

# 事業継続計画書（BCP）作成のてびき

－大規模自然災害に備えるために－

第一章 全社レベルの事業継続計画書（BCP）

第二章 IT部門の事業継続計画書（BCP）

平成25年4月



一般社団法人日本倉庫協会

## 発刊の言葉

東日本大震災の発生は、約2万人の死者・行方不明者のほか、各地に甚大な被害をもたらしました。また、倉庫事業者も、東北地方を中心に多大な被害を受けたことは記憶に新しいところです。発生直後は、各地でサプライチェーンが寸断され、被災地への支援物資輸送はもちろん、企業のサプライチェーンも一時的に機能不全に陥りました。

その折に改めて判明したのは、倉庫事業者が大規模災害時に果たす役割と社会からの期待の大きさです。公共的な性格が強い倉庫事業に携わる私達が一刻も早く通常の事業活動を復旧し、社会的インフラとしての役割を果たすことは、倉庫事業者にとって社会的使命であると同時に、自然災害に対して自らの会社と従業員を守り、経営を継続していくためにも必須のことです。

日本は、古来より地震や津波、台風などの自然災害を数多く経験してきたことから、防災について極めて高い意識を有しています。日本倉庫協会でも「地震防災のてびき」を発刊して、倉庫事業者の防災対策の一助とすべく努めて参りましたが、東日本大震災の発生を機に、地震防災を一步進めた事業継続計画、すなわちBCPの策定が社会的にも求められるようになりました。

倉庫業界は、今日、行政と共に広域防災に取り組んでおり、広域ブロックごとの協議会の設置や、支援物資拠点の指定などの取り組みを進めておりますが、ひるがえってBCPの策定状況を見ますと、多くの会員事業者が必要性を理解しつつも、実際の策定には苦勞されている実情がうかがえます。

このような状況を踏まえ、日本倉庫協会では、業務委員会と情報システム委員会が中心となって、大規模自然災害を対象とした会員事業者のための「事業継続計画書（BCP）作成のてびき」および「事業継続計画書（BCP）モデル」を作成し、会員事業者の皆様にお届けすることとしました。

まずは同モデルを参考にBCPを策定いただき、その後、皆様固有の事情を反映したものに改定して頂くことをお薦めいたします。

また、倉庫事業者にとっては、受寄物の保全のみならず、情報、とりわけ在庫データを災害から守ることが事業継続にとって極めて重要な要素であることから、情報システム部門を対象としたBCP作成についても多くの紙数を費やして詳しく説明いたしました。会員事業者の皆様におかれましては、本書を参考に、BCP策定への第一歩を踏み出していただけたら幸いです。

平成25年4月1日

一般社団法人 日本倉庫協会

会長（業務委員長）

岡本 哲郎

副会長（情報システム委員長）

川合 正矩

## 本書のご利用にあたって

日本倉庫協会では、事業継続計画書作成のてびきシリーズとして下記の二つの成果物を用意させていただきました。

1. 事業継続計画書（BCP）作成のてびき-大規模自然災害に備えるために- …… 本書  
（事業継続計画書作成にあたっての解説書）
  2. 事業継続計画書（BCP）モデル（全社レベル編・IT部門編） …… 別冊  
（架空の中堅倉庫会社を設定し、作成した事業継続計画書モデル）
- 本書と合わせ、2. についてもご活用ください。

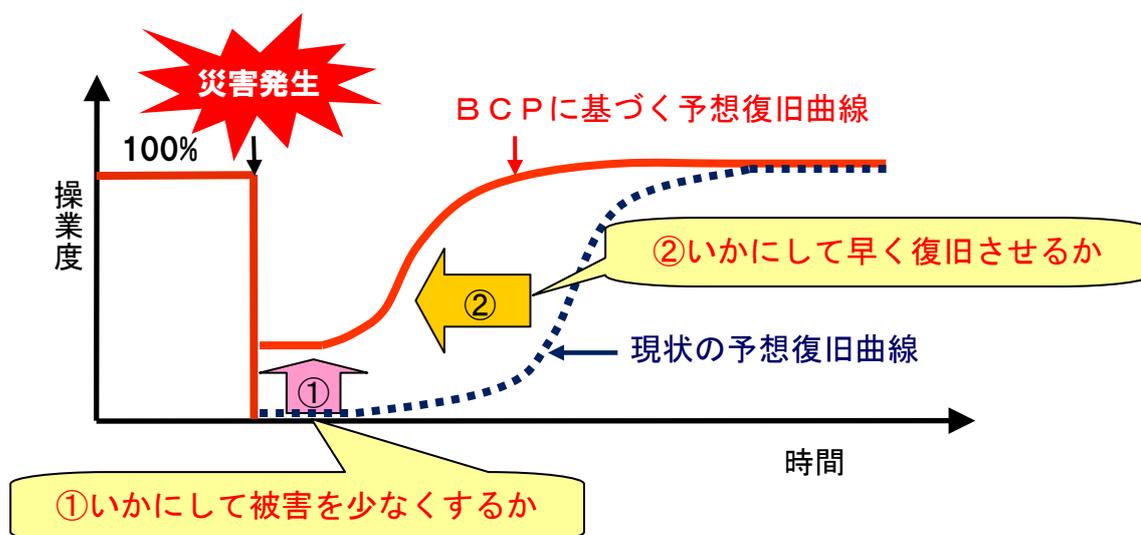
## 目次

○事業継続とは .....	1
○事業継続マネジメント .....	2
<第I章> 全社レベルの事業継続計画（BCP）を作成する .....	4
I-1 事業継続の体制を整備する .....	5
I-2 事業継続計画書（BCP）を作成する .....	7
2.1 目的を明確にする .....	7
2.2 想定するリスクを決める .....	8
2.3 基本方針を決める .....	10
2.4 中核事業の特定とその目標復旧時間を決める .....	11
2.5 平時の事業継続活動を決める .....	13
2.5.1 事前対策計画【PLAN】 .....	13
2.5.2 BCP定着と事前対策の実施【DO】 .....	19
2.5.3 訓練を計画する .....	19
2.5.4 点検と評価【CHECK】 .....	22
2.5.5 経営者による見直し【ACT】 .....	23
2.6 災害時の事業継続活動を決める .....	24
2.6.1 発動基準 .....	25
2.6.2 緊急対応行動【初動フェーズ】 .....	26
2.6.3 行動チェックリストを作成する .....	28
2.6.4 復旧のための役割分担【復旧体制の立ち上げ】 .....	29
2.6.5 復旧体制による復旧活動【復旧フェーズ】 .....	32
2.7 復旧宣言 .....	33

<第Ⅱ章> I T部門の事業継続計画書（BCP）を作成する.....	34
Ⅱ－1 I T環境を把握する.....	36
1.1 情報システム一覧表の作成.....	36
1.2 ネットワーク環境の把握.....	38
1.3 クライアント環境の把握.....	39
1.4 バックアップ取得状況の把握.....	40
Ⅱ－2 情報システムの目標復旧時間（RTO）を決める.....	43
Ⅱ－3 事前対策を検討する.....	46
3.1 事前対策計画を作成する.....	46
3.2 要員確保と復旧体制のための対策を検討する.....	46
3.3 情報システムの対策を検討する.....	49
3.3.1 予防対策 .....	50
3.3.2 復旧対策 .....	55
Ⅱ－4 緊急時行動計画を整備する.....	57
4.1 I T復旧に向けた行動チェックリスト（標準） .....	58
4.2 被害状況チェックリストを作成する.....	61
Ⅱ－5 訓練の実施 .....	63
Ⅱ－6 I T部門の事業継続計画書としてまとめる.....	65
<参考資料>	
第Ⅰ章関係 .....	68
1. 防災用物資の例とその備蓄量の目安.....	68
2. 防災用資器材の例.....	69
3. 事業別目標復旧時間の設定.....	70
第Ⅱ章関係 .....	73
1. 安否確認における効果の高い対策.....	73
2. データバックアップにおける効果の高い対策.....	74
3. 災害に対応した効果の高い設備機器の設置.....	75
4. 効果の高い電源対策.....	76
5. 二重化・冗長化.....	77
6. 復旧対策における効果の高い対策.....	80
7. 効果の高い訓練.....	81

## ○事業継続とは

事業継続(BC:Business Continuity)は、従来の防災対策の考え方をベースに「重要業務の継続・復旧」、「サプライチェーンの対応」といった経営に及ぼす影響の視点を加えたものです。災害や事故など大きな危機が会社を襲った際に、①重要な業務をできるだけ中断させず、②中断があっても早急に復旧させるための活動を表す概念です。【図 1】

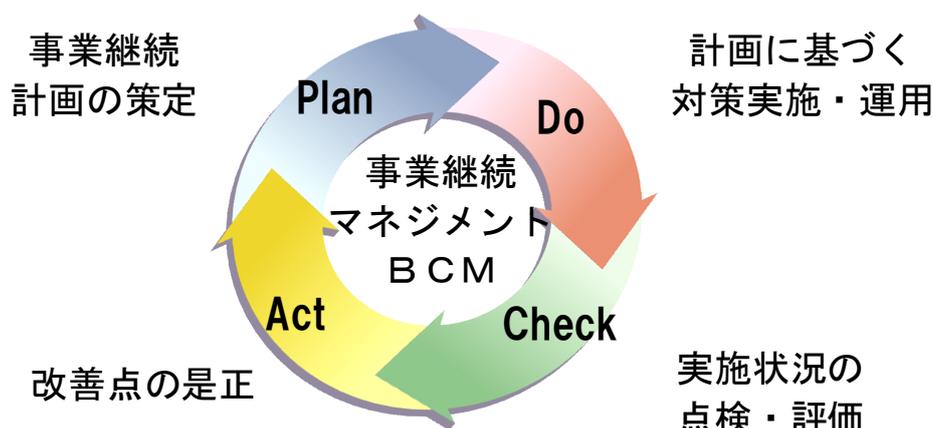


【図 1】事業継続の概念

## ○事業継続マネジメント

事業継続を達成するための管理の仕組みを、事業継続マネジメント（BCM：Business Continuity Management）と呼びます。事業継続マネジメントは、事業継続計画（BCP：Business Continuity Plan）の策定（Plan）、計画に基づく対策実施・運用（Do）、実施状況の点検・評価（Check）、評価で見つかった改善点を是正（Act）していくPDCAのマネジメントサイクルです。【図2】

事業継続マネジメントのPDCAサイクルを回して、継続的に改善を行うことで、組織の事業継続対応力は強化されていきます。このサイクルのベースとなるのは事業継続計画（BCP）です。BCPは文書化されたものを指す用語として事業継続計画書とも呼ばれます。



【図2】事業継続マネジメント

事業継続マネジメントのサイクルは、組織の規模によって全社レベルのみにとどめたり、業務部門、情報システム部門などのレベルに細分化し、そこに役割分担させる場合があります。



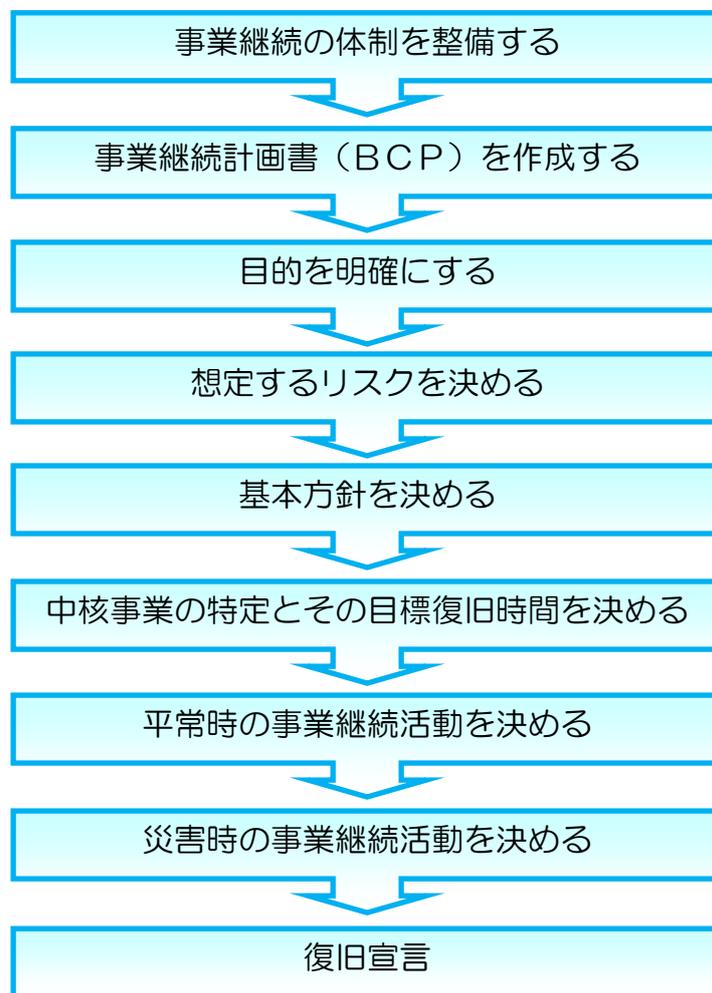
※東日本大震災の事例として、「ISOの認証を取得していたため復旧活動の際にPDCAサイクルが円滑に機能した。」との報告がありました。

社内の既存の制度・活動などを上手く活用して災害対策を構築させていくこともひとつの方策です。



## <第 I 章>

### 全社レベルの事業継続計画（BCP）を作成する



## I-1 事業継続の体制を整備する

### <経営者のリーダーシップ>

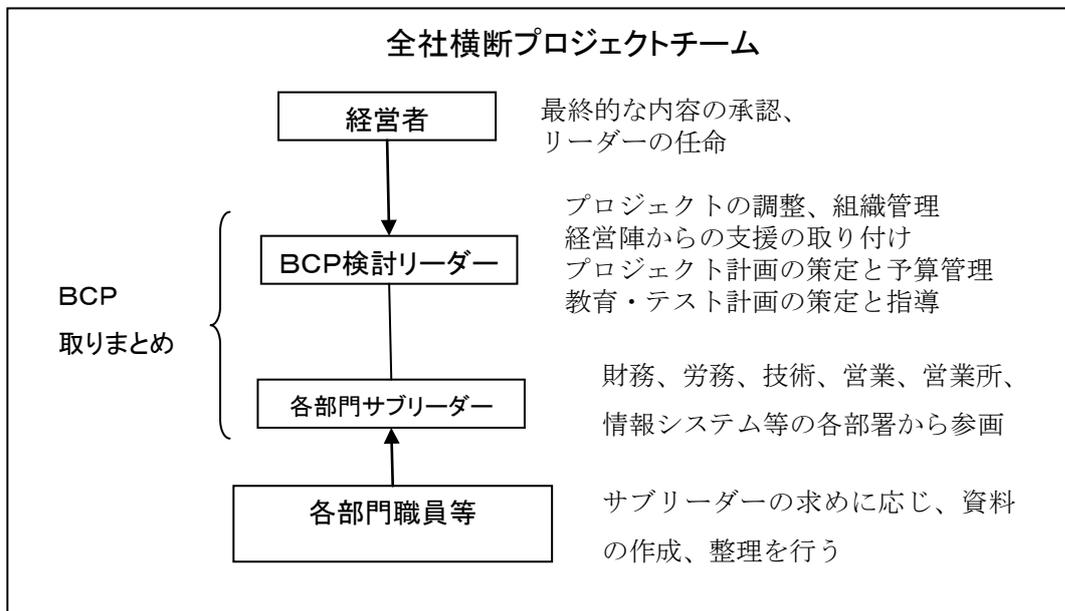
事業継続の体制整備に当たっては、経営者の強いリーダーシップが欠かせません。東日本大震災では、被災事業者の経営者が強いリーダーシップを発揮し、様々な困難な状況を乗り切ってこられたことが報告されています。事業継続の体制構築に当たっては、整備の段階から、経営者の十分な関与が必要となります。

その上で、会社として役職員を担当毎に割り当て、規程やルールなどを整備してマネジメントの仕組みを構築して行く必要があります。その際、「マネジメントの仕組みを構築するための体制」と「構築した仕組みを維持・運用する体制」に分けて考える必要があります。

### <事業継続マネジメント(BCM)構築体制>【BCPを構築するための組織】

事業継続は、組織内の様々な問題を扱うため、原則全ての部署が参画します。

BCM構築に当たっては、経営者のもと、危機管理を担う部署長（総務部門、リスク管理部門など）をリーダーとし、財務、労務、技術、営業、情報システム等の各部署長をサブリーダーとするプロジェクトチームを立ち上げ活動します。プロジェクトチームは各部署の意見を元に方針を確認したり、役割分担の整理を行ったりして、全社レベルのBCPを策定します。



【図 3】BCM構築体制の例

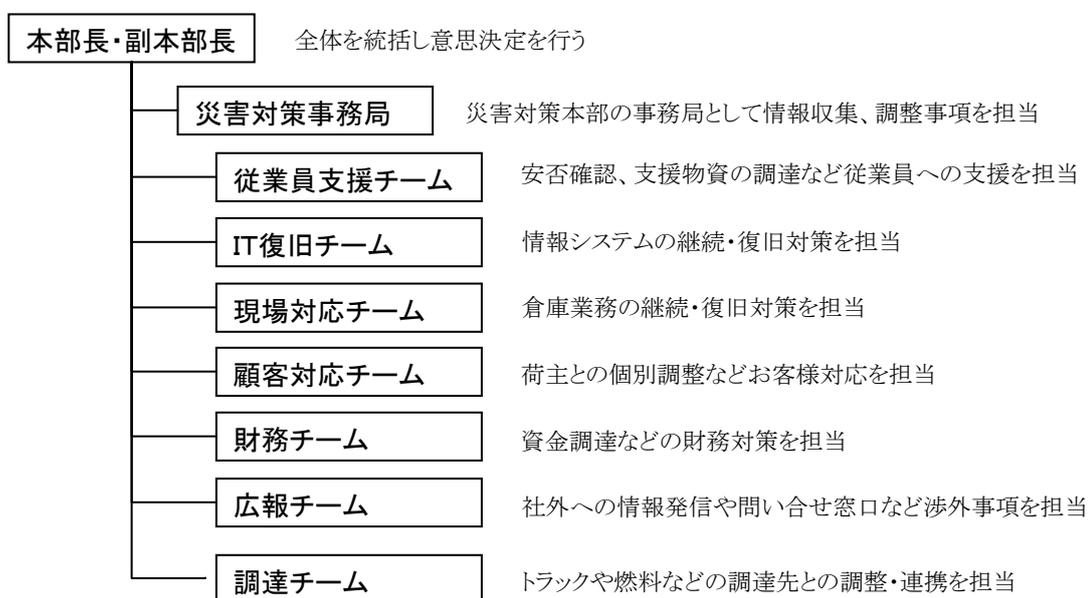
## ＜事業継続マネジメント(BCM)運用体制＞【緊急時に対応するための組織】

運用体制は、構築体制で作成した事業継続計画書（BCP）に基づいて構築し、役割に応じた活動を行います。有事の時には事業継続活動の核となる「災害対策本部」を立ち上げ、初動対応や復旧活動を担うチームを編成します。

チームは、事業活動に必要な機能毎に編成し、情報収集・発信や復旧活動を行います。この体制は、平時から編成しておき、機能毎に復旧に必要と想定される環境整備や資材調達方法等について検討したり、訓練を実施したりして会社の事業継続対応力を維持・向上させる活動が求められます。

### 災害対策本部組織図(例)

経営者を本部長とする最高意思決定機関



本部長・副本部長	社長、取締役が担当する
事務局	総務(庶務)部長等がリーダーとなり、同部職員が補佐する
従業員支援チーム	総務(庶務)部長等がリーダーとなり、同部職員が補佐する
IT復旧チーム	情報システム部長等がリーダーとなり、同部職員が補佐する
現場対応チーム	営業所長等がリーダーとなり、同所職員が補佐する
顧客対応チーム	営業部長等がリーダーとなり、同部職員が補佐する
財務チーム	経理部長等がリーダーとなり、同部職員が補佐する
広報チーム	総務部長等がリーダーとなり、同部職員が補佐する
調達チーム	経理部長等がリーダーとなり、同部職員が補佐する

※各担当は組織の規模により兼務する

【図4】BCM運用体制の例

## I-2 事業継続計画書（BCP）を作成する

事業継続計画書（BCP）は、会社として事業継続にどのように取り組んでいるかを社内外に説明する上で拠り所となる文書です。作成に当たっては目的を明確にするとともに、マネジメントの仕組みとして維持・改善していくための各活動について定義づけします。

本項では、以下にBCPに記載する各項目毎に考え方を解説したうえで、記載例を示すこととします。

### 2.1 目的を明確にする

BCPを何のために作成するのかについて、経営者の意思を反映した内容で記載します。たとえば「経営に重大な影響を及ぼす事件・事故・災害が発生した時に重要業務を中断させない」、「中断しても目標時間内で復旧させる」ためであること等を記載します。

同時に「用語の定義」を記載しておくこと、読み手の理解がスムーズになります。

#### <記載例1>

##### 【目的】

本書は、当社の経営に重大な影響を及ぼしうる地震等の災害発生時において、重要業務を中断させないよう、万一、事業活動が中断した場合でも目標復旧時間内に重要業務を再開させられるよう、各活動に関する基本的事項について定めるものである。

##### 【用語の定義】

本書、または事業継続活動に係る文書で用いる用語について以下の通り定義する。

用語	定義内容
事業継続計画	災害や事故等に備え、事業を継続させるために必要な事項を盛り込んだ計画のこと。BCP (Business Continuity Plan)ともいう。 －被害を最小化する予防対策 －重要業務継続のための、あるいは重要業務中断時の迅速な復旧のための手順、体制など
事業継続管理	事業継続計画を策定し、実際に機能させるために継続的に検証し維持管理していく管理プロセスのこと。BCM(Business Continuity Management)ともいう。
事業影響度分析	事業が停止した場合の影響度を評価し、事業を継続させる業務の優先順位と目標復旧時間を決めること。BIA(Business Impact Analysis)ともいう。
目標復旧レベル	重要業務をどの範囲まで復旧させるかの度合いのこと。RLO (Recovery Level Objective)ともいう。
目標復旧時間	予め設定した目標復旧レベルにまで重要業務を復旧する目標時間のこと。RTO (Recovery Time Objective)ともいう。
目標復旧ポイント	目標復旧時間を達成するために、情報システムで必要とするバックアップデータの取得目標タイミング。どの程度までデータが喪失することが許容できるかを表す。RPO (Recovery Point Objective)ともいう。
事業資源	事業を継続するための資源、インフラ、リソースともいう。倉庫業の場合、施設・設備、フォークリフト、コンベア、荷役機械、燃料、電力、要員等が事業資源となる。

## 2.2 想定するリスクを決める

BCP策定に当たっては、リスクの種類を問わずその検討対象とすべきですが、「考えられる全てのリスク」を対象にしてしまうと、検討事項が多岐にわたってしまい多大な労力が必要となります。そこで国の中央防災会議では、現実的なアプローチとして、日本企業にとって想像が付きやすく、対峙すべきもっとも大きな自然災害リスクである地震を想定リスクとして取り組みをスタートすることを推奨しています。

地震に備えた事業継続は、地震以外のリスクである火災、風水害、テロ等へも適用できる共通的な対策要素が多いと言われています。

倉庫事業者においても被害を想定しやすいリスクとして「震度6強以上の地震」からまず検討を開始し、順次対応するリスクを増やす進め方を推奨します。

またリスクの想定に関しては、国や地方自治体がホームページ等においてハザードマップを公表しており、豪雨や津波などによる浸水、液状化、土砂災害の危険性など、様々な自然災害に応じた被害想定が公表されています。また自治体によっては電気・ガス・水道などの社会インフラの被害想定を公表していますので、これら立地毎の被害想定を加味して自社施設の被害想定をより具体的に定めることができます。

例として「東京湾北部地震」では【図5】のようになります。

ライフライン	発災時直後	発災3H	6H後	12H後	1日後	2日後	3日後	4日後	7日後	10日後	20日後	30日後
電気	停電	初期復旧				8割復旧		ほぼ復旧				
ガス	供給停止						一部復旧					5割復旧
水道	断水					一部復旧						8割復旧
加入電話	90%不通	通話制限						制限終了予定		8割復旧		
携帯電話	輻輳	通話制限・輻輳						制限終了予定				
公衆電話	不通の可能性あり			仮設始まる(優先電話)								
(携帯)メール	遅配	遅配						利用可能				
道路	通行止め	車両通行止め					麻痺	渋滞				
電車	不通											

【図5】東京湾北部地震の被災想定

<記載例2>

【想定するリスク】

事業継続活動上の想定リスクを「地震(震度6強以上)」とする。

【ライフラインの被害想定】

ライフライン	発災時直後	発災3H	6H後	12H後	1日後	2日後	3日後	4日後	7日後	10日後	20日後	30日後
電気	停電	初期復旧					8割復旧	ほぼ復旧				
ガス	供給停止						一部復旧					5割復旧
水道	断水						一部復旧					8割復旧
加入電話	90%不通	通話制限						制限終了予定		8割復旧		
携帯電話	輻輳	通話制限・輻輳						制限終了予定				
公衆電話	不通の可能性あり			仮設始まる(優先電話)								
(携帯)メール	遅配	遅配						利用可能				
道路	通行止め	車両通行止め					麻痺	渋滞				
電車	不通											

【自社の被害想定】

<倉庫被害関係>

- ・ 建屋 ○○営業所 倒壊の被害なし  
▲▲営業所 シャッター 一部損壊
- ・ ラック 一部損壊
- ・ 貨物エレベーター 停電により使用不能
- ・ トラック、ガソリン・軽油フォーク 被害なし
- ・ 電動フォークリフト 停電により一時使用のみ可能
- ・ 保管貨物 一部荷崩れ ○○貨物

<事務機器被害関係>

- ・ コンピュータ、パソコン 停電により使用不能
- ・ 一部ノートパソコン 一時使用可能
- ・ 加入電話 停電により使用不能
- ・ F A X 停電により使用不能

<人的被害>

- 地震発生 午前○時 ○%出社可能
- 地震発生 午前○時 ○%出社可能
- 地震発生 午前○時 ○%出社可能

## 2.3 基本方針を決める

基本方針は、平時および有事の際に行動する時の拠り所になります。事業継続に取り組む目的はもとより、経営理念や倉庫事業者としての社会的責任、取引先との関わりなどを考慮して方針を定めます。

検討の視点には以下があります。

- ・ 人命尊重
- ・ 社会的責任
- ・ 社会貢献
- ・ 経営へのインパクト

経営者は、社内外の関係者に対して、事業継続に関する活動について了解を取り付けていかなければなりません。そのためにも基本方針の決定には、経営トップ自らが関与し、計画の実効性を確保していくことが求められます。基本方針は、社内外に公表することが望まれます。

### <記載例3>

#### 【基本方針】

当社は、事業継続への取り組みを行うにあたって、人命尊重を第一とし、以下の基本方針に基づき活動する。

- ① 従業員、来訪者などの生命の安全確保を第一に行動する
- ② お客様の事業のダメージを最小化する
- ③ 事業停止により生じる当社事業へのダメージを最小化する
- ④ 被災支援物資の物流拠点として社会的責任を果たす
- ⑤ 事業継続への取り組みを通じて企業価値を向上させる

## 2.4 中核事業の特定とその目標復旧時間を決める

有事の際に最優先で復旧すべき事業（中核事業という）を特定します。

東日本大震災の被災事業者の声として「被害が広範囲に及んだ場合は、全ての業務に対応することができない」、「非常事態において、不可欠なものや緊急性の高い事項を迅速に選別しないと、取り返しがつかない事態が生じる」といった感想が聞かれました。予め優先的に復旧すべき事業の順位を定めておくことで、緊急時の対応を早め、損害を最小化することができます。また、「事業の絞り込みをいざ実行するとなると、なかなかできないことが多いので、“絞り込む”という訓練も必要であった」との感想もありました。

### ○中核事業の絞り込み

災害時には人的にも設備的にも経営資源が不足することから、中核事業の範囲を通常の3割程度の人員や設備で回せる規模に絞り込むことが望ましいとされています。また、人的資源については、「復旧に必要な“人材”の確保が重要であり、人数だけいても復旧は進まない。緊急時における組織・人事について予め決めておくことが必要である」といったことが被災事業者より指摘されています。

事業の優先順位を考える上での基準としては、以下の様な項目が考えられます。

- ・ 事業収入への影響度（荷主別事業規模、拠点別・倉庫別事業規模など）
- ・ 施設的な影響度（倉庫面積、倉庫別事業規模、荷主別倉庫利用面積など）
- ・ 社会への影響度（社会的影響度の大小など）

専門的にはこれらの指標を予め定めて、事業影響度分析(BIA:Business Impact Analysis)を実施した結果で求めることが推奨されますが、初めてBCPを作成する場合は、経営者や事業責任者の経験から判断する方法で検討を進めることもできます。

### ○目標復旧時間（RTO）の設定※

中核事業が特定できたら、災害が起こった際に中断した中核事業をどの程度の時間内に復旧させるのか、目安としての「目標復旧時間」を定めます。「目標復旧時間」の設定で考慮すべき点は以下の2点です。

- ・ 中核事業に対する利害関係者（顧客、協力会社、株主、金融機関など）からの要請  
→取引停止や市場のシェア低下、ブランド失墜などを最小にでき、利害関係者から許容される限界時間を想定します。
- ・ 自社財務状況の悪化  
→取引停止に伴う収入の途絶など企業が財務上耐えられる限界時間を想定します。

ここで定めた「目標復旧時間」は有事に備えた事前対策の実施や顧客との事前協議など、事業継続を検討する上で目安となります。

※中核事業の目標復旧時間（RTO）を中核事業の遂行に必要な「重要業務」及び「情報システム」のRTOに展開する方法については、本紙<参考資料>にある「3. 事業別目標復旧時間の設定」（70 ページ）を参照して下さい。

<記載例4>

**【中核事業と目標復旧時間】**

経営上最も重要であり、有事の際に最優先で復旧すべき事業を「中核事業」として定める。被災後1週間以内に中核事業を再開することを復旧方針とし、個別の業務における復旧目標は以下の通りとする。

中核事業	目標復旧時間
優先度：A 〇〇荷主事業 (取引量第1位)	建物全壊 復旧見込み不明 建物一部損壊の場合は、1週間以内に復旧
優先度：B ××荷主事業 (取引量第2位)	建物全壊 復旧見込み不明 建物一部損壊の場合は、2週間後に復旧

**【参考】**

事業影響度分析 (BIA : Business Impact Analysis 読み方 : ビーアイエー) の詳しい手順については、下記を参考にして下さい。

中小企業庁『中小企業BCP策定運用指針』

( <http://www.chusho.meti.go.jp/BCP/index.html> )

→基本コース・中級コースの「3.1 事業を理解する」

## 2.5 平時の事業継続活動を決める

平時には、有事に備えて様々な準備を実施します。事前に行っておくべき対策の検討や訓練・教育などの定着活動などを通じて、事業継続マネジメント（BCM）のPDCAサイクルを確立します。以下にPDCAサイクルの各フェーズに沿って解説します。

### 2.5.1 事前対策計画【PLAN】

事前対策計画の段階で検討すべき項目は、まずは、緊急時に適切に社内各所と連絡を取り、経営判断に必要な情報を収集するための社内体制を確立すること及び重要な利害関係者との連絡体制を確保することです。そして、中核事業を継続または目標復旧時間内で再開するために必要な対策を実施することです。

<計画段階で定めること>

- ・ 緊急時体制の確立
- ・ 重要な顧客・主要協力会社の連絡先
- ・ 事前対策計画の整備

#### (1) 緊急時体制の確立

緊急時の対応体制および指揮命令系統は、有事の際に迅速に情報収集し、事業継続に向けての活動を実施するために明確にしておく必要があります。緊急事態の時には、トップや各部門の責任者が不在や通信不可などで、必ず連絡がつくとは限りません。そこで最低でも第3優先順位まで責任者候補を任命しておきます。

#### <記載例5>

##### 【緊急時体制の確立】

災害発生時に事業継続活動を行う責任者を以下のとおり定める。なお、これらの者が不在又は連絡が取れない場合、担当する部門の何れかの者がこの任に当たる。

##### <緊急時における体制>

役割	第1優先順位	第2優先順位	第3優先順位
災害対策本部長	〇〇社長 携帯：～ メール：～	〇〇常務 携帯：～ メール：～	〇〇取締役 携帯：～ メール：～
災害対策事務局	〇〇総務部長	〇〇次長	〇〇課長
従業員支援チーム	〇〇総務部長	〇〇次長	〇〇課長
IT復旧チーム	〇〇情報システム部長	〇〇次長	〇〇課長
現場対応チーム	〇〇営業所長	〇〇所長代理	〇〇課長
顧客対応チーム	〇〇営業部長	〇〇次長	〇〇課長
財務チーム	〇〇経理部長	〇〇次長	〇〇課長
広報チーム	〇〇総務部長	〇〇次長	〇〇課長
調達チーム	〇〇経理部長	〇〇次長	〇〇課長

また、本店所在地以外に支店や営業所を擁する組織の場合、本店に災害対策本部を立ち上げるだけでは不十分です。被災地の営業所を管轄する支店などに災害対策支部を立ち上げ、対策本部と対策支部で役割分担をしながら災害復旧に取り組む必要があります。対策支部には対策支部長以下、事務局、従業員支援チーム、現場対応チーム、調達チームなど対策本部と同様、必要な機能別にチームを設置します。

対策本部は全社レベルでの高度な経営判断を中心に意思決定を行い、対策支部では対策本部で決定した方針に沿って、被災現場での復旧作業に直結する意思決定を行い、連携しながら復旧を進めるようにします。

なお、連絡は必ず対策本部と対策支部とのルートに一元化しておくことが重要です。無秩序に被災現場に問合せが集中すると、被災現場は混乱を来し、復旧作業の妨げとなります。すべての情報を対策本部と対策支部に集約して、関係者が正確な情報を共有できるようにします。

当然のことながら、対策本部と対策支部の連絡が途絶する事態は可能な限り避けられるように、緊急時にも利用可能な連絡手段（衛星電話、MCA無線等）について、平常時から検討して、事前対策の一つとして用意しておくことが望まれます。

## **(2) 重要な顧客・主要協力会社の連絡先**

倉庫事業者が顧客に対して提供するサービスは、自社だけの資源で成立するものではありません。緊急時には、パートナーである協力会社との的確かつスムーズなコミュニケーションも必要です。重要な顧客や主要な協力会社と直ちに連絡ができるよう連絡先一覧を整備しておきます。

また、大規模災害時には、建物の損壊の他、荷役機器や電気系統、水まわりに不具合が生じます。施設・設備の管理を委託している業者についても、早期に連絡が取れるよう、リストに整理しておきます。災害が大規模になると、工事業者への修繕依頼が殺到するため、早めの対応が必要になります。東日本大震災では、早期に出入りの施工業者を手配したことで、専属的に対応してもらおうよう繋ぎとめることができたなどの報告がありました。

<記載例6>

【重要な顧客・主要取引先の連絡先】

重要な顧客と主要な取引先の連絡先は以下の通りである。

<重要顧客>

社名	取引内容	担当者	担当者 TEL	担当者メール
〇〇社	XX 保管業務	鈴木 一郎様	03-123-XXXX	xxx@~
:	:	:	:	:

<主要協力会社>

区分	項目	通常連絡先	TEL	メール
ライフ ライン	電気	〇〇電力〇〇営業所	03-456-XXXX	aaa@~
	上下水道	〇〇水道	XX-XXX-XXXX	bbb@~
	ガス	〇〇ガス	XX-XXX-XXXX	ccc@~
	電話・通信	〇〇電話〇〇営業所	XX-XXX-XXXX	ddd@~
協力 会社	運送会社	〇〇運送(株)	:	:
		〇〇運輸(株)	:	:
	マテハン	〇〇工業(株)	:	:
		〇〇機械(株)	:	:
	I T 業者	〇〇システム(株)	:	:
	建築土木業者	〇〇建設(株)	:	:
行政	地方運輸局	運輸局〇〇課	:	:
	市町村窓口	〇〇市〇〇課	:	:
	警察	〇〇警察署〇〇課	:	:
	消防	〇〇消防署〇〇課	:	:
協会	地区倉庫協会	〇〇倉庫協会	:	:

### (3) 事前対策計画の整備

有事に中核事業を継続したり、目標復旧時間内の復旧を目指すには、事前に何らかの対策が必要になります。対策の多くは、投資が必要になりますので、中期的な対策を含めて立案し、「事前対策計画」としてまとめます。対策項目、担当部署、計画の実行に必要なとなる資金やその調達方法、予定時期などを検討します。

対策の検討は、担当部署が主体的に実施して全社（災害対策事務局）に答申するといった役割分担が多いと想定されます。“担当部署”を決めて、確実に対策が実行されるよう全社でサポートすることが重要です。定めた「事前対策計画」は、対策を実施した実績や、毎年の訓練結果を反映させ、継続的に見直していくことが求められます。

#### <記載例7>

##### 【事前対策計画の整備】

中核事業の目標復旧時間内で再開させる環境を整備するため、以下の対策を実施していく。

##### <事前対策計画>

該当	対策済み	対策項目	担当部署	対策が必要な場合		
				必要資金 (百万円)	資金調達方法	予定年
■	■	備蓄品（食料・水・毛布等）準備	総務部	済み	←	←
■	■	倉庫建屋の耐震診断	総務部	済み	←	←
■	□	倉庫建屋の耐震強化	総務部	30	自己資金	20xx年
■	■	倉庫の防火対策	総務部	済み	←	←
■	□	津波避難場所の確保	総務部	10	自治体融資制度	20xx年
■	■	倉庫内保管棚等の転倒防止	営業所	済み	←	←
■	■	倉庫内の壁・照明器具等の落下防止	営業所	済み	←	←
■	□	コンピュータシステムのバックアップ	情報システム部	8	自己資金	20xx年
■	□	自家用発電機の導入	総務部	30	自己資金	20xx年
□	□	応急給水設備の整備 (浄水器、給水槽など)	総務部	優先度低い	←	←
■	□	緊急時通信機器の整備 (MCA無線、衛星電話)	総務部	1	自己資金	20xx年
■	□	社員安否確認手段の整備 (連絡方法の複線化)	総務部	1	自己資金	20xx年
■	□	震災発生時の資金繰り計画	経理部	優先度高い	自治体融資制度	20xx年
■	□	事業資源復旧手配 (燃料、トラック、代替倉庫用地など)	総務部	優先度高い	協力会社	20xx年
■	□	顧客向け契約内容の事前説明	営業部	0.5	自己資金	20xx年
□	□	地震保険の加入	総務部	優先度低い	←	←
□	□	・・・				



＜参考：事前対策項目の補足 東日本大震災の事例を踏まえて＞

### 【倉庫内保管棚等の転倒防止と各種機器の配置換え】

保管棚等の転倒防止対策は、確実に行っておきましょう。2・3階は1階に比べ揺れによる荷崩れの被害が大きかったとの報告もあり、特に高層階の荷崩れ対策を講じるようにします。また、作業員の避難スペースを設け、避難訓練などを通じて確実な避難・退避ができるようにしておきます。

1階部分に津波や浸水が想定される倉庫では、予めキュービクル（受変電設備）や情報・通信機器を2階以上に設置しておくことも有効な対策と考えられます。このような措置を講じていたため、1階に浸水があったものの、復旧が早まったという報告が寄せられています。

海水や泥水によってキュービクルや情報・通信機器がダメージを受けると、電気等インフラが復旧しても機器を稼働させることはできません。また、発災直後は代替品の入手が困難であることも想定され、その分復旧が遅れることとなります。

### 【社員安否確認手段の整備（複線化）】

安否確認の手段は、複数準備しておくことを推奨します。固定電話や携帯電話は、災害時に通話規制がかけられるため、繋がりにくい状態が続きます。東日本大震災でも、固定電話で最大80%～90%の通話規制が、携帯電話でも最大で70%～95%の制限が実施されています。一方、交換機を経由しないIP電話や基地局がきめ細かく設置されているPHSは、比較的通話できる可能性が高かったようです。インターネットも比較的接続できた連絡手段のひとつです。Twitterなどのソーシャルネットワークシステム（SNS）が安否確認に役立った例も報告されています。MCA無線も災害時に繋がりやすい通信手段であり、東日本大震災においては大津波の接近を港頭地区倉庫に連絡し、職員を早期に避難させることができたとの事例も報告されました。社員との連絡については、可能な限り複数の通信手段を確保しておくことが望まれます。

＜安否確認に利用可能な主な通信手段＞

固定電話、携帯電話、PHS、衛星電話、MCA無線、インターネット電話（LINE、Skypeなど）、災害用伝言板（web171、171など）、SNS（Twitter、Facebookなど）

### 【事業資源等に関する事前対策】

事業資源（燃料、トラック、代替倉庫用地など）については、「事前に優先手配の契約をしておくべきであった」との感想がありました。特に燃料は入手が困難となるので、多様な供給経路を検討しておくことが必要となります。

また、「古い倉庫が被災して建て直しをすることになったが、倉庫建物や設備の仕様等を検討していなかったので非常に手間がかかった。事前に準備すべきであった。」との意見がありました。

資金対策については「緊急時対応では、資金繰りが重要な要素となることが多い。銀行の短期融資を利用する等の平常時からの検討のほか、災害が長期化した場合を想定した資金繰り方策の検討も重要」との指摘もありました。

その他、見落としがちなものとして、「一定規模の宿泊施設は想定しておくべき」との意見がありました。災害が大規模になると、移動手段の確保が困難になったり、自宅が被災して、従業員が会社にとどまらざるを得ないケースがでてきます。また、協力会社等の応援部隊などに休憩・宿泊施設を提供することも必要になります。復旧活動に必要な人員を想定しつつ、それに見合った施設も合わせて手当てをしておくことが望まれます。

東日本大震災では観光バスをチャーターし、宿泊施設として急場をしのいだ例もありました。

#### **【顧客向け契約内容の事前説明】**

「標準倉庫寄託約款」では、地震、津波、高潮、大水などでの損害は、免責（発券業者用の（甲）では第 40 条、非発券業者用（乙）では第 37 条）となっていますが、契約当時の説明が不十分な場合、先方から了承を得るまでに期間がかかり、出庫や処理業務なども滞ってしまいます。また、被災貨物の処理費用、輸送費用なども予め取り決めがないと、顧客との交渉に多大な労力を費やすこととなります。震災では、「双方の意見のすり合わせや調整の打合せだけで膨大な時間がかかってしまい、初動が大幅に遅れた」との感想が寄せられました。このような事態を避けるため、予め非常時における寄託貨物の損害や処理費用について顧客に十分な説明を行ったり、覚書等を取り交わすなどの対策が有効となります。

## 2.5.2 BCP定着と事前対策の実施【DO】

定着・実行段階では、有事の際に従業員がBCPで定めた基準やルールに従って行動できるよう、組織内にBCPを浸透・定着させることが必要です。定着のためには、教育と訓練が非常に有効です。実施方法と実施時期、頻度を記載して、確実に実施できる環境作りが求められます。

実際に訓練を行ってみると、大小様々な問題点が浮かび上がります。「想定よりも避難時間がかかった」、「連絡がなかなか取れなかった」、「救急用品の収納箱に鍵がかかっている使えなかった」、「無線機を導入していたが、実際に使ってみると操作方法が分からなかった」などです。現実の災害を想定した訓練を繰り返し実施し、緊急時対応の精度を向上させていくようにします。

また、計画段階で定めた「事前対策計画【PLAN】」に基づいた対策を着実に実施していくことも必要です。計画通りに進んでいるか確認する作業も盛り込んだほうが良いでしょう。

通常の作業でも、災害対策に繋がるものがあります。はい付けとして交互ブロック積み、レンガ積み、ピンホイール積みなどの採用は勿論のことですが、必要であれば水平バンド掛け、シート挿入、シュリンク包装やボックス枠などを使用して強化します。(日本倉庫協会「地震防災のてびき」参照)

また、荷崩れにより倉庫内に複数あった避難用通路の扉が全て塞がり、作業員が庫内に閉じ込められたという報告もありました。通路扉の周辺は高積み厳禁といったルールを習慣化し、平時からの防災対策を定着させます。

その他にも、企業・自治体からの災害備蓄品を保管していた事業者から、「震災時に緊急出庫の要請を受けたが倉庫の最上階などで保管していたため、停電でエレベーターが動かない中、人海戦術で1階に降ろすなど非常に苦労した」という体験談がありました。保管貨物が災害備蓄品などの場合は災害時の出庫が想定されるため、1階に保管するなど、「災害を想定して、日常のロケーション管理を行うべきだった」という意見が寄せられています。

## 2.5.3 訓練を計画する

緊急時行動チェックリストや事前対策が整備できたら、その有効性・実現性を確認するために訓練を実施します。訓練の狙いは、万一の緊急事態に要員を含めた組織全体の対応能力を向上させることにあります。

緊急事態の発動は非日常的であり、日頃から計画の実効性を確認することが難しいものです。従って、訓練は単なる模擬的な活動に止まらず、計画や手順そのものを評価し実効性を確認する作業であり、災害対応能力向上のためには非常に重要な活動となります。訓練には、様々な方法がありますが、代表的なものとして、次のようなものがあります。

方法	内容
机上訓練 (座学)	計画や手順の内容を机上で確認(レビュー)したり、作成した手順などに基づいて机上でシミュレーションして、議論形式で計画・手順の妥当性を評価する方法。
実地訓練 (演習)	被害を想定して、実際の設備や人員などを用いて実運用及び実作業を行い、計画・手順の妥当性を検証したり、対策の改善点を把握したりする方法

事業継続対策として定めた計画や手順の企業内での周知度合いや事業継続対策の進行度合いなど、企業の事業継続マネジメント力のレベルに応じて、テーマ、方法、実施時期、回数、対象組織などを選定してください。

#### <記載例8>

##### BCP定着と事前対策の実施

###### 【緊急時行動計画の周知徹底】

総務部は、災害発生時における行動計画を社員に周知徹底させ、訓練を定期的実施する。

定期的な訓練として以下の教育・訓練を実施する。

区分	項目	対象	実施単位	方法	時期	頻度
教育	BCP講習会	全社員	部門単位	座学	2月	年1回
訓練	安否確認訓練	全社員	全社一斉	演習	2月	年1回
	防災訓練(地震・火災)	全社員	全社一斉	演習	9月	年1回
	防災訓練(津波)	全社員	全社一斉	演習	9月	年1回
	机上訓練(BCP)	災害対策本部 メンバー	本部のみ	座学	10月	年1回
	IT復旧訓練	情報システム部 経理部・倉庫部	部門単位	実地	5月	年1回

###### 【事前準備施策の実行】

「事前対策計画」に基づき、各計画の担当部署は関連部門と連携の上、施策を実行する。事務局は、定期的に(原則、半期に1回)対策の実施状況を確認する。

###### 【重要な顧客との連絡体制の確立】

顧客対応チームは、主要な顧客への連絡体制を確実にするため、定期的に顧客の連絡先を確認し、連絡先の一覧を最新に維持する。

###### 【重要な協力会社との協力体制の確立】

調達チームは、主要な協力会社との協力体制を確実にするため、定期的に主要協力会社の連絡先を確認し、連絡先の一覧を最新に維持すると共に、事業継続への協力を要請する。



### 【訓練実施の重要性】

東日本大震災で被災された事業者からは、「日頃から実地訓練を行っておくことが大事」との意見が寄せられています。「倉庫の立地や構造等を勘案した防災・避難マニュアルを個別に作成しておき、それに基づいた現場レベルでの訓練を日頃から積んでおく」というものです。「マニュアルの有効性を検証するためにも、想定訓練の実施は必須」であり、非常事態におけるパニック緩和の効果も期待できます。

また、4月7日の大規模な余震（マグニチュード7.1 宮城県沖）を振り返り、「本震より被害が大きく、現場の整理が振り出しに戻って心が折れたが、本震の復旧ノウハウが活きて、現場は思ったより早く立ち直った」と語る事業者の方もおられました。想定訓練を励行するなど、PDCAサイクルの各プロセスを確実に実行することで、より高度な事業継続マネジメント（BCM）が構築されます。

### 【訓練後は反省会を】

東日本大震災で被災された事業者からは、「現場レベルにおける訓練の後などは、従業員に直接指導できる反省会の場を設けることも大事」との意見が寄せられています。訓練毎に点検箇所をクリアし、より高い事業継続マネジメント（BCM）を目指します。

## 2.5.4 点検と評価【CHECK】

BCPの運営状況を定期的に確認し、問題点を改善することで、組織にとって最適なBCPにして行く必要があります。例えば、人事異動による災害時体制の見直しを実施したり、訓練で発見された手順の不備を修正したり、事前対策計画の進捗を確認して、必要であれば事前対策計画の見直しも必要になります。また、企業全体で一貫した事業継続活動を継続するためには、全社レベルの文書だけではなく、各部門で作成した手順書など事業継続のために作成した文書類は全て点検の対象にしておく必要があります。

常に点検と改善が求められる主要な項目についてその点検と改善方法について記述します。

<点検の対象となる項目>

- ・災害時体制
- ・事業継続活動に関する文書（事業継続のための規程・基準・要領・手順書など）
- ・人命に関わる備蓄品（医療品、食料、水など）の状況
- ・事前対策計画の実施状況

<記載例9>

### 点検(CHECK)

#### 【災害時体制の維持管理】

総務部(災害対策事務局)は、定期的に(原則年1回)および人事異動時に、災害対策本体制の見直しを行う。

#### 【文書の維持管理】

事業継続計画に影響を及ぼす事象が発見された場合は、文書を主管する部門が各文書の見直しを実施する。

事業継続計画に影響を及ぼす変更要因となるものは、以下の通りである。

- ① 定期見直し(原則年1回実施)
- ② 各種訓練の結果
- ③ 人事異動、組織変更を行ったとき
- ④ 荷主や取扱貨物が変わったとき
- ⑤ 大規模な社内情報システムの変更があったとき
- ⑥ 新規事業への参入や既存事業の見直しを行ったとき

#### 【備蓄品の維持管理】

総務部(災害対策事務局)は、災害対策本部に設置する備蓄品が災害時に問題なく使用できる状態であるかを定期的に(原則年1回)点検する。

#### 【事前対策の実施状況検証】

総務部(災害対策事務局)は、担当部署が実施した事前準備対策の状況を定期的に(原則年1回)確認し、必要があれば対策内容を見直す。

### 2.5.5 経営者による見直し【ACT】

経営者は、平時の点検結果等の状況から判断し、事業継続活動を継続的に改善していくため、必要であれば復旧方針を見直したり、事業資源を割り当てたりするなど、対応策について改善を指示します。

#### <記載例 10>

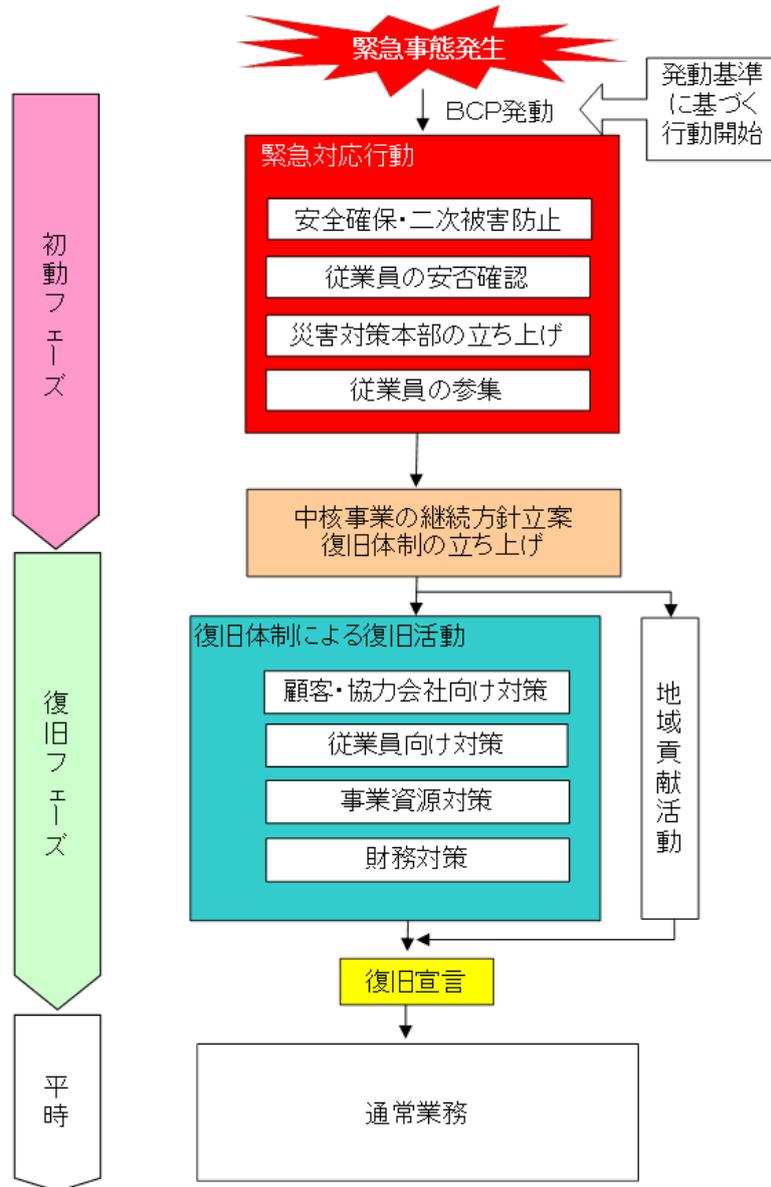
##### **【経営者による見直し】**

経営者は、訓練結果等の事業継続活動全般の実施状況の報告を受けるとともに、必要であれば対応策について改善を指示する。

## 2.6 災害時の事業継続活動を決める

有事の時は、関係者全員が緊急事態であることを認識し、一刻も早く緊急対応行動に移ることが求められます。BCPでは、発動基準を定め、緊急対応行動と情報収集や復旧活動に向けた災害対策本部の立ち上げや各部門の役割について記述します。

また、復旧活動が収束し、平時に戻るための災害対策本部長の復旧宣言についても記載しておきます。BCP発動から復旧までの流れは【図6】のようになります。



【図6】災害時行動フロー

## 2.6.1 発動基準

発動基準は、平時から緊急事態に体制・行動を移行するための基準です。初動の混乱を避けるためにも明確に定義しておく必要があります。基準欄には、何処でどういった事象が発生したかを記載します。事業継続活動に従事する全ての人が理解できてわかり易い基準にすることが望まれます。

また、事象を何段階かのレベルを設けて、警戒を促すことは初動の混乱を避けるために有効な方策です。

### <記載例 11>

#### 【発動基準】

災害規模により非常レベル、警戒レベルの2段階に分け、災害発生直後の行動を規定する。

レベル	基準 (以下の条件が一つでも当てはまる場合)
非常レベル	<ul style="list-style-type: none"><li>・当社活動拠点がある地域で震度6強以上の地震 東京都/埼玉県・・・</li><li>・政府による地震に関する警戒宣言の発令</li></ul>
警戒レベル	<ul style="list-style-type: none"><li>・当社活動拠点以外の地域で震度6強以上の地震</li><li>・当社活動拠点における震度5程度の地震</li><li>・当社活動拠点における大型台風の接近</li></ul>

## 2.6.2 緊急対応行動 【初動フェーズ】

災害発災から2～4時間の緊急時対応行動を定めるものです。

ここには発動基準（前ページ参照）で定めた災害が発生した場合の各レベルに応じた行動を記述します。災害発生直後の安全確保・二次被害防止、従業員の安否確認、災害対策本部の立ち上げ、復旧活動の開始方法について定めます。

### <記載例 12>

#### 【緊急対応行動】

初動フェーズは、災害発生から約2時間（就業時間外は約4時間）を想定する。災害発生をきっかけとして、自身の安全確保、避難、けが人の応急手当、重傷者搬送など緊急対応行動を実施する。緊急対応行動後、要員の安否確認を行い、復旧体制を決定する。

#### 【非常レベルの災害時における行動】

##### <社員・家族・来訪者ほかの安全確保と安否確認>

非常レベルの事象の時、まずは下記の緊急対応行動に従い、人命尊重を主とした行動を行う。

手順	就業時間中(社内)	就業時間中(社外)	就業時間外 (休日・早朝・夜間など)
1	<ul style="list-style-type: none"> <li>○自身の安全確保 (ビル防災センターから指示) (自衛消防隊発動)</li> <li>○自衛消防隊の指示を順守</li> <li>○負傷者を救護</li> <li>○家族・自宅の状況を確認</li> </ul>	<ul style="list-style-type: none"> <li>○自身の安全確保</li> <li>○家族・自宅の状況を確認</li> </ul>	<ul style="list-style-type: none"> <li>○自身・家族の安全確保</li> <li>○自宅の状況を確認</li> </ul>
2	自分自身・家族の安否、家屋の状況を上司等に連絡	同左	同左
3	○災害対策本部の指示があるまで事務所内又は避難場所待機	<ul style="list-style-type: none"> <li>○災害情報の把握 (テレビ、ラジオ、Web等)</li> <li>○原則として帰宅 ・帰宅困難な場合は帰社 or 最寄りの避難所に避難し、災害対策本部の指示があるまで待機</li> </ul>	<ul style="list-style-type: none"> <li>○災害情報の把握 (テレビ、ラジオ、Web等)</li> <li>○災害対策本部の指示があるまで自宅(滞在先)で待機</li> </ul>

～

～

### <災害対策本部の立ち上げ>

①非常レベルの災害時には災害対策本部長候補者（優先順位 1、2、3）はお互いに連絡を取り、本部長を決定する。本部長は、災害対策本部を設置し、各メンバーに本部設置を伝える。

本部設置場所は、以下の候補地から災害対策本部長が決定する。

優先順位	本部設置場所(候補地)
1	本社ビル XX 会議室
2	〇〇営業所 事務室

②災害対策本部メンバーは、自分自身、自宅、家族が無事で、かつ自分自身が行動可能な場合には、本部設置場所へ参集する。災害対策本部は、以下の部門メンバーで構成する。不在の場合は優先順位 2、3 の順で任に当たる。

災害対策本部長	〇〇社長
災害対策事務局	〇〇総務部長
従業員支援チーム	〇〇総務部長
I T 復旧チーム	〇〇情報システム部長
現場対応チーム	〇〇営業所長
顧客対応チーム	〇〇営業部長
財務チーム	〇〇経理部長
広報チーム	〇〇総務部長
調達チーム	〇〇経理部長

③災害対策事務局（総務部）は、従業員の安否の状況を把握して、逐次、災害対策本部長に報告する。

### <従業員の参集>

①災害対策本部長は、要員の参集方針を災害対策本部メンバーに指示する。

②災害対策の各復旧担当チームのリーダーは、従業員に、職場への参集方針を伝え、復旧活動に向けた準備体制を整える。

### 【警戒レベルの災害時における行動】

警戒レベルの災害が発生した場合は災害対策事務局（総務部）が逐次情報を把握し、担当役員に報告の上、災害対策本部設置の可否について決定する。

### 2.6.3 行動チェックリストを作成する

有事の時は、行動チェックリストの各項目を実施する毎にチェック欄を記入しながら、未実施項目が無いように復旧作業を進めます。補足欄には、参照する資料名などの補足事項を記載しておくとい良いでしょう。組織の規模によって体制が異なりますので、標準を元に自社に合った行動チェックリストを作成してください。

#### 発災直後の全社緊急対応行動に準じた行動チェックリスト(標準)

##### <記載例 13> 【初動フェーズ】全社緊急対応行動例

##### 就業時間中（社内）に発災

#	アクション	チェック	補足
1	<b>自身の安全確保:</b> <input type="checkbox"/> 自身の安全確保を行い、来訪者・社員の安全を確認する。負傷者がいた場合は、救護を行う。 <input type="checkbox"/> 家族・自宅の安否を確認し、自身の安否とともに上司や社内関係者に連絡する。		
2	<b>二次被害の防止:</b> <input type="checkbox"/> 避難指示があった場合や建屋に留まっていることが危険な場合は、来訪者、社員と共に建屋の外に避難する。 <input type="checkbox"/> 火災などの二次被害発生を防止し、火災が発生していれば可能な範囲で初期消火を行う。 <input type="checkbox"/> ビル管理会社からの指示があれば、その指示に従う。		
3	<b>災害対策本部からの指示:</b> <input type="checkbox"/> ホームページやテレビ・ラジオなどで可能な手段でできるだけ災害情報の収集に努める。 <input type="checkbox"/> 災害対策本部の指示があるまで、事務所内または、避難場所で待機する。		

##### 就業時間中（社外）に発災

#	アクション	チェック	補足
1	<b>自身の安全確保:</b> <input type="checkbox"/> 自身の安全確保を行い、同行社員の安全を確認する。負傷者がいた場合は、救護を行う。 <input type="checkbox"/> 家族・自宅の安否を確認し、自身・同行社員の安否とともに上司や社内関係者に連絡する。		
2	<b>二次被害の防止:</b> <input type="checkbox"/> 訪問先建屋での避難指示があった場合や建屋に留まっていることが危険な場合は、建屋の外に避難する。 <input type="checkbox"/> 火災などの二次被害発生を防止し、火災が発生していれば可能な範囲で初期消火に協力する。 <input type="checkbox"/> 訪問先のビル管理会社から指示があれば、その指示に従う。		
3	<b>災害対策本部からの指示:</b> <input type="checkbox"/> ホームページやテレビ・ラジオなどで可能な手段でできるだけ災害情報の収集に努める。 <input type="checkbox"/> 原則として帰宅するか、最寄りの避難場所に避難し、災害対策本部の指示があるまで、事務所内または、避難場所で待機する。		

## 就業時間外（休日・早朝・夜間など）に発災

#	アクション	チェック	補足
1	<b>自身・家族の安全確保:</b> <input type="checkbox"/> 自身・家族の安全確保を行い、負傷者がいた場合は、救護を行う。 <input type="checkbox"/> 自宅の状況を確認し、自身・家族の安否とともに上司や社内関係者に連絡する。		
2	<b>自宅からの避難:</b> <input type="checkbox"/> 自治体などから避難指示があった場合や自宅に留まっていることが危険な場合は、最寄りの避難所に避難する。		
3	<b>災害対策本部からの指示:</b> <input type="checkbox"/> ホームページやテレビ・ラジオなどで可能な手段でできるだけ災害情報の収集に努める。 <input type="checkbox"/> 災害対策本部の指示があるまで、自宅または最寄りの避難場所で待機する。		

### 2.6.4 復旧のための役割分担 【復旧体制の立ち上げ】

復旧に向けての各担当の体制づくりを記述します。復旧に必要な役割を定めて、誰が担当するかを明確にします。復旧活動は多岐にわたり、活動の詳細をBCPに記述するのは難しいため、最低限各担当者の役割を明確にしておきます。

復旧活動に必要な役割には以下の表のような活動があります。

復旧に必要な機能	実施内容
建物損害評価	建物、設備等の被害状況の調査と状況整理
安否確認	社員、来訪者等の安否確認と状況整理
IT損害調査・復旧	IT（情報システム）の被害状況の調査と復旧作業
セキュリティ対策	二次災害防止、防犯対策
情報発信	社外（顧客、取引先、社会一般、マスコミ等）や社内への情報発信
問合せ対応	社内外からの問合せの対応
財務対応	緊急用資金調達と支払いの調整・実施
調達対応	必要な設備・備品の緊急調達
保険対応	保険用損害調査と請求手続き
記録	損害状況、復旧活動等の記録
応援要員対応	要員の移動手順や宿泊等の手配・確保
被災者支援	医療サポート、帰宅者支援、帰宅困難者支援
法務	訴訟対応、緊急時契約への法務アドバイス
業務管理	災害時の例外処理・資金の流れ・違法行為の監視
外部情報収集	マスコミ等からの災害情報収集
人的資源管理	人員の調達、配置の決定
人事支援	従業員人事支援策（勤務、補償等）の決定
顧客情報確認	顧客の損害状況調査と状況整理
協力会社情報確認	協力会社（調達先、出荷先）の損害状況調査と情報整理
保管貨物等損害確認	保管貨物の損害状況調査と情報整理
重要業務の復旧	復旧優先順位の見直し検討、代替手段の発動、切替作業、代替業務運用の維持

<記載例 14>

役割分担は、会社毎に組織の構成や業務分担により異なりますので、自社の実態に合った機能分担を行ってください。

役割名称	役割詳細	対策事務局 (総務担当)	従業員 (総務担当) 支援チーム			IT 復旧チーム	現場 対応チーム	顧客 対応チーム	財務 チーム	広報 チーム	調達 チーム
			総務	人事	法務						
建物損害評価	建物、設備等の被害状況の調査						◎				
	建物、設備等の被害状況の整理	△	◎								
安否確認	社員、来訪者等の安否確認		◎	△			◎				
	社員、来訪者等の安否情報の整理	△	◎								
IT損害調査・復旧	IT(情報システム)の被害状況の調査					◎	△				
	IT(情報システム)の被害状況の報告受け・整理					◎					
	IT(情報システム)の被害状況の復旧					◎	△				
セキュリティ対策	二次災害防止、防犯対策					◎					
情報発信	社外(顧客、取引先、社会一般、マスコミ等)向け情報発信							△		◎	
	社内(従業員)向け情報発信		◎				△	△			
	関連会社(親会社、子会社)への情報発信(報告)	◎									
問合せ対応	社内外からの問合せの対応					△	△			○	
財務対応	緊急用資金調達								○		
	支払いの継続								○		
調達対応	社用備品等の緊急調達		○								
	顧客用仕入れ品の緊急調達							○			△
保険対応	保険用損害調査						△		○		
	損害保険請求								○		
記録	損害状況、復旧活動等の記録	◎	◎			◎	◎				
応援要員対応	要員の移動手順の確保			○			△				
	要員の宿泊手段の確保						○				
被災者支援	医療サポート						◎				
	帰宅支援(帰宅経路等)						○				
	帰宅困難者への支援 (食料配給など)						○				
流通処理	物流体制の被害調査						○			○	
法務	訴訟対応、緊急時契約への法務アドバイス			○							
業務管理	災害時の例外処理・資金の流れ・違法行為の監視			○							
外部情報収集	マスコミ等からの災害情報収集	◎								◎	
人的資源管理	人的資源の調達、配置の決定			◎							
人事支援	従業員人事支援策(勤務、補償等)の決定			○							
顧客情報確認	顧客の損害状況調査						△	◎			
	顧客の損害状況受け、整理	◎									
協力会社情報確認	協力会社(調達先、出荷先)の損害状況調査						△	◎			
	協力会社(調達先、出荷先)の損害状況受け、整理	◎									
商品、仕掛損害確認	仕掛在庫、商品在庫の損害状況調査							○			
	仕掛在庫、商品在庫の損害状況受け、整理										○
重要業務の復旧	復旧優先順位の見直し検討、代替手段の発動、切替作業、代替業務運用の維持	◎						◎			

## <参考：各復旧担当の役割補足>

### 【対策事務局】

- ・ 掲示板の設置や命令の記録などによって、的確な情報を正確に伝達するようにします。東日本大震災では「全ての決定事項の記録」、「必要情報を全て掲示」、「写真での記録を義務付け」といった対応を徹底して正確な情報収集及び伝達ができただ事業者がありました。
- ・ 復旧時には、協力会社、あるいは周辺企業の方々との情報交換、安否確認や被害状況の確認に加えて、支援物資や燃料の入手ルートなど、復旧につながる様々な情報が行き交いますので、こうした情報を必要とする全ての部署や人に届くような体制づくりが求められます。

### 【現場対応チーム】

- ・ 指示の混乱を防ぐため、現場では職場長の指示だけに従うようにするなど、指揮・命令系統の統一を徹底します。
- ・ 復旧作業は、余震などによる二次災害を防止するため、建物・付帯設備の損壊状況を確認のうえ、避難場所や経路などを確保しながら行います。東日本大震災では、地震が発生した3月中だけでM（マグニチュード）5以上の余震が466回発生、うち3回はM7以上で本震に迫る規模でした。また、余震発生期間も長く観測されており、二次被害には細心の注意が必要です。
- ・ 落下物や転倒などで強い衝撃を受けた電動フォークリフトは、バッテリー部分が発火の原因となる恐れがあります。移動可能であれば可燃物から遠ざけ、移動が不可能な場合は、周囲の可燃物を移動させます。また、十分な事前点検を行った後でなければ充電を行わないようにします。

### 【財務チーム】

- ・ 大規模災害では、各種優遇措置や負担軽減措置など、何らかの支援措置が講じられますので、中小企業庁、国税庁、都道府県・市町村などの公的機関については、ホームページなどを常にチェックするようにします。
- ・ 経営者自らが金融機関等へ状況説明を行うことが必要な場合も想定されます。

### 【顧客対応チーム】

- ・ 大規模災害では、人員、機材、資材不足やインフラの未回復などもあって全ての顧客に対応することは不可能です。事前に決めた中核事業、重要業務の基準に照らして、復旧作業に当たるようにします。
- ・ 被災された事業者からは「被災状況や顧客との関係により対応方法に相違点がでてくるため、BCPは顧客と一緒に策定するとよい」といった意見が寄せられています。

### 2.6.5 復旧体制による復旧活動 【復旧フェーズ】

緊急対応行動で落ち着きを取り戻したら、経営者が、中核事業の復旧方針を決めて、復旧に向けた活動を開始します。方針の決定は、被害の状況によっても異なりますし、復旧活動の進行によって見直すことが必要になります。重要なのは、被害や復旧の情報を災害対策本部で的確に把握していくことです。BCPでは、被害状況や、復旧活動の状況報告のタイミングなど記載して、確実に情報が災害対策本部に集約されるようにします。

報告基準として定めるものとしては、最低限以下のものがあります。

- ・ 初期フェーズでの状況報告（緊急対応行動後）
- ・ 中核事業の復旧方針の決定
- ・ 災害対策本部で方針の見直しや必要な対策の決定・指示を行う間隔
- ・ 復旧現場から災害対策本部へ状況を報告する間隔

#### <記載例 15>

##### 【復旧体制による復旧活動】

予め決められた復旧体制に従って、復旧活動を開始する。

復旧活動の状況報告は、以下の報告時間基準に基づいて行う。

##### <報告の時間基準>

- ・ 発災後○時間以内（就業時間外○時間以内）：初期段階の状況を報告する。（緊急対応行動後）
- ・ 発災後○時間以内：中核事業の復旧方針を決定する。
  - －最低○時間毎には災害対策本部で方針の見直しや必要な対策の決定・指示を行う。
- ・ 復旧現場からは、最低○時間毎に災害対策本部へ状況を報告する。

##### 【中核事業の復旧方針の決定】

経営者は、災害対策本部に集約された情報を元に中核事業の復旧方針を決定する。以後、最長でも○時間毎に方針の見直しを行い、必要な対策を指示する。

##### 【状況の報告】

各復旧活動の従事者は、各復旧チームの責任者に活動状況を報告する。責任者は、逐次、収集した情報を災害対策本部長に報告する。（最低○時間毎に報告する。）

##### 【運輸局への事故報告】

大規模自然災害等によって倉庫が損傷した場合、発生後二週間以内に、損傷の概要を記入した事故届出書（則第24条第4項）を運輸局長に提出する。

## 2.7 復旧宣言

復旧活動中は、災害時緊急対応が発動された状態です。重要業務が復旧し、BCP発動状態から平時の状態に戻った場合、復旧を宣言します。

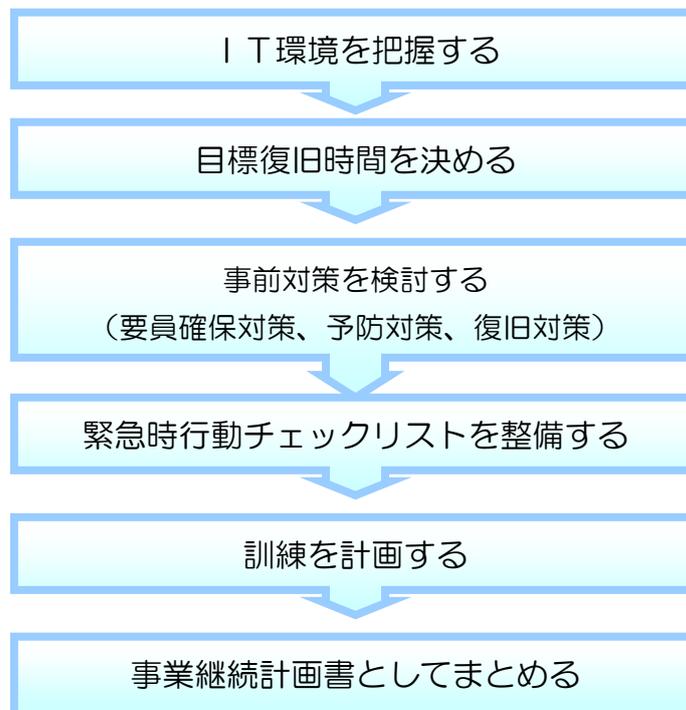
### <記載例 16>

#### **【復旧宣言】**

災害対策本部長は、重要業務が復旧し、災害時体制をこれ以上維持継続する必要がなくなったと判断した時点で全社に対して復旧宣言を行い、災害対策本部を解散する。

## < 第Ⅱ章 >

### I T 部門の事業継続計画書（BCP）を作成する



## 〇はじめに

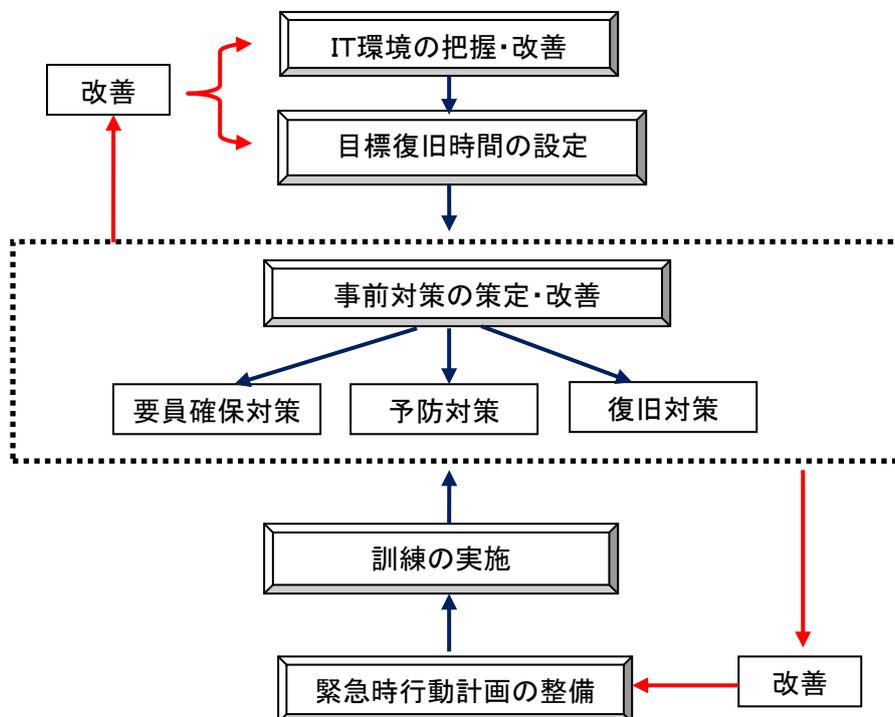
東日本大震災では、地震の揺れでサーバが転倒・停止した結果、業務に大きな影響が出ました。また、津波でデータが流され業務の復旧が困難になるなど、情報システムの停止に起因する事業への影響が数多く発生しています。

東日本大震災の被災企業から「**情報システムは、事前対策が取られていないと復旧に最も時間と費用がかかる。普段から最重要危機管理項目として管理しておくべき**」との声も上がっているほどで、事業継続上の位置付けは非常に重要です。

そこで、第二章では情報システム部門における事業継続計画書の作成の仕方について解説することといたしました。事業継続計画書作成において、一番重要な部分は災害が発生した際の情報システムの**目標復旧時間（RTO）を設定**ことです。情報システムの目標復旧時間は、当然情報システムを利用する業務から大きな影響を受けますので、関連する重要業務の洗い出しなども必要となります。

目標復旧時間を設定したら、それを実現するための環境が整っているかを検証し、もし不十分であれば環境整備を行います。そのための作業が、現状のIT環境の把握と事前対策としての要員の確保、予防対策、復旧対策の検討になり、補完するものが緊急時行動計画の整備と訓練の実施になります。

以上を冊子等にまとめたものが「事業継続計画書」であり、その計画をPDCAサイクルを通じて管理する仕組みが「事業継続マネジメント（BCM）」となります。



【図 7】事業継続マネジメント（BCM）イメージ

## Ⅱ－１ IT環境を把握する

### 1.1 情報システム一覧表の作成

まず始めに行うことは情報システム一覧表の作成です。まとめ方は「倉庫管理システム」、「経理システム」、「輸配送システム」などの単位に行います。一つのハードウェア上（サーバ上）で複数のシステムが稼働している場合も、それぞれをひとつのシステムと見て整理します。

SaaS などクラウド型サービスを活用している場合も同様です。事業に必要なシステムは全て対象に含める必要があります。

まとめる内容としては下表のようなものになります。（記載例は<記載例 17>参照）

対象	調査項目	調査内容
システム概要	名称	社内で通用可能なシステム呼称
	用途	システムの用途
	主管部門	対象システムの主管部門
	システム形態	クライアントサーバ、Web システム、SaaS、IaaS 等のシステム形態
ハードウェア	機種名	メーカーなどが識別可能な機種名
	設置場所	本番用システム(サーバ・ホスト)の設置場所
	保守業者	ハードウェアの保守業者
代替機器	代替機器の有無	本番機が壊れた場合の代替機となるハードウェアの有無と機種名
	設置場所	代替機の設置場所
ソフトウェア	OSの種別	Windows～、Linux～など
	アプリケーション名	パッケージ名や製品名などアプリケーションの名称。個別開発の場合は”個別開発”
	バックアップ有無	OSおよびアプリケーション環境(データ領域を除く)のバックアップ有無
	バックアップ形態	前項バックアップがある場合のバックアップの形態で、ボリュームイメージ、論理セーブなどの形態。 ※バックアップ専用ツールを使用している場合は、ツール名称も記載
	バックアップ媒体保管場所	OSおよびアプリケーション(データ領域を除く)のバックアップ媒体保管場所

#### <事業継続の観点から特に確認が必要な項目>

ハードウェア管理台帳、ソフトウェア管理台帳等の管理資料があれば情報システム一覧表の代わりに利用できますが、その場合でも以下の情報について確認し、不足しているようであれば補っておきましょう。

- ・ 本番機の設置場所
- ・ 代替機器の有無、設置場所
- ・ 保守業者
- ・ ソフトウェア（OS、アプリケーション）のバックアップの有無、セーブ形態、媒体形式



## 1.2 ネットワーク環境の把握

LAN、WAN、クラウドなど、ネットワークを使用している場合には、ネットワーク機器※の故障や通信回線の停止に備え、その環境を把握して、ネットワーク構成図として整理しておきます。このときバックアップ回線も含めて漏れが無いように記載します。

※ネットワーク機器：ルータ、ファイアウォール、光回線終端装置（ONU：Optical Network Unit）など

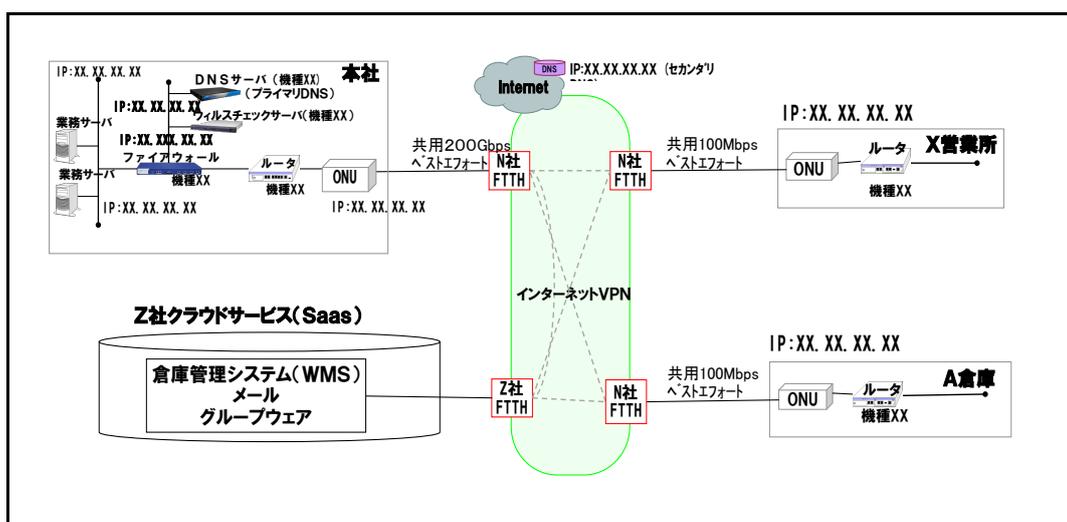
調査項目としては、以下のものが挙げられます。（記載例は<記載例 18>参照）

対象	調査項目	調査内容
回線関連	通信事業者	通信事業者名(キャリア名)
	回線種別	回線の種別・サービス名・スピード
	電話番号/アドレス	電話番号、IP アドレスなどのアドレス識別情報
機器関連	機能	ルータ、ONU、モデムなどの機能名称
	機種名	ハードウェア機種名、型番
	設置場所	機器設置場所
	アドレス	IP アドレスなどのアドレス識別情報

ネットワーク構成図を作成済みの場合は改めて作成する必要はありません。しかし、使用している機器、設置場所、回線種別など上表に記載の情報が網羅されていることを確認する必要があります。不備があれば手直しを行います。

外部業者にシステム構築を依頼した場合は、業者がネットワーク構成図を作成するケースが多いので、構築した外部業者等に相談してください。

### <記載例 18> ネットワーク構成図（イメージ）



### 1.3 クライアント環境の把握

有事の際にはクライアントPCやスタンドアロンPCも必要になります。部署、営業所、倉庫毎に台数や配置状況を調査しておきます。この時、有事を想定した最低限必要台数も把握しておきましょう。復旧活動時の再調達や再配置の参考になります。

その際、荷主端末やハンディターミナル等倉庫業務に必要な端末も含めることが必要です。

資産管理台帳に個々のPCが管理されている場合は、その情報を元に整理しておけばよいでしょう。

調査項目としては、以下のものが挙げられます。（記載例は<記載例 19>参照）

調査項目	調査内容
部門	クライアントPC配置部門
設置場所	クライアントPC設置場所
タイプ (ノート or デスクトップ)	ノート形式・デスクトップ形式などPCのタイプ ※バッテリーの有無で被災時継続使用の判断も可能
OS	WindowsなどのOS種別、バージョン
主要OAソフト	Office系ソフトなどのOA目的のソフト
業務アプリケーション	基幹業務遂行のためのクライアントアプリケーション
現有台数	現在の保有台数
最低必要台数	有事の際に、業務遂行上最低限必要と思われる台数

#### <記載例 19> クライアント環境一覧表

① 部門	② 設置場所	③ タイプ (ノート or デスクトップ)	④ OS	⑤ 主要OAソフト	⑥ 業務アプリケーション	⑦ 現有台数	⑧ 最低必要台数	
倉庫部	横浜倉庫	ハンディターミナル	WindowsCE5.0	—	専用ソフト	15	3	
		荷主A社端末		—	専用ソフト	3	1	
		デスクトップPC	WindowsXP Professional SP3	Office 2003 pro メール Outlook 2003 ブラウザ IE6	WMS	2	1	
経理部	本社	デスクトップPC	Windows7 Professional SP1	Office 2007 pro メール Outlook 2007 ブラウザ IE6	勘定奉行	10	1	
営業部	北海道(支店)	ノートPC	Windows7 Professional SP1	Office 2007 pro メール Outlook 2007 ブラウザ IE6	WMS	2	1	
		荷主B社端末		—	専用ソフト	1	1	
						ハンディターミナル合計	15	3
						クライアントPC合計	15	4

## 1.4 バックアップ取得状況の把握

データが消失すると、伝票の再入力や注文の取り直しなど自社だけでなく取引先やその関連会社にまで影響が及び、事業継続に多大な支障をきたします。

東日本大震災では、津波でサーバと一緒にデータが消失したケースが数多く見受けられました。しかし、そのような時でも、バックアップを取っていた事業者では遠隔地に保存したデータから復元することで、復旧活動がスムーズに行われたとの報告がありました。IT部門のBCPでは、このバックアップ体制の整備が最重要課題であると言っても過言ではありません。

重要な情報のバックアップ漏れを防ぐため、まずは現状のバックアップ状況を把握することから始めます。バックアップについては実施サイクル、媒体、方式、対象データ、実行者、保管方法などについて確認します。SaaSを利用している場合は、バックアップの有無をサービス提供事業者を確認しておきます。

調査項目としては、以下のものが挙げられます。（記載例は<記載例 20>参照）

調査項目	調査内容
システム名	対象システム名
対象データ	バックアップ対象データ (以下バックアップの特性が同じであれば総合的に記載しておけば良い)
サイクル	「日次」、「週次」、「月次」、「随時」、「ミラーリング」等のバックアップサイクル
世代	何世代まで遡ってバックアップしているかの世代数 日次セーブで3日前まで戻すためには”3世代”必要
媒体	「カートリッジMT」、「ディスク」など媒体の種別
方式 (フル、差分)	「フル」か「差分」かのバックアップ方式
容量	対象データの容量 (概数で可)
ツール	バックアップツールの名称 (ARCserve など)
方法 (イメージ、ファイル、データベース)	「イメージ」か「ファイル」かのバックアップ方法
データが含まれるか?	含まれるものに“○”を記入
アプリケーションが含まれるか?	
OSが含まれるか?	
バックアップの保管場所 (遠隔地、同一区画、別区画)	バックアップデータの保管場所 遠隔地か同一区画かなどの原データとバックアップの位置関係を示す

<記載例 20> バックアップ取得状況一覧表

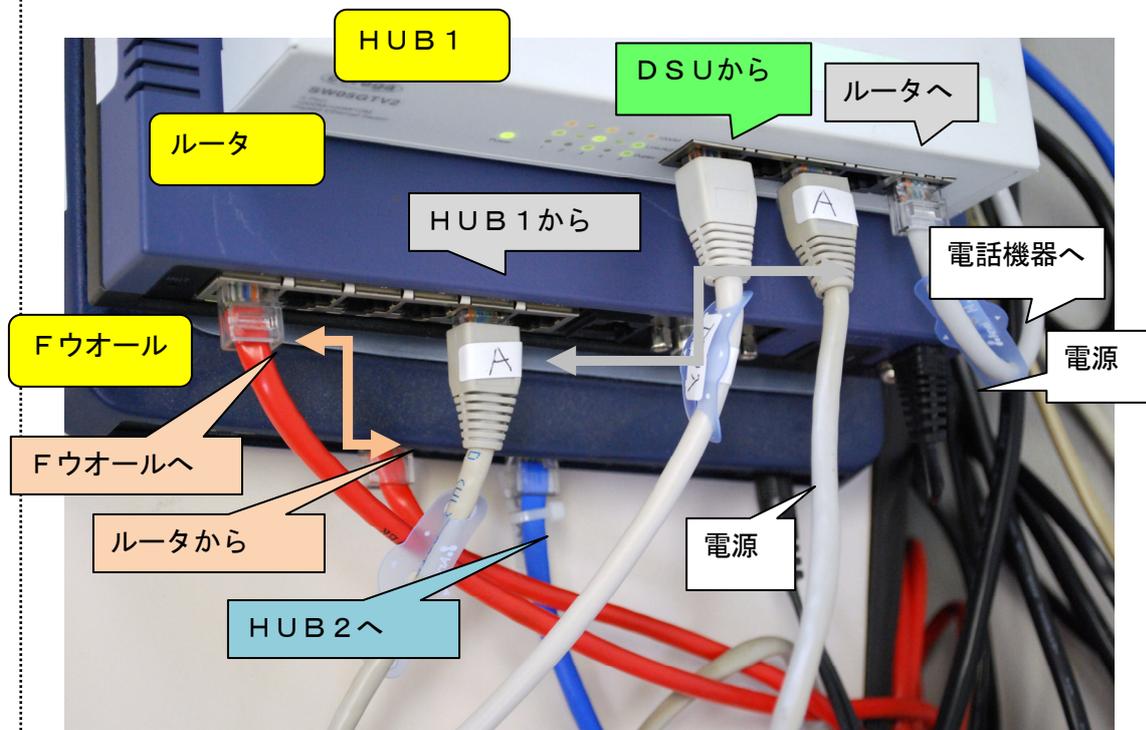
①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬
システム名	対象データ	サイクル (日次、週次、月次、随時、 ミラーリング)	世代	媒体	方式 (フル、差分)	容量	ツール	方法 (データ、イメージ、ファイル)	データが 含まれるか?	アプリケーション が含まれるか?	OSが含ま れるか?	バックアップの 保管場所 (遠隔地、同一区画、別区画)
会計システム	売掛データ、買掛データほか	週次	3	カートリッジMT	フル	1TB	ArcServe ファイル	ファイル	0	x	x	遠隔地
		日次	6	カートリッジMT	差分	1TB	ArcServe ファイル	ファイル	0	x	x	遠隔地



## 意外に便利な写真による整理

一覧表による整理が終わったら、各機器の配置や配線について写真に撮っておきましょう。地震などの混乱にまぎれ、配線がぐちゃぐちゃになってしまったときに便利なのが配線図などの写真です。図を描くのは手間がかかりますが、写真なら手軽です。加えてコードの色などからも判断できます。是非覚えておいて利用しましょう。

H A B 1 ルーター ファイア・ウォール配線図

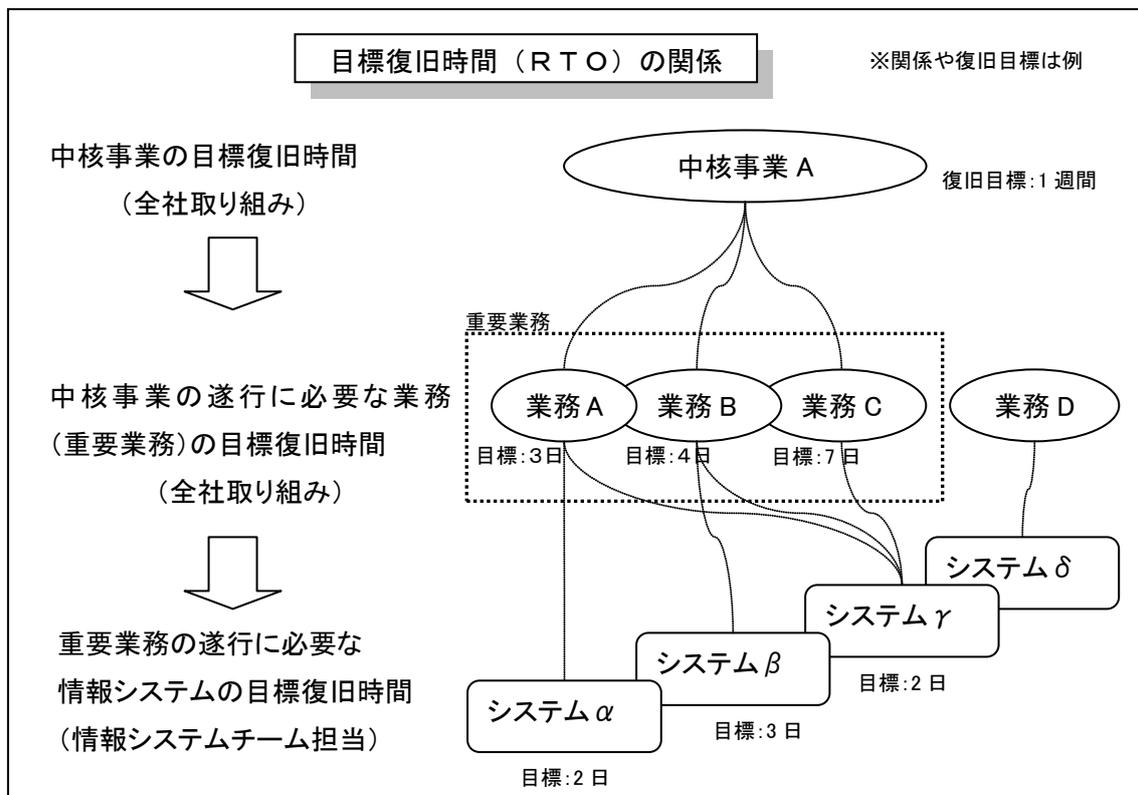


## Ⅱ-2 情報システムの目標復旧時間（RTO）を決める

第一章「2.4 中核事業の特定とその目標復旧時間を決める」（11 ページ～）で定めた目標復旧時間＝RTO（Recovery Time Objective）の達成を目指し、中核事業の遂行に必要な業務（重要業務）の特定及び目標復旧時間の設定とその遂行に必要な情報システムの目標復旧時間を検討します。

検討の多くは全社的な取組みになりますが、情報システムに係る目標復旧時間は情報担当者が設定します。

これら関係を図示すると【図8】のようになります。

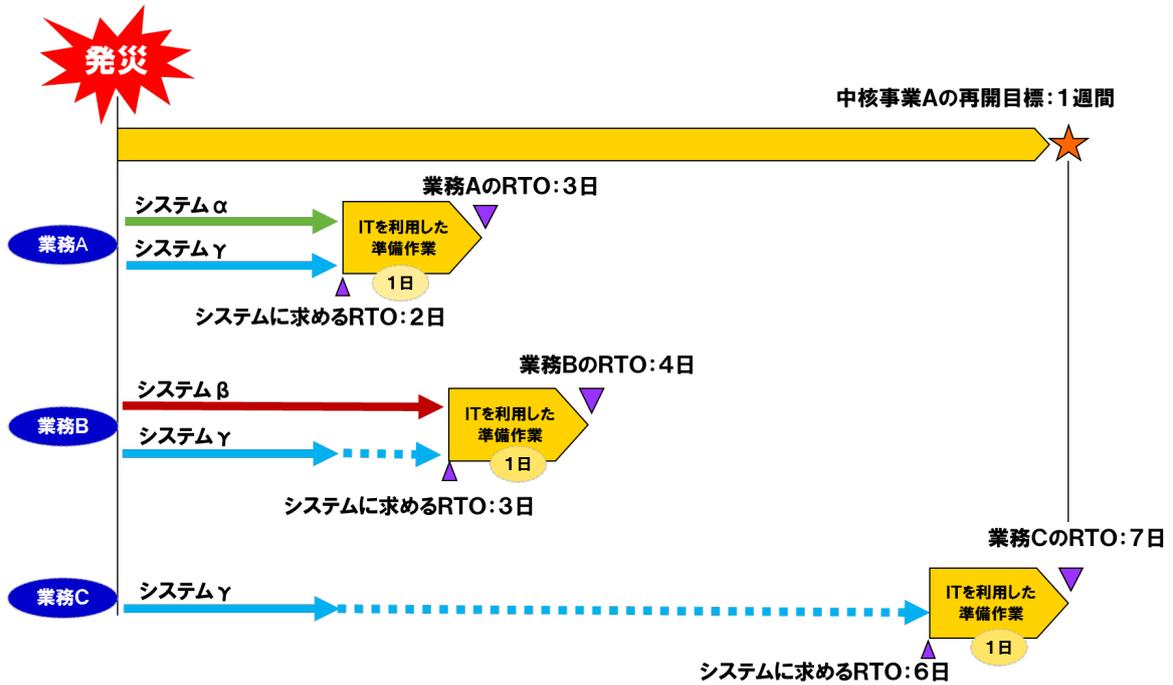


【図8】目標復旧時間の3つのレベル

### 情報システムの目標復旧時間の設定

～簡易的には全社で決めた目標復旧時間の1日前に設定

上掲【図8】の内容から業務とシステムの間を考えると、業務Aの目標復旧時間は3日であるため、同業務に関係するシステムα、γは業務Aの作業開始前に復旧している必要があります。つまり、ITを利用した準備作業を考慮し「業務Aの目標復旧時間」 $\geq$ 「システムα又はγの目標復旧時間」という関係になります。ただし、複雑になることを避けるため、簡易的に準備作業期間＝1日として検討作業を進め、その後のPDCAサイクルを通して、より詳細な目標復旧時間の設定に進む方が良いでしょう。この例を図に表したのが【図9】です。



【図 9】 業務のRTOとシステムのRTOの関係

システム単位で見た場合、複数の業務遂行に関係していることがあります。その時は、関係している業務の最短の目標復旧時間が、そのシステムの目標復旧時間になります。

例えば、下表のようにシステムγは業務A、B、Cの何れにも関係しているので、その目標復旧時間は、(業務Aが2日、業務Bが3日、業務Cが6日)のうち最も短い業務Aの目標復旧時間=2日が、システムγの目標復旧時間となります。

重要業務	中核事業との関係	業務の目標復旧時間	システムの目標復旧時間	システムα	システムβ	システムγ
業務A	◎	3日	2日	○		○
業務B	◎	4日	3日		○	○
業務C	○	7日	6日			○

↓  
システムγの目標復旧時間=2日

これら各事業とシステムの関係情報を情報システム業務影響度調査表（＜記載例 21＞参照）としてまとめます。

<記載例 21> 情報システム業務影響度調査表

【基準となる目標復旧レベル(RLO)】  
 優先度A:〇〇倉庫事業を1週間以内に復旧する(建物が一部損壊の場合)  
 ※優先度Aの復旧が出来れば、原則優先度B以下の事業も復旧対応可能である。

【業務&システムマトリックス】

部門 (または業務分 類)	業務	中核事業 との関係	業務の 目標復旧時間 (RTO)	システムの 目標復旧時間 (RTO)	代替策の有 無	システム											
						倉庫管理	販売管理	物流管理	会計管理	ゲ グ (安否確認 ウェア)	ホームページ	メール					
倉庫部	入庫管理	◎	3日	2日	無し	○											
	出庫管理	◎	3日	2日	無し	○											
	在庫管理	◎	3日	2日	無し	○											
	輸配送管理	◎	7日	6日	無し	○			○								
販売部	受発注管理	◎	6日	5日	有り						○						
	受注管理	◎	7日	6日	有り						○						
経理部	資金調達	○	20※	19日	有り						○						
	安否確認	○	1日	1日	有り						○						
総務部	広報	○	1日	1日	有り									○			
	仕入管理	x	14日	13日	有り												
:	:	:	:	:	:												
◎:不可欠						システムの目標復旧時間(RTO)	2日	5日	6日	19日	1日	1日	1日				
○:間接的に必要						※間接的に必要な業務(○印)のRTOは、中核事業のRTO(今例の場合1週間に設定=45P参照) より長い場合がある											
x:不要																	

## Ⅱ－3 事前対策を検討する

### 3.1 事前対策計画を作成する

前項で調査したシステムの目標復旧時間内での復旧を実現するには、事前の対策が必要です。事前対策は「要員確保・復旧体制」、「インフラ」の2つの側面から検討します。

それぞれ優先的に実施すべき対策、推奨される対策について検討し、実施が予定されるものについては、費用等の制約条件を加味して「事前対策計画」（記載例7）としてまとめます。事前対策計画は基本的には全社的な取り組みになりますが、情報システムに関するものは情報システム部門で単独に作成してもかまいません。何れの方法にするかは会社としての判断によります。

（第一章「2.5.1 事前対策計画（3）事前対策計画の整備」16ページ参照）

#### <記載例22> 全社事前対策計画（IT部門に関するものの抜粋）

対策有無	対策項目	担当部署	対策が必要な場合		
			必要資金 (百万円)	資金調達方法	予定年
<input type="checkbox"/>	コンピュータシステムのバックアップ	情報システム部	8	自己資金	20xx年
<input type="checkbox"/>	自家用発電機の導入	総務部	30	自己資金	20xx年
<input type="checkbox"/>	緊急時通信機器の整備 (MCA無線、衛星電話)	総務部 (情報システム部)	1	自己資金	20xx年
<input type="checkbox"/>	社員安否確認手段の整備 (連絡方法の複線化)	総務部 (情報システム部)	1	自己資金	20xx年

### 3.2 要員確保と復旧体制のための対策を検討する

有事の際には、いち早く要員を確保して、復旧活動をスムーズに進めることが必要です。そのためには要員確保が最重要課題となります。

東日本大震災で被災した多くの企業からも、「復旧には人材の確保が重要。ただし、人数だけいても復旧は進まない。緊急時における適切な人員配置と指揮命令システムが必要だった」などの意見が寄せられています。

スムーズな体制の立ち上げのために事前に決めておくことは以下の3点です。

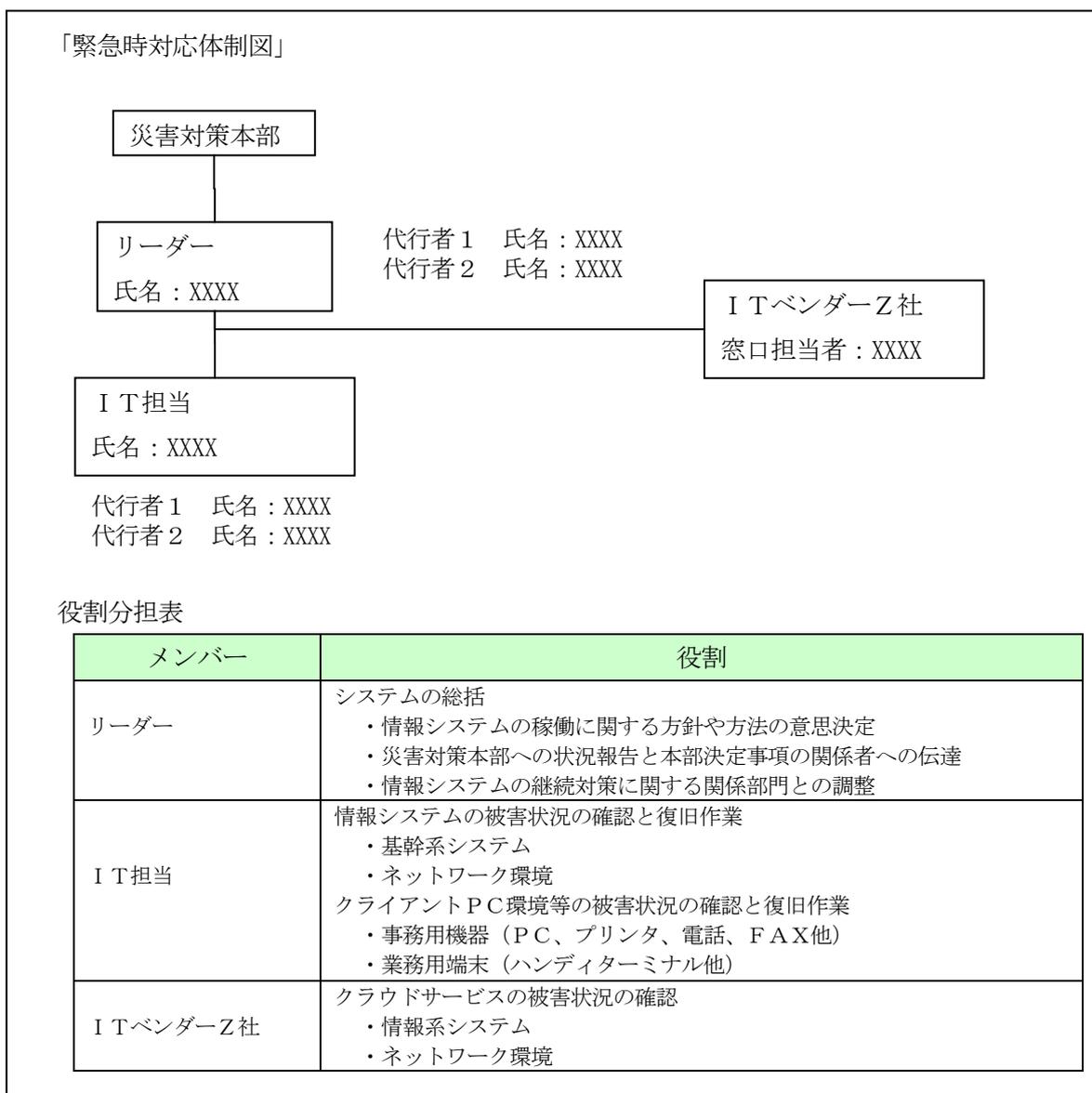
- (1) 役割・指揮命令系統の明確化
- (2) 安否確認方法の決定
- (3) 発動基準の決定

(1) 役割・指揮命令系統の明確化

役割・指揮命令系統を明確化することは、情報ルート of 混乱を防ぎ、スムーズな復旧活動を行うために不可欠です。全社的な事業継続体制を前提に、IT復旧チームの緊急時の対応体制を決めておきます。

<記載例 23> 緊急時対応体制図（組織図）及び役割分担表

体制図には役割毎に名称を定めるとともに、担当する者とその代行者を決めます。役割分担表には担当者が果たすべき役割について明確に記載しておく必要があります。





### 3.3 情報システムの対策を検討する

情報システムにおける対策は、有事の時に情報システムによるサービス（以下、「ITサービス」という）を停止させないための「予防対策」と、ITサービスが停止した場合に、別の手段を使ってITサービスを再開する「復旧対策」の2つに分けることができます。「予防対策」で防ぎきれなかった事象に対して「復旧対策」が補完するという関係にあります。

まずは、予防対策として必要な対策を検討し、その上で目標復旧時間が短く、復旧優先順位が高い業務について復旧対策を施すか否かを検討します。

本項では、以下の対策項目毎に優先レベルを踏まえた対策について解説します。

#### <対策項目>

	対策項目	内容
予防対策	①データバックアップ	データを保全する対策
	②災害に対応した設備機器の設置	主要な災害である火災・風水害・地震に備えた設置環境上の対策
	③電源対策	瞬断などの電力異常や停電などに備えた対策
	④二重化・冗長化	サーバ、ネットワーク、空調設備の停止に備えた冗長化対策
復旧対策	①代替サイト	本番機設置場所が使えなくなった時に代替となる設置場所の確保
	②代替機器	本番機が故障した場合の代替機器(PC、サーバ、ネットワーク機器)の準備
	③代替要員	定常時のシステム担当者が職務遂行困難な場合の代替となる要員での対応策

### 3.3.1 予防対策

予防対策は、災害や事故が発生した場合に被害を最小限に食い止めるために行う事前対策です。自社で採用する対策を下記のような予防対策一覧にまとめます。（記載例は<記載例 25>参照）

情報システムの予防対策には様々なものがありますが、システムの重要度や投資可能額を勘案し、数ある対策の中から自社に最善と思われる対策を導入すればよいでしょう。本項では、自社に情報システムを持つ企業を前提に、必要な対策について次ページ以降に記載しています。中でも「データバックアップ」は、最優先で検討しておく事項です。また、クラウド型サービスを活用している場合には、サービス提供元の環境がどのレベルにあるかを確認しておく必要があります。

なお効果の高い対策、機器については<参考資料>を参照して下さい。

#### <記載例 25> 予防対策一覧表（推奨される主要なもの）

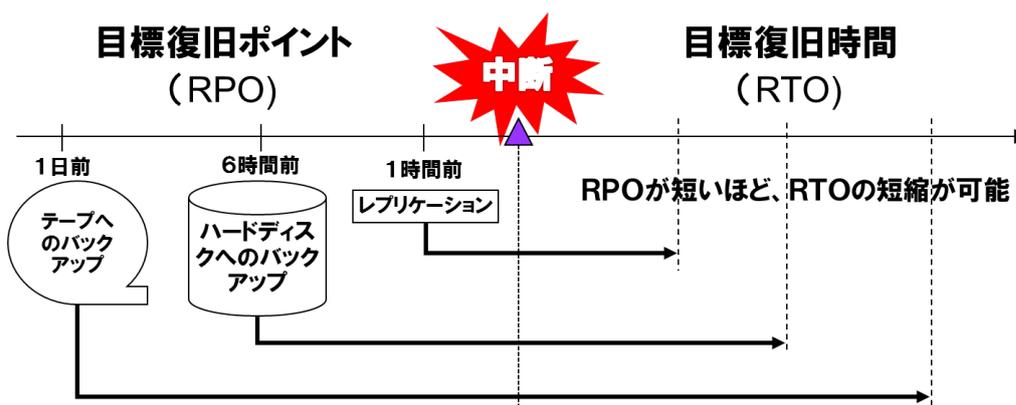
対策項目		必要な対策
(1) データバックアップ		同一拠点内でバックアップした媒体の遠隔地保管
(2) 災害に対応した 設備機器の設置	火災	火災の原因となる設備の設置回避 消火器の設置
	風水害	十分な防水性能のある建物への設置
	地震	耐震ビル設置 機器固定
(3) 電源対策		電源異常対策（UPS：無停電電源装置の導入等）
(4) 二重化・ 冗長化	サーバ	—
	ネットワーク	—

### (1) データバックアップ

地震等により突然コンピュータが止まると処理していたデータが失われ、再入力などを行って復旧に当たらなければなりません。元データが無い場合、復旧作業は簡単にはいきません。場合によっては取引先の協力を仰ぐこととなります。このような事態を最小化するにはデータのバックアップが必須となります。

データのバックアップは、処理するデータ量にもよりますが目標復旧時間（RTO）を何処の時点に置くかによって対策のレベルが異なってきます。【図 10】はRTOとRPOの関係イメージしたものです。RPO（Recovery Point Objective）とは目標復旧ポイント、とも呼ばれ、目標復旧時間（RTO）を達成するために、どの程度までデータの喪失が許されるかを表す時間軸のことです。ポイントを短時間に設定すればするほどデータの損失量が少なくて済み、目標復旧時間も短くなる半面、対策レベルは高度になります。

バックアップ方式を検討するに当たっては、「システムの重要度と目標復旧時間」、「データ量」、「媒体（テープやハードディスク等）」、「保護対象のデータとバックアップ先の位置関係」、「バックアップのタイミングの視点」を勘案して検討します。

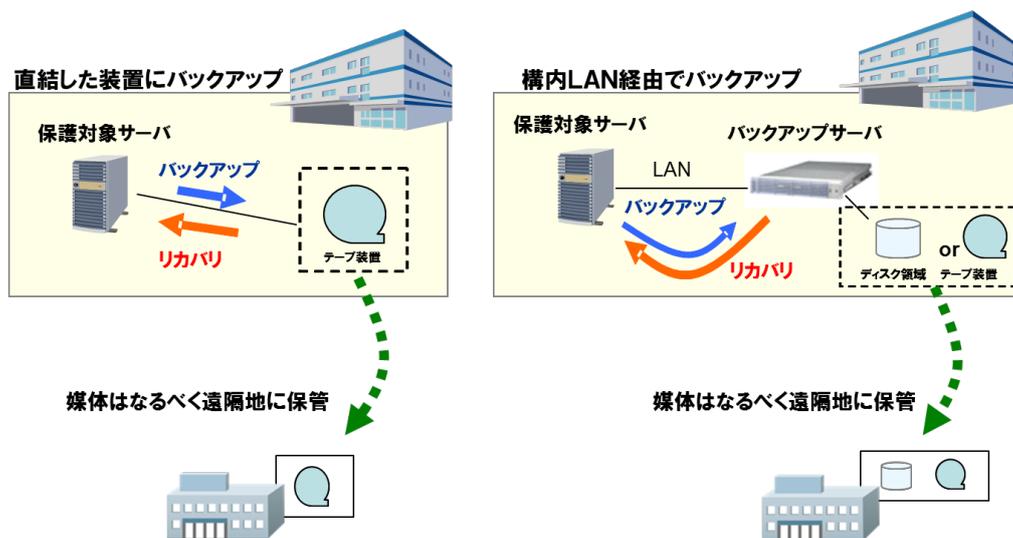


【図 10】 RPOとRTOの関係

#### 【対策例】 同一拠点内でバックアップした媒体の遠隔地保管

サーバと直結した、あるいは構内LANで接続したバックアップ機器にデータを保存する方法は、保護対象の情報システムと同一環境下になるため運用が容易な反面、災害時にはデータも情報システムと一緒に被災する可能性が高く、局所的なシステム障害のみに対する予防対策になります。こうした保存方法では、本番データとバックアップデータの同時被災は免れません。

同時被災を避けるためには、バックアップデータをテープ等の可搬型媒体に移すとともに社内便やメール便などを利用し、本番機とは別の場所（他の営業所など）に保管する必要があります。可能な限り遠隔地に移送して保管することが求められます。【図 11】



【図 11】同一拠点内でバックアップした媒体の遠隔地保管

※より高度なバックアップ方法は参考資料（74 ページ）をご参照ください。



### 本番環境とバックアップ環境の距離

本番機とバックアップサーバが同時に被災しないためには、充分離れた距離を保つ必要があります。金融情報システムセンター（FISC）が発行する「金融機関等コンピュータシステムの安全対策基準・解説書」に「60 キロメートル離れていれば直下型地震の影響を回避できる」という過去に国が発表していた予測が紹介されていましたが、2011 年 3 月発行の同書の第 8 版では、予測が古くなったとして、この記述は削除されました。

なお、東日本大震災での電力不足の教訓から本番サイトとバックアップサイトは異なる電力会社の管内に設置することを提案している機関もあります。

## (2) 災害に対応した設備機器の設置

火災、風水害、地震は情報システムの停止につながる主要な脅威です。本項ではこれら災害に対する設備機器の設置対策を検討します。検討対象は、情報システム機器（サーバなどのホスト系機器）になります。

### <火災対策>火災の原因となるものの持ち込み禁止、消火器の設置等

- ・情報システム機器の設置室には、火気類は持ち込まない。
- ・情報システム機器の設置室には、危険物を貯蔵しない。
- ・情報システム機器の設置室には、燃焼設備（ガス湯沸器など）を設けない。
- ・情報システム機器の設置室には、消防法に適合した消火器を設置する。

### <風水害対策>十分な防水／排水施工を施した建物への機器の設置等

- ・情報システム機器は、十分な防水対策を施した建物に設置する。
  - ①屋根・外壁及び窓は、防水施工とする。
  - ②屋根・外壁などを貫通する吸排気口・ダクト・配管の周りは防水施工とする。
- ・排水口・配管などには、目詰まりや逆流の防止対策を施す。

### <地震対策>新耐震基準を満たした建物内への機器の設置、又は機器固定

- ・情報システム機器は、建築基準法の新耐震基準（1981年に強化された耐震基準）を満たした建物に設置する。
- ・情報システムの機器は転倒しないよう、以下の対策を実施する。
  - ①サーバ本体や格納されたラックは建物等に固定する。  
(アンカーボルト、吸着板など)
  - ②ラックに搭載した機器は固定し、落下を防止する。

※より高度な設備機器については参考資料 75 ページをご覧ください。



#### 情報機器の固定

日本倉庫協会が東日本大震災後に行った実態調査でも、サーバラックなどをアンカーボルトによる機器の固定で、実際に転倒を防止することができたとの報告は数多くありました。機器やデータを破損から守るだけでなく、機器の転倒・移動による怪我や物損などの2次被害を防ぐためにも、比較的lowコストで実施できるアンカーボルトや吸着板の固定処置は必ず実施しておきましょう。

### (3) 電源対策

情報システムの安定稼働のためには電源対策は必ず実施します。

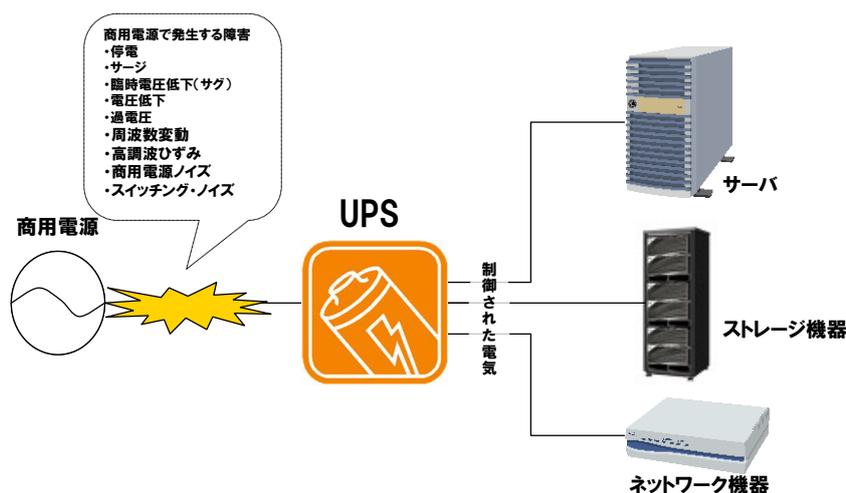
また、対策に当たっては電源供給停止や落雷などの影響で一時的に電圧が変動することへの対策など電源品質の安定化対策も考慮に入れておく必要があります。

#### 【対策例】 無停電電源装置（UPS : Uninterruptible Power Supply）

UPSは、バッテリーを搭載しており、急に電源が停止したり電圧の変動があったりしても短時間であれば、情報システムの各機器に安定的に電源を供給することができる装置です。【図 12】

商用電源と各機器の間に設置され、瞬断やごく短時間の停電であれば稼働を継続できますし、10分間程度の電力供給が可能のため、安全に情報システムを停止することができます。停電対策、雷などの異常電圧などの対策としても必須の機器と言えます。

<参考>UPSが機器に電力を供給できるのは一般的には10分程度です。また、バッテリーは時間の経過と共に劣化が進むため、定期的に点検を行い、有効な電力が供給できるよう保守しておくことが重要です。



【図 12】 無停電電源装置（UPS）

※より高度な電源対策については76ページをご覧ください（より高度な電源対策は、電力会社の計画停電〔輪番停電〕対策としても有効です）。



#### 災害時に電源の確保に困ったら

倉庫業者ならではの方法として、バッテリーフォークやトラックの蓄電池と発電機の活用があります。一時的なものですが、急場しのぎとして活用できます。

直流から交流への切替はDC/ACインバーターを備えておくことで対応できます。

### (4) 二重化・冗長化

予防対策には、以上のほか「二重化・冗長化」がありますが、これ自体が高度な対策となるためここでは省略します。（但し、参考資料（77ページ～）で紹介しています。）

### 3.3.2 復旧対策

復旧対策とは、災害や事故によってITサービスが停止した際に、速やかに通常の状態に戻すための事前準備をいいます。復旧対策は、予防対策では防ぎきれなかった事態に対応するために準備するもので、重要業務の復旧時間に大きくかかわります。ここでは、復旧対策で不可欠な「場所」、「機器」、「要員」に関する対策方法に絞って紹介します。

#### <記載例 26> 復旧対策一覧（推奨される主要なもの）

対策項目	対策内容
(1) 代替サイト	コールドサイト
(2) 代替機器	クライアント環境
(3) 代替要員	代替要員の決定

#### (1) 代替サイト

代替サイトとは、現在の場所で情報システムが稼働できなくなった時、新たな場所に情報システムを設置し稼働させる場所で、本番時の“代わりになる場所”のことを言います。自社内で場所だけを確保する場合と、稼働に必要な機器類を予め設置しておく場合では復旧に要する時間は大幅に異なります。以下にレベル毎の代替サイトの考え方についてご紹介します。

代替サイトの一種にコールドサイトと呼ばれるものが有ります。これは、情報システムを稼働させるために最低限な資源（電源、空調、区画など）を設備した場所のことです。有事の時には、サーバなどの主要な機器を移設したり、調達したりして情報システムの機能を復旧させることができます。

現実的には、資金に余裕がある企業でないと、情報システム専用の代替サイトを準備しておくことは困難と思われるますが、最低限、代替サイトとして活用できそうな場所（会議室やオフィスの片隅など）を予め決定し、明文化しておくことは必要です。

なお、より高度な対策（ウォームサイト、ホットサイト）については80ページの参考資料をご覧ください。

#### (2) 代替機器

情報システムの機器の調達には、時間がかかります。災害時にはなおさらです。予め代替機器を準備しておくことで復旧時間の短縮を図れます。

##### ①クライアント環境

クライアントPCやハンディターミナルなどは、サーバやネットワークに比べると機器1台当たりの調達コストは小さく、リース切れの機器を再リースし代替機器として準備しておくことは比較的容易です。現状の調査結果をもとに最低限必要な台数を予め準備しておくことが望まれます。準備する機器としては、以下のものがあります。

- ・PC本体（キーボード、マウス、HDD含む）
- ・ディスプレイ
- ・プリンタ
- ・電話／ファクシミリ

- ・業務用端末（荷主端末、ハンディターミナルなども含む）
- ・記録媒体読み取り装置（DVD用、磁気媒体用など）ほか

## ②ネットワーク機器

現在では、ネットワークなしでは業務は遂行できません。ネットワーク機器についても、予め代替機器を準備しておくことが望ましいといえます。

準備する機器としては、以下のものがあります

- ・ルータ
- ・スイッチ
- ・ファイアウォール
- ・HUB
- ・LANケーブル
- ほか

## (3) 代替要員

事業継続において、要員不足は大きな阻害要因になります。情報システムを使用できる状態に復旧するためには、情報システムの運用要員は欠かせません。有事の時は、情報システムの担当者が出勤できなくなったり、連絡がつかなくなったりすることを前提に必要な対策を検討します。

### ①代替要員の決定

代替となりうる者を要員に定め、体制図や役割分担票で役割を明文化しておきます。

明文化の方法は、「3.2 要員確保と復旧体制のための対策を検討する」（46 ページ）を参照してください。

### ②手順書の整備

要員不在であってもシステムの運用が図れるよう、情報システムの手順書（日常的なオペレーション）は整備しておきましょう。

代表的な手順書には以下の様なものがあります。

#### [オペレーションマニュアル]

文書	内容
システム操作マニュアル	各ハードウェア、ソフトウェアの起動・停止手順
システム保守マニュアル	修正パッチなどの環境更新手順等
システム障害対応マニュアル	発生頻度の高いシステム障害時の対応手順等
バックアップ手順書	バックアップ設定、バックアップ手順説明等
リストア手順書	リストア（データの復旧）手順説明等
オペレーションチェックリスト	日常オペレーションに関するチェックリストなど

#### [媒体管理]

文書	内容
バックアップ媒体一覧表	バックアップ媒体の管理台帳等
インストール媒体一覧表	OSや業務ソフトウェアのインストール媒体の管理台帳等

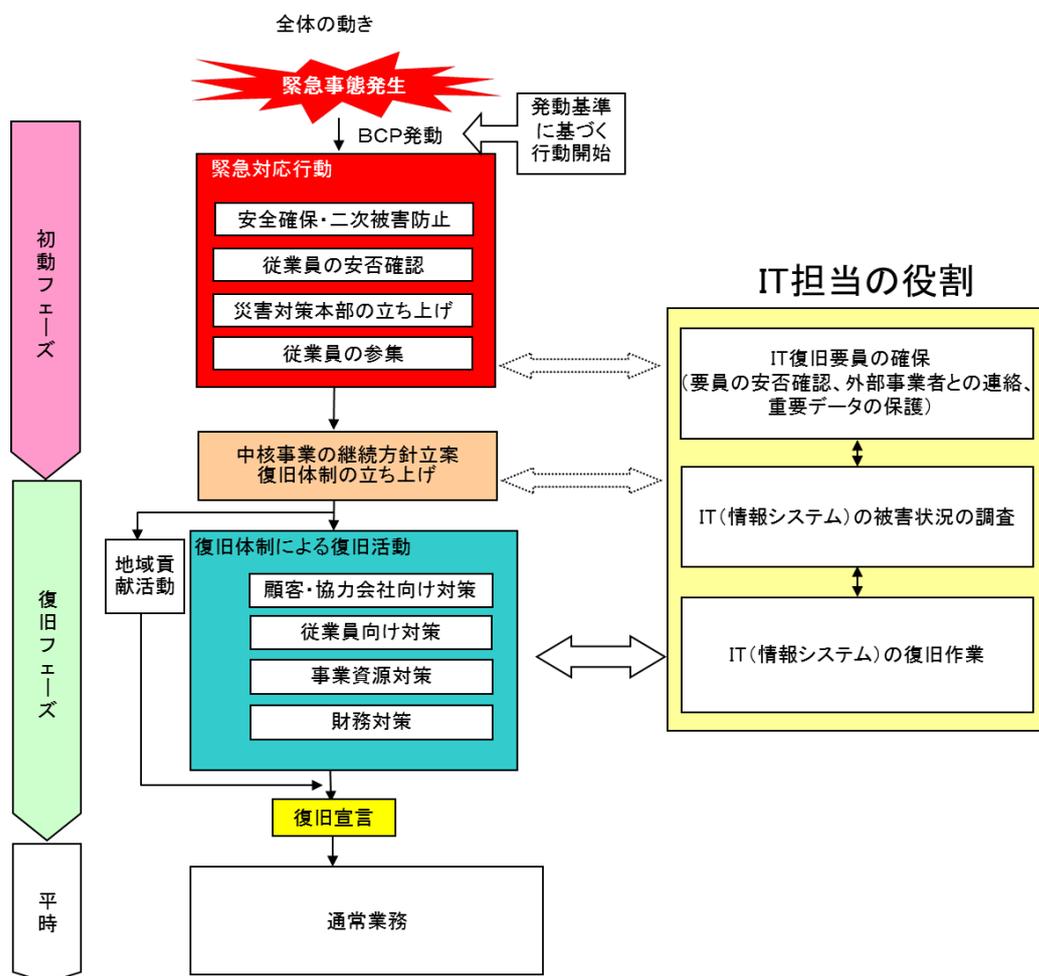
有事の時の対応手順は、まずは「緊急行動チェックリスト」を整備し、訓練を通じて追加に必要な手順を整備していくことが望まれます。

## Ⅱ-4 緊急時行動計画を整備する

有事におけるIT担当の役割は、復旧要員を確保した上で情報システムの被害状況を調査・整理し、災害対策本部と情報共有しながら、情報システムの機能を復旧させることです。有事の際は、IT担当を含む各部署が混乱状況に陥るため、スムーズに復旧活動を実施することは難しいものです。冷静に対応するためには、緊急時行動計画を予め決めておく必要があります。

行動計画としては、①緊急時の行動を確認しながら進めるための「行動チェックリスト」と、②復旧の方向性を決める上で重要な判断材料となる被害状況をまとめるための「被害状況チェックリスト」の2種類を最低限作成しておくとい良いでしょう。

次頁以降に掲載した「行動チェックリスト（標準）」、「被害状況チェックリスト」を元に自社の環境にあった行動計画を作成します。



【図13】 全社の動きとIT担当の役割

#### 4.1 I T 復旧に向けた行動チェックリスト（標準）

本項で記載した内容は、I T 担当に焦点を絞って作成したものです。各情報システムの個別の復旧手順は、メーカーやOS、パッケージなどによって大きく異なりますので、各社の状況にあわせたチェックリストを作成してください。なるべく事前に作成しておき、I T 担当以外の方でも復旧作業に当たることができるようにしておくことが必要です。

##### <記載例27> 【初動&復旧フェーズ】 I T の被害状況の調査と復旧活動

###### 就業時間中（社内）に発災

#	アクション	チェック	補足
1	<b>IT担当メンバーの安否確認:</b> <input type="checkbox"/> 避難の必要がなく、負傷者救護、二次被害防止の対応が落ち着いたタイミングで、リーダーは、I T 担当メンバーの安否状況を確認する。 <input type="checkbox"/> 外出者や休暇中のメンバーがいる場合は、固定電話、携帯電話又は携帯メール等で連絡がつく範囲で安否確認を行う。ただし、至急連絡を取る必要がなければ、ある程度落ち着いてからでもよい。 <input type="checkbox"/> 確認結果は、災害対策本部に報告する。途中経過でも構わない。時間の定めがない場合は、災害対策本部の立ち上げを見計らって第一報を上げる。		「被害状況チェックリスト」62 ページ参照
2	<b>重要書類・データ類の保護:</b> <input type="checkbox"/> 建屋の損傷で漏水等が懸念されるなど、フロアから退去が必要な場合、重要書類、バックアップ媒体等が損傷するおそれのある場合は、(危険が迫り至急避難する場合を除いて) それらを建屋内の安全な場所に移動させるか、建屋外へ持ち出す。		
3	<b>外部事業者(ITベンダー等)との連絡確保:</b> <input type="checkbox"/> 至急対応を要請すべき外部事業者 (I T ベンダー等) との連絡手段を確保する。(固定電話、メール、災害対策本部の災害時優先電話、携帯電話、携帯メールなど) <input type="checkbox"/> 必要によっては、社員・外部事業者による直接の移動(状況によっては自転車等を利用)などあらゆる手段を講ずる。 <input type="checkbox"/> 緊急連絡先一覧を参照して、外部事業者と連絡を取り、被害状況調査や復旧活動への協力を要請する。		「緊急連絡先一覧」48 ページ参照
4	<b>被害状況の調査:</b> <input type="checkbox"/> 被害状況チェックリストを使用して情報システム、インフラに関する被害を確認し、災害対策本部に必要な報告を行う。 <input type="checkbox"/> 倒壊の危険がある建屋、二次被害が発生している場所がある場合、I T 担当は、入館可能かどうか災害対策本部に確認する。 <input type="checkbox"/> 被害状況は時間の経過により変化するため、継続的に状況把握を行う。		「被害状況チェックリスト」62 ページ参照
5	<b>復旧活動の開始:</b> <input type="checkbox"/> リーダーは、被害状況及び要員の参集状況を考慮して、どのような情報システムの復旧活動を開始するかを判断する。 <input type="checkbox"/> 全社の災害対応、復旧活動と整合を取りつつ、I T 担当メンバーに情報システムの復旧作業を指示する。		

#	アクション	チェック	補足
6	<b>復旧活動の実施:</b> <input type="checkbox"/> IT担当メンバーは、復旧作業を実施する。 <input type="checkbox"/> 復旧作業の進捗状況は、定期的（2～6時間毎）に報告し、災害対策本部および関係部署と情報共有しておく。		
7	<b>復旧活動の完了報告:</b> <input type="checkbox"/> リーダーは、各システム毎の復旧が完了した時点で、災害対策本部および関係部署に連絡し、復旧完了を報告する。		

#### 就業時間中（社外）に発災

#### 就業時間外（休日・早朝・夜間など）に発災

#	アクション	チェック	補足
1	<b>自身および家族の安否確認:</b> <input type="checkbox"/> 災害・事故発生時においては、自身及び家族の安全の確認後、自宅の火災発生などの二次被害の防止策を講じた上で、自動参集対応に入る。 <input type="checkbox"/> 速やかに上司や社内関係者に連絡を取り、可能であれば出勤できる時間の目安も伝える。すぐにつながらない場合には、暫く待って連絡を試みる。 <input type="checkbox"/> 自身又は家族が負傷した場合や自宅が大きく被災した場合は、参集できない旨を連絡する。		「被害状況チェックリスト」 62 ページ 参照
2	<b>自動参集対応:(自身や家族の安全が確保され、自宅などの被害がなく参集が可能な場合のみ)</b> <input type="checkbox"/> 情報システムが設置してある場所が、震度〇以上の地震の場合、全員が自動参集する。当該場所の震度が確認できない場合は、近隣の震度から想定して、確実に問題ない場合を除き、原則として参集を開始する。 <input type="checkbox"/> 参集に当たっては、通勤途上の安全に配慮し、靴、服装などに留意する。また、水、食糧を持参するよう努める。 <input type="checkbox"/> 以下のケースのように自動参集すべきか判断に迷う場合は、災害対策本部の指示に従う。 <input type="checkbox"/> 集合場所までの距離があり、公共交通機関が途絶している場合 <input type="checkbox"/> 自宅周辺及び参集途上において、救助の必要がある被害者がいる場合		
3	<b>IT担当メンバーの参集状況及び安否確認:</b> <input type="checkbox"/> 出社後、IT担当メンバーの参集状況及び未参集者の安否確認を行う。 <input type="checkbox"/> 安否の確認がとれないメンバーがいる場合は、固定電話、携帯電話又は携帯メール等で継続して安否確認を行う。ただし、至急連絡を取る必要がなければ、ある程度落ち着いてからでもよい。 <input type="checkbox"/> 確認結果は、災害対策本部に報告する。途中経過でも構わない。時間の定めがない場合は、災害対策本部の立ち上げを見計らって第一報を上げる。		「緊急連絡先一覧」 48 ページ 参照

#	アクション	チェック	補足
4	<b>重要書類・データ類の保護:</b> <input type="checkbox"/> 建屋の損傷で漏水等が懸念されるなど、フロアから退去が必要な場合、重要書類、バックアップ媒体等が損傷するおそれのある場合は、(危険が迫り至急避難する場合を除いて) それらを建屋内の安全な場所に移動させるか、建屋外へ持ち出す。		
5	<b>外部事業者(ITベンダー等)との連絡確保:</b> <input type="checkbox"/> 至急対応を要請すべき外部事業者 (ITベンダー等) との連絡手段を確保する。(固定電話、メール、災害対策本部の災害時優先電話、携帯電話、携帯メールなど) <input type="checkbox"/> 必要によっては、社員・外部事業者による直接の移動(状況によっては自転車等を利用) などあらゆる手段を講ずる。 <input type="checkbox"/> 緊急連絡先一覧を参照して、外部事業者と連絡を取り、被害状況調査や復旧活動への協力を要請する。		「緊急連絡先一覧」 48 ページ参照
6	<b>被害状況の調査:</b> <input type="checkbox"/> 被害状況チェックリストを使用して情報システム、インフラに関する被害を確認し、災害対策本部に必要な報告を行う。 <input type="checkbox"/> 倒壊の危険がある建屋、二次被害が発生している場所がある場合、IT担当は、入館可能かどうか災害対策本部に確認する。 <input type="checkbox"/> 被害状況は時間の経過により変化するため、継続的に状況把握を行う。		「被害状況チェックリスト」 62 ページ参照
7	<b>復旧活動の開始:</b> <input type="checkbox"/> リーダーは、被害状況及び要員の参集状況を考慮して、どのような情報システムの復旧活動を開始するかを判断する。 <input type="checkbox"/> 全社の災害対応、復旧活動と整合を取りつつ、IT担当メンバーに情報システムの復旧作業を指示する。		
8	<b>復旧活動の実施:</b> <input type="checkbox"/> IT担当メンバーは、復旧作業を実施する。 <input type="checkbox"/> 復旧作業の進捗状況は、定期的(2~6時間毎)に報告し、災害対策本部および関係部署と情報共有しておく。		
9	<b>復旧活動の完了報告:</b> <input type="checkbox"/> リーダーは、各システム毎の復旧が完了した時点で、災害対策本部および関係部署に連絡し、復旧完了を報告する。		

## 4.2 被害状況チェックリストを作成する

混乱した状況の中で情報システムの被害状況を把握するために、確認すべき項目を「被害状況チェックリスト」（記載例 28 次ページ参照）に整理しておきます。

主要な確認項目は以下の様なことが挙げられます。

### (1) 要員・ライフライン等

- ・要員：安否状況（死傷者、行方不明者）、会社に参加可能な人数など
- ・ライフライン等：情報システム稼働に不可欠な電気・ガス・水道の供給状況など
- ・交通網：電車、バス、幹線道路の状況など

### (2) 建屋・付帯設備

- ・建屋：物理的被害の状況や入館可能かどうか
- ・電源設備：停電の有無、配電盤・ブレーカーの稼働状態、UPS 装置の稼働状況など
- ・空調設備：空調機器の稼働状況（冷却温度異常、圧力異常、漏水の有無など）
- ・通信設備：交換機、データ通信設備（主にWAN）などの稼働状況

### (3) 情報システム関連機器

- ・サーバ系機器：物理的損傷、稼働状況（異常ランプ状況）  
→ここではハードウェアとしての機能の状況を確認。システムの稼働状況（アプリケーションの稼働状況を含む）は、システム毎に確認する。
- ・ネットワーク機器：主に構内ネットワーク（LAN）に関する機器類の物理的損傷・稼働状況
- ・クライアント機器：PCや業務端末（ハンディターミナルなど）の物理的損傷、稼働状況
- ・データ類（ハードディスク装置）：サーバとは独立したストレージ機器などのハードディスク装置の物理的損傷、稼働状況
- ・データ類（可搬型媒体）：磁気テープ、CDなどの可搬型媒体の物理的損傷

<記載例 28> 被害状況チェックリスト

状況確認日時 年 月 日 時 分 現在

分類	項目	被害	確認方法
要員安否	死者		就業時間内は点呼で、時間外は電話簿を使用して確認する。 就業時間内の場合は来客、外部要員及び帰宅・休職要員の安否も合わせて確認すること。 死者、行方不明者、負傷者に該当者がいる場合は、氏名も記録すること。 参集者の氏名も参考として記入する。
	行方不明者		
	負傷者		
	IT担当メンバーの参集者(在勤者)		
	参集可能と連絡がとれた者		

分類	項目	被害レベル			被害なし	確認方法
		大	中	小		
ライフライン	電気	<input type="checkbox"/> 全面停電	<input type="checkbox"/> 大部分停電	<input type="checkbox"/> 一部停電	<input type="checkbox"/> 被害なし	災害対策本部(事務局)が把握している情報を確認する。
	ガス	<input type="checkbox"/> 全面停止	<input type="checkbox"/> 大部分供給停止	<input type="checkbox"/> 一部供給停止	<input type="checkbox"/> 問題なし	
	水道	<input type="checkbox"/> 全面停止	<input type="checkbox"/> 大部分供給停止	<input type="checkbox"/> 一部供給停止	<input type="checkbox"/> 問題なし	
	電網	<input type="checkbox"/> 全面運行停止	<input type="checkbox"/> 大部分運行停止	<input type="checkbox"/> 一部運行停止	<input type="checkbox"/> 問題なし	
	バス	<input type="checkbox"/> 全面運行停止	<input type="checkbox"/> 大部分運行停止	<input type="checkbox"/> 一部運行停止	<input type="checkbox"/> 問題なし	
交通網	幹線道路	<input type="checkbox"/> 全面通行停止	<input type="checkbox"/> 大部分通行停止	<input type="checkbox"/> 一部通行停止	<input type="checkbox"/> 問題なし	災害対策本部(事務局)が把握している情報を確認する。
	建物(物理的被害)	<input type="checkbox"/> 全壊	<input type="checkbox"/> 大部分損壊	<input type="checkbox"/> 一部損壊	<input type="checkbox"/> 問題なし	
	建物(入館可能か否か)	<input type="checkbox"/> 全面入館不可	<input type="checkbox"/> 大部分入館不可	<input type="checkbox"/> 一部入館不可	<input type="checkbox"/> 入館可	
	コンピュータ室	<input type="checkbox"/> 全面入館不可	<input type="checkbox"/> 大部分入室不可	<input type="checkbox"/> 一部入室不可	<input type="checkbox"/> 入室可	
	電源設備	<input type="checkbox"/> 全損・稼働不可	<input type="checkbox"/> 大部分損傷	<input type="checkbox"/> 一部損傷	<input type="checkbox"/> 問題なし	
情報システム関連機器	空調設備	<input type="checkbox"/> 全損・稼働不可	<input type="checkbox"/> 大部分損傷	<input type="checkbox"/> 一部損傷	<input type="checkbox"/> 問題なし	目視で外観上の破損、異常ランプの点灯、出火、漏水、異音などがないかを確認する。被害がある建屋内に入る場合は、できる限り複数名で行動すること。
	通信設備(交換機)	<input type="checkbox"/> 全損・稼働不可	<input type="checkbox"/> 大部分損傷	<input type="checkbox"/> 一部損傷	<input type="checkbox"/> 問題なし	
		<input type="checkbox"/> 全面入館不可	<input type="checkbox"/> 大部分入室不可	<input type="checkbox"/> 一部入室不可	<input type="checkbox"/> 入室可	
		<input type="checkbox"/> 全損・稼働不可	<input type="checkbox"/> 大部分損傷	<input type="checkbox"/> 一部損傷	<input type="checkbox"/> 問題なし	
		<input type="checkbox"/> 全損・稼働不可	<input type="checkbox"/> 大部分損傷	<input type="checkbox"/> 一部損傷	<input type="checkbox"/> 問題なし	
情報システム稼働状況		<input type="checkbox"/> 稼働不可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 問題なし	システム単位に稼働状況を確認。 ・コンソールに異常メッセージが出力されていないか ・端末から接続可能か
		<input type="checkbox"/> 稼働不可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 問題なし	
		<input type="checkbox"/> 稼働不可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 問題なし	
		<input type="checkbox"/> 稼働不可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 問題なし	
		<input type="checkbox"/> 稼働不可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 問題なし	
		<input type="checkbox"/> 稼働不可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 問題なし	
		<input type="checkbox"/> 稼働不可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 問題なし	
		<input type="checkbox"/> 稼働不可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 問題なし	
		<input type="checkbox"/> 稼働不可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 問題なし	
		<input type="checkbox"/> 稼働不可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 部分的に稼働可	<input type="checkbox"/> 問題なし	

## Ⅱ－5 訓練の実施

### 要員の安否確認、バックアップデータの確認、非常用設備の稼働

有事では、初動対応が非常に重要です。「要員の安否確認」は、必ず訓練を実施しましょう。

また、情報システムの復旧作業に欠くことが出来ない事項として、「バックアップデータの確認」と「非常用設備の稼働」の訓練は定期的の実施しましょう。

訓練は、計画的かつ継続的に対象や手法を見直しながら実施することが必要です。

(「第一章2.5.2 BCP定着と事前対策の実施」19ページ参照)

<記載例29> <訓練計画(全社例の一部 IT部門に関するもの)>

区分	項目	対象	実施単位	方法	時期	頻度
訓練	IT復旧訓練	情報システム部 経理部・倉庫部	部門単位	実地	5月	年1回

訓練事項	訓練の狙い	適した手法
安否確認	<ul style="list-style-type: none"> <li>安否確認の手順は従業員に周知されているか?</li> <li>安否確認にどの程度時間がかかるか?</li> </ul>	机上訓練 実地訓練
バックアップデータの確認	<ul style="list-style-type: none"> <li>バックアップは正しく取得できているか?</li> <li>バックアップ媒体の保管場所は明らかになっているか?</li> <li>バックアップデータは利用可能か? (データの復旧テストができるベスト)</li> </ul>	実地訓練 <small>※本番作業の結果確認や本番用のバックアップ媒体の目視確認なども含まれます</small>
非常用設備の稼働	<ul style="list-style-type: none"> <li>非常用設備を稼働する手順は周知されているか?</li> <li>非常用設備は正常に稼働するか?</li> </ul> <非常用設備> 非常用電源、代替コンピュータ機器など	実地訓練

<補足>

<記載例 30> 訓練チェックリスト

【表3-16-2】技術訓練チェックリスト様式例(バックアップリストア訓練の場合)

行動	担当者	想定作業時間	作業開始時間	作業完了時間	結果備考
1 代替サーバへの電源投入		1分	:	:	
2 コンソールにエラーが表示されないかを確認する。		5分	:	:	
3 BIOSおよびファームウェアのバージョンを確認する。		5分	:	:	
4 OS立ち上げ成功の確認		5分	:	:	
5 イベントビューアーの確認		10分	:	:	
6 サーバの名称を本番用名称もしくはテスト用名称に変更する。		10分	:	:	本番ネットワーク環境に接続する場合は、本番用名称には変更しないこと
7 ネットワークへの接続状況の確認		10分	:	:	
8 セキュリティパッチを適用する。		30分	:	:	
9 代替サーバを本番用ドメインに参加させる。		10分	:	:	
10 ディスクドライバの整合性チェック		5分	:	:	
11 以下のソフトウェアをインストールする。 -ウィルスチェックソフト -RAIDマネージャー -ミドルウェアのクライアントソフト など		60分	:	:	
12 最新の状態に戻すために、どのバックアップテープに戻す必要があるかを確認する。		30分	:	:	
13 *ドライブのデータをリストアする。		24時間	:	:	
14 ネットワークプリンタを登録する。		30分	:	:	
15 書き込み、読み込み権限の設定を行う。		60分	:	:	
16 ネットワークプリンタでテスト印刷を実施する。		10分	:	:	
17 *ドライブへのアクセスをテストする。 (*ドライブの**ファイルにアクセスできるか確かめる)		10分	:	:	
18 責任者への作業完了報告		5分	:	:	
19 データを全て削除する。 (インストールしたOSとRAID構成はそのままでも良い)		30分	:	:	後作業(必ず実施すること)
20 本番用ドメインから切り離す。					後作業(必ず実施すること)
21 データボリュームを完全に削除する。:					後作業(必ず実施すること)
22 代替サーバの電源消去:					後作業(必ず実施すること)

補足:各プロセスに要した時間や問題点を記録しておくようにする

総務省「地方公共団体における ICT 部門の業務継続計画策定に関するガイドライン(平成 20 年 8 月)」より引用



運用の不徹底がまねくデータ消失

日本倉庫協会が東日本大震災後に行った実態調査では、データ保全環境が整えられていながら、バックアップの運用が不徹底であったことから、データが消失してしまったケースが報告されています。

この会社では、重要なデータは、日々、各社員の PC からサーバへの転送が義務付けられていましたが、一部でその運用が守られていませんでした。そのような中、震災が発生し、クライアントのデータが壊滅的な被害をうけました。通信網は2週間が経過しても復旧されないことから、サーバ内にあるデータを使用して復旧作業を始めることとなりましたが、サーバには、殆どデータが保存されていない業務があり、復旧には多大な労力を強いられました。

地震・津波・火災等の自然災害に備えた対策がシステムの構築されていても、従業員のデータ保全に対する意識が低いと意味がなくなってしまいます。データバックアップの社内規定を周知させるだけでなく、バックアップデータにより復元テストなどの訓練を重ねることでより実践的な災害対応力が醸成されます。

前述の会社では今回の経験を踏まえ、情報資産としてのデータ管理の徹底を強固なものに再構築しています。また、ベンダーの協力のもと、2日以内に業務が再開できるよう定期的なテストも実施するようにしたとのことです。

## Ⅱ－６　ＩＴ部門の事業継続計画書としてまとめる

第Ⅱ章ではＩＴに関する災害対策を含め、事業継続計画書の作成の仕方について説明してきました。これらを参考に事業者の皆様ご自身で事業継続計画書としておまとめ下さい。

なお、日本倉庫協会では、事業者の皆様が簡便に計画書を作成いただけるよう「事業継続計画書（ＢＣＰ）作成のてびき」（本紙）、モデル、ひな形・様式を日本倉庫協会ホームページ（<http://www.nissokyo.or.jp/>）の会員専用サイトに掲載しています。ご自由にダウンロードし、自社の実情にあわせた形に変更してご活用ください。

ＩＴ部門における事業継続計画書の構成は以下のようになります。

### <構成>

#### １．情報システム環境一覧

- 情報システム一覧表（記載例 17）
- ネットワーク構成図（記載例 18）
- クライアント環境一覧表（記載例 19）
- バックアップ取得状況一覧表（記載例 20）

#### ２．情報システム復旧計画書

- 情報システム業務影響度調査表（記載例 21）  
（中核事業・重要業務・各システムの目標復旧時間）
- 全社事前対策計画（ＩＴ部門に関係するものの抜粋）（記載例 22）
- 緊急時対応体制図（組織図）及び役割分担表（記載例 23）
- 緊急連絡先一覧表（記載例 24）
- 予防対策一覧表（推奨される主なもの）（記載例 25）
- 復旧対策一覧表（推奨される主なもの）（記載例 26）
- 緊急時行動計画
  - 【初動フェーズ】全社緊急対応行動表（記載例 13）
  - 【初動&復旧フェーズ】ＩＴの被害状況の調査と復旧活動（記載例 27）
- 被害状況チェックリスト（記載例 28）
- 訓練計画表（記載例 29）
- 訓練チェックリスト（記載例 30）

<参考資料>



## 第 I 章 関係

### 1. 防災用物資の例とその備蓄量の目安

区分	物資の例	備蓄量の目安
飲料水	ペットボトル入り飲料水等	・従業員数×1.2ℓ×必要日数を備蓄 ※一般に飲料水は1人1日 1.2ℓが必要 (注1)
調理不要食品	アルファ化米、クラッカー等 ※アルファ化米は乾燥した米飯であり、水・お湯を加えて利用する ※乾パンは硬いため高齢者に適さないとされている	従業員数×3食×必要日数を備蓄 ※調理不要食品・簡易調理食品の組み合わせ方は各事業所で判断する
簡易調理食品	即席麺・レトルト食品等 ※調理用の水・カセットコンロの備蓄も必要となる	
食器	紙皿、紙コップ、割箸	従業員数×3個×必要日数を備蓄 ※1食につき1個を使用と想定
トイレ	簡易トイレ・携帯トイレ等 (注2) 仮設トイレは使用しない ※汚物収納袋、薬剤の備蓄も必要となる	従業員数 60 人当り1個を備蓄(注3) ・簡易トイレで使用する汚物収納袋と薬剤のセットは、1人1日当たり排泄回数を5回として(注4) 従業員数×5セット×必要日数を備蓄
トレットペーパー		従業員数×0.11ロール×必要日数を備蓄(注5)
寝具	寝袋・毛布・敷物	・寝袋は従業員数分 ・毛布と敷物はそれぞれ従業員数分 (注6)
暖房	ストーブ・使い捨てカイロ等	・ストーブは事業所規模・従業員数を考慮して備蓄 ・カイロは従業員数×必要日数を備蓄(注7)
炊事用具	鍋・カセットコンロ・点火用具(ライター等)等	事業所規模・従業員数を考慮して備蓄
医薬品	消毒薬、包帯、ガーゼ、絆創膏、三角巾、カット綿、胃腸薬、やけど薬、ピンセット等	従業員数を考慮し、医薬品販売事業者等と相談して決定

注1)「熱中症環境保健マニュアル」環境省 平成 21 年

※上記資料では、1人1日当りの水分摂取量を計 2.5ℓとし、その内訳を食事から 1.0ℓ、体内で作られる水 0.3ℓ、飲み水 1.2ℓとしている。

注2) 仮設トイレは汲み取りとその処理の問題が生じるため使用しないものとした。

注3)「地震時におけるトイレ機能確保のための調査研究」NPOトイレ研究所 平成20年

注4)「帰宅行動シミュレーション結果に基づくトイレ需給等に関する試算について」内閣府 平成 20年

注5)「トイレットペーパーに関するアンケート調査」(クリーンネットサービス株式会社)において 1人1ヵ月平均 3.3 ロール使用とされていることから、1ヵ月を 30 日として1日当たり必要量を算出した。

注6) 毛布を1人当たり2枚備蓄し、1枚を敷物とすることも考えられる。

注7) 市販の使い捨てカイロの使用可能時間は通常 12 時間程度のため、1日1個が必要とした。

## 2. 防災用資器材の例

区分	資器材の例	備蓄量の目安
照明器具	懐中電灯（予備電池も用意）等	事業所規模・従業員数等を考慮し備蓄量を決定
情報収集機器	携帯ラジオ（手回し充電型及び電池利用型／電池利用型は予備電池も用意）、携帯電話、モバイルパソコン等	事業所規模・従業員数等を考慮し備蓄量を決定
連絡・通信用資器材	衛星電話、PHS、MCA無線、停電対応電話機、自転車、バイク等	事業所規模・従業員数等を考慮し備蓄量を決定
エネルギー確保用資器材	自家発電機、太陽電池式充電器等	事業所規模・従業員数等を考慮し備蓄量を決定
作業用具	スコップ、のこぎり、ハンマー、はしご、ロープ等	事業所規模・従業員数等を考慮し備蓄量を決定

### 3. 事業別目標復旧時間の設定

事業別目標復旧時間（RTO）の検討を行うに当たっては、「中核事業」及びそれに関連する「重要業務」、「情報システム」についてもRTOを設定する必要がありますが、そのためには、以下のような項目について調査・整理が必要です。

#### <調査・整理すべき項目>

- (1) 中核事業の目標復旧レベルの決定
- (2) 中核事業に関係する業務の洗い出し
- (3) 重要業務の特定と重要業務の目標復旧時間の設定
- (4) 重要業務と情報システムとの紐付け
- (5) 情報システムの目標復旧時間の設定

以下に調査・整理すべき項目毎の検討のポイントについて解説します。

#### (1) 中核事業の目標復旧レベル（RLO）の決定

RTOを決定する際は、必ず「目標復旧レベル」とセットで決定します。目標復旧レベルとは「業務をどの範囲まで復旧させるかの度合い（操業の水準）」のことで、RLO（Recovery Level Objective）ともいわれます。“機械稼働率”、“サービスを再開する顧客の範囲”など、様々な考え方がありますが、中核事業の絞り込みの範囲を、RLOとして捉えることもできます。例えば、第一章「2.4 中核事業とその復旧目標を決める」（11ページ）の記載例で示したように復旧活動で目指す事業範囲のレベルがRLOとなります。

具体的には、

RTO：1週間以内、RLO：〇〇荷主事業の事業復旧の100%復旧

RTO：2週間以内、RLO：(〇〇荷主事業に加えて) ××荷主事業の100%復旧

となります。（下表の赤枠のとおり）

なお、倉庫業の場合の中核事業の切り口としては取引荷主の取引量、同保管貨物に求められる緊急度、営業所単位、倉庫棟単位などが考えられます。

○中核事業の絞り込みの範囲をRLOとした例

	中核事業	目標復旧時間
優先度Aの 目標復旧 レベル⇒	優先度：A 〇〇荷主事業 (取引量第1位)	建物全壊の場合 復旧見込み不明 建物一部損壊の場合 1週間以内に 100%復旧
優先度Bの 目標復旧 レベル⇒	優先度：B ××荷主事業 (取引量第2位)	建物全壊の場合 復旧見込み不明 建物一部損壊の場合 2週間後に 100%復旧

## (2) 中核事業に関する業務の洗い出し

中核事業の復旧レベルが決まったら関連する業務の洗い出しを行います。

### ・中核事業に関する業務が一部に限定される場合：

調査開始段階から、中核事業に関する業務だけを抽出して整理することも可能です。

### ・中核事業が多くの業務から成り立っている場合：

中核事業にとらわれず、まずは社内各部署で業務を洗い出した後に、中核事業との紐付けをした方がスムーズに行く場合があります。業務分掌などを元に調査を進めると漏れなく業務の抽出が出来ます。組織の規模に応じて柔軟に進めてください。

中核事業との関係は、3段階に分け、関係を整理します。以下の基準を参考に洗い出した業務をレベル分けします

◎：不可欠	(業務遂行なくして中核事業の復旧は不可能)
○：間接的に必要	(無くても業務遂行は可能だが、あると復旧はスムーズになる)
×：不要	(中核事業遂行には無くても問題がない)

43 ページの【図 8】の例だと下表のように表せます。

<優先度 A:○○倉庫事業 に関する業務>

部門	業務	中核事業との関係
倉庫部	業務 A	◎
販売部	業務 B	◎
経理部	業務 C	○
調達部	業務 D	×

## (3) 重要業務の特定と重要業務の目標復旧時間の設定

前述 (2) でレベル分けをした時、◎ (不可欠)、○ (間接的に必要) に該当する業務が中核事業に必要な『重要業務』となります。

これら重要業務のそれぞれについて復旧時間を設定します。重要業務の目標復旧時間を設定するときは、業務担当者の意見を求めることが必要です。“代替策の有無”や“他の業務との関係”を考慮に入れ、災害発生時を起点に最大この時間までには復旧しなければならないという時間を設定します。

代替策がある場合は、代替策でカバー可能な時間までが目標復旧時間になります。

他の業務との関係では、例えば、A業務 (復旧目標 3 日) ⇒ B業務 (必要日数 1 日) の順で業務遂行が行われる場合、B業務の目標復旧時間は 3 日 + 1 日 = 4 日になります。

しかし、あまり複雑に考えすぎると調査そのものが頓挫してしまいますので、当初は業務担当者の裁量で目標復旧時間を設定しても良いでしょう。

43 ページの【図 8】の例だと下表のように表せます。

<重要業務の R T O>

部門	業務	中核事業との関係	業務の R T O
倉庫部	業務 A	◎	3 日
販売部	業務 B	◎	4 日
経理部	業務 C	○	7 日

#### (4) 重要業務と情報システムとの紐付け

重要業務と情報システムの関係を整理します。整理の方法として、例えば、下表のように「重要業務」を縦軸に、「情報システム」を横軸に置き、当該業務が使用するシステムに“○”などのマークをします。

43 ページの【図 8】の例だと下表のように表せます。

重要業務	システム α	システム β	システム γ
業務 A	○		○
業務 B		○	○
業務 C			○

#### (5) 情報システムの目標復旧時間の設定

本項については、第二章「情報システムの目標復旧時間（R T O）を決める」の「情報システムの目標復旧時間の設定」をご覧ください（43 ページ参照）。

## 第Ⅱ章関係

### 1. 安否確認における効果の高い対策

#### (1) 通信手段の複線化

通信手段を複線化することで要員とのコミュニケーションの迅速化が図れます。例えば、東日本大震災では、固定電話や携帯電話に比べて、インターネットによる通信はつながりやすく、特にSNS※は効果があったとの報告もあります。各手段の長所、短所を考慮して、下表の中から複数の手段の導入を検討して下さい。

※SNS (Social Network Service) : 友人・知人間のコミュニケーションを円滑にする手段や場を提供したりするコミュニティ型のWebサイト。Facebook、GREE、mixi などが有名。

#### <通信手段として活用可能なツール（主要なもの）>

通信手段	長所	短所
災害用伝言ダイヤル (171 等)	PC/電話以外の新たな設備が不要	発信者・受信者双方の周知が必要 災害以外は使えない
固定電話 (一般電話)	普及率が高い	災害時通信規制でつながりにくい 電力供給が止まると使えない可能性が高い
IP電話	固定電話、携帯電話に比べるとつながりやすい	電力供給が止まると使えない可能性が高い
携帯電話	端末の普及率が高い	災害時通話規制でつながりにくい
携帯メール	端末の普及率が高い 通話に比べるとつながりやすい	災害時通信網輻輳で遅延が発生する
インターネットメール	端末(PC)の普及率が高い 通信規制・輻輳がない	電力供給が止まると使えない可能性が高い
SNS	通信規制・輻輳がない (携帯メール、PCメールに比べるとつながりやすい傾向あり)	ID管理が個人に依存する
衛星電話	災害時でもつながりやすい 音声・データ通信が可能	機器が高価 通話料金が高い
MCA無線	災害時でもつながりやすい 通話料金が不要	機器が高価

#### (2) 安否確認システムの導入

安否確認を目的に開発された「安否確認システム」は災害発生を一斉に同報したり、安否状況を一覧で確認したり、安否情報の整理・蓄積・活用の面で大きな効果があります。

かつては、ハードウェア（サーバ類）や専用ソフトウェア（パッケージソフト）を自前で準備して導入しなければならず、費用も高く、システムの運用に手間がかかる等のデメリットがありました。しかし、最近では、SaaS型の安否確認システムが提供され、コスト面、運用面でのデメリットが少なくなってきたことから、比較的導入し易くなりました。

従業員が多い、拠点数が多いなど電話やメールに頼った安否確認方法に不安がある企業にとっては非常に有効なツールといえます。

## 2. データバックアップにおける効果の高い対策

### (1) 広域ネットワーク経由での遠隔バックアップ

本番機が稼働するサイト※から離れた場所にある遠隔地サイトにバックアップデータを転送する方式です。【図 14】

バックアップ機器を自社で導入設置する方法とクラウド型サービスを活用する方法があります。バックアップサーバを経由して、遠隔地サイトにデータを送信する場合には、ネットワークの性能にも留意する必要があります。遅い回線の場合、データ送信に予想以上の時間がかかってしまい、通常業務にも影響するので、所要時間の見積りは厳密に行う必要があります。

※サイト：本来は敷地、用地などの意味。コンピュータ用語としては情報を提供するサーバを意味し、インターネットでは情報を提供するページやその集合のことをいう。

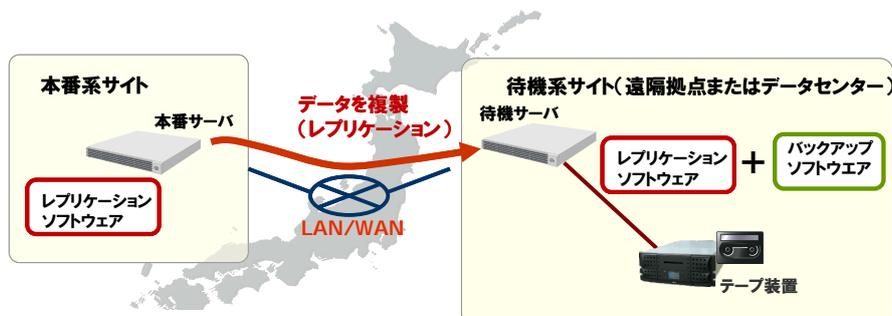


【図 14】広域ネットワーク経由の遠隔バックアップ方式

### (2) レプリケーション

レプリケーションとは、データベースと全く同じ内容の複製（レプリカ）を別のコンピュータ上に作成し、常に同期させることで目標復旧ポイントを限りなくゼロに近づける方式です。【図 15】

マスターデータ（複製のもとになるデータ）の更新情報を遠隔地サイトに送信するため、ネットワークの性能に留意する点は、広域ネットワークでの遠隔バックアップの場合と同様です。



【図 15】レプリケーション方式

### 3. 災害に対応した効果の高い設備機器の設置

#### <火災対策>

##### ○防火区画への機器の設置

- ・サーバ類は専用の部屋（防火区画内）に設置する。

##### ○不活性ガス消火設備

- ・情報システムを設置した部屋には、不活性ガス消火設備を設ける。

不活性ガス消火設備は、消火剤がガスの為、消火後の汚染が少なく、電気絶縁性と冷却効果に優れているため、情報システムへの影響を少なくすることができます。不活性ガスとして、人体に影響がある二酸化炭素を使用しないイナート系新ガス消火設備（IG-55～窒素とアルゴンの混合物～など）が推奨されます。

#### <風水害対策>

##### ○浸水しにくいフロアへの機器の設置

- ・2階以上に設置するか1階または地下に設置する場合は以下の対策を実施する。

- ①防水堤または防水扉
- ②排水設備

##### ○漏水検知

- ・情報システムを設置した部屋には、漏水検知措置を講じる。

#### <地震対策>

##### ○免震装置

- ・情報システムは、免震装置上に設置する。

情報システムの免震装置として代表的なのが、TCR（Tuned Configuration Rail）免震装置と呼ばれるもので、地震等の振動をレール・車輪間の抵抗力で軽減する装置です。

#### 【図 16】

本装置上にサーバラックなどを設置することで、サーバ自身にかかる揺れを抑えます。メーカー・機種によって性能は異なりますが、揺れを10分の1程度にまで抑えることができます。



【図 16】 免震装置

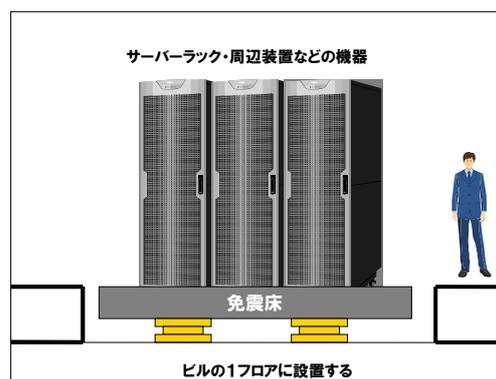
##### ○免震構造の建物や免震床への設置

- ・情報システムを免震構造のビル・建物に設置する。

免震ビルは、地震からの影響が直接建物に伝わらないように、地面と建物の上に免震装置を備えた建築物です。サーバラックの免震装置に比べて、建物全体が揺れから守られるので、ビル内の設備全般への被害が防止又は軽減されます。免震装置には、ゴムに減衰機能を持たせた「積層ゴム支承」や、内部の作動油という液体の力で揺れを押さえる「オイルダンパー」などがあります。

免震構造をビル全体ではなく、床面だけに応用した「免震床」も有効です。【図 17】

建物全体の改築が必要ないので、免震ビルに比べて低コスト・短期間で免震構造にすることが可能です。



【図 17】 免震床

#### 4. 効果の高い電源対策

##### (1) 非常用電源装置

非常用電源装置は、自家発電装置とも呼ばれ、軽油やA重油などを燃料とする発電装置です。【図 18】

非常用電源装置を企業独自で準備しておくことで、長時間の電源供給停止にも対応が可能です。電源供給可能時間は、装置に予め蓄えられた燃料の量と給油可能な状態で備蓄している燃料の量に依ります。データセンターなどの災害に強い建物に設置されているものでは、無給油で 24 時間～48 時間、備蓄した燃料で数日間の電源供給が可能なものがあります。

非常用電源装置が起動から電源供給可能な状態になるまで最低でも数分程度の時間が必要なことから、無停電にするためには、非常用電源に切り替わるまでUPSが電源を供給する構成にしておく必要があります。



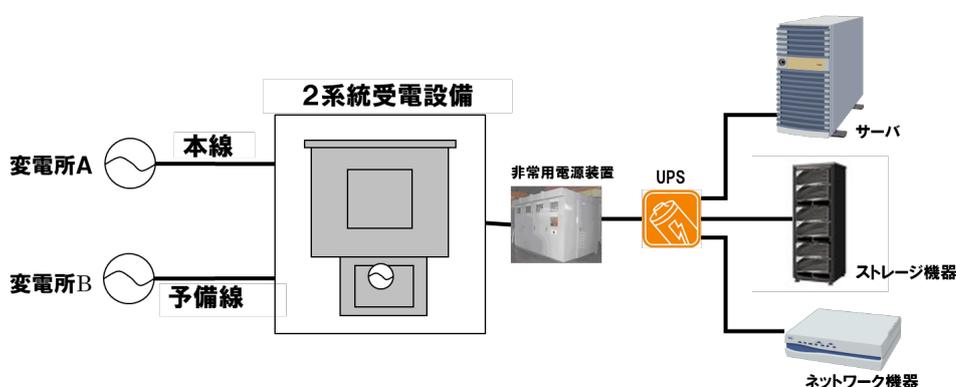
【図 18】 非常用電源装置

## (2) 2系統受電設備

2系統受電設備は、電力会社より異なる変電所から本線と予備線の2系統で受電し、どちらか一方の系統が停電した場合でも、ビル内の電力が供給されるよう設計された受電システムです。【図19】

2回線受電するための設備、回線を切り替えるための設備が必要になるため、1回線受電方式よりもコスト増になります。

2006年、東京の江戸川を航行するクレーン船が送電ケーブルに接触し、断線したために都内の一部と横浜市等が停電になる事故がありました。2系統受電であればこうした事故で本線からの送電が停止しても、予備線で電源供給が継続します。



【図19】 2系統受電設備

## 5. 二重化・冗長化

サーバやネットワークを二重化したり、冗長化※することで、一方の機器や回線が停止しても、残った機器で機能を補完・維持することができます。

IT継続対策として非常に効果が高い反面、機器やソフトウェアが二重に必要になり、コストが高くなりますので、IT継続の要件が高い業務システムの場合に導入を検討します。

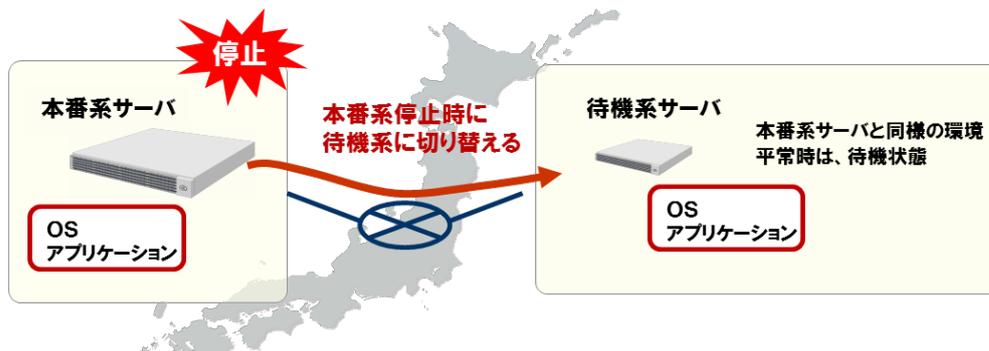
二重化・冗長化の対象や方式には様々なケースがありますが、本項では事前対策として特に重要と思われるサーバとネットワークについて代表的な方式を紹介します。

※冗長化：予備の設備・機器を用意しておき、故障してもサービスを継続して提供できるようにシステムを構築すること

### (1) サーバデュプレックス構成

デュプレックス (Duplex) 構成は、2系列のシステムを用意し、一方は現用系として本稼働させ、もう一方は待機系として現用系の障害に備えておくシステム構成です。【図20】

現用系のシステムに障害が発生した場合には、待機系のシステムに切り替えて処理を継続します。



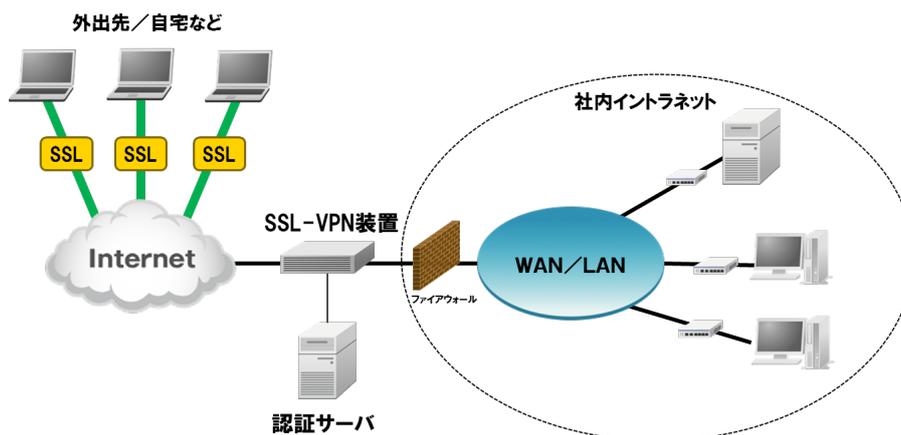
【図 20】 デュプレックス構成

## (2) ネットワークのリモート接続

インターネット回線、その他回線を介してサーバへのリモート接続を行えるよう環境を整えておく方式です。【図 21】

例えば、サーバが稼働しているにも関わらず、クライアントPCを設置している倉庫や営業所が災害に遭って構内LAN利用できない場合、別の営業所や自宅などからインターネット回線を利用して接続することで業務を継続することができます。

インターネットなどの公衆回線網に暗号化された仮想回線を構築し、企業の拠点間などを安全に結ぶ技術をVPN (Virtual Private Network) といいます。暗号化にSSL (Secure Socket Layer) を利用すると、主要なWebブラウザやメールソフトはHTTPSやPOP over SSLに対応しているため、イントラネットのWeb閲覧やメールの送受信などに活用できます。

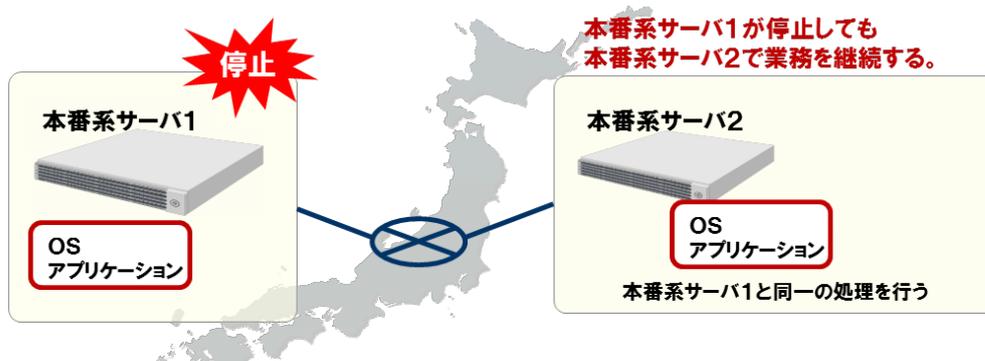


【図 21】 リモート接続の例

### (3) サーバデュアル構成

デュアル (Dual) 構成は、同じ処理を行うシステムを 2 系列用意し、一定時間ごとに処理結果の比較・照合を行う非常に信頼性の高いシステム構成です。【図 22】

どちらかの系列に障害が発生した場合には、その系列を切り離し、残りの系列で中断することなく処理を続行します。

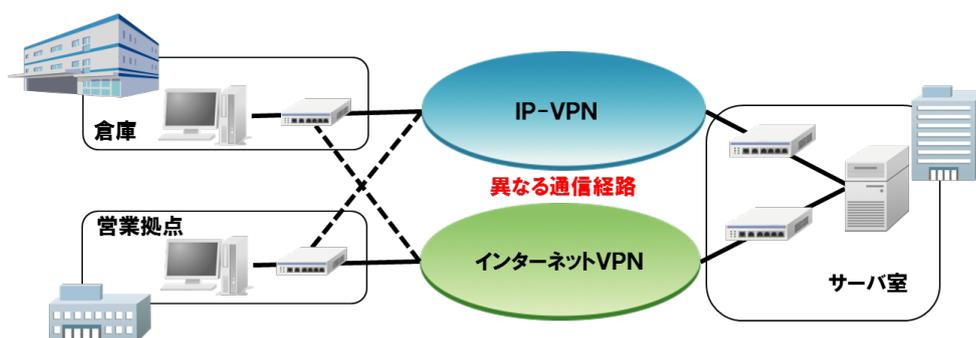


【図 22】 デュアル構成

### (4) ネットワークの冗長化

拠点間を異なる通信キャリアや異なる通信方式で結ぶことによって、災害時の通信機能停止に強い環境にする方法です。【図 23】

冗長構成モデルは、インターネット VPN、閉域型 VPN、IP-VPN や広域イーサネットといった異なるバックボーン（通信会社や通信サービス）を持ったネットワークを組み合わせます。どちらかのネットワークが停止しても片方のネットワークで通信を継続できます。



【図 23】 ネットワーク冗長化の例

## 6. 復旧対策における効果の高い対策

### (1) 代替サイト

#### ①ウォームサイト

ウォームサイトとは、遠隔地に設けた施設に本運用とほぼ同じシステムを導入し、非稼働状態で待機しておき、障害発生後にシステムを起動して運用を引き継ぐ方式です。サーバの構成としては、デュプレックス構成（77 ページ参照）となります。機器の準備に掛かる時間は不要ですが、情報システムの起動や本番業務に必要なデータの移行作業が必要になるため、その時間は復旧時間に含まれます。

#### ②ホットサイト

ホットサイトとは、本番システムと同じシステムを稼働させて常にデータの同期などを行いながら待機し、障害時に即座に切り替えられるようにする方式です。サーバの構成としては、デュアル構成（79 ページ参照）となります。常に本番環境が二重化されているので、情報システムの復旧に掛かる時間を限りなくゼロに近づけることができます。

### (2) 代替機器の準備

#### ○サーバ

サーバの調達には、時間が掛かります。代替機器を予め準備しておくことで目標復旧時間の短縮が可能です。サーバの代替機器をどこに設置しておくかは、代替サイトとの関係で考えなければなりません。代替サイトとあわせて検討する必要があります。準備する機器としては、以下のものがあります

- ・サーバ本体（キーボード、マウス、HDD含む）
- ・ディスプレイ
- ・プリンタ
- ・ストレージ（本体から独立したもの）
- ・記録媒体読み取り装置（DVD用、磁気媒体用など） ほか

### (3) 代替要員

#### ○代替要員の訓練

代替要員によるオペレーションを可能にするためには訓練が有効です。

予め整備したオペレーションマニュアルなどの手順書に従って訓練を実施します。

## 7. 効果の高い訓練

### ①被害状況把握

訓練が成熟してきたら、より被害想定に近い状況を設定した訓練を実施します。初動対応においては、安否確認と同時平行的に実施される「被害状況把握」を対象に加えます。

この訓練では、情報システムの稼動に必要な資源（建屋、電源、通信、情報システム機器など）の確認にとどまらず、組織全体の報告ルートや報告内容の妥当性も検証します。例えば、IT復旧メンバー⇒IT担当（リーダー）⇒災害対策本部といった情報の流れをロールプレイングなどの手法で時間を記録しながら訓練を行います。

さらに、実効性のある訓練として、以下のような訓練も検討してください。

- ・ 平時の要員以外での訓練
- ・ 情報システムの復旧訓練（データの復旧からサービス稼動まで）

訓練事項	訓練の狙い	適した手法
被害状況把握	<ul style="list-style-type: none"><li>・ 把握すべき対象に漏れはないか？</li><li>・ 報告ルートに混乱はないか？</li></ul>	机上訓練 実地訓練

### ②関係部門と一体になった訓練

IT復旧作業の最終的な狙いは、情報システム機能の回復だけではなく、情報システムが支える重要業務までを含めて復旧させることです。訓練の計画・実施においても、重要業務の再開を視野に、情報システムの利用者・利用部門を巻き込んだ訓練を実施することが望ましいといえます。

訓練対象	訓練の狙い	適した手法
IT担当部門	<ul style="list-style-type: none"><li>・ 情報システムの機能回復</li><li>・ 利用部門とのコミュニケーションに問題はないか？</li></ul>	実地訓練
利用部門 利用者	<ul style="list-style-type: none"><li>・ 情報システム部門とのコミュニケーションに問題はないか？</li><li>・ 情報システム停止時の対応手順に問題はないか？</li><li>・ 情報システム稼動後の作業手順に問題はないか？</li></ul>	

#### <商標について>

本てびきに記載されている会社名または製品名は、それぞれ各社の商標または登録商標です。

なお、本てびきでは、登録商標を表す TM (Trade Mark) 及び ® (Registered Trademark) は明記していません。

#### <参考文献>

【中小企業庁】中小企業BCP策定運用指針

【経済産業省】事業継続計画（BCP）策定ガイドライン（第二版）

【経済産業省】ITサービス継続ガイドライン

【総務省】地方公共団体におけるICT部門の業務継続計画（BCP）策定に関するガイドライン

【財団法人 日本規格協会】事業継続マネジメント（BCM）構築の実際

発行日 平成25年4月 第1版

一般社団法人 日本倉庫協会

〒135-8443 東京都江東区永代1丁目13番3号

電話 (03) 3643-1221

FAX (03) 3643-1252