。	・バックアップとして取得したデータを、実際に利用できるかリカバリテストの実施
	バックアップの実施によって新たに発生する恐れのある情報セキュリティ上の脆弱性に対し、対策を実施すること。	・バックアップデータに対するデータ暗号化及びデータ改ざん防止措置 ・ネットワークの暗号化（いずれも情報セキュリティに係る府省庁の基準に則り、適切に実施する）

8. 事前対策計画の検討

「優先的に取り組むべき対策一覧（首都直下型地震）」

構成要素	実施内容	対策例
システム運用体制	担当者が出勤できない場合の対応手段を講じること。	・ネットワークの遠隔監視手段の整備
	迅速な安否確認を可能にするための対策を実施すること。	・緊急連絡網の整備 ・安否確認システムの導入
	迅速な情報共有のための対策を実施すること。	・Web会議/TV会議システム ・（クラウド等を利用した）待機系電子メールサービス ・ローカルPC 等を使った簡易システムによる業務代替戦略
	情報システム復旧のための体制と役割分担を整備すること。	・非常時体制の整備
	情報システム復旧のための手順を作成すること。	・非常時における対応手順書の整備
	非常時に利用する備品類を確保し、迅速な対応を可能にすること。	・固定電話・携帯電話不通時の連絡手段の確保（衛星電話、広域無線）
ベンダの継続能力	早期にシステムを復旧するために、必要に応じベンダとの契約を見直すこと。	・情報システムベンダとの保守契約の見直し、非常時の対応内容の明確化等

９．非常時の対応計画の検討

９．１　非常時体制の構築

■検討内容と留意事項

① 平常時の情報システム運用継続体制を踏まえ、非常時において情報システムを復旧する責任者、担当者及びそれぞれの代行者を定める。下表は、情報システムの復旧対応に必要な体制・役割の例である。組織の業務内容や組織構造等に応じ、体制・役割の追加や変更をすること。

② 情報システムを復旧する責任者・担当者は、非常時におけるベンダとの協議、情報システムの復旧作業を承認する役割を担うほか、各組織からの情報システムの復旧に関する催促及び問合せに対応し、報告も行わなければならない。このため、復旧作業の担当者と各部局からの連絡窓口を分離したり、IT-RTO の短いシステムの担当が特定の担当者に集中しないようにしたり、各担当者が適宜交代で休憩が可能なように配慮する等、非常時における職員の負荷を考慮し、体制を構築する必要がある。また、被災者が出た場合のOB・OGによる部外からの応援も考えておく必要がある。

９．非常時の対応計画の検討

９．２　非常時における対応手順の作成

■検討内容と留意事項

① 情報システム復旧に係る判断基準の作成
復旧対応に必要な判断基準を定める（要員参集や情報システム切り替え等）。

② 全体フローの作成
非常時の初動から復旧までの大まかな流れを決めるために、危機的事象発生後の要員参集から情報システム復旧作業を完了させるまでの非常時の一連の流れ（全体フロー）を作成する。
作成に当たっては、各担当間の指示・報告等の情報連携のタイミングに留意する。また、全体フローには、実施事項の概要を記載するに留め、詳細な資料（規程類・個別手順・チェックリスト等）については、参照資料として資料名を全体フロー内に記載しておくとよい。

③ 全体フローを踏まえた対応手順の作成
全体フローを踏まえ、非常時の体制で定めた各担当が、どのような対応するかをより明確にした、非常時における対応手順書を作成する。対応手順を作成するに当たっては、情報システムの復旧に係る技術的な手順だけでなく、初動時の対応や、関連組織への連絡も含め作成する。

９．非常時の対応計画の検討

９．２　非常時における対応手順の作成

④ 代替拠点における運用計画の作成

代替拠点を設置する場合、代替拠点における通常運用（運用時間、ジョブ運用、運用監視、セキュリティ監視、トラブル対応等）及び保守運用（計画停止、活性保守等）に関する方式についても検討し決定しておく必要がある。代替拠点における通常時の運用計画は、本番環境における各部門の情報システム運用計画の形式に準じ、必要な項目の漏れがないよう留意すること。

⑤ 情報システムの迅速な復旧に配慮した必要な対応を行うこと

復旧作業を円滑に進められるよう、復旧に必要な要員の不足時には他組織からの人的支援の獲得が得られるようにしたり、復旧要員は会社の近隣に住めるよう就業規程を改正する等、IT-RTO達成のための対策を講じる。

⑥ 最低限実施すべき非常時の情報セキュリティレベルを決定する

非常時には混乱に乗じ、情報システム環境へ不正侵入等が発生する可能性もある。情報システムの運用上、適切な情報セキュリティレベルが確保されるよう配慮した計画を作成すること。不正な機器の接続防止やマシン室等への入退室管理等を徹底し、必要な箇所に監視員を配置する。

９．非常時の対応計画の検討

９．２　非常時における対応手順の作成

⑦ 情報システムベンダにも復旧体制と復旧手順書の整備を促す
実質の復旧作業を遂行するのは、通常保守運用を担当している情報システムベンダであることが多い。よって運用管理者は監督責任者としての立場から、各情報システムベンダに情報システムの復旧体制と復旧手順書の整備を依頼する。

⑧ 災害発生時の緊急対応用携帯カードを作成し、所持すること
外出先での被災等、災害発生時の対応手順書を所持していない状況もありうるため、非常時の初期段階で必要となる最低限の行動と緊急連絡先を記載した携帯カードを別途作成し、財布や定期入れ等の中に入れて、常に携行しておくこと。

10. 教育訓練計画・維持改善計画の検討

10. 1　教育訓練計画の検討

■検討内容と留意事項

① 年間で取り組む訓練の内容と対象範囲を定める（年間の教育訓練計画を作成する）。情報システムに関わる教育訓練は、目的を踏まえ大きくは以下の3つに分類される。それぞれの内容を踏まえ教育や訓練を計画する必要がある。

１）平常時の情報システム運用継続計画の維持改善活動への理解の向上
２）非常時対応計画の理解と対応能力の向上
３）事前対策内容の動作確認と検証

② 平常時の情報システム運用継続計画の維持改善活動への理解の向上
情報システム運用継続計画の継続的な維持改善を図るためには、維持改善を担当する担当者（情報システムの運用を継続する責任者及び担当者）が、業務継続に関する適切な知識と力量を身につけておくことが重要である。

10. 教育訓練計画・維持改善計画の検討

10. 1　教育訓練計画の検討

③ 非常時対応計画の理解と対応能力の向上

非常時対応計画に定められる実施手順については、関係者が内容に習熟しておくとともに、計画の内容自体に不備や改善点がないか、事前に検証しておくことが必要である。また実際の非常時には、計画や訓練で想定したどおりの事態が発生するとは限らないため、どのような状況が発生しても適切に対応できるように、復旧要員の危機対応能力を高める訓練を実施すること。

④ 事前対策内容の動作確認と検証

事前対策の一環として実施したバックアップや構築した代替環境については、被災時に期待どおりに機能・動作するか、定期的に訓練を通し確認・検証をしておくこと。平常時バックアップを取得していても、そのバックアップから本当にデータを復旧できるのかについては、検証がされていないケースが多い。
非常時にバックアップからデータを復旧できない場合、システムが復旧困難となる恐れもあることから、バックアップからデータが復旧できることを確認するシステムリカバリ訓練は、定期的に実施されるよう、教育訓練計画に含めることが望ましい。

10. 教育訓練計画・維持改善計画の検討

10. 2　維持改善計画の検討

① 情報システム運用継続計画の見直し時期・見直し内容・実施主体を検討する。
見直しの時期を設定する場合は、新たな事前対策の実施が必要となる等、
予算要求の必要性が生じる可能性もある。
このため、見直し時期としては、予算編成の検討時期を踏まえ設定することが
望ましい（2 月～3 月等）。

② 情報システム運用継続計画の策定・運用プロセスを、既存の情報システム企画
開発・運用プロセス内に組み込むこと。情報システム企画開発・運用時に従う
べき標準的な手順が定まっている場合は、情報システム運用継続計画の
策定・運用プロセスを同手順内に盛り込むよう改訂することが望ましい。
これにより、情報システムの企画開発・運用のライフサイクルの中で、
情報システム運用継続計画の視点で必要な検討が必ずなされるようになる。

第３部　「IT-BCP 策定モデル」をもとに
監査の視点で、IT－BCPの課題を考察する

IT-BCP 策定モデルとは

■IT-BCP 策定モデル
http://www.nisc.go.jp/active/general/pdf/IT-BCP.pdf

東日本大震災の事例をもとに検討すべき諸課題について、

１、今後の大規模災害の発生に備えた強靭な情報システムの構築
２、政府機関における情報システムの安全性・信頼性の向上

を目的に、「各省庁における情報システム運用継続計画」の策定状況を調査し、調査から得られた知見・情報をもとに、より実効性の高い計画策定のモデルとして取りまとめた

IT-BCP 策定状況調査から得られた課題

IT-BCP の整備における課題や情報システム運用継続計画ガイドライン（以下ガイド）における説明や例示の不足が指摘された。

表－２モデル調査の結果から抽出された課題

調査課題	確認された事実	必要な対処
(1) 非常時の意思決定に関する在り方	【部門間の連携】 業務部門における担当業務個別の非常時行動計画等が十分に整備されていないため、情報システム部門単独でIT-BCP の策定を進めている。	情報システム部門は IT-BCP を策定する際に連携が必要な関連部門を確認し、連携するための体制づくり（環境整備）を行う必要がある。
(2) 非常時の情報収集・伝達・発信や業務系の情報システムの在り方	【危機的事象の特定】 発生事象として首都直下地震を想定しているが、被災の程度が当該想定に対して十分適合していないと考えられる部分も見られる。	現状が正しく反映されていない調査は、その後の検討等で適正な結果が得られない可能性が高い。災害時の社会環境や情報システムの稼働に必要な様々なリソースが制限されている状況を前提とした検討の実施が望まれる（対策の検討時に情報システムによる対応が困難な事象に直面した場合に、手作業等で業務を継続し、その時間で（一部/全部の）情報システムを復旧させる等の柔軟な対応も必要である）。

IT-BCP 策定状況調査から得られた課題

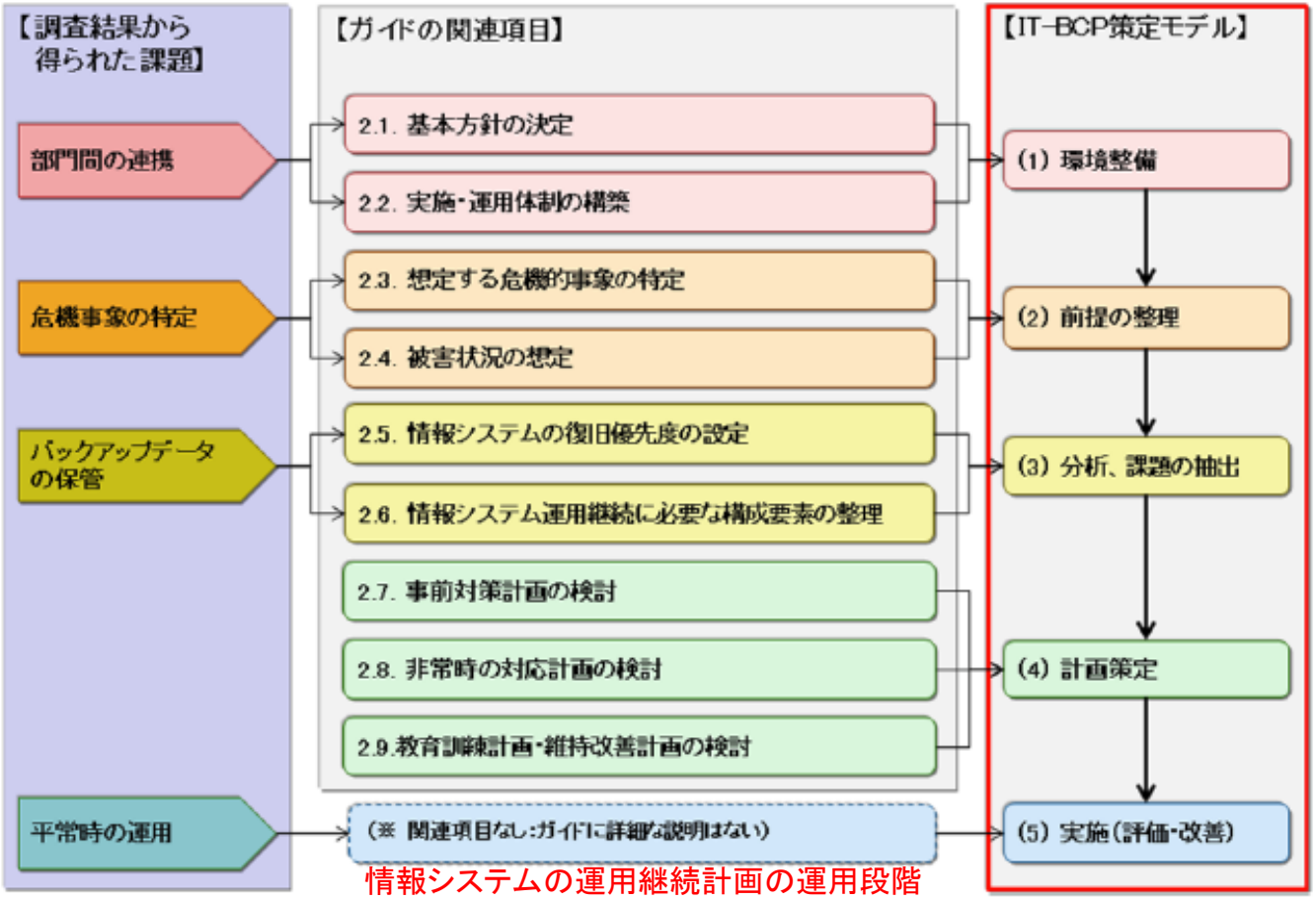
表－２モデル調査の結果から抽出された課題（続き）

調査課題	確認された事実	必要な対処
(3) データの消失を回避するための対策の在り方	【バックアップデータの保管】 重要なデータについてバックアップの取得は実施されているが、首都直下地震の発生時に同時被災しない場所にデータを保管していない例があった。	業務再開時に必要なデータが失われないように保管し、必要なときに即時に利用できる状態に保持しておくことは、システムの復旧優先度によらず実施すべき対策である。
(4) 教育・訓練の在り方	【平常時の運用】 IT-BCP を策定済みの府省庁において、教育・訓練が実施されていなかった。	訓練を実施する意義が正しく理解されていないので、個人の非常時対応能力を向上させる目的の訓練以外にも、部門間の連携訓練や情報システムの切替/切戻の手順確認等 IT-BCP の継続的改善につながる訓練の実施を検討することが望まれる。

実効性の高い計画策定のモデルとして取りまとめ

IT-BCP 策定モデルの構成

各省庁における情報システム運用継続計画の策定手順を5ステップに簡略化し、抽出された課題を中心に解説



図－１ 調査で確認された課題とIT-BCPの策定モデルにおける策定ステップ、ガイドの構築手順との対比

「IT-BCP 策定モデル」 P.4

IT-BCP 策定モデルの5ステップ

表－３ IT-BCP の策定モデルにおける策定ステップの概要

モデルの項目	必要な対処
(1) 環境整備	情報システム部門で、IT-BCP策定の方向性を検討する。 ・IT-BCPの策定に必要な体制を整備する。 ・IT-BCPの基本方針について関係者間で合意する。 ・IT-BCPの対象範囲について関係者間で合意する。
(2) 前提の整理	・危機的事象を特定する。 ・危機的事象の顕在化がもたらす被災状況を想定する。
(3) 分析、課題の抽出	・業務部門と合意した対象範囲の組織や非常時優先業務、情報システム等のたな卸を行う。 ・対象業務の目標復旧時間を明らかにする。 ・ 情報システムを支える構成要素（リソース）を洗い出す。 ・構成要素ごとに目標対策レベルを設定し、それに基づく情報システムの復旧優先度を設定する。
(4)計画策定	【事前対策計画の策定】 ・危機的事象の発生時に情報システムに生じる被害状況の想定に対する情報システムの抱える脆弱性（情報システムの運用継続を阻害する課題）を把握する。 ・ 把握した現状の脆弱性を解消する対策（事前対策）を、システムごとに検討する。 ・ 検討した事前対策により、目標対策レベルとシステム環境の現状のギャップを解消し、運用継続能力を継続的に強化していく実施計画を策定する。 【非常時対応計画の策定】 ・府省庁の防災対策等と非常時に連携する情報システムの復旧継続活動に必要な対応体制を構築する。 ・非常時の初動から復旧までの大まかな流れを決めるために、全拠点における危機的事象の発生から復旧までの対応が示された「対応の全体フロー」を作成する。 ・非常時の体制で定めた担当が、それぞれどのような対応するかをより明確にした、非常時における「対応手順書」を作成する。

IT-BCP 策定モデルの5ステップ

表－３ IT-BCP の策定モデルにおける策定ステップの概要

モデルの項目	必要な対処
(4)計画策定	【教育・訓練計画の策定】 ・教育・訓練計画は、担当者の理解度や対応力を向上させるとともに、事前対策の改善つなげることを意識して策定することが望ましい。計画は、年度単位で策定するとよい。 ・教育・訓練は、それぞれの対象者に適切な内容・時期で実施することで、その効果を高めることができると考えられる。以下に、体系的な訓練の実施パターンを例示する。 ・非常時には様々な対応が求められるので、全ての必要事項を一度の訓練で扱うと十分な成果を得ることが難しくなると考えられる。継続的に、府省庁の実力（理解度、対策の進捗状況等）を勘案し危機的事象・情報システム・非常時の対応等のうち優先順位の高いものから段階的に取り組み、徐々に難易度を高めていく、計画時に配慮することが望ましい。 【維持改善計画の策定】 ・維持改善計画は、事前対策計画、非常時対応計画、教育訓練計画それぞれを定期的に見直し、情報システム運用継続計画の実行性を継続的に維持できるよう検討する。維持改善計画を着実に実施して、定期的に全体を確認できるようにすることが重要である。
(5) 実施（評価・改善）	・運用段階においては、策定された事前対策計画と教育訓練計画に則り、対策実施や教育訓練等の活動を行うことで、業務継続能力の強化を推進する。また、「維持改善計画」に基づいて、適宜各種計画の見直しを行い、計画の陳腐化を防ぎ、常に計画の新化を維持するように努める。 ・ 計画の見直し時には、関連部局や組織のレビュを必要に応じて受けるべきである。（防災、情報セキュリティ等の推進部門に、それぞれの分野の観点から指摘を受けることは有効である。）