# IT-BCP 策定モデル

平成 25 年 6 月

内閣官房情報セキュリティセンター

本調査は、「東日本大震災を踏まえた政府機関における情報システムの運用継続に向けた対処要件等に係る調査」として、内閣官房情報セキュリティセンター 政府機関総合対策促進担当が株式会社富士通総研に委託し、実施した。

# 目次

# 1. IT-BCP 策定モデルの概要

## 1.1. IT-BCP とは

本報告書で取り扱う「IT-BCP」とは、「情報システム運用継続計画」の略称である。「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（以下、「ガイド」とする。）」においては、以下のように定義されている。

- 正式な名称は「情報システム運用継続計画」である。
- 府省庁における事業継続計画（業務 BCP）の情報システムの復旧について書かれた部分をより詳細化した計画である。
- 災害や事故等の非常時に情報システムを早期に復旧させ継続して利用するために必要な非常時の行動手順で構成される計画である。
- IT-BCP には、非常時に適切な対応を取るために必要な事前対策や教育訓練等の平常における実施計画が含まれる。

本調査において、IT-BCP と平常時のシステム障害に対する対応手順が混同されている事例が見られた。中央府省庁における IT-BCP は震災等の過酷な状況下において、優先的に再開させなければいけない業務を支える情報システムの復旧について検討するものであることを理解されたい。例えば、「今、首都直下地震が発生してしまったら」という想定に対して、情報システム部門として適切な行動を示せるかどうか、それぞれの部門において確認されたい。

## 1.2. 「IT-BCP 策定モデル」を取りまとめた背景

東日本大震災による未曾有の被災により、政府機関の情報通信基盤や情報システムの災害復旧性について、想定外の脆弱性が多数指摘されることとなった。そのため、情報セキュリティ政策会議において、行政の継続性や情報セキュリティ維持の観点から、大規模災害の発生に備えた強靭な情報通信システム基盤構築の推進や東日本大震災の被災経験を踏まえた大規模災害時の情報システム運用継続のための対処要件の検討が決定された。

NISC においては、前述のガイドの改訂後に実施したアンケート調査の結果から、各府省庁において IT-BCP が順調に整備されている状況が確認され、策定にガイドが活用されていることが確認できた。しかし、情報システムの更改に合わせて計画策定の実施時期を先送りする等の状況も確認されており、「今、首都直下地震が発生した場合の対応手順を検討すること」という認識が十分に理解されていない等の課題も明らかになった。

**表－ 1 IT-BCP 策定状況及びガイドの利用状況調査により確認された課題認識**

| 課題認識 | 本調査における対応方針 |
|---|---|
| **現在の情報システムの対策状況に基づいた運用継続計画が策定されていない。**<br>「重要システムの計画策定を優先したため、残りのシステムについては検討されていない」、「新しいシステムの構築に合わせて策定する」、「内閣府の新しい被害状況の想定が出てから検討する」等の回答が散見され、IT-BCP の位置付けや、ガイドに示す作成文書の利用シーンが適切に理解されていないと考えられる。 | **⇒ 改めて、IT-BCP 策定の意義や策定文書の内容について説明を加え、現状の対策をベースとした IT-BCP の策定を促し、速やかな情報システム運用継続管理の実現を支援する。** |
| **ガイドに示されている対処要件が要求する対策の水準が高度で具体的でない。**<br>ガイドに示す対処要件や、それに基づく対策例が「現在の対策実施状況からかい離している」、「予算の制約上実現が困難」等の回答が多く挙げられている。 | **⇒ ガイドで提示している対処要件を見直し、主要な要件に対する対策例を復旧優先度別等に分けて取りまとめる。** |

本調査では、検討すべき諸課題について、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及び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モデル調査を実施し、調査から得られた知見・情報を、「業務継続計画（以下、「BCP」とする。）」と IT-BCP の間をつなぎ、より実効性の高い計画策定に資する「IT-BCP 策定モデル（以下、「策定モデル」とする。）」として取りまとめることとした。

策定モデルは、ガイドやモデル調査において確認した府省庁の「情報システム運用継続計画（IT-BCP）」の策定状況に基づき、今後、情報システム担当者が IT-BCP の策定や見直しの実施の際に何をすべきか示唆する目的で整備した。策定モデルは、府省庁の情報システム担当がガイドを参照しながら IT-BCP を策定するときに参考となる策定手順の解説や作業上の工夫、成果物の詳細な例示等の実践的な内容を含んでいる。

## 1.3. IT-BCP 策定モデルにおける策定ステップ

本モデル策定に当たり、IT-BCP 策定への取組状況の調査（以下、「モデル調査」とする。）を実施した。結果からはガイドの内容が適切に理解され、実効性の高い IT-BCP の整備が進められていることが確認できた反面、復旧目標の設定等の工程で情報システム部門と業務部門との連携が不十分な事例が確認される等の課題やガイドにおける説明や例示の不足が指摘された。

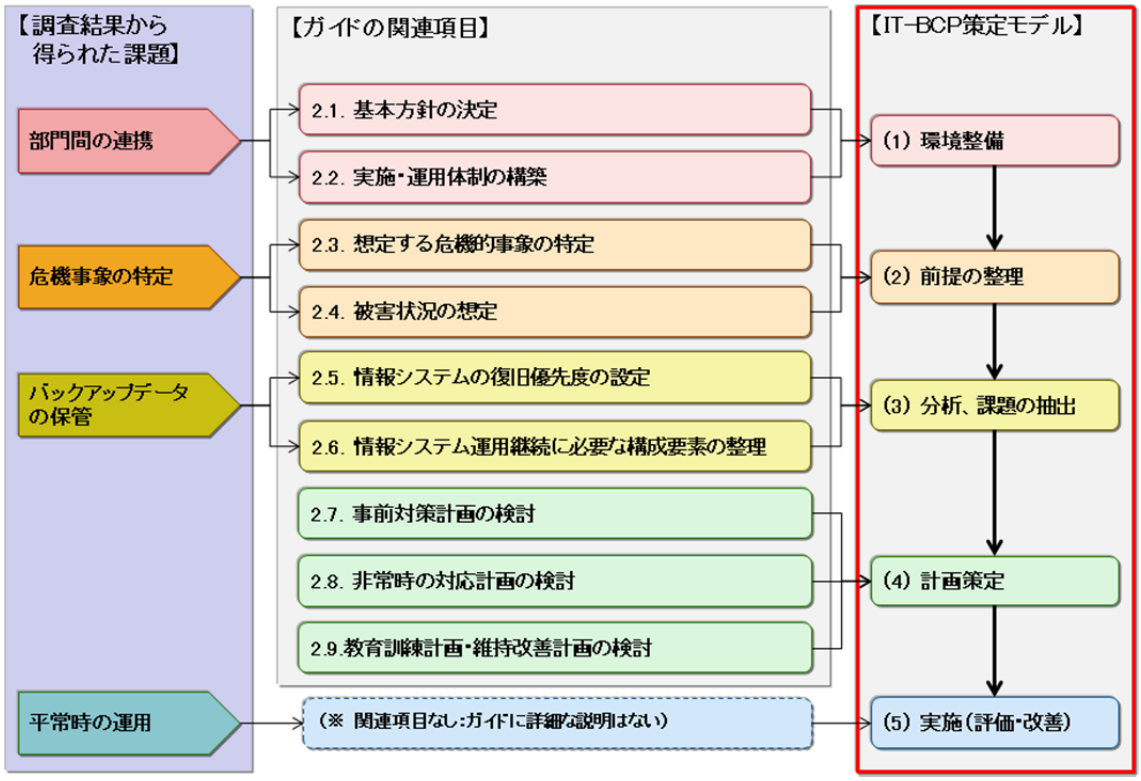
**表－ 2 モデル調査の結果から抽出された課題**

| 調査課題 | 確認された事実 | 必要な対処 |
|---|---|---|
| (1)<br>**非常時の意思決定に関する在り方** | **【部門間の連携】**<br>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)<br>**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】**<br>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。<br>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）。 |
| (3)<br>**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】**<br>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)<br>**教育・訓練の在り方** | **【平常時の運用】**<br>IT-BCP を策定済みの府省庁におい | 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 |

| | | |
|---|---|---|
| | て、教育・訓練が実施されていなかった。 | 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。 |

ガイドの第 2 章において、非常時優先業務で利用される情報システムを特定し、それごとに構成要素の詳細な分析を行い、非常時に業務を復旧・継続するために必要な対策を決定するまでの過程が簡潔に示されている。段階的な調査・分析の実施は、策定手順の各工程の作業内容や相互の関連を的確に理解し、注視している対象を意識して作業に当たることで、より効率的でバランスのとれた対策をとることができると考えられる。

「IT-BCP 策定モデル」では、策定作業を進める過程における情報の連携を意識し、9 段階の IT-BCP の策定手順を以下の 5 ステップ簡略化して、情報システム部門において現状で適切な対応がとられていない点を中心に解説するモデルを取りまとめた。




**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 策定モデルの５ステップは、上図のとおり、原則としてガイドに示されている作業内容に対応している。

表－ 3　IT-BCP の策定モデルにおける策定ステップの概要

| 策定ステップの概要 |
| --- |
| (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。<br>● IT-BCP の策定に必要な体制を整備する。<br>● IT-BCP の基本方針について関係者間で合意する。<br>● IT-BCP の対象範囲について関係者間で合意する。 |
| (2) 情報の収集・整理 |
| ● 危機的事象を特定する。<br>● 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。<br>● 対象業務の目標復旧時間（以下、「業務 RTO[1]」とする。）を明らかにする。<br>● 情報システムを支える構成要素（リソース）を洗い出す。<br>● 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】<br>● 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。<br>● 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。<br>● 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。<br>【非常時対応計画の策定】<br>● 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。<br>● 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。<br>● 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。<br>【教育・訓練計画の策定】<br>● 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（雛形 「4.1.教育訓練計画」の例を参照 |

[1] Recovery Time Objective：目標復旧時間

のこと）。

- 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）

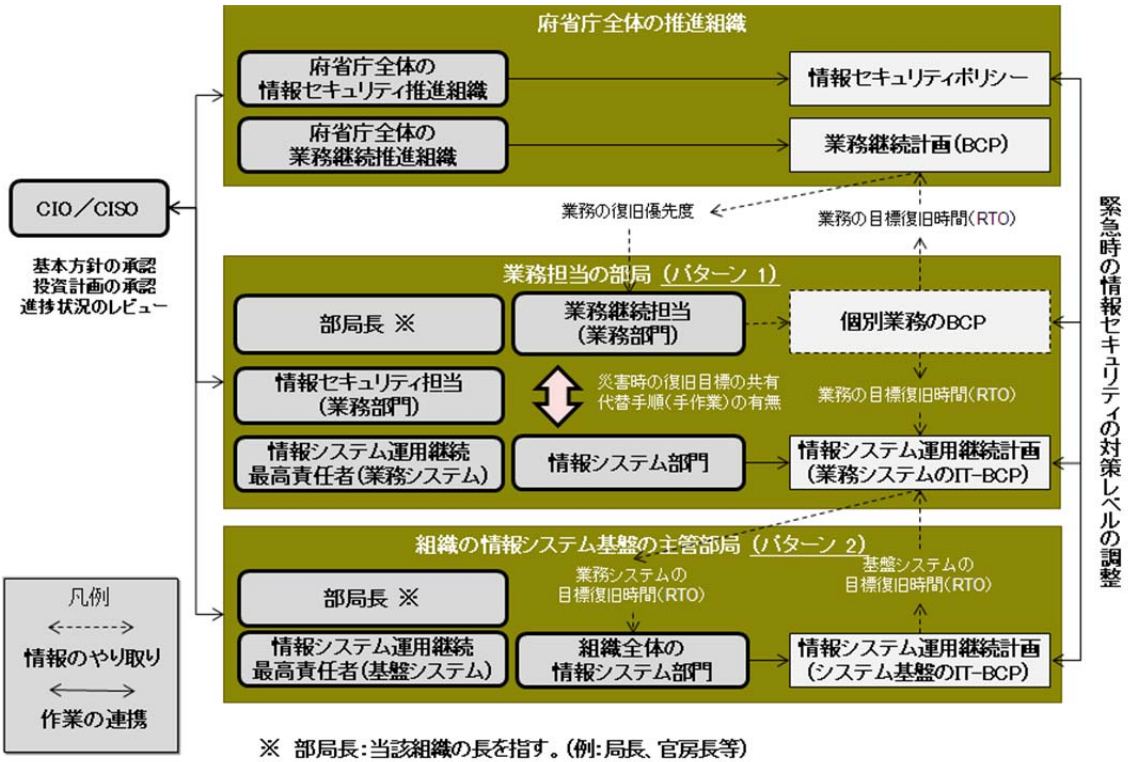
- 運用段階においては、策定された事前対策計画と教育訓練計画に則り、対策実施や教育訓練等の活動を行うことで、業務継続能力の強化を推進する。また、「維持改善計画」に基づいて、適宜各種計画の見直しを行い、計画の陳腐化を防ぎ、常に計画の最新化を維持するように努める。
- 計画の見直し時には、関連部局や組織のレビュを必要に応じて受けるべきである。（防災、情報セキュリティ等の推進部門に、それぞれの分野の観点から指摘を受けることは有効である。）

## 1.4. IT-BCP 策定モデルのパターン分け

モデル調査の結果から、情報システム部門と業務部門やその他の関連部門と十分な情報連携が行われず、目標設定を情報システム部門単独で行っている事例も見受けられた。

この事実は、府省庁における組織構造や日常的な部局間の連携不足が原因と想定される。また、部局内においても、組織全体の目標が課室単位の平常業務に反映されにくく、課室単位の課題認識が組織全体に共有されにくい現状と相まって、特に情報システムの運用継続においては必須と考えられる部局間の連携の実現を妨げているものと考えられる。

そこで、IT-BCP 策定モデルでは、主管する情報システム部門の所属する組織及びシステムを利用する業務部門との関係性に着目し、分類を検討し、その結果、情報システム部門が所属する組織の違いにより2つのパターンを設けることとした。以下に、情報システム運用継続の検討や運用に関係すると想定される利害関係者とパターン分けの概要図と、それぞれのパターンの概要を示す。




**図－ 2 IT-BCP の策定・運用で想定される利害関係者**

**表－ 4 IT-BCP 策定モデルのパターン分け**

| 情報システム部門の所属 | 概要及び例示 |
|---|---|
| 【パターン 1】<br>業務部門の一部局 | ● 各府省庁において業務を所管する部局に所属し、業務システムや業務システムの基盤の構築や運用を受け持つ情報システム部門を想定する。<br>● 情報システム部門が、業務を担当する部門と同一の部局内に属する。<br>● 主に、業務システムや業務システムが共通に利用する情報システム基盤の構築や運営を担当する。<br>（例） 業務システムを担当する。<br>（例） 特定の業務で利用する情報システム基盤の全部又は一部を担当する。 |
| 【パターン 2】<br>組織全体の情報システム部門 | ● 各府省庁の組織全体の情報システム基盤の構築や運用を受け持つ情報システム部門を想定する<br>● 情報システム部門が、現場部局とは異なる部門（大臣官房総務課や情報システム課等）に属する。<br>● 主に、各府省庁の情報システム基盤等の構築や運用を担当する。<br>（例） 庁内ネットワークや認証基盤、メール、グループウェア等のシステムを担当する。 |

コラム　－　基幹 LAN の IT-BCP

IT-BCP 策定モデルのパターン2における典型例として、各府省庁の基幹 LAN が挙げられる。基幹 LAN はどの府省庁においても必ず存在しており、他の業務システム全般の稼働における前提であるため、停止時の影響は非常に大きい。

基幹 LAN の所管部門においては、府省庁内の基幹 LAN 上で稼働する全ての業務システムの所管部門に対して、基幹 LAN の IT-RTO 及びその際の復旧レベルを通知しておく必要がある。各情報システム所管部門は自部門の業務システムの IT-RTO を達成するために必要な検討を行い、必要に応じて基幹 LAN の停止を想定し、一時的に基幹 LAN の復旧を待たずに独自の限定された環境で復旧を行うこと（基幹 LAN が利用できない場合の業務の在り方）も検討することが望ましい。さらに、その検討結果は基幹 LAN の所管部門とも共有しておくことが重要である。

なお、これらの検討の結果、業務システム及び基幹 LAN に改修の必要が生じたとしても、システム運用途中での改修は難しい場合も想定される。したがって、IT-BCP はシステムのライフサイクルに合わせた見直しが必要であり、IT-BCP の要素は、システム更改時の調達要件の一つとして考慮すべきである。

基幹 LAN の復旧においては、職員に対する迅速なサービス再開を図るための復旧手順を事前に検討しておくことが必要である。なお、この場合、復旧すべき箇所が複数あり、かつ復旧作業に係るリソース（人的資源）が不足する場合も考えられることから、システムごとの復旧手順だけでなく、復旧すべきサービスの優先順位についても検討することが望ましい。

また、物理的な LAN の断線については、早期復旧を最優先した暫定的な仮設配線による復旧も併せて検討しておくことが望ましい。なお、遠隔地の拠点との通信が切断された場合には、早期にキャリアと連絡を取り、遠隔地拠点の停電による電源断によるものか、ネットワーク経路上における物理的な断線によるものかを切り分けることが重要である。

基幹 LAN が物理的なネットワークのみを指している場合には、ネットワーク機器の設定を含むハード面の復旧が主な作業となるが、一般にはメールや認証基盤等のサービスも含まれる場合が多い。その際には、単なる物理的なネットワークだけでなく、基盤系のサービスも同時に復旧させることが必要となるため、必要となる技術者も多くなることが想定され、役割に応じた適切な対応が重要となる。

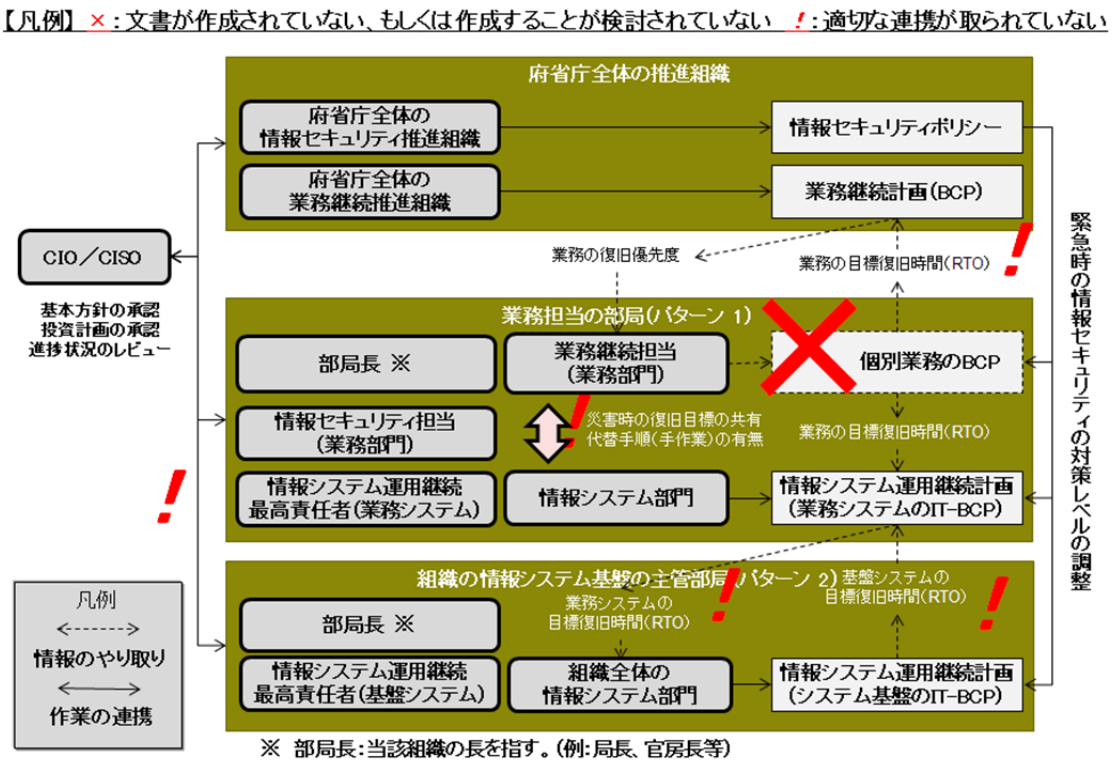
# 2. IT-BCP 策定モデル

## 2.1. 環境整備

| |
|---|
| 【関連するガイドの項目】<br>2.1. 基本方針の決定<br>2.2. 実施・運用体制の構築 |
| ● 情報システム部門で、IT-BCP 策定の方向性を検討する。<br>● IT-BCP の策定に必要な体制を整備する。<br>● IT-BCP の基本方針について関係者間で合意する。<br>● IT-BCP の対象範囲について関係者間で合意する。 |
| IT－BCP の策定や運用プロセス全般において、情報システム部門は非常時優先業務の継続に必要な活動や判断に関係するすべての関係者を確認に主導的な立場で関与し、業務の継続に必要な情報システム運用継続の対象範囲や基本方針を協議し、合意を得る事が望まれる。<br><br>東日本大震災発生直後の政府機関においては、災害対策本部に関係する府省庁の担当者や民間の重要インフラ事業者等が参集し、その場で情報の確認や判断、一次判断等が行える態勢を整備していた状況が見られた。これは、非常時対応のための体制整備がうまくいっている望ましい事例といえる。<br><br>他の事例においても、府省庁の担当者と情報システムの運用を担当する事業者との間で、非常時の参集や対応時の役割分担について事前に協議する、委託先事業者において平常時から稼働している対応窓口で非常時の利用者対応を受け持つことを合意する等の工夫が見られた。他の府省庁においても、業務部門内で、IT-BCP 策定の事務局を部門の情報セキュリティ担当が受け持ち部門専用の IT-BCP の雛形を用意し、各業務システムの担当に配布する等の部局間の連携も見られた。 |

### 2.1.1. IT-BCP の策定に必要な体制の整備

IT-BCP の策定に着手するに当たり、情報システム部門と「業務部門」や「その他の関連部門」との間で検討体制を整備することが必要である。モデル調査等の結果から、現状は以下に示すとおり、多くの場合において連携が取られていないことが確認されている。（これは、パターン 1、2 に共通している。）




**図－ 3 情報システム部門と業務部門等の関連部門との間の連携不足**

この連携不足は、それぞれの組織間でどのようなやり取りを行い、IT-BCP の方針決定や具体的対策の検討に必要な情報収集を行えばよいか十分に理解されていない結果であると考えられる。また、非常時優先業務の継続に関する各部門の役割分担について認識のずれが存在し、適切に運用されていないため、部門間で連携を取ったが期待した成果を上げられなかった事例も見られた。

### 2.1.2. 業務部門との連携について

#### (1) 業務部門との連携について

情報システム部門が、第一に検討すべき連携先は「業務部門」である。ここまで、単に業務部門と述べてきたが、情報システム部門の所管する情報システムの違い（パターン 1、2）により連携対象や検討のポイントが異なることに留意されたい。

**① パターン 1 の場合**

情報システムに設定する目標復旧時間（以下、「IT-RTO[2]」とする。）は、業務部門で設定する非常時優先業務の業務 RTO を確認し、その時間を超過しないよう設定されるのが理想である。また、情報システムの復旧優先度を検討する際には、業務の復旧優先度や手作業による代替手段の有無、代替手段による業務継続が可能な時間等の情報が業務部門から提示されることが望ましい。

業務部門において復旧対象に設定した非常時優先業務が、組織全体の情報システム基盤（庁舎内のネットワークや認証基盤、電子メール等）を利用することが前提となっている場合には、基盤の IT-RTO 等を組織全体の情報システム部門に確認する必要がある。

**② パターン 2 の場合**

組織全体の情報システム基盤の IT-RTO は、システム基盤上で稼働する業務システムの IT-RTO や情報システム基盤を利用して処理される業務の RTO 等に対して、それらの復旧を妨げないために、最優先で復旧するよう設定されなければならない。

しかし、この場合に想定される連携の対象は、府省庁における全部局であり場合によっては地方組織が含まれることも有り得る。そのため、先に情報システム部門において「たたき台」となる目標の復旧時間等を設定した上、BCP で定めた非常時優先業務を所管する業務部門と優先的に調整する等、現実的な対応を検討する必要がある。

[2] IT-Recovery Time Objective：IT（情報システム）の目標復旧時間

### (2) その他の関連部門との連携について

ガイドにおいては、以下に示す事項について情報システム部門と部局や組織との間で、以下の事項について連携を検討することが望ましいとされている。(ガイド P.10-12 参照)

**表－ 5 IT-BCP の策定におけるその他の関連部門と連携すべき事項**

| その他の関連部門 | 連携すべき事項 |
|---|---|
| 組織の業務継続推進体制 | ● 非常時の優先業務の確認(府省庁の BCP の確認)<br>● 非常時の初動体制の確認 |
| 組織の情報セキュリティ推進体制 | ● 非常時の情報セキュリティの水準の確認<br>● 採用した非常時の対策の情報セキュリティ面のレビュ |
| 組織の最高情報管理責任者(CIO)や<br>最高情報セキュリティ責任者(CISO) | ● 非常時優先業務及び優先復旧システムの承認<br>● 事前対策計画(投資計画)の承認 |
| 庁舎の電力管理等の関連組織 | ● 非常時の電力や情報通信ネットワークの利用の割当<br>● 非常時の執務場所の確保 |

これらの部門においては、それぞれ担当業務において府省庁の業務継続に関する重要なリソースの管理や、組織全体の対策の総括等の役割を受け持っている。

情報システム部門は、非常時にはこれらの部門と確実に連携を取り、情報システムの復旧に必要なリソースを確保する必要がある。具体的には、必要なリソースを確認し、事前対策計画や非常時行動手順等の IT-BCP を策定の上、上記部門の合意を得る事が望まれる。

特に、他部門と円滑に連携していくためには、適宜 CIO・CISO の承認を得ながら、策定作業を進めることが有効である。

### (3) 被災時における情報セキュリティの対策レベル調整の例示

ここまで述べてきた、情報システム部門と業務部門等との連携について、モデル調査等で確認された事実等に基づき、非常時の情報セキュリティ対策について非常時の行動について例示を展開してみる。震災等の被災時には、発災後一定時間が経過した後に、業務部門が手作業による業務再開を準備すると同時に、情報システム担当においても復旧対応を開始するものと考えられる。その際には、各部門間において以下のような情報連携が行われると想定できる。

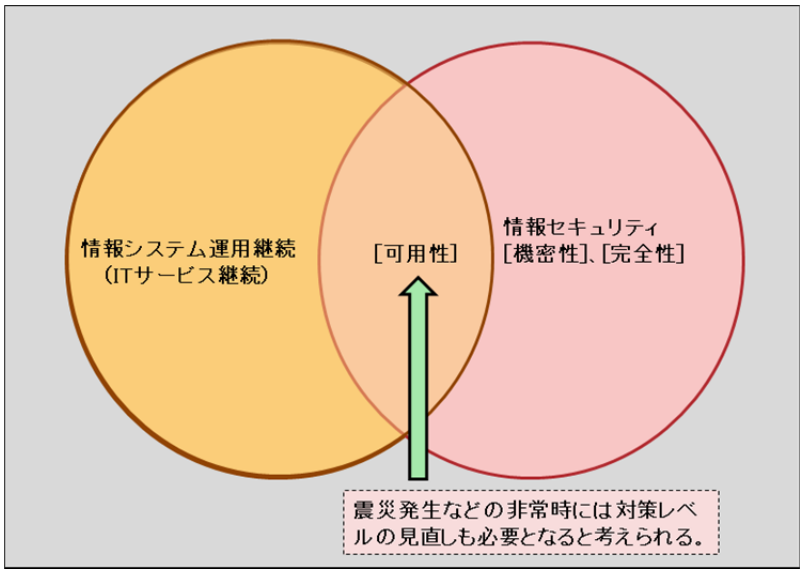
**表－ 6 被災時における業務部門の情報システム部門と業務部門等との連携**

| 情報システムの主管部門 | 連携相手 | 連携の内容 |
|---|---|---|

| | | |
|---|---|---|
| 業務部門の情報システム担当 | 業務部門 | ● 業務の再開に必要な情報を確認する。<br>● 組織全体を所管する業務継続推進組織に、執務場所の確保状況等を確認し、必要な執務スペース等の割り当てを受ける。 |
| | 組織全体の情報システム部門 | ● 庁内 LAN 等の情報システム基盤の復旧状況や、IT サービス提供の再開目標時間等を確認する。<br>● 業務再開に必要な、パソコン等の準備を依頼する。 |
| | その他関連部門 | ● 組織全体を所管する情報セキュリティ推進組織に、業務の再開に必要な情報や情報の利用者、利用環境、情報セキュリティ上のリスク等について報告し承認を得る。<br>● 組織全体を所管する業務継続推進組織に、非常用電源供給設備の稼働状況や、外部との通信の疎通、庁内の被災状況等と被災している場合には復旧に要する時間を確認する。 |

このケースにおいて、庁舎の被災状況等の条件によっては、庁舎等の施設・設備や社会インフラ（電力供給や通信ネットワーク）、業務システム全体等の復旧を待たず、外部保管しておいたデータを外部のクラウドサービス等に移動し、職員が自宅やモバイル環境に必要な個所をダウンロードして利用できる環境を整備する緊急時対応等も想定される。

IT-BCP は、平常時の情報セキュリティ管理態勢における「可用性（利用の可用性）」と重複し、場合によっては相反する対策の実施を求める場合がある。




「IT サービス継続ガイドライン　改訂版」（経済産業省）の図を基に作成

**図－ 4 情報システム部門と業務部門等の関連部門との間の連携不足**

震災等の緊急時の対応においては、以下の点について情報セキュリティ上の対策を免除又は一部軽減することも想定される。しかし、非常時においても機密性を確保しなければならない情報が存在することも自明であり、震災発生時等にはその相反する要求に対する判断ができずに対応の遅れや、逆に重要情報の流出等の事例が過去には発生している。

したがって、IT-BCP を検討する情報システム部門は、部門の情報セキュリティ担当や府省庁の情報セキュリティ推進組織等と十分に協議し、被災時における情報の機密レベルの調整や、個別の情報の取扱いを決定し、必要に応じ組織の CIO や CISO の承認を得ることが望まれる。

### 2.1.3. 連携が取られていない理由

本調査においては、現場の業務部門に情報連携や確認を行わずに、情報システム部門単独で実施している事例が散見された。しかし、モデル調査の対象となった省庁においては、部門の情報セキュリティの推進担当が IT-BCP 策定の事務局となり情報システム部門と連携を取りながら策定を推進する体制が整備されている事例等の望ましい工夫が複数確認できたことも特筆すべきである。

組織の情報セキュリティや業務継続を推進する部門や庁舎の電力管理等の関連組織と連携した事例もあまり確認できなかった。例えば、庁舎内に設置した業務処理サーバが非常時の電力供給の対象に含まれているか未確認の事例等、非常時の対策について未確認・未実施の事項が多数残されてしまっている状態が散見される結果からも、IT-BCP を情報システム部門が独自に策定し、本来 IT-BCP を策定する際に必要な情報について関連部門に確認を行わず検討が進められていることも少なくないと推測される。

調査結果からは、組織的な連携が取られていないことについて、情報システム部門の独断や組織的な連携不足だけが阻害要因ではないことも確認されている。

例えば、業務部門において震災発生時等の対応手順や手作業による代替作業等について十分検討されていないことも指摘されている。

府省庁全体の業務継続については、組織の防災担当等によりガイドに沿って策定されているが、業務部門において個別業務の復旧手順が文書化され、情報システム部門に提供されている事例は確認されていない。例えば、組織の業務継続推進組織と連携を取ることを検討したが、相手側が主に震災発生時の初動体制について検討をしていたため、個別業務の復旧について有用な情報交換ができなかったとの事例が確認されている。

このような場合には、情報システム部門でできるだけガイドに沿った情報収集や各種検討を進め、適宜作業結果について業務部門やその他の関連部門の合意を得ながら IT-BCP の策定を進めていく等の工夫も必要である。

情報システム部門が単独で IT-BCP 策定を検討するための体制を整備し、重要業務の復旧方針や対象範囲の設定を推進することは困難が想定される。IT-BCP 策定の担当者及び課室においては、部局の長に必要な体制整備について理解を得るとともに、場合によっては部局間の調整に必要な支援を依頼することも必要である。

### 2.1.4. 基本方針や対象範囲の検討

IT-BCP の基本方針を策定することで、情報システム運用継続における非常時の対応の方針や継続的に実施される活動について整理することができる。

情報システム部門は、IT-BCP を策定するための方針を決定し、業務部門やその他の関連部門の合意を得ることが望ましいことは、前述のとおりである。また、業務部門に働き掛けて、非常時優先業務の概要や、業務の継続に必要なリソース、非常時の対応等の情報提供を受け、IT-BCP の基本方針や対象範囲について合意を得ながら設定すべきである。

特に、検討体制については、多くの場合そのまま運用へと組織が引き継がれる場合が多く、この段階で業務継続及び情報システム運用継続に関係する各部門において担当者に適任者を人選してもらうことが望ましい。

## 2.2. 前提の整理

| |
|---|
| **【関連するガイドの項目】**<br>**2.3. 想定する危機的事象の特定**<br>**2.4. 被害状況の想定** |
| ● **危機的事象を特定する。**<br>● **危機的事象の顕在化がもたらす被災状況を想定する。** |
| **首都直下型地震が発生した場合の停電や通信網の途絶等の被災状況を明らかにして、対象の情報システムの早期復旧や運用継続を阻害する要因である被害状況を想定する。情報システム部門においては、この被害想定が情報システムの「脆弱性」を分析する前提となることを理解し、適正な想定を行うように留意されたい。**<br><br>**大規模災害発生時の対策本部を担当する府省庁においては、内閣府防災担当から公表されている危機事象の想定に基づく被害の想定を取りまとめ、いかなる時間帯においても本部員が 30 分以内に対策本部設置場所に参集するための事前対策を実施している。**<br><br>**他の事例においては、様々な制約から現状での対応が困難と思われる被害想定について、対応可能なレベルまで緩めたりしている事例があることが散見された。**<br><br>**このような調整は、対策を未実施な危機事象が放置されることとなり、継続的な改善の対象からも外れてしまいかねないことに留意されたい。** |

### 2.2.1. 危機的事象の想定

中央府省庁において BCP を策定するに当たり、危機的事業の想定については内閣府防災担当の策定した「中央省庁業務継続ガイドライン　第 1 版　～首都直下地震への対応を中心として～（平成 19 年 6 月）（以下、「業務継続ガイドライン」とする。）」[3]を参考にしている。モデル調査においても、ほとんどの省庁においてこの業務継続ガイドラインの想定に基づき、以下のような前提で首都直下地震の発生状況を想定している。[4]

- 基本的には、休日の夕方に首都直下地震が発生し、震度 6 強の揺れが観測された場合を想定する事を推奨する
- 府省庁の BCP における想定条件を確認し、IT-BCP で想定する危機的事象もそれと整合性

[3] 「中央省庁業務継続ガイドライン　第1版　～首都直下地震への対応を中心として～」（内閣府　防災担当　平成 19 年 6 月）
http://www.bousai.go.jp/jishin/gyomukeizoku/pdf/gyoumu_guide_honbun070621.pdf

[4] 危機的事象には、自然災害のほかにも「インフルエンザや感染症などによるパンデミック」や「停電」、「通信回線関連の故障」、「外部コンピュータシステムの故障」、「テロやサイバー攻撃等の外部からの攻撃」等も想定できる。

を保つことが望ましい

地震等の発生時間については、最も厳しい条件と思われる休日夜間の設定を推奨されるが、条件を変えることで、それぞれの状況下に固有の問題が発生するものと思われるので、複数パターンで検証することが理想である。例えば、平日の業務時間内で職員が庁舎内にいる状況で震災が発生した場合だと、情報システム基盤の利用者も多く、優先して復旧する業務の精査や限られたリソースの割り当て等の計画に反映すべき事項がある。

### 2.2.2. 被害状況の想定

前項で特定した危機的事象が顕在化したときの情報システムの被害状況を想定し、情報システムの運用継続を阻害する課題を明らかにする。

ガイドには、「首都直下型地震発生時」と「予期せぬシステム停止発生時」、「その他危機的事業発生時」の 3 つの状況下における被害状況に分けて想定を行っている。[5]地震発生とシステム停止については、それぞれ固有の事象が発生することがあるため個別に検討することを推奨し、その他の事象については前述の 2 つの想定に基づいた検討を推奨している。

現状で、IT-BCP は各府省庁で策定した BCP で設定した危機的事象や被害状況の想定を踏襲して策定することが推奨されている。これは、そもそも IT-BCP が BCP における情報システム部分を詳細化した内容であるとの立場から、府省庁内で業務と情報システムの復旧対策に齟齬が生じることが無いよう配慮した結果である。

一般に精緻に被害状況を想定して策定した IT-BCP は、想定どおりの被害状況が発生した際の実効性は向上するが、想定からずれた場合の実効性はかえって低下すると考えられる。現実的には危機的事象発生時の被害状況を正確に詳しく予測することは不可能なので、検討に要する労力等も勘案し、ある程度幅を持たせた被害状況の想定に基づき、前提条件から多少外れても対応可能な計画を検討することが望まれる。[6]

[5] 「2.4. 被害状況の想定」（ガイド P.14,15）
[6] 東日本大震災当時の電力及び通信インフラの復旧については、参考となる資料を掲載している。（「3.1.2 東日本大震災による社会インフラの被災と復旧の状況」）

### (1) 被害想定を行う際の注意点

厳しすぎる被害想定により事前対策の検討が進まなくなることへの懸念等を背景に、現状で対応不可能な被害想定の一部を当面検討対象に含めないことにする可能性がありうるが、その場合は、業務部門に代替手段の有無を確認することや、検討事項が残された場合でも、そのことを認識し続けること等の対応が必要である。

以下に、ガイドに掲載されている被害状況の想定の例を示す。(ガイド P.14 参照)情報システムの運用を支えるリソースを被害想定の単位とした被害想定のまとめ方として参考とされたい。

表－ 7 被害状況の想定

| 被害想定の単位 | 説明 | 参考にする業務継続計画の被害想定結果 |
|---|---|---|
| 情報システムの設置場所 | 情報システムの設置場所の被害状況を想定する。 | 庁舎 |
| 交通機関 | IT 復旧に必要な職員や外部委託者が参集するための交通機関の被害状況を想定する。併せて、参集可能な要員の把握等、要員の被害状況も想定する。 | 周辺環境 |
| 電力 | 電力の被害状況を想定する。 | 電力 |
| 水道 | 水冷式の空調を利用している場合、水道復旧までシステムが停止する。水道の被害状況を想定する。 | 上水道 |
| 電話 | 固定電話、携帯電話、携帯メールの被害状況を想定する。 | 電話、携帯電話 |
| 情報通信ネットワーク | 府省庁内外のそれぞれの情報通信ネットワークの被害状況を想定する。また、ASP 等の外部サービスを利用している場合は、その被害状況も想定する。 | インターネット |
| 情報システム機器(サーバ等) | IT 拠点に設置された設備機器の被害状況を想定する。 | 建物内部 |
| データ | 情報システムの OS やアプリケーション、業務等のデータの被害状況を想定する。また、バックアップデータがある場合、バックアップデータの被害状況を想定する。<br>※ 非常時の利用において、民間事業者の提供するクラウドサービス上に読み込んだり、職員の個人所有パソコンにダウンロードしたりして利用する等、情報セキュリティ対策の軽減を検討しなければいけない場合もある。 | データ |

### (2) 関連部門における対応状況の確認

上記被害想定の単位には、非常時の電力供給やインターネット等へのアクセス回線等の施設・設備の対策、要員の参集ルール等について他の関連部局が管理しているリソースが含まれている。そのため、前提として以下に示す点について確認の上、検討作業を進める必要がある。

- 情報システムの設置場所については、管理対象とする情報システム以外に、省庁の執務環境等も想定の対象に含めること。
- 府省庁の BCP や業務継続を推進する部門において個別に被害想定を実施している場合には、その結果を活用することが望ましい。
- システムの設置場所が複数にわたる場合には、それぞれの拠点で被害想定を実施する。

## 2.3. 分析、課題の抽出

| |
|---|
| **【関連するガイドの項目】**<br>**2.5. 情報システムの復旧優先度の設定**<br>**2.6. 情報システム運用継続に必要な構成要素の整理** |
| ● **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。**<br>● **対象業務の目標復旧時間（以下、「業務 RTO」とする。）を明らかにする。**<br>● **情報システムを支える構成要素（リソース）を洗い出す。**<br>● **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。** |
| **情報システム部門は、首都直下地震発生時に優先して復旧する業務の「業務 RTO」を確認し、その業務の復旧に必要な情報システムの洗い出しと、それぞれのシステムと業務の関係からIT-RTO を設定し、対策レベル別にグループ分けを行う。また、情報システムの復旧に必要な「構成要素」を分析し、復旧優先度ランク別の対策の目標を設定した基準（目標対策レベル）を作成する。**<br><br>**大規模災害発生時の対策本部を担当する府省庁においては、要求される対策のほとんどが概ね最高レベルの水準を要求されていたため、復旧優先時間等の決定に特別な工夫を考える必要はなかった。**<br><br>**他の事例においても、それぞれの情報システムについて特別な構成要素を保有している府省庁は無く、固有の対策が必要なかったため、ガイドの例示を参考に対策目標の基準を設定している。**<br><br>**今後、IT-BCP の運用を継続し、復旧時間の短縮や対応の効率化等態勢のレベルアップを検討する場合には、添付の「対処要件一覧」や「個別対策事例」、その他の参考文献等を基に目標対策レベルの見直しを行うことも検討されたい。** |

### 2.3.1. 非常時優先業務の特定と情報システムの洗い出し

IT-BCP の策定を進める際には、業務と情報システムの関係を確認し、以下に示す適切な段階に沿って実施することが望まれる。

- BCP を確認し、対象業務の復旧優先度や業務 RTO を確認する。
- それぞれの業務で利用している情報システムを洗い出す。
- 認証や DNS[7]等の洗い出した情報システムの稼働の前提となる基盤系システムを洗い出す。

[7] Domain Name System：インターネット上のホスト名と IP アドレスを対応させるシステム。

業務と情報システムの関係整理が行われずに IT-BCP が検討されると、業務側で設けた復旧目標とかい離した対策を採用する可能性があるだけではなく、震災等によりシステムが停止した場合の行動計画が不適切で、十分に業務部門を支援することができない可能性もある。

非常時優先業務や業務 RTO は、府省庁の BCP に基づいて確認することが望ましいが、BCP に業務 RTO が明記されていない場合が散見される。また、非常時優先業務の業務 RTO や非常時の対応手順を業務部門が検討していた事例も確認できていないことから、IT-BCP を策定するためには、情報システム部門から働き掛けを行い必要な情報を特定していく必要があると考えられる。

必要な情報が業務部門等から入手できない場合でも、情報システム部門がたたき台を作成して協議する等、相手方の了解を得た上で作業を継続するよう留意されたい。

洗い出しの作業を実施する場合に活用できる書式として、ガイドの雛形には以下の例示がある。（ガイド雛形 「5.3. 情報システムの復旧優先度の設定 （1）業務の目標復旧時間と情報システム停止時の代替手段の検討」 参照）

**表－ 8 業務の目標復旧時間と情報システム停止時の代替手段分析結果（例）**

| 非常時優先業務 | 業務の目標復旧時間 | 業務を支える情報システム | 情報システム停止時の代替手段の有無 | 代替手段で継続可な時間 | 本業務における IT-RTO |
|---|---|---|---|---|---|
| ○○業務 | 3 時間 | メールシステム | 初期段階では電話による業務遂行が主なため、メールは必須ではない。 | 12 時間 | 15 時間 |
| … | | | | | |

また、今日において業務とその遂行のために利用する情報システムが 1 対 1 の関係にあることはまれで、複数の業務システムや情報システム基盤が関係することがほとんどである。

情報システム部門においては、情報システムの停止が業務に与える影響を業務部門や業務システムを管理する情報システム部門等と十分に協議した上、業務の普及優先度や業務 RTO の確認、利用している情報システムの洗い出し等を実施することが望まれる。

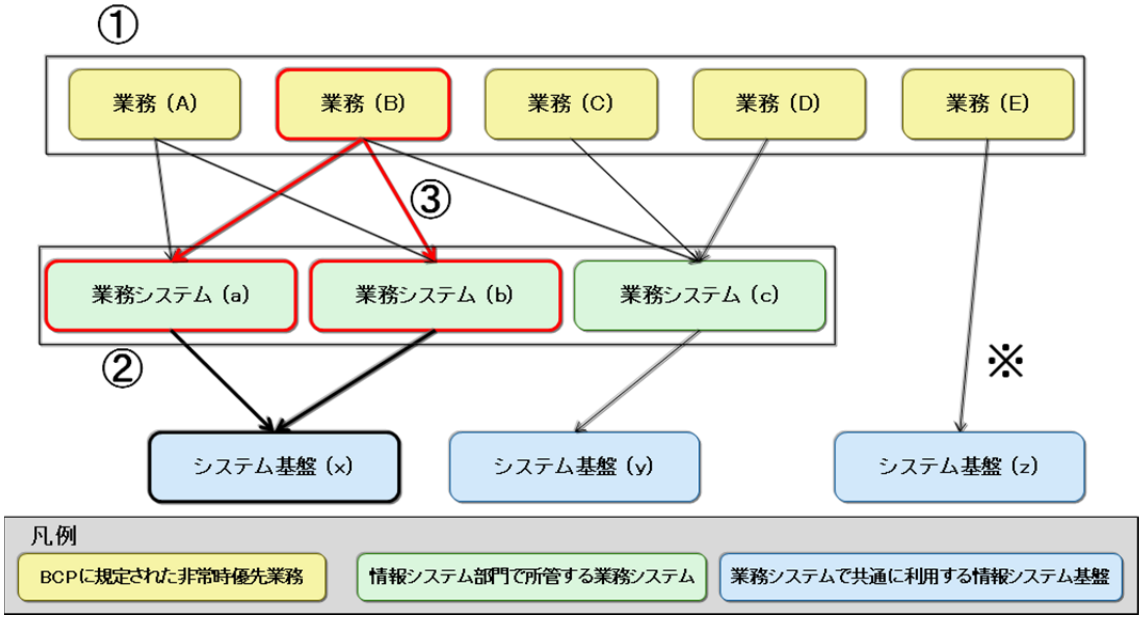
情報システム部門の担当範囲により分類したパターンにより、確認対象や手順が若干異なるので、ここで比較を行い確認しておく。以下にパターンごとに示す図は、情報システム部門における「非常時優先業務」と「情報システム」の関係を管理する際の概念図である。

### (1) パターン 1 の場合

情報システム部門が、業務システムや業務システム基盤の管理を担当している場合には、同じ部局に所属する業務部門と連携して以下の手順で作業を進めることが想定される。

① 業務部門における非常時優先業務を特定する(論理構成※)。
② 対象業務が利用する情報システムを洗い出す(必要に応じて、情報システムが利用する基盤系システムも洗い出す)。
③ 各業務の非常時対応や業務 RTO、手作業による代替の有無等を確認し、情報システムの IT-RTO を設定する。

(※ ここで洗い出す情報システムの単位は、サーバ等物理的な構成要素ではなく、業務側で意識をしているサービスを単位とする。)




**※ 業務で直接利用しない情報システムの稼働を支える基盤系のシステムについては別途確認すること。**

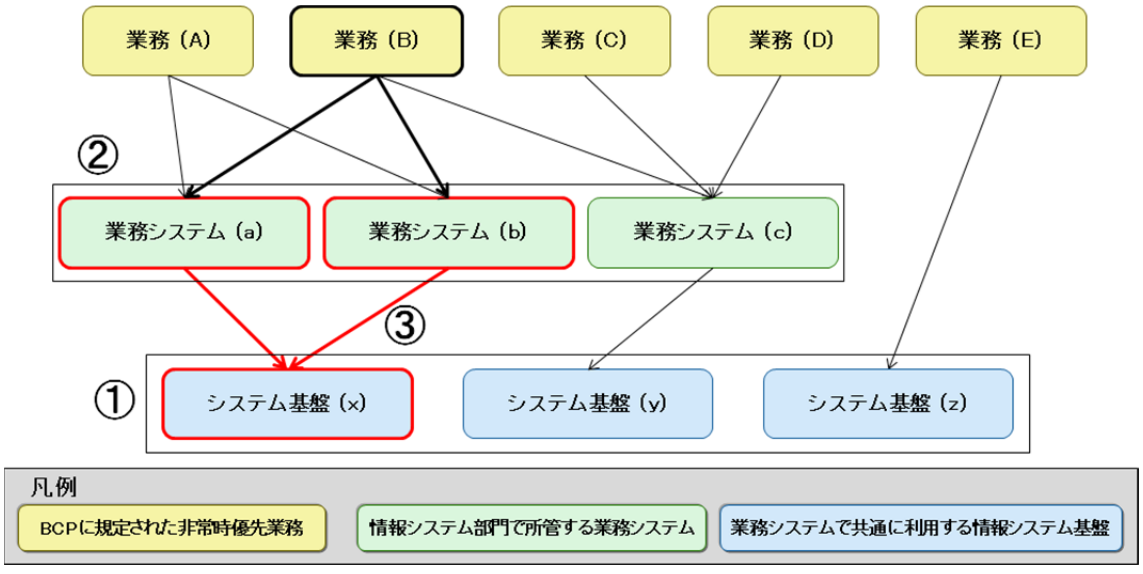
**図ー 5 優先業務と情報システムの関連整理(パターン 1)**

情報システム部門において、所管している業務システムを起点に重要業務の洗い出し等の作業に着手すると、庁内 LAN や業務で使用するパソコン等の業務執行に必要な情報資産が調査対象から除外される可能性があることに留意し、対策実施状況の確認等必要な対応を実施することが望まれる。

### (2) パターン 2 の場合

組織全体の情報システム基盤を担当する情報システム部門においては、直接業務部門と連携を取り作業を進めることは物理的に困難であると想定される。そのため、一旦は情報システム部門で IT-RTO の設定等を行い、システム基盤の利用部門から合意を得る等の作業手順の工夫が求められる。

① 情報システム部門が所管する情報システム基盤を洗い出す（必要に応じて、他の基盤や情報システムとの連携を確認する）。
② 基盤を利用している業務システムを洗い出す。
③ 業務システムの IT-RTO を確認し、情報システム基盤の IT-RTO を設定する。




**図－ 6 優先業務と情報システムの関連整理（パターン 2）**

パターン 2 の場合には、主管する情報システム基盤における対策の実施状況等を確認し、現状における情報システムの復旧可能時間を前提に、業務システム部門と非常時行動手順や復旧目標の設定について相談することを想定する。なぜなら、前述のパターン 1 においては、業務部門と直接連携を取り、必要な情報を確認することができるが、組織全体の情報システム基盤を管理す

る情報システム部門（パターン 1）においては、対象とすべき業務や関連部局が多く、確認作業が膨大な量となることが容易に想定できるからである。

### 2.3.2. 代替手段の確認と業務 RTO の調整

IT-RTO 設定の前提となる業務 RTO は、原則として府省庁の BCP に設定された非常時優先業務の目標復旧時間を用いる。しかし、業務部門において業務再開に情報システムを利用しない手作業等による代替が可能な場合は、業務 RTO の値が大幅に調整できる可能性があることに留意すべきである。

例えば、災害発生時に電話やファックスを利用した手作業により一定期間であれば暫定的な対応としてもさほど支障がないのであれば、業務を継続可能な時間の間に情報システムを復旧させることとし、IT-RTO をこの期間に合わせて設定しても問題ないと考えられる。また、パソコン内のデータの利用等の代替手段によって、暫定的に業務を再開可能な場合等も有り得る。以下に、モデル調査のヒアリング調査結果から抽出した事例等に基づき作成した、手作業による代替策の例を示す。

**表－ 9 手作業等による代替手順の例**

| 対応 | | 概要 |
|---|---|---|
| 電話やファックスの活用 | | 東日本大震災発生当時には、膨大な情報を適時に関係先に通知に当たり、極限まで対応時間を削減するために情報システムを介さずに、電話で連絡を受けながらメモを作成し、即座にファックスにより配布する等手業で情報連携を行う傾向にあった。 |
| ソーシャルメディアの活用 | | 東日本大震災発生当時は、（主に地方公共団体において）正規の情報発信と連携して、Twitter 等のソーシャルメディア経由で震災情報の周知や共有を行い、特に震災発生直後に効果を発揮した。 |
| クラウドサービスの利用 | 連絡手段や情報連携の代替 | 民間の事業者の提供するサービスを利用した電子メールや掲示板機能を利用し、モバイル回線経由で職員の情報連携を支援する対策を検討している。 |
| | 業務処理の一部復旧 | 外部保管しておいたデータをパソコンやクラウドサービス上に構築した別環境に転送し、個別処理により業務で利用するデータを集計や印刷等の対応を行うことも検討している。 |

手作業等による代替手段で業務を再開する場合には、代替可能か期間や処理可能な業務量等について業務部門と協議し、合意する必要がある。また上記の例示のように、復旧業務の一部に情報システムを利用することで、作業効率や処理速度が向上し、時間とともに処理量の増加が想定される状況への対応が可能になると考えられるので、柔軟な復旧対応について協議されることが望ましい。

### 2.3.3. IT-RTO（情報システムの目標復旧時間）と復旧優先度ランクの設定

非常時優先業務と業務 RTO を確認し、それぞれの業務が利用している情報システムとシステムの IT-RTO を設定する。

- 情報システムを利用している各業務の業務 RTO のうち、時間が最も短いものを IT-RTO として設定する。
- 基盤系システムの IT-RTO が基盤を利用している業務システムの IT-RTO より長い時間に設定されていないか確認し、適正な値に調整する。

一連の作業の実施に当たり、ガイドでは雛形の末尾に作業例としてワークシートの記入について例示している。

**表－ 10 非常時優先業務の洗い出しと情報システムの目標復旧時間の設定の例**

| No. | 情報システム名 | 業務名 | 部局 A | | | 部局 B | | | 情報システムの目標復旧時間（最小値） |
|---|---|---|---|---|---|---|---|---|---|
| | | | 優先業務 1 | 優先業務 2 | 優先業務 3 | 優先業務 4 | 優先業務 5 | 優先業務 6 | |
| | | 目標復旧時間 | 3 時間 | 1 日 | 3 日 | 3 日 | 7 日 | 30 日 | |
| 1 | システム A | | ● | | ● | | | | 3 時間 |
| 2 | システム B | | | ● | | | | | 1 日 |
| 3 | システム C | | | ● | ● | | | | 1 日 |
| 4 | システム D | | | | | ● | ● | | 3 日 |
| 5 | システム E | | | ● | | | ● | ● | 1 日 |
| | | | | | | | | | |
| | | | | | | | | | |

洗い出した情報システムの復旧優先順位やIT-RTOの値はから復旧優先度ランクを設定し、復旧優先度グループに分類する。ランクによるグループ分けを行うことで、対象とする情報システム全体を俯瞰し、検討対象に抜け漏れが無いことや優先順位付けに不整合が無いこと等が確認できる。

表－ 11 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 |

情報システムの復旧優先度ランクは、以降の作業の対象とする情報システムを絞り込む基準として用いる。情報システム部門は、前項で洗い出した情報システムの復旧優先順位やIT-RTOの値から復旧優先度ランクを設定し、「復旧優先度グループ」に分類する。

### 2.3.4. 構成要素の明確化と目標対策レベルの設定

#### (1) 構成要素について

構成要素とは、非常時の情報システムの運用継続に必要なリソースのことで、「何に対して、どの程度の対策を実施する」という行動における「何に対して」の部分に該当するもので、IT-BCPごとに確認して取りまとめておく必要がある。

以下の例示にあるように、サーバやデータ、施設・設備、情報通信ネットワーク、人員、行動手順書、外部委託している事業者等の構成要素を網羅的に洗い出し、現在の管理状況について整理する。本調査においては調査の課題認識に合わせ、ガイドでは7項目だった例示に「IT-BCPの検討体制」と「システムの代替」の2項目を追加し、9項目に拡張した。

**表－ 12 情報システムの構成要素の例**

| 構成要素 | | 構成要素の説明 |
|---|---|---|
| 1 | ハードウェア | サーバ等のハードウェア機器の役割、台数及び所在（代替機がある場合はそれも含む） |
| 2 | システム領域 | アプリケーションやシステム設定情報等の情報システム復旧に必要なデータの所在及び管理状況（バックアップ媒体の外部保管等） |
| 3 | データ領域 | 重要なデータの所在及び管理状況（バックアップ媒体の外部保管等） |
| 4 | 施設 | 情報システム機器の設置環境（庁舎、データセンタの場所・堅牢性・自家発電設備の有無・バックアップセンターの有無、電力系統の多重性、上下水道等） |
| 5 | 情報通信ネットワーク | 情報システムを利用するために必要な情報通信ネットワーク（庁舎内及び拠点間等の外部）の敷設状況（利用キャリア・種類・ルート分散状況等） |
| 6 | IT-BCP の検討体制 | （※ 本調査で追加した項目）<br>IT-BCP の内容を検討する平常時の体制 |
| 7 | システム運用体制 | システムの被害状況の早期確認や適切な対応を実施するための運用の人的体制と役割分担、手順書の整備及び連絡手段の確保 |
| 8 | ベンダの事業継続能力 | 非常時における情報システムベンダの支援・協力体制<br>（ベンダの事業継続能力把握、サービス品質保証契約の締結等） |
| 9 | システムの代替 | （※ 本調査で追加した項目）<br>非常時に、情報システムが停止している状態で業務を再開するための代替手順 |

### (2) 目標対策レベルの設定

情報システム部門は、情報システムの構成要素それぞれに対し、復旧優先度に応じて必要となる対策について検討し、対策レベルを判定するための基準として構成要素ごとに「目標対策レベル」の一覧を設定する。情報システム部門において、レベル設定を行う際には、後述の例示や別添の対策の例示等を活用することも検討されたい。

目標復旧レベルは、今後の IT-BCP の策定や対策の実行管理のための基準となる。目標対策レベルを設定することにより、IT-RTO を達成するために必要な対策の目標（ゴール）が明確化され、現在の対策の実施状況の乖離や、今後実施すべき対策の検討に活用されることが期待できる。

### (3) 目標対策レベルの設定単位

目標対策レベルは、策定する IT-BCP ごとに検討の上、設定されることが望ましいが、似通った構成要素や環境で稼働する情報システムについては、共通の目標対策レベルを適用できると考えられる。

そのため、設置場所や利用するシステム環境（基盤）、同一の管理部門等の単位で、組織に共通の目標対策レベルをあらかじめ整備しておくことも考えられる。逆に、対象部局と異なる部局が管理している構成要素であっても、調整が必要な事項は課題として記録しておくべきである。例えば、非常時の電力供給設備や庁内 LAN 等 IT-BCP で管理対象に設定した範囲と異なる部局の管理する構成要素については、所管部局による現状の対策レベルや今後の事前対策実施計画等を確認の上、レベル設定を行うべきである。

### 2.3.5. 目標対策レベルの例示

目標対策レベルの例示は、ガイドに 2 種類の例示が掲載されている。しかし、ガイドの利用状況に関するアンケート調査の回答で、例示の少なさが指摘されている。ここでは、目標対策レベルの一助となることを企図し、例示の追加を行った。(ガイド　P.24 参照))

情報システムの復旧優先度ランクに対応する対策目標(目標対策レベル)をシステム構成要素ごとに整理した。以下に設定結果の例を示す。

#### ① ハードウェアの目標対策レベル

| 復旧優先度ランク | 対策目標 | 対策レベル |
|---|---|---|
| S<br>A | **ホットスタンバイ用ハードウェアの確保**<br>・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し、データの同期を取る。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。<br>・被災時用の代替クライアント PC を用意する。 | 3 |
| B<br>C | **コールドスタンバイ用ハードウェアの確保**<br>・現在の拠点と同時被災しない拠点にデータのセットアップが必要な状態の予備機を準備する。<br>・シンクライアントを用い、執務環境の被災によるクライアント環境への影響を回避する。 | 2 |
| D<br>E | **ハード保守の締結による保守切れ品の根絶(被災拠点での復旧)**<br>・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。<br>・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。<br>・クライアント PC の動作環境のデータを定期的に退避する。 | 1 |

### ② システム領域の目標対策レベル

| 復旧優先度ランク | 対策目標 | 対策レベル |
|---|---|---|
| S<br>A | **ホットスタンバイ方式**<br>・本番機のシステムメンテナンス時前後に、本番機のシステム領域のバックアップデータを代替拠点の代替機上に転送している。<br>・代替機についても、代替拠点固有の環境に合わせたシステムメンテナンスを行い、切替可能な環境を保っている。 | 3 |
| B<br>C | **外部保管**<br>・システムメンテナンスの前後にバックアップ媒体(テープ等)にシステム領域をバックアップし、本番機と同時被災しない遠隔地に保管している。災害発生時は、バックアップを取り寄せる。 | 2 |
| D<br>E | **内部保管**<br>・システムメンテナンスの直前にバックアップ媒体(テープ等)にシステム領域をバックアップし、本番機と同じ拠点内の堅牢な金庫に保管している。災害発生時は、バックアップを取り出し、システムメンテナンスを行って復旧する。 | 1 |

### ③ データ領域の目標対策レベル

| 復旧優先度ランク | 対策目標 | 対策レベル |
|---|---|---|
| S<br>A | **データ同期**<br>・代替拠点で、データ同期を利用し本番環境における災害発生直前のデータを保全している。 | 3 |
| B<br>C | **外部保管**<br>・データ領域を週次でフルバックアップ、日次で差分バックアップを行い、バックアップ媒体(テープ等)へバックアップし、本番機と同時被災しない遠隔地に保管している。災害発生時は、バックアップを取り寄せる。 | 2 |
| D<br>E | **内部保管**<br>・週次でバックアップ媒体(テープ等)にデータ領域をバックアップし、本番機と同じ拠点内の堅牢な金庫に保管している。災害発生時は、バックアップを取り出して用いる。 | 1 |

### ④ 施設の目標対策レベル

| 復旧優先度ランク | 対策目標 | 対策レベル |
|---|---|---|
| S<br>A | **堅牢なデータセンタ**<br>・震度6強を超える地震に耐える耐震性の高いデータセンタの免震床にサーバ機器を耐震固定して設置している。<br>・自家発電装置があり、停電後 3 日間程度は全てのシステム機器に給電が可能である。 | 3 |
| B<br>C | **一般のデータセンタ**<br>・震度6強の地震に耐えるデータセンタ内でサーバ機器を免震ラック上に設置している。<br>・自家発電装置があり、停電後 3 日間程度は重要システムの運用に限定したシステム機器に給電が可能である。 | 2 |
| D<br>E | **一般のビル**<br>・震度6強の地震に耐える一般のビルにサーバ機器を設置している。<br>・無停電電源装置（UPS）が設置され、停電後 10 分程度の給電を維持できる。 | 1 |

### ⑤ 情報通信ネットワークの目標対策レベル

| 復旧優先度ランク | 対策目標 | 対策レベル |
|---|---|---|
| S<br>A | **冗長化構成**<br>・ネットワーク機器及び構内回線（LAN）を冗長化している。<br>・外部とのネットワーク（WAN）のキャリアを冗長化している。 | 3 |
| B<br>C | **一部冗長化構成＋WAN の冗長化**<br>・主要なネットワーク機器及び構内回線（LAN）を冗長化している。<br>・外部とのネットワーク（WAN）のキャリアを冗長化している。 | 2 |
| D<br>E | **一部冗長化構成**<br>・主要なネットワーク機器及び構内回線（LAN）を冗長化している。<br>・主要な外部とのネットワーク（WAN）のみを冗長化している。 | 1 |

### ⑥ IT-BCP の検討体制の目標対策レベル

| 復旧優先度ランク | 対策目標 | 対策レベル |
|---|---|---|
| S<br>A | ・情報システム部門が関連部門と協議を行い、IT-RTO 等を決定する。<br>・構成管理を行い、システムの部分停止が業務に与える影響範囲を把握している。 | 3 |
| B<br>C | ・情報システム部門が関連部門と協議を行い、IT-RTO 等を決定する。<br>・システムの重要度を把握し、被災時の復旧優先度が明確になっている。 | 2 |
| D<br>E | ・情報システム部門が主体となって IT-RTO 等を検討し、関連部門が追認する。<br>・構成管理を行い、優先業務と情報システムの関連を把握している。 | 1 |

### ⑦ システム運用体制の目標対策レベル

| 復旧優先度ランク | 対策目標 | 対策レベル |
|---|---|---|
| S<br>A | ・被災時の対応体制と役割が明確になっており、意思決定者不在の場合の代行者が規定されている。<br>・実機を用いたシステムの復旧や切替の訓練が実施されている。<br>・非常時の対応計画が整備されており、継続的な改善が行われている。 | 3 |
| B<br>C | ・被災時の対応体制と役割が明確になっており、意思決定者不在の場合の代行者が規定されている。<br>・非常時の対応計画が整備されており、対応計画の読み合わせによる検証が実施され、継続的な改善が行われている。 | 2 |
| D<br>E | ・被災時の対応体制と役割が明確になっている。<br>・非常時の対応計画が整備されており、対応計画の読み合わせによる検証が実施されている。 | 1 |

### ⑧ ベンダの事業継続能力の目標対策レベル

| 復旧優先度ランク | 対策目標 | 対策レベル |
|---|---|---|
| S<br>A | ・被災時の SLA があり、対応が明確になっている。<br>・実機を用いたシステムの復旧や切替の訓練が実施されている。<br>・ベンダの非常時の対応計画が整備されており、継続的な改善が行われている。 | 3 |
| B<br>C | ・ベンダに被災時の優先対応を依頼している。<br>・ベンダの非常時の対応計画が整備されており、対応計画の読み合わせによる検証が実施され、継続的な改善が行われている。 | 2 |
| D<br>E | ・ベンダの非常時の連絡先を把握し、最新化している。<br>・ベンダの非常時の対応計画が整備されており、対応計画の読み合わせによる検証が実施されている。 | 1 |

### ⑨ システムの代替の目標対策レベル

| 復旧優先度ランク | 対策目標 | 対策レベル |
|---|---|---|
| S<br>A | ・システム停止時の代替対応として、手作業による対応で用いる業務マニュアルが整備されている。<br>・参照専用の機能が用意され、バックアップデータが参照できる。 | 3 |
| B<br>C | ・システム停止時に手作業による代替対応で用いる様式が整備されている。<br>・クライアント PC 上の事前退避したローカルデータを参照する機能がある。 | 2 |
| D<br>E | ・システム停止時に手作業による代替対応で用いる様式が整備されている。<br>・定期的に台帳印刷を行い、非常時に参照できる。 | 1 |

また、本調査報告書では、情報システムの構成要素ごとに対処要件を取りまとめ、それぞれの要件について対策例と詳細な解説を加えた資料を参考に添付しているので参照されたい。

## 2.4. 計画策定（全体、個別）

2.7. 事前対策計画の検討

2.8. 非常時の対応計画の検討

2.9. 教育訓練計画・維持改善計画の検討

【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。

【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（雛形 「4.1.教育訓練計画」の例を参照のこと）。
- 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等、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。

IT-BCP にとって、計画の策定は以下の 2 つの意味を持つことに留意されたい。

- 非常時の行動と、それに必要なリソースを明示すること（順番より必要最小限の実施事項の明確化）。
- 継続的な運用改善に必要な活動の整理と、それぞれの観点を明示すること。

IT-BCP は、非常時の対応計画のみで構成されるものではない。策定した対応計画に基づく訓練を実施し、計

**画の不備や非効率な個所については課題として明確にした上、継続的に改善する対象として管理し続ける必要がある。**

**大規模災害発生時の対策本部を担当する府省庁においては、必要な計画を整備し、それに基づく教育・訓練の実施や継続的な改善が日常業務の一環として定着していることや、東日本大震災の発生当時には、即座に本部員が対策本部に参集し、対応業務が開始されたことが報告されている。**

**一方、府省庁においては定期的な人事異動等の組織的な制約が、中長期的な課題管理や計画策定を適切に行うことの阻害要因となっている事実も見られた。モデル調査の結果からは、IT-BCP に含まれる個別の計画について、それぞれ以下のような懸念点が見られた。**

- **受容を決定したリスク(危機的事象)を事前対策計画に反映していない。**
- **ガイドに例示した全体フローをそのまま流用したため、効率的な対応を取ることができるか判然としない。**
- **IT-BCP 策定に合わせて教育訓練計画を立てたが、実際には実施していない。**

**IT-BCP に関する情報システムの対策は、大掛かりなシステム構成等の変更や費用負担を要するものも多く、システム更改の時期に合わせて採用することを検討する以外に導入の機会がほとんどない場合もある。そのような場合においては、継続的な改善活動で確認された課題を中長期的な対応により解消することも十分想定される。そのため、事前対策計画には、次のシステム更改のタイミングで対処する予定の課題等、中・長期的に対処を予定している未解決の事項も記載しなければならないことに留意されたい。**

### 2.4.1. IT-BCP の文書体系について

IT-BCP は、情報システム運用継続の体制を整備し、継続的に維持するための一連の活動を規定する文書の集合として策定されるものである。ガイドに添付されている雛形は、「非常時の対応計画」を中心に、「事前対策計画」や「教育・訓練の計画」、「維持改善に関する計画」等が含まれた一つの文書として提供している。

策定した IT-BCP の文書が組織における規定文書に該当するかどうか、ガイドには明示されていないが、モデル調査においては、文書の策定単位や更新頻度の違いや部門における取扱い等の観点から、複数の文書に分割して IT-BCP を構成する工夫が確認されている。例えば、更新頻度の高い情報については、IT-BCP 本文に含めないで別紙として部門等の承認の対象から除外している事例は複数確認された。

今後、部門のルールとして IT-BCP を取り込むことを検討する場合には、更新頻度の高い事項

に（例えば緊急時連絡体制図等）ついてIT-BCPから分離して部門限りの文書として整理する等、文書体系についても十分検討することを留意されたい。

### 2.4.2. 事前対策計画の検討

「事前対策計画」は、現状の情報システムの「脆弱性」を解消し目標対策レベルに近づけていくために、対策の実施について短期と中・長期等いくつかのステップに分けて段階的な実施を検討して作成される実施計画である。情報システムの運用継続能力は、この計画に沿って段階的に対策を実施していくことで強化される。また、脆弱性を継続的に管理する枠組みを整備することで、解消されずに残る残留リスクにはどのようなものがあり、どのような対策を実施することで解消されるか等の情報システム運用継続における課題を評価し適切に管理することができる。

事前対策計画は、以下の手順に沿って現状対策レベルの確認と脆弱性の評価を実施することで策定できる。

① 前項で設定した、情報システムの構成要素ごとの目標対策レベルに対する現状の対策レベルを確認する。
② 確認した現状の対策レベルを総括し、情報システムの重大な脆弱性を洗い出す。
③ 確認した重大な脆弱性について、目標対策レベルと現状の対策レベルのギャップを解消するための事前対策実施方針を検討し、それに基づく対策の詳細ステップを作成する。

ガイドでは、構成要素ごとに短期、中期、長期等のステップに分けて実施する対策の内容や必要予算、実施主体等について事前対策計画として取りまとめることを推奨している。以下に、ガイドに掲載されている構成要素ごとの現状の対策レベルと脆弱性の分析結果の例を示す。

**表－ 13 現状の対策レベルと脆弱性の分析結果（メールシステムの例）**

| 管理部局 | | 復旧優先度（IT-RTO） | 目標対策レベル |
|---|---|---|---|
| 部局 A | | A（数時間～数日） | 4 |
| 首都直下型地震における脆弱性 | | | |
| 構成要素 | 現状対策レベル | 構成要素ごとの脆弱性 | |
| ハードウェア | 0 | ● 現状、免震／耐震措置が取られておらず、サーバが損壊する可能性が高い。サーバが損壊した場合、同等機の再調達に長期間（約〇週間）を要する。 | |

| | | |
|---|---|---|
| システム領域 | 0 | ● バックアップ媒体が、非常時に損壊する可能性のある場所に保管されている。 |
| データ領域 | 0 | ● バックアップが未取得であり、被災時に必要なデータが消失する可能性がある。 |
| ・・・ | | |
| ベンダの継続能力 | ― | |
| ・・・ | | |

**(1) 確認された脆弱性に対して対策が未実施の場合の取扱いについて**

前述のとおり、事前対策計画は短期と中・長期等いくつかのステップに分けて段階的な実施計画を取りまとめたものであり、非常時の業務継続を阻害する要因を管理するリスク管理のサイクルを確立するための重要な作業である。しかし、実態としては、実施が決定していなかったり、予算の裏付けが取られていなかったりする対策案を正式な文書(IT-BCP)に含めない事例が見られた。

実施が決定していない対策を計画文書に掲示することで、その課題に対して対処していると誤解を与えてしまうことが懸念された等計画に残留リスクに対する継続的な取組を記載しないことの理由は様々だが、分析の過程で確認された業務再開を阻害する可能性のある脆弱性が管理されていない状態のまま放置されてしまうことは問題がある。

IT-BCPの策定を担当する情報システム部門においては、確認された脆弱性については確実に記録に残すべきであり、情報システム運用継続の責任者や最高責任者は、脆弱性分析の結果や事前対策計画の内容をレビュし、残存リスクを十分認識しなければならない。

### (2) 事前対策実施方針と対策実施の詳細ステップ

IT-BCP 策定の過程で確認された情報システムの重大な脆弱性については、対策の実施が決定されていない事項についても、事前対策計画の中・長期的な課題として採用し、対応の継続検討を方針に明記することが望まれる。

表－ 14 事前対策実施方針の取りまとめの例

<table>
<tr><th>管理部局</th><th>復旧優先度(IT-RTO)</th><th>目標対策レベル</th></tr>
<tr><td>部局 A</td><td>A(数時間～数日)</td><td>4</td></tr>
<tr><td colspan="3">事前対策実施方針</td></tr>
<tr><td colspan="3">ステップ 1(実施予定年度:〇〇年度～〇〇年度)</td></tr>
<tr><td></td><td>実施内容</td><td>(1)首都直下型地震に備えた現状のシステムの堅牢化<br>・サーバの免震／耐震措置の推進<br>・バックアップの実施と同時被災しない拠点への外部保管<br>・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<br>・・・<br>(2)予期せぬシステム停止に備えたルール・手順書の整備<br>・マルウェア感染によりシステムが停止した場合の対処方法の手順化<br>・・・</td></tr>
<tr><td></td><td>期待効果</td><td>• サーバの免震／耐震措置により、首都直下型地震発生時もシステムが停止する可能性が低減される。<br>• バックアップの確実な実施によりデータの消失を防ぎ、非常時に少なくとも復旧可能な状態となる。<br>・・・</td></tr>
<tr><td></td><td>残存リスク</td><td>• 想定以上の被害に見舞われた場合は、情報システム機器の再調達が必要になり、システムの復旧まで 1～3 ヵ月強の時間を要し、いずれの情報システムも IT-RTO 内で復旧できない可能性がある。<br>・・・</td></tr>
<tr><td colspan="3">ステップ 2(実施予定年度:〇〇年度～〇〇年度)</td></tr>
<tr><td colspan="3">・・・</td></tr>
</table>

また、対策の実施が決定していない場合でも、対策実施の詳細ステップには中・長期的な計画についてもステップを設定し、対策の「あるべき姿」を部門内で管理し、継続的に見直しを実施する体制を維持すべきである。

**表－ 15 対策実施の詳細ステップの例**

1. メールシステム（例）

| | |
|---|---|
| ステップ1 | 実施予定年度：○○年度～○○年度<br>（1） 首都直下型地震に備えた現状の情報システムの堅牢化<br>（2） 予期せぬシステム停止に備えたルール・手順書の整備 |

ステップ 1-(1)「首都直下型地震に備えた現状のシステムの堅牢化」対策の詳細一覧

| 構成要素 | 現状レベル | ステップ 1 到達レベル | 対策実施内容 | 必要予算（千円） | 実施主体 |
|---|---|---|---|---|---|
| ハードウェア | 0 | 1 | ・免震ラックの導入<br>・・・ | | 部局 A<br>○担当 |
| システム領域 | 0 | 1 | ・バックアップ頻度の検討<br>・バックアップ方式検討<br>・・・ | | 部局 A<br>○担当 |
| データ領域 | 1 | 1 | ・バックアップ頻度の検討<br>・バックアップ方式検討<br>・・・ | | 部局 A<br>○担当 |
| ・・・ | ・・・ | ・・・ | ・・・ | | |

### (4) 簡易的な脆弱性分析の実施

ガイドには、事前対策計画の策定手順とともに、優先的に実施すべき対策の一覧も掲載されている。様々な理由から情報システム部門において個別に脆弱性評価を実施できない場合には、一覧の内容を確認し、管理している情報システムの対策実施状況を確認することが望まれる。

**表－ 16 優先して検討すべき脆弱性の例**

| 重大な脆弱性 | 注意すべき例 |
|---|---|
| 危機事象発生時の対応体制及び連絡方法の整備状況 | ● 情報システムの復旧と継続作業を行うための、体制、役割分担及び復旧の手順書が無い。<br>● 復旧継続に必要な要員（職員及び外部委託業者）の連絡先一覧表が最新のものに更新されていない。<br>● 復旧継続に必要な情報（府省庁内 LAN 構成図・ホームページ更新手順・復旧マニュアル等）が未整備である。<br>● 休日や夜間の連絡方法及び参集方法が明確になっていない。<br>● 特定の要員に依存しており、当該要員が不在の場合には復旧継続ができない（ホームページ更新、LAN の設定等）。 |
| 同一拠点内でのハードウェアへの対策状況 | ● 重要な業務で利用するサーバが二重化対応されていない（ハードウェア故障時に予備サーバに切り替わる等。平常時のハード障害でも業務に大きな支障をきたす恐れがあると共に、災害時にハードウェアの被災で停止する可能性や復旧にかかる時間が長期化する可能性が高まる）。 |
| 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 | ● 重要なデータのバックアップを取得していない、あるいはバックアップの頻度がデータの更新頻度と比較して少なすぎる（毎日更新されるデータに対して、月 1 回程度等）。<br>● バックアップ媒体が無造作に置かれており損壊や紛失の危険性がある。<br>● 情報システムの設置場所と同じ場所にバックアップ媒体が保管されており、情報システム設置場所に立ち入れない場合、利用できない恐れがある。<br>● バックアップしたデータを復元利用するテストを実施したことが無い。 |
| 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 | ● 既に販売終了しており調達困難なハードウェア・ソフトウェアを利用している。<br>● 再調達に極めて時間を要する機器類を利用している（ホストやオフィスコンピュータ 、特殊な仕様で発注した特注品等）。 |

### 2.4.3. 非常時対応計画の検討

非常時対応計画は、大地震等の被災時や予期せぬシステム停止が発生した場合等の非常時に、業務を継続するために、復旧作業に当たる担当者が、非常時に必要な実施事項を確実に抜け漏れなく実施できるようにすることを目的に作成される。計画は、非常時における情報システム部門の対応手順や業務部門等との連携を俯瞰するための「全体フロー」と、それぞれの対応を具体的に記した「対応手順」について検討し、取りまとめなければならない。また、非常時に業務を継続するために、関連する部門間で情報の共有や分類・整理を行い、適切な意思決定者に報告(伝達)するための手順を整備しておくことが必要である。そのため、平常時から部門間の役割分担や業務の継続に必要な事項を整理し、対応手順を検討しておくことが望まれる。

また、非常時の情報システム部門の役割分担や各担当が不在の場合の代行順位を定めた体制図や、府省庁の内外の組織との連携を示す連絡先一覧表等についても、平常時から整備し定期貴的に内容を更新することが望まれる。非常時対応計画には、以下の事項が含まれているべきである。

**表－ 17 非常時対応計画に含まれる事項**

| 作成文書 | 概要 |
|---|---|
| 非常時の対応体制 | 非常時に、既存の非常時体制と連携し情報システムの復旧継続活動を効率的に実施できるよう、情報システムの復旧にかかわる非常時の対応体制を構築し役割分担を定める。 |
| 情報システム復旧にかかわる判断基準 | 要員参集基準や情報システム切り替え基準等の復旧対応に必要な判断のための基準を定める。 |
| 全体フロー | 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を流れ図(フロー)にまとめる。 |
| 対応手順 | 全体フローを踏まえ、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。 |
| 代替拠点における運用計画 | 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、本番環境における各府省庁の情報システム運用計画の形式に準じ、必要な項目の漏れのない計画を作成する (※ 代替拠点がある場合)。 |

また、モデル調査の結果から、非常時対応を運用委託先の情報システムベンダに依頼し、情報システム部門として復旧手順の内容を確認していないという状況が見られた。

非常時対応計画の策定時は、運用業務等を委託している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依頼し、情報システム部門は復旧目標の協議や復旧手順の確認等ベンダの整備作業に適切に関与し、府省庁の監督責任者としての責務を果たすことが望まれる。

### 2.4.4. 教育訓練実施計画の検討

情報システム部門が、緊急対応をスムーズに実施できるようにするために、平常時に教育・訓練を継続的に実施する必要がある。

モデル調査の結果から、IT-BCP を策定済みの府省庁においては訓練計画が策定されていた。しかし、実際に訓練は実施されている実績は少なかった。これは、IT-BCP の策定状況にかかわらず、情報システム部門における非常時の対応組織や行動手順が十分に検討されていないことが理由であることが考えられる。

訓練の実施について、ガイドには大別すると 2 つの意義が示されている。(ガイド P.35 参照)

**表－ 18 教育訓練の意義**

| 訓練の意義 | 概要 |
|---|---|
| 担当者の理解や対応力の向上 | ● 災害発生時に情報システムを復旧継続する計画行動に対する担当者の理解や対応力を向上させる。 |
| 計画や対策の改善 | ● 実施した事前対策の有効性を確認し、これらの計画や対策に改善すべき点があれば、改善活動につなげる。 |

教育・訓練を実施する目的として、個人や組織の対応力向上は比較的容易に理解することができると思うが、それ以上に策定したIT-BCP の実効性を確認し、必要に応じて改善するための数少ない重要な機会であることを理解されたい。

情報システム部門においては、年間の訓練計画等についても、自らの組織の体制や対策実施の進捗度合い等を確認の上、達成目標を明確にすべきである。その上で以下の分類等の資料を参照し、適切な訓練方法を検討、実施することが望まれる。

情報システムにかかわる教育訓練は、上記の目的に沿って以下の3つに分類される。

**表－ 19 教育訓練の分類**

| 分類 | 訓練目的の概要 |
|---|---|
| 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 | ● 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、維持改善を担当する担当者が、業務継続に関する適切な知識と力量を身につける。 |
| ② 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の内容を関係者が習熟し、計画内容に不備や改善点がないか事前に検証する。<br>● 非常時に、どのような状況が発生しても適切に対応できる「危機対応能力」を高める。 |
| ③ 事前対策内容の動作確認と検証 | ● バックアップや代替環境等の情報システムに対する事前対策が被災時に機能・動作するか、訓練を通して確認・検証する。 |

以下に分類に応じた、教育訓練の手法及びその概要を示す。教育訓練の種別は、机上と実働の2つに分類される。机上は座学又はシミュレーションであり、実働は実機を用いて研修又は訓練を行う。

**表－ 20 教育訓練の分類**

| 分類 | 手法 | 種別 | 概要 |
|---|---|---|---|
| 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 | 研修会 | 机上 | 民間団体等の主催するセミナー等を受講し、基礎的な考え方を理解する。 |
| ② 非常時対応計画の理解と対応能力の向上 | 読み合わせ | 机上 | 被災想定に基づき訓練時の状況を設定し、その状況下での対応を、計画に沿って確認する。 |
| | モックディザスタ | 机上 | 事前に訓練時の状況を設定するが、発生する事象については参加者に知らさず、その都度情報を与えて対応を検討させる。 |
| | 総合訓練 | 実働 | データセンタと庁舎等、複数の拠点において、時間の同期を取りながら事前に決めた被災シナリオに沿って実機を用いた対応を実施する。 |
| ③ 事前対策内容の動作確認と検証 | システム復旧訓練 | 実働 | 本番環境又は開発環境を用い、実際にシステムの復旧や切替を実施する。 |

### 2.4.5. 維持改善計画の検討

維持改善計画は、前述の 3 つの計画についてそれぞれを定期的に見直し、継続的に IT-BCP の実効性を維持することを目的に作成する。維持改善計画には、主に IT-BCP の見直し時期や見直しの内容、実施主体について取りまとめられている。

特に、見直しの時期については、十分に検討の上、計画に記載すべきである。モデル調査においては、定期的な見直しに加えて、以下に示すような計画見直しのタイミングについて示されている事例が確認された。

**表－ 21 計画の見直しを行うタイミングの例**

| タイミング | 概要 |
|---|---|
| 組織変更 | ● 情報システム部門や業務部門、その他関連部門における組織変更に伴う担当者や連絡先の変更等<br>● 委託先事業者における組織変更に伴う担当者や連絡先の変更等 |
| 情報システムの更改等 | ● 情報システム（ハード/ソフト/施設・設備）の新規開発や追加等<br>● 情報システム（ハード/ソフト/施設・設備）の更改等 |
| 環境の変化 | ● 被災状況等の想定の変化<br>● 最新の技術動向等 |
| 制度改正や基準等の改訂 | ● 準拠法や制度、ガイドライン等の改正 |
| 訓練の終了後 | ● 訓練実施後に、アンケート調査や聞き取り等により抽出された課題に対応 |

## 2.5. 実施（評価、改善）

| （ガイドには該当する記述はない） |
| --- |
| ● 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、常に計画の最新化を維持するように努める。<br>● 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。） |
| 平常時には、IT-BCP が発動される機会は無く、適切な維持管理の活動を実施しなければ、組織や個人における習熟度は低下するばかりで、非常時に適切に対応できる状態を維持することは困難である。<br>前述のとおり、大規模災害発生時の対策本部を担当する府省庁においては、定期的な訓練の実施により、習熟度の低下を防ぐとともに、継続的な維持完全活動を実施し、より効率的な非常時の対応について検討を続けている。モデル調査の結果からも、情報システムの構築や運用を委託した事業者に定期的な非常時対応の訓練実施を義務付けたり、システム更改を協議する際の議題の一つとして非常時の情報システム運用継続を取り上げたりする等の工夫は見られた。また、定期的な訓練についても、徐々に実施を検討する府省庁が増加傾向にあると想定される。<br>今後は、IT-BCP の維持改善に必要な活動の実施とともに、活動の記録を残すことに留意されたい。 |

情報システム運用継続を検討する体制の重要性や、連携すべき部局等については、先に述べたとおりである。同様に、情報システムの運用時においても関係部局と緊密に連携を取らなければならない。

運用時において特に重要な活動の一つが維持管理活動であり、継続的に実施することが望まれる。文献調査で収集した情報で、過去にシステム復旧において問題となった事項が調査されている。[8]結果は、「復旧手順が未整備、手順が不明確」が最も多くの回答を占めた例もあるとおり、IT-BCP の維持改善計画に規定したタイミングで適宜計画や行動手順の見直し等を実施し、現状の手順における課題を洗い出すことが重要である。その結果抽出された課題を解決する対策を実施し、計画や行動手順の最適化を行う。

[8] 「3.1.1 東日本大震災による情報システムに対する被害状況(3) 情報システム復旧の課題」（P.61）

# 3. 参考資料

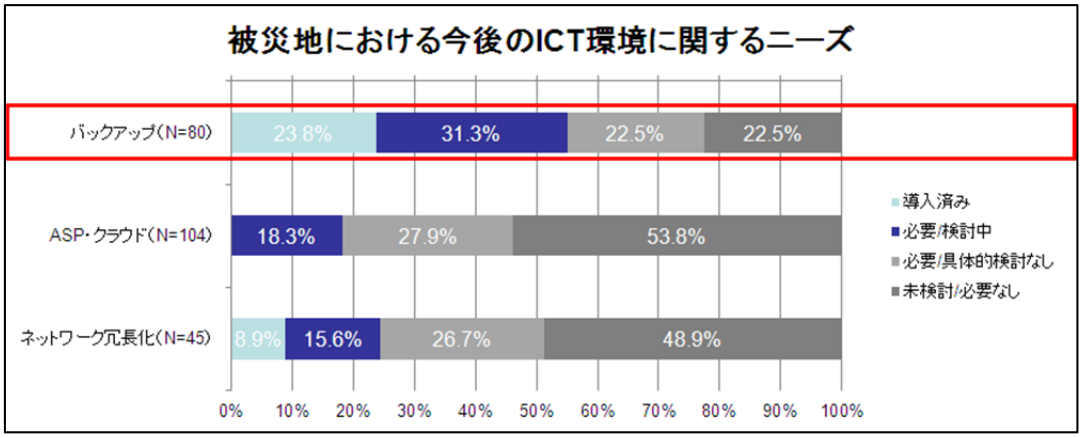
## 3.1. 東日本大震災の被災から得られた IT-BCP に関する教訓

2011 年（平成 23 年）3 月 11 日に発生した東日本大震災により、政府機関の情報通信基盤は甚大な被害を受け、被災地における迅速な情報収集や連絡、意思決定を支援する本来の役割を果たすことができなかった。発災当初の広域な電力の喪失やこれに起因するネットワーク障害による通信回線の遮断、輻輳は想定していた水準を大きく超え、被災地との連絡が一時途絶する状況にまで至った。ここでは、東日本大震災の被災経験から得られた教訓や IT-BCP 策定状況、採用されている対策について、前述のガイドや過年度に NISC が公開した「東日本大震災における政府機関の情報システムに対する被害状況調査及び分析（最終報告書）（以下、「被害状況調査」とする。）」や独立行政法人情報処理推進機構　技術本部ソフトウェア・エンジニアリング・センター（以下、「IPA/SEC」とする。）が 2012 年 7 月公開した「情報システム基盤の復旧に関する対策の調査（以下、「IPA 調査」とする。）」[9]との対比を試みた。

### 3.1.1. 東日本大震災による情報システムに対する被害状況

#### （1） 被災地におけるニーズ

総務省が実施した調査[10]の結果から、被災した企業や団体における IT 環境においてはバックアップのニーズが高く、被災経験者がデータ保全対策を重要であると認識していることが分かる。

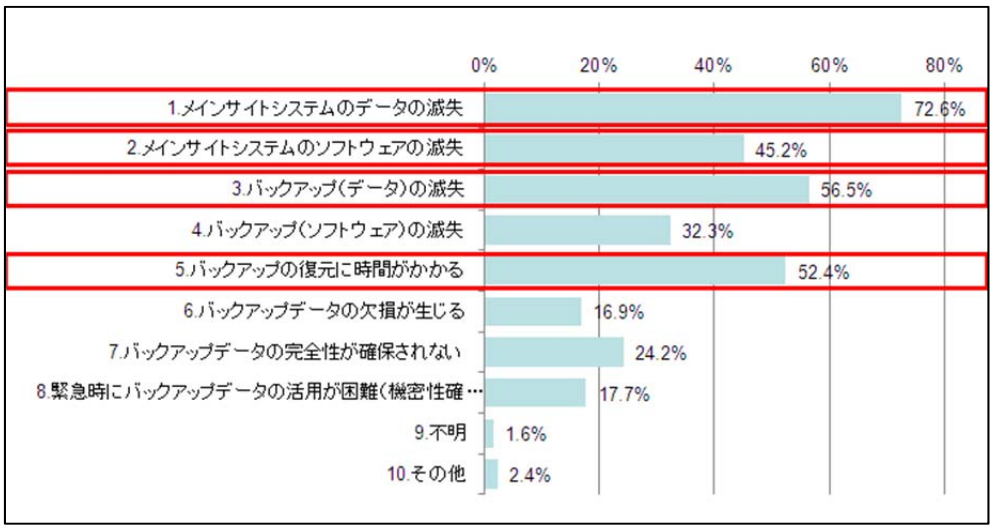



「災害時における情報通信の在り方に関する調査結果」（2012 年 3 月総務省　P.50）のデータを基に作成

**図－ 7　被災地の企業や地方公共団体における IT 環境に関するニーズ**

[9] 「情報システム基盤の復旧に関する対策の調査報告書」（独立行政法人情報処理推進機構　2012 年 7 月）
http://sec.ipa.go.jp/reports/20120725.html
[10] 「災害時における情報通信の在り方に関する調査結果」（2012 年 3 月総務省）
http://www.soumu.go.jp/menu_news/s-news/01tsushin02_02000036.html

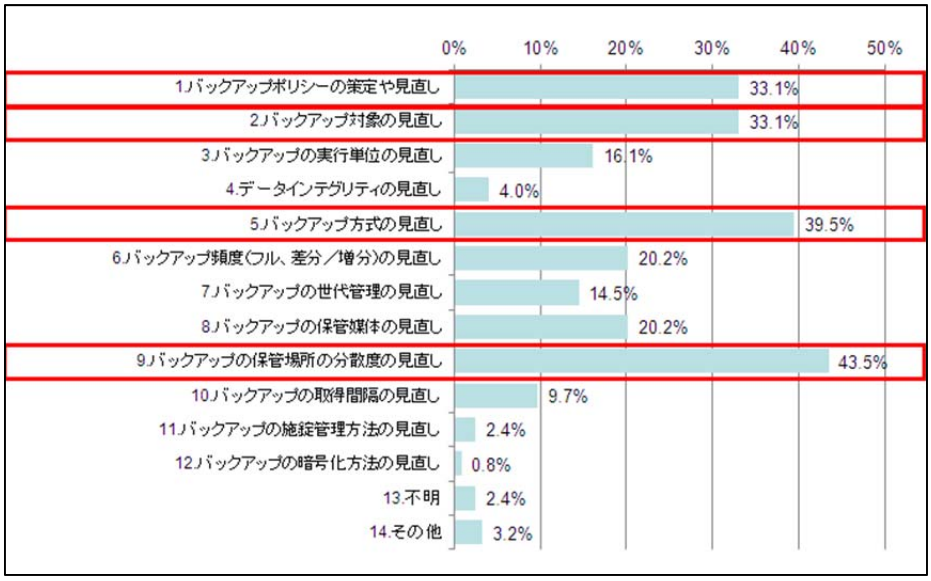
民間企業において震災で経験した又は今後懸念する、データの保管（バックアップ）に関する被害や問題は、「メインサイトのシステムのデータの滅失」が最も多く回答され、以下「バックアップ（データ）の滅失」や「バックアップの復元に時間が掛かる」、「メインサイトのシステムのソフトウェアの滅失」等の被害や懸念事項が示されている。




「情報システム基盤の復旧に関する対策の調査報告書」（独立行政法人情報処理推進機構　P.100）のデータを基に作成

**図－ 8　震災で経験した又は今後懸念する、データの保管（バックアップ）に関する被害や問題**

また、震災後に検討を開始したデータの保管（バックアップ）に関する対策として、「バックアップの保管場所の分散度の見直し」が最も多く、対策を検討した企業の半数近くが挙げている。




「情報システム基盤の復旧に関する対策の調査報告書」（独立行政法人情報処理推進機構　P.101）のデータを基に作成

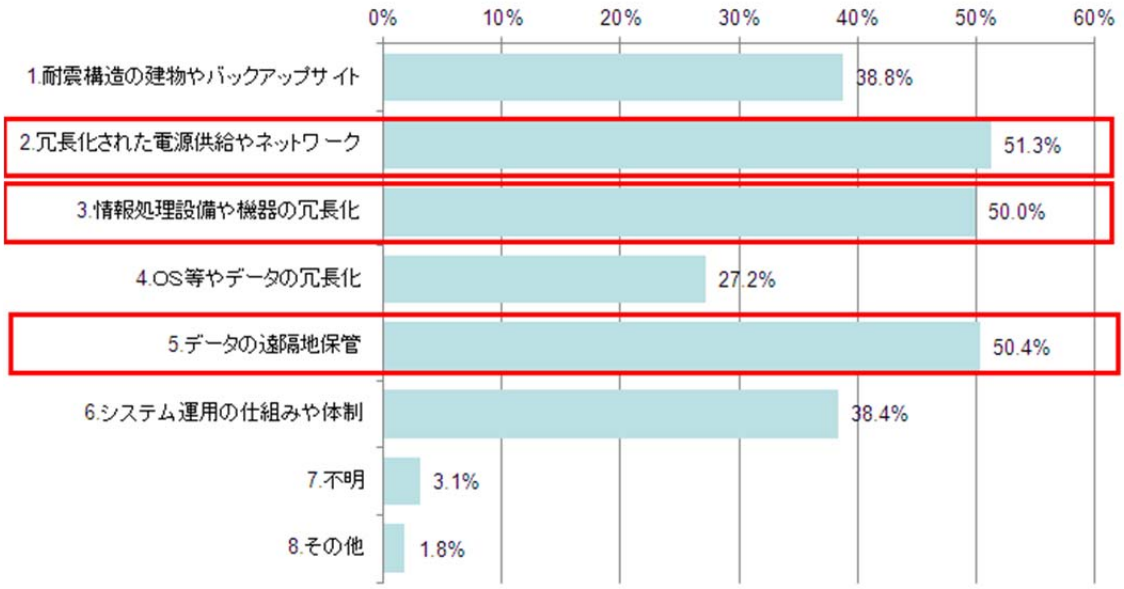
**図－ 9 震災後に検討を開始したデータの保管（バックアップ）に関する対策**

被害状況調査においては、データの遠隔地保管時の留意点として以下の点を示している。

- **データ領域及びシステム領域のバックアップを取得すること、特にデータバックアップはデータ消去を回避するため、同時被災しない拠点への外部保管が必要である。**
- **保管先は、遠隔地であることが望ましいが、被災後の物流網の乱れから媒体の輸送が滞ることで時間を浪費する可能性がある。したがって、保管先については複数箇所に分散させることが望ましい。**
- **システム領域のバックアップは定期的に外部媒体に取得し、その保管先は耐火・耐震性の高い堅牢な金庫だけでなく、同時被災しない遠隔地にも併せて保管することが望ましい。**
- **バックアップの手段は、外部媒体の輸送が安価ではあるが物理的な日数を要するため、ネットワーク経由での伝送が望ましい。**

### (2) 震災後に情報システムの運用継続において重点的に取り組んでいる領域

民間企業において重点的に取り組んでいる情報システムの運用継続に関する領域の上位 3 件は「冗長化された電源供給やネットワーク」、「データの遠隔地保管」、「情報処理設備や機器の冗長化」であることが確認されている。同様に、被害状況調査においても、ネットワーク[11]やハードウェア[12]の冗長化対策、データの遠隔地保管[13]について一定の効果があったと結論付けられている。

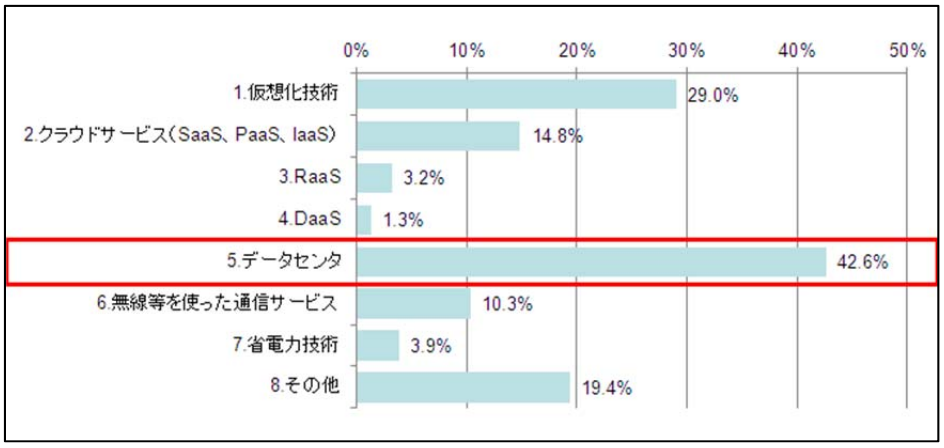



「情報システム基盤の復旧に関する対策の調査報告書」(独立行政法人情報処理推進機構 P.80)のデータを基に作成

**図ー 10 情報システムの運用継続において重点的に取り組んでいる領域**

[11] 「4.2.4. ネットワーク(LAN)に関する被害の傾向と対策の分析」(P.23-25)
[12] 「4.2.10. ハードウェアに関する被害の傾向対策の分析」(P.43-46)
[13] 「4.2.11. データ(システム領域・データ領域)に関する被害の傾向と対策の分析」(P.47-49)

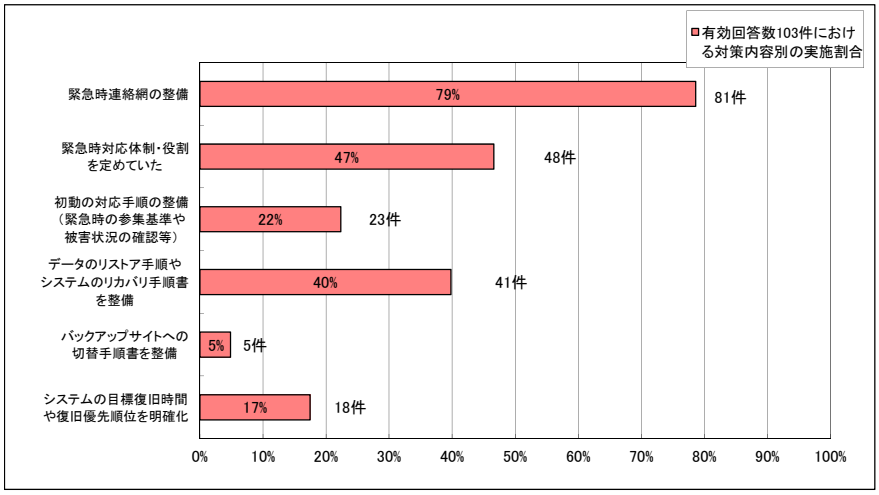
システム復旧に有効であった技術やサービスとして、「データセンタ」が上位で回答されているが、「仮想化技術」や「クラウドサービス」等の回答も上位を占めている。[14]




「情報システム基盤の復旧に関する対策の調査報告書」(独立行政法人情報処理推進機構　P.103)のデータを基に作成

**図ー 11　システム復旧に有効であった技術やサービス**

被害状況調査において、東日本大震災後のシステム環境の災害対策について調査した結果が報告されている。[15]政府機関が緊急時対応計画とシステム復旧手順について実施していた対策とその実施割合について調査した結果を以下に示す。




「東日本大震災における政府機関の情報システムに対する被害状況調査及び分析(最終報告書)」から引用

**図ー 12　緊急時対応計画とシステム復旧手順**

[14] それ以外の回答としては、「無線等を使った通信サービス」や「その他」と回答した内訳に「専門業者によるデータのサルベージ」や「バックアップ電源(設備電源切替システムへ)」等が挙げられていたほか、技術・サービスに該当しないものの、「マンパワー」、「詳しい社員」といった人的要素が有効であるとする回答もあった点が特徴的であった。

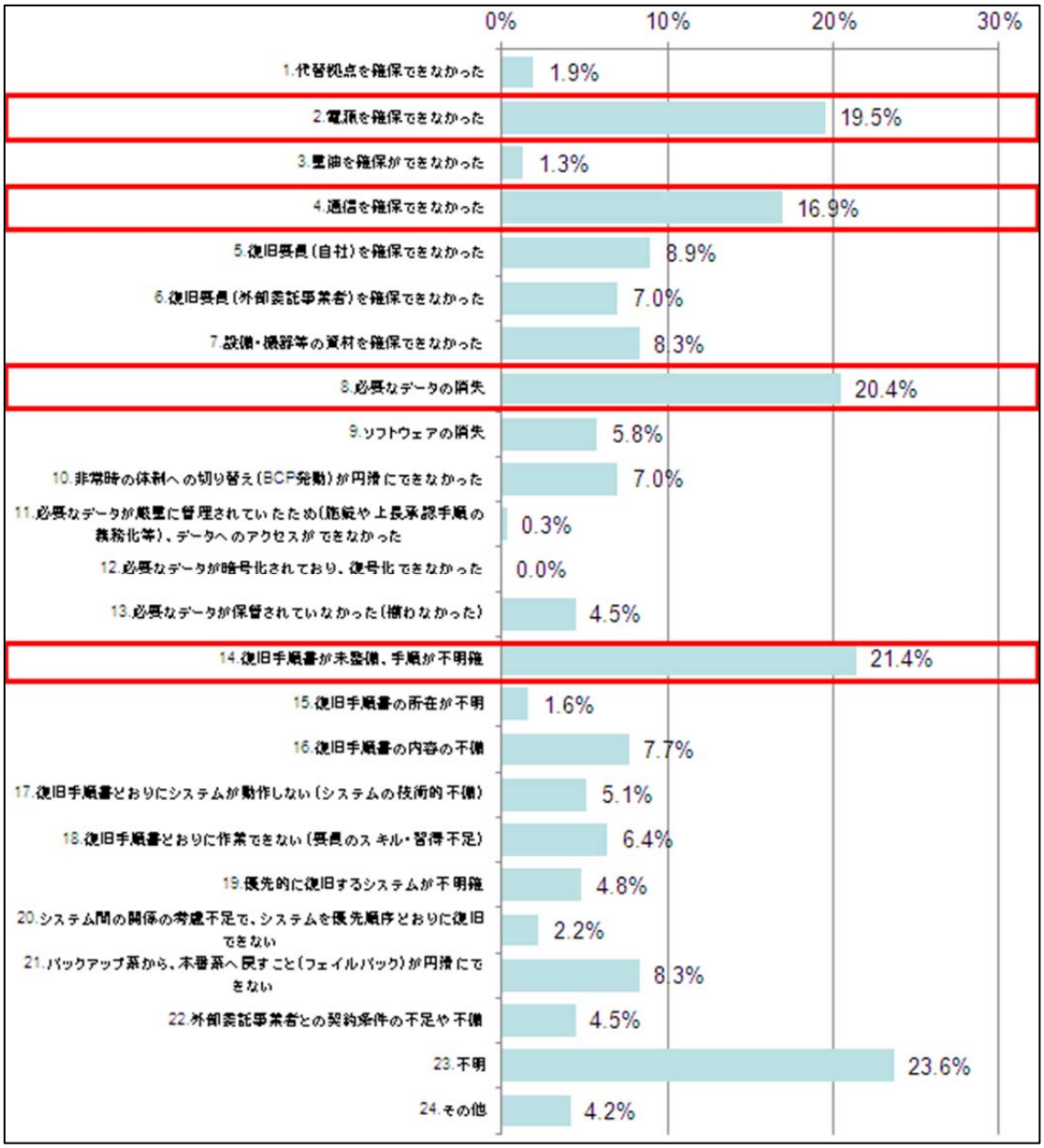
[15] 「4.2.14.　緊急時対応計画とシステム復旧手順に関する対策の分析」(P.55,56)

政府機関において実施していた対策は、回答の多い順に「緊急時対応連絡網の整備」、「緊急時対応体制・役割を定めていた」、「データのリストア手順やシステムリカバリ手順を整備」となっていて、回答内容の詳細な分析からもそれぞれ一定の効果があったとされている。また、個別の回答から、以下のような知見も得られている。

- 緊急時連絡網の整備は、簡便化（使いやすさ）と最新化（定期的に更新する）に留意すべき。
- 緊急連絡時の固定電話や携帯電話以外の日常的に使用しない通信手段（衛星電話や MCA 無線等）については、訓練を実施し使用方法や電波状況等を確認する。また、バッテリー等の消耗品については、定期的にメンテナンスすることが望ましい。
- データのリストア手順やシステムリカバリ手順書の整備については、（自明ではあるが）システム自体の被害を抑えることや、日頃からリカバリ訓練を実施しておくことが望ましい。
- システム目標復旧時間や復旧優先順位の明確化については、訓練や使えるマニュアル（分かりやすく、作成者のスキルに依存しない）の整備が望ましい。

### (3) 情報システム復旧の課題

IPA の実施したアンケート調査では、過去にシステム復旧において問題となった事項として「復旧手順が未整備、手順が不明確」が最も多く、次いで「必要なデータの消失」や「電源を確保ができなかった」、「通信を確保できなかった」等の回答が上位を占めた。




「情報システム基盤の復旧に関する対策の調査報告書」(独立行政法人情報処理推進機構 P.102)のデータを基に作成

**図ー 13 過去にシステム復旧において問題となった事項**

### (4) クラウドサービスの活用

総務省の実施した調査において以下の事項が報告されている。[16]

東日本大震災においては、

- 被災した自治体等に対してホームページの開設やメールサービスなどの提供
- 被災した自治体や救援活動を行うNPO等を対象として、避難所での避難者管理、ボランティアの管理、救援物資等の管理を支援するためのサービス

などの業務運営を支援するクラウドサービスが提供されたほか、

- 都道府県等とネットワークシステムが構築されていた住民関連データなどについては、バックアップデータの活用により迅速な復元や円滑な事業継続が可能であった
- 一方、津波により流出した被災者等に関する情報に関し、ハードディスクが損傷したものや、紙ベースで保管されていたものについては、その復元に時間と費用がかかった

との事例があり、自治体等における重要な情報保全の在り方及び業務運営の確保の観点から、クラウドサービスの利用を推進していくことが望まれる。

（※ 直ちにクラウドへの移行が難しい場合でも、隣接地域等へのバックアップサーバの設置など、重要な情報の多重化による情報保全を行う等の方策も考えられる。）

東日本大震災においては、自治体や企業の情報システムが損壊・喪失する等甚大な被害が生じたところであるが、クラウドサービスを用いることで損壊した情報システムの回復を迅速かつ低廉に行うことが可能となる。また、クラウドサービスの活用がサービスの継続性の確保や、クラウド内に蓄積された多様な情報の連携に向かうことで新たな付加価値を生み出すことも可能である。震災からの復興にクラウドサービスが有効であり、引き続き、官民が連携しつつ、事業継続性、公共サービス等の付加価値等を高めるクラウドサービスの一層の普及促進に取り組んでいくことが必要である。

また、震災発生直後から、民間の事業者により継続的に「クラウドサービス」を無償で提供されたことも確認されている。行政関連業務も、これらの民間企業の支援を受け、早期に業務復旧を実現したり、不足する情報システムのリソースを調達したりして地域住民に対する情報提供や避難活動の支援を行った事例が IPA の調査で報告されている。[17]

---

[16] 「大規模災害等緊急事態における通信確保の在り方について最終とりまとめ参考資料」（総務省　2011 年 12 月）
（http://www.soumu.go.jp/menu_news/s-news/01kiban02_02000043.html）

[17] 「2011 年東日本大震災に際して提供されたクラウドサービスの事例」（震災時の緊急支援に役立てられたクラウドサービスの事例と、復旧・復興に向けたクラウドサービス安全利用に関する資料の公開　2011 年 12 月 19 日　IPA）
（http://www.ipa.go.jp/security/cloud/cloud_sinsai_R1.html）

### 3.1.2. 東日本大震災による社会インフラの被災と復旧の状況

#### (1) 電力の被災と復旧

電力供給については、以下の点に留意し被害想定を行うことが望ましい。

- 東日本大震災の発生当時は、被災エリアにおいて約 900 万戸弱において停電が発生したが、1～2 日間で半減し、1 か月後にはほぼ完全復旧した。
- 震度 6 弱以下の被災地域においては、外部からの電力供給の二重化により多数の企業等が停電を免れた。
- 被災エリアにおいては、主要な発電所が停止し大幅な電力供給不足が発生した。

＜参考情報＞

停電は、電力各社の復旧対応により震災発生から 1 か月後にはほぼ解消した。

東北電力管内では、停電戸数の半減に 1～2 日間を要し、震災発生 1 か月後には一部地域を除き解消した。東京電力管内では、翌日には茨城県を除きほぼ停電が解消し、茨城県においても 3 月 19 日には解消した。東日本大震災発生当時には、東北エリアを中心に主要な発電所が停止した。そのため、エリア内の電力供給能力が著しく低下し、大幅な電力供給不足が発生した。また、震災により変電所等の電力流通設備への影響で、東京電力及び東北電力管内を中心に広範囲にわたって停電が発生した。東京電力管内で約 405 万戸、東北電力管内で約 466 万戸において地震発生直後から停電が発生した。

被害状況調査の結果からは、震度 6 強以上の地震が発生した地域では自家発電装置を設置していた一部の企業を除き、被災により情報システムへの電力供給が停止している。[18]震度が 6 弱以下の地震で被災した地域については、外部からの電源供給の二重化により被害を回避している事例が多数確認できた。

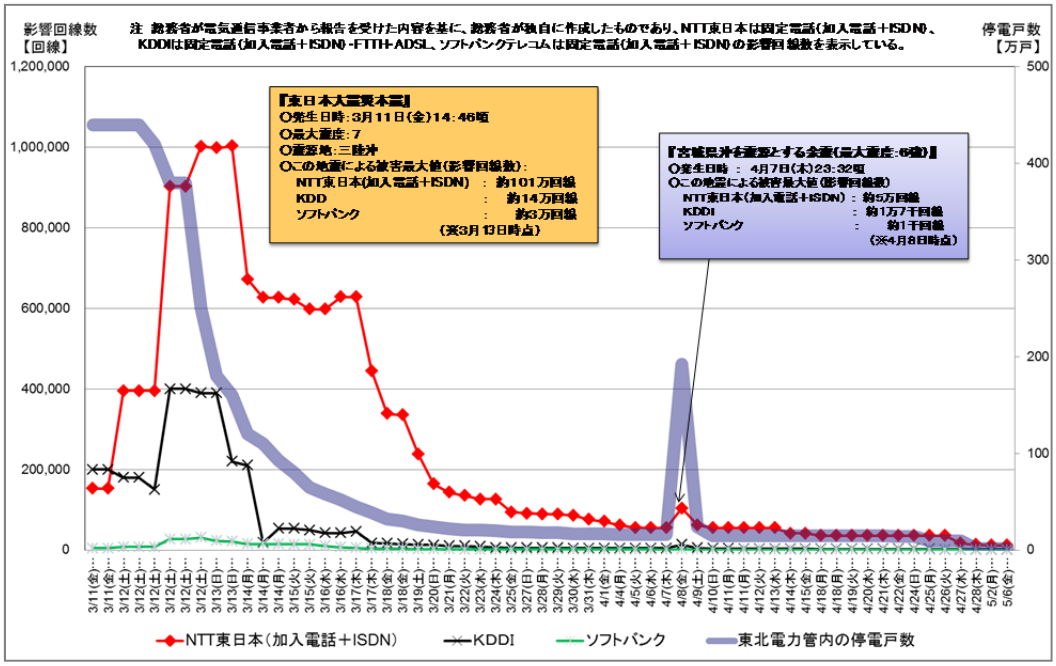
#### (2) 通信の被災と復旧

情報通信ネットワークについては、以下の点に留意し被害想定を行うことが望ましい。

- 東日本大震災の発生当時は、被災エリアにおいて固定電話の約 190 万回線が被災した。同様に携帯電話の最大約 29,000 局が停波した。
- 被災の影響は、約 2～3 日間で半減し、4 月末にはほぼ完全復旧した。
- 震災当日は、通信規制が実施され電話はつながりにくい状態だった。

以下に示すとおり、東日本大震災の被災時には、通信事業者の応急・復旧対応により、影響回線数は 2～3 日で半減し、最終的に、2011 年 4 月末までに一部地域を除き、ほぼ復旧した。

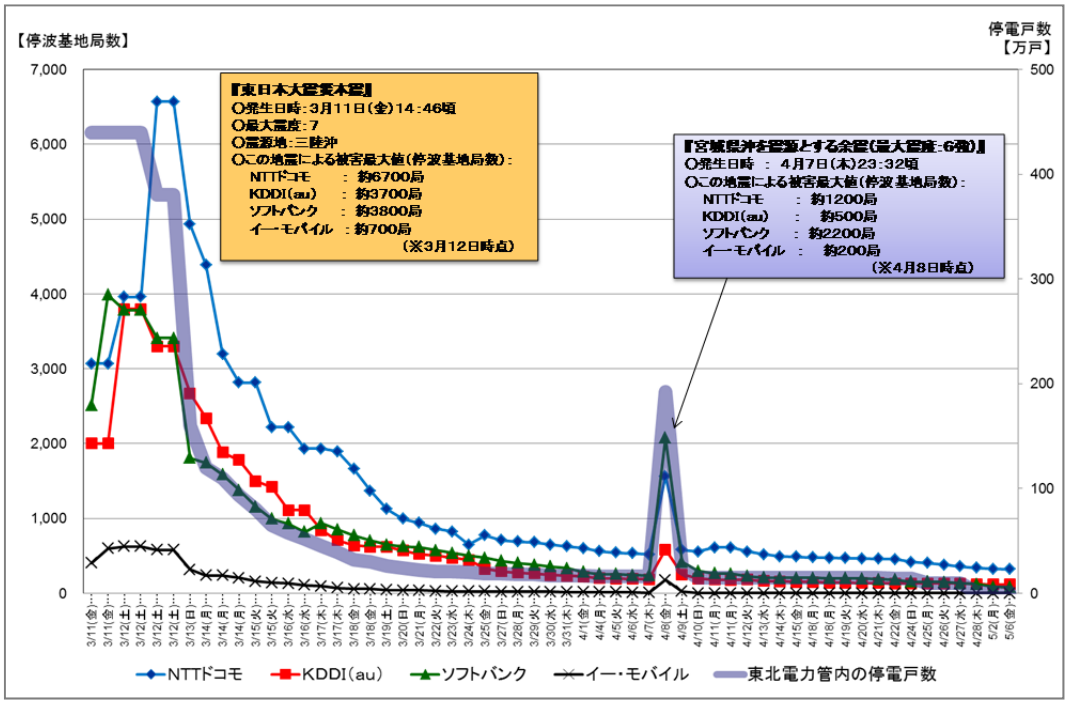
[18] 「4.2.2. 電源に関する被害の傾向と対策の分析」(P.14-16)




「大規模災害等緊急事態における通信確保の在り方について(別紙３ 参考資料)」

(大規模災害等緊急事態における通信確保の在り方に関する検討会 スライド 8)を引用

**図－ 14 固定電話の影響回線数の推移**




「大規模災害等緊急事態における通信確保の在り方について(別紙３ 参考資料)」

(大規模災害等緊急事態における通信確保の在り方に関する検討会 スライド 9)を引用

**図－ 15 携帯電話基地局の停波基地局数の推移**

固定通信網については、NTT 東日本、KDDI、ソフトバンクテレコムの 3 社で約 190 万回線が被災し、携帯電話及び PHS 基地局についても、NTT ドコモ、KDDI、ソフトバンクモバイル、イー・モバイル及びウィルコムの 5 社合計で最大約 29,000 局が停波した。

上記の調査結果から、電力供給の復旧と影響回線の減少が連動していることがうかがえる。東日本大震災の発生当時、東北を中心とする被災地においては、地震や津波により通信施設や機器が倒壊や水没、流出、通信ケーブルの切断等の大な被害を受け、長期的な停電もあり、通信サービスが途絶する結果となった。また、通信事業者の構築する中継網も大きな被害が生じ、太平洋沿岸に沿って設置されている基幹回線及び重要な通信施設が損傷したことにより、国内外の通信が遮断される等の影響を受けた。

さらに、震災発生時の通信集中による混雑を緩和するために、各通信事業者は独自に発信規制を実施した。固定電話については、NTT 東日本、KDDI が 90%、ソフトバンクテレコムが 80%の規制を実施したが、極端な通信の増加が発生しなかったため、早い段階で規制を解除した。携帯電話の音声通信は、最大で NTT ドコモが 90%、KDDI が 95%、ソフトバンクが 70%の規制を実施した。他方、パケット通信については、一時、NTT ドコモのみが 30%の規制を実施したが、すぐに規制は解除された。

**表－ 22 通信集中による混雑**

| 種別 | 事業者名等 | 発信規制値（最大）（%） |
|---|---|---|
| 固定通信 | NTT 東日本 ＊1 | 90 |
| | KDDI | 90 |
| | ソフトバンクテレコム | 80 |
| 移動通信 | NTT ドコモ（音声） ＊2 | 90 |
| | NTT ドコモ（パケット） | 30 |
| | au（音声） | 95 |
| | au（パケット） | 0 |
| | ソフトバンクモバイル（音声） | 70 |
| | ソフトバンクモバイル（パケット） | 0 |
| | イー・モバイル | 発信規制非実施 |

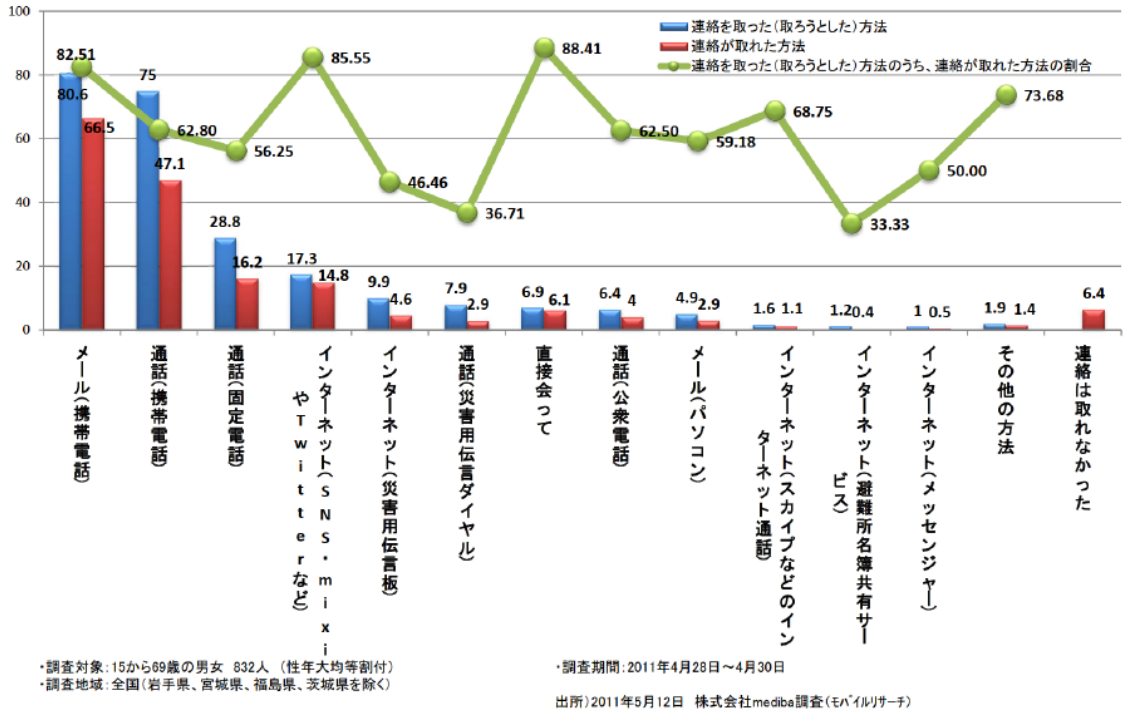
*1 通常時の約 4～9 倍の通信量が発生。 *2 通常時の約 50～60 倍の通信量が発生。

総務省「大規模災害等緊急事態における通信確保の在り方について最終とりまとめ参考資料」（2011 年 12 月）より作成 （掲載 URL：http://www.soumu.go.jp/menu_news/s-news/01kiban02_02000043.html）

### (3) ソーシャルメディアを活用したコミュニケーション

東日本大震災が発生した直後は、音声による通話が通信回線の輻輳により制限されたのに対して、データ通信は比較的制限を受けずに利用できたことが明らかになっている。そのため、震災発生直後は、ソーシャルメディアによる情報発信が活発に行われた。

前出の総務省による調査では、災害発生時の連絡手段として「携帯電話のメール」、「通話(固定電話・携帯電話)」に次いで「インターネット(SNS、mixi や Twitter 等)」が 3 番目に多く利用され、そのうちの約 8 割が連絡を取ることができたと回答していることからも、震災発生当時は有効な連絡手段として機能したことが推定できる。




「大規模災害等緊急事態における通信確保の在り方について(別紙 3 参考資料)」

(大規模災害等緊急事態における通信確保の在り方に関する検討会 スライド 14)を引用

**図－ 16 災害発生時の連絡手段**

ここでは、主に「Twitter」を例として取り上げて、ソーシャルメディアの活用状況や利用上の課題等について解説を試みる。Twitter は、簡易的なメッセージ交換の仕組みでユーザ間の情報交換を行うが、利用上の文字数制限により被災地を中心とした通信規制下においても比較的つながりやすく、アカウント取得の容易さもあり活用されたと考えられる。

前述の、総務省の公開している「大規模災害等緊急事態における通信確保の在り方について最終とりまとめ」において、インターネットの効果的な活用の一つの例として、ソーシャルメディアサービスの活用について言及されている。まず、ソーシャルメディアには以下のような特徴があり、インターネット接続や携帯電話によるアクセスが可能であった地域においては、安否確認や震災関連情報の共有に有効であったと報告されている。

- 自分の近況等リアルタイムの情報を友人等に知らせることが可能である。
- GPS機能と連動して自分の居場所を発信することが可能である。
- 共通のテーマについて情報交換を可能とするコミュニティ機能がある。

主に、個人間の情報発信や共有を目的としたサービスであることは、上記特徴からも明らかであるが、報告書においては「行政機関等が個々のサービスの特長を活かす形でソーシャルメディアサービスを活用して情報発信することにより、情報の周知・共有がより効果的な可能になると考えられる。このため、行政機関においては、ソーシャルメディアサービスの積極的な活用を検討することが重要である。」と位置付けている。

その反面、「一方、ソーシャルメディアサービスは、誰でもアカウントを開設することが可能であるため、成りすまし等の懸念が指摘されている。[19]」と注意喚起を行っている。

モデル調査においても、情報発信の新たな手段として新規の Twitter アカウントを取得した省庁の事例が確認されている。その事例おいては、アカウント取得において発生した問題として、省庁の略称（英文字）が民間企業によって既に登録されていて取得できず、対応に苦慮したとの報告があった。

中央府省庁におけるソーシャルメディア利用については、インターネット活用を推進する「オープンガバメントラボ」において、有用な指針や留意点等の情報が公開されている。今後利用を検討する府省庁においては、参考とされたい。

- 国、地方公共団体等公共機関における民間ソーシャルメディアを活用した情報発信についての指針（http://www.openlabs.go.jp/smp/guideline）
- 公共機関において Twitter を活用する際の留意点（http://www.openlabs.go.jp/smp/twitter）
- 公共機関の方向けの Twitter 開始の手引き（http://wiki.openlabs.go.jp/home/art-399）
- 公的アカウント管理システム（http://govtter.openlabs.go.jp/）

[19] 「国、地方公共団体等公共機関における民間ソーシャルメディアを活用した情報発信についての指針」（平成23年4月5日 内閣官房情報セキュリティセンター、情報通信技術（IT）担当室、総務省、経済産業省）
http://www.openlabs.go.jp/smp/guideline

## 3.2. 府省庁及び民間企業における IT-BCP 策定及び運用の状況

### 3.2.1. 中央省庁における IT-BCP 策定状況調査

NISC においては、本報告書の冒頭(「1.1.調査の背景」)において紹介したガイド改訂版を公表後に、各府省庁を対象にアンケート調査を実施し、計画策定の進捗とガイドの利用状況を調査した。

**【参考】『中央省庁における IT-BCP 策定状況調査』の実施概要**

1. 実施時期

発出:平成 24 年 7 月 19 日　期限:平成 24 年 8 月 31 日

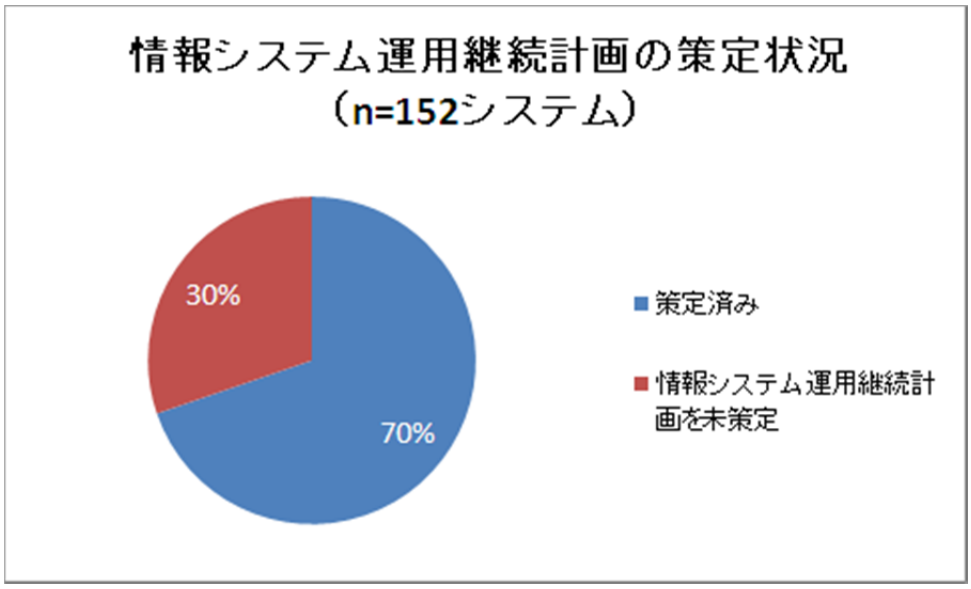
2. 対象とした省庁

内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、警察庁、金融庁、消費者庁、復興庁、総務省法務省、外務省、財務省、文科省、厚労省、農水省、経産省、国交省、環境省、防衛省(合計 21 府省庁)

3. アンケートの送付先

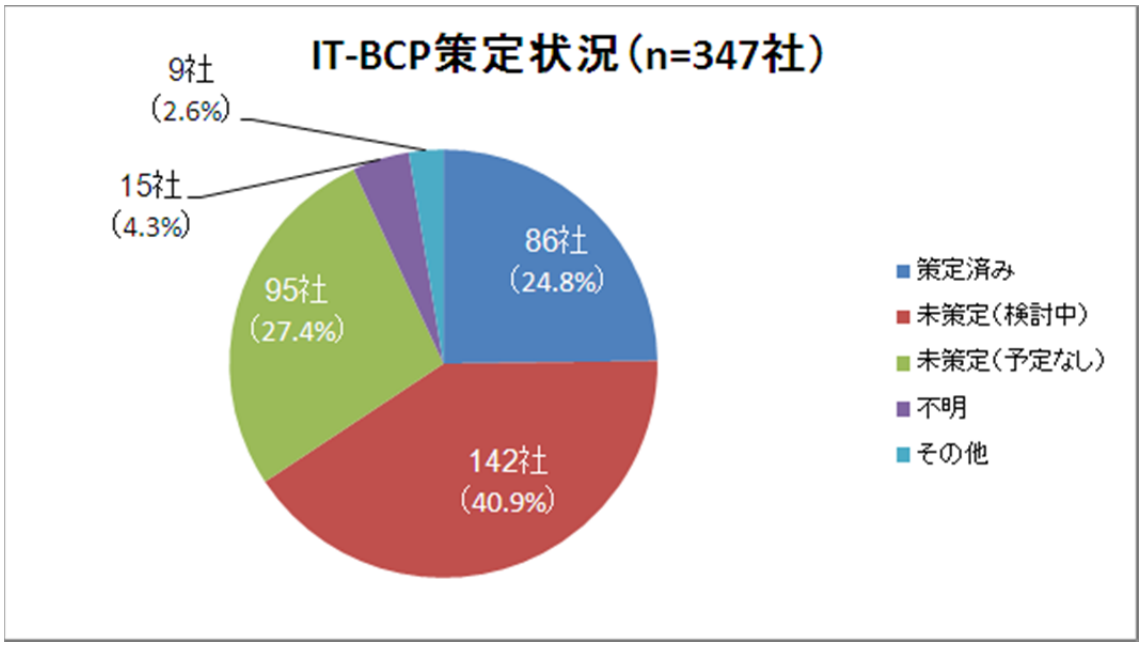
各府省庁の IT セキュリティ部門に送付し、府省庁内の情報システム部門が回答した。

府省庁を対象に、IT-BCP の策定状況を確認したところ、21 府省庁のうち 18 府省庁から策定済みとの回答があった(策定済みの割合は、8 割以上)。所管する情報システムのうち組織の非常時優先業務で利用されるシステムについて IT-BCP の策定状況を調査した結果、全体の約 7 割が「策定済み」という調査結果が得られた。




図－ 17 中央省庁における情報システム運用継続計画(IT-BCP)の策定状況

この調査結果を詳細に確認すると、未策定の約 3 割の情報システムについても、共通する情報システム基盤で策定済みのため個別に作成していない等の理由が確認されていて、IT-BCP の検討に未着手の情報システムはほとんどないという結果となっている。また、府町長における現状は、民間の調査結果における策定済み企業が全体の1／4程度という結果と比較して、非常に高い割合である。(図-2)




「情報システム基盤の復旧に関する対策の調査報告書」(独立行政法人情報処理推進機構　P.46)のデータを基に作成

**図ー 18　民間企業における情報システム運用継続計画(IT-BCP)の策定状況**

### 3.2.2. IT-BCP の策定に未着手の理由

アンケートで「未策定」と回答のあった府省庁から挙げられたコメントから、ガイドに示した手順やIT-BCP の位置付け等について適切に理解されていることが確認された反面、誤解されていると思われる回答も散見された。

**参考 アンケートの回答から抽出された課題と想定される対応**

**【課題1:復旧優先度の低いシステムについては運用継続に必要な対策を実施していない】**

- 重要システムの計画策定を優先したため、残りのシステムについては検討されていない
- 業務継続計画の被害想定において、情報システムが被災することが想定されていなかったので情報システム運用継続計画の策定は検討されていない

**⇒ 復旧優先度が低く設定された情報システムについては、IT-BCP 策定の作業負荷軽減のために個別の検討対象から除くことはガイドでも推奨している。しかし、復旧優先度が低く設定された情報システムについても、IT-BCP を全く検討しなくて良いわけではなく、復旧に必要な事前対策は最低限実施することが望ましい。**

**【課題 2:システムの更改や参照基準の改訂が予定されているので、今は計画を策定しない】**

- 今後、システム更改の時期に合わせて策定(改定)する
- 個別システムの復旧手順(操策定順)があるので策定していない
- 中央防災会議の被害想定が改訂されたタイミングで見直しを実施する予定

**⇒ 「今、大地震が発生した」場合の対応について検討しなければならない。現状の対策実施状況のもとで震災が発生した場合の被害を想定し、必要な対策を実施することが望ましい。**

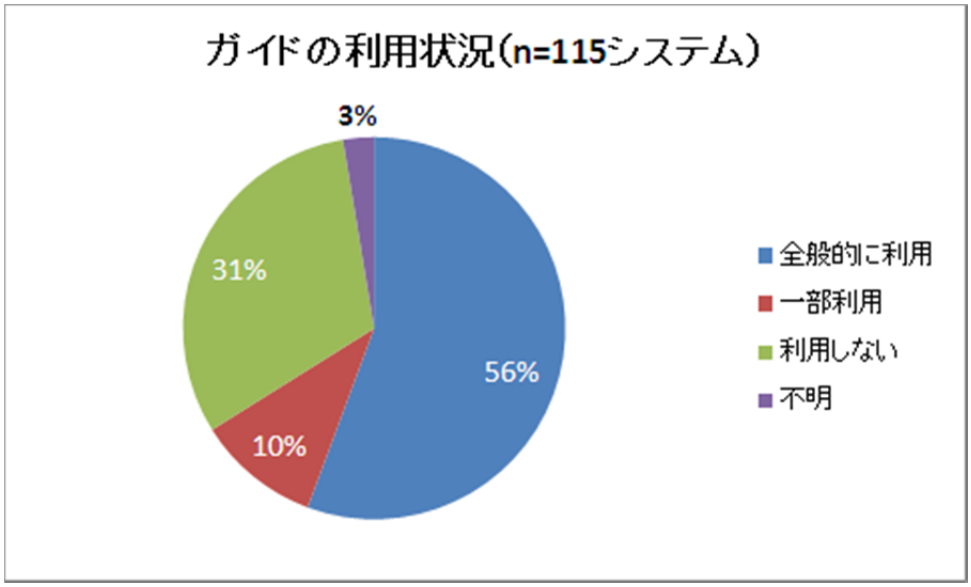
未策定の府省庁においては、できるだけ早くIT-BCP を策定し非常事態の業務継続に資する情報システム運用継続を実現することが望まれる。また、すでに策定している府省庁においては、教育・訓練や対策の見直し等を継続的に実施し、計画の迅速化や効率化、確実な実施等を目指すことが望まれる。

また、IT-BCP は、現状のシステム環境や対策実施状況の下で大規模な震災等が発生した場合を想定して取りまとめる、非常時の対応を中心とした計画群である。業務部門と連携し復旧目標を決定の上、情報システム部門において情報システムの復旧優先順位付けや非常時の対応手順を整備することが望ましい。

### 3.2.3. ガイドの利用状況

前述の IT-BCP を策定している府省庁のうち、**全体の 7 割弱（約 65%）が計画策定時にガイドを利用した**ことが確認された。IT-BCP を未策定の府省庁においては、**ガイドを活用し計画文書を策定することで、業務側が求める目標復旧時間と現状のシステム復旧可能時間のギャップや、それを解消する（縮める）ために必要な対策等を短期間で明らかにすることが望まれる。**

また、IT-BCP を策定済みの府省庁においても、ガイドや本報告書の提言を活用することで、非常時の行動をより確実に効率的に実施できるよう継続的な改善を行うことが望まれる。




**図－ 19 情報システム運用計画策定時のガイドの利用状況**

### 3.2.4. IT-BCP の策定時にガイドを利用しなかった理由

府省庁の IT-BCP 策定において、ガイドの利用が必須と定められてはいないので、この結果そのものを評価することは行わない。アンケートの回答とともに挙げられたコメントに、今後ガイドとして充実すべき内容や課題が含まれていた。

**参考 アンケートの回答から抽出された課題と想定される対応**

**【課題3:対処要件や対策の事例が少なく実施困難なものも多い】**

- 構成要素ごとの目標対策レベル設定がわかりにくい
- 対処要件の設定が厳しすぎる(実現不可能)
- 予防的対策の例示が少ない、若しくは予算に見合った対策の例示がない
- 予算の制約上、運用業務の委託先に対策の実施を指示できない(業務委託先に関する記述が不足している)

**⇒ 目標対策レベル別に対処要件と取りうる対策の例示をまとめ、対処要件の洗い出しや、実施する対策を比較検討できる例示を充実させる。**

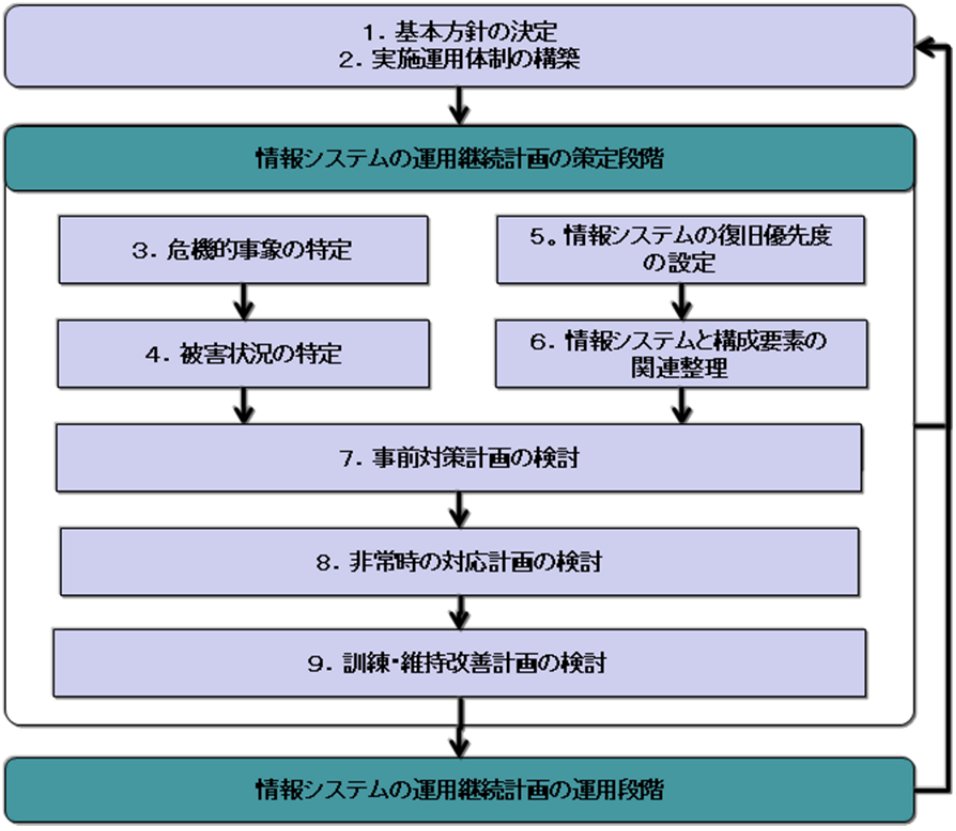
ガイドでは、主に IT-BCP の策定について手順を解説し、特に、情報システム部門の活動を中心に取り上げている。各府省庁における業務担当や防災活動、情報セキュリティの担当部署と、目標対策レベルの決定や具体的な対策実施の前提について、具体的なすり合わせ内容や方法について深く言及していない。

今後は、現状で IT-BCP を未策定の情報システムについても以下の事項を検討の上、最低限必要な管理体制の構築や行動手順の整備を実施することが望まれる。

- 対象業務の特定と利害関係者の確認
- 被害状況の特定
- 事前対策計画、非常時行動計画の検討

## 3.3. モデル調査の実施

モデル調査は、前述のとおりNISCが選定した府省庁について、IT-BCP の策定及び見直しの現状を調査した。調査は、「アンケート調査及び文書収集」と「ヒアリング調査」で実施し、「個別報告書（本報告書）」を作成した。調査は、以下に示すガイドに規定されている IT-BCP の策定手順に沿って実施し、各省庁の検討状況や対策の実施について確認した。




図－ 20 ガイドに示す IT-BCP 策定手順の概要

### 3.3.1. アンケート調査の実施

先に述べたとおり、本調査ではガイドの「策定手引書」に沿って IT-BCP の策定及び見直しを実施することを前提として調査を設計し実施した。調査では、各モデル省庁における IT-BCP 策定プロセスの実施状況を評価し、実施手順や計画書等を収集して文書の整備状況を確認した。(アンケート調査 43 項目、収集文書　15 点)

**表ー 23 アンケート調査票**

| テーマ | 質問項目 | 回答 |
|---|---|---|
| (1) 基本方針の決定 (3 問) | ① 情報システムの運用継続の対象とする範囲が明確にするための文書(情報システム運用継続計画書)を作成していますか？ | |
| | ② その文書で規定する対象範囲に以下の情報システム(システム基盤)は含まれていますか？<br>- メールや Web 等の情報収集・共有・伝達手段<br>- 基幹 LAN 及びこれにアクセスするための認証基盤 | |
| | ③ 新規に情報システムを導入するに当たり、業務継続に必要なシステム要件や、運用計画の検討を実施していますか？ | |
| (2) 実施・運用態勢の構築(4 問) | ① 情報システムの運用継続体制が組織されていますか？ | |
| | ② 体制に以下の役割が設けられていますか？<br>- 情報システムの運用を継続する最高責任者<br>- (各システムの)情報システムの運用を継続する責任者<br>- (各システムの)情報システム運用を継続する担当者 | |
| | ③ 情報システム運用継続体制に全庁の業務継続推進体制のメンバーは含まれていますか？ | |
| | ④ 全庁の業務継続推進体制に情報システムの運用を継続する責任者は参画していますか？ | |
| (3) 想定する危機的事象の特定(4 問) | ① 情報システムの運用が停止してしまうリスク事象が特定されていますか？ | |
| | ② 業務継続計画書で特定されたリスク事象が、情報システム運用継続書にすべて含まれていますか？ | |

| | | |
|---|---|---|
| | ③ 特定したリスク事象に以下の事項が含まれていますか？<br>- 首都直下型地震の発生<br>- マルウェア感染や不正侵入（外部からの攻撃） | |
| | ④ 危機的事象の発生時間等前提条件場を決めていますか？ | |
| （4） 被害状況の想定（3 問） | ① 危機的事象（特定したリスク事象）が顕在化したときの情報システムの被害状況を想定していますか？ | |
| | ② 危機的事象が顕在化した場合の脆弱性（システムの運用継続を阻害する要因）について検討した上、以下の事項を明らかにしていますか？<br>- 影響の大きさ<br>- 発生確率 | |
| | ③ 被害想定が全庁の事業継続計画で想定している被害との整合性を確保していますか？ | |
| （5） 情報システムの復旧優先度の設定（4 問） | ① 運用を継続する情報システムの対象を決定するために、全庁の業務継続計画に定められた非常時優先業務を確認した上、情報システムとの関係を整理していますか？ | |
| | ② 非常時優先業務の確認に当たり、関連する部局（管理部局）を特定し、ヒアリングを実施する等の対応を行いましたか？ | |
| | ③ 特定した非常時優先業務の目標復旧時間を決定する手順を決めていますか？ | |
| | ④ 特定した非常時優先業務で利用する情報システムについて、それぞれ目標復旧時間を設定していますか？ | |
| （6） 情報システム運用継続に必要な構成要素の整理（2 問） | ① 以下の構成要素（リソース）ごとに洗い出して、一覧を作成していますか？<br>- 施設、設備<br>- ネットワーク<br>- 周辺機器<br>- ハードウェア<br>- バックアップ（システム領域）<br>- バックアップ（データ領域）<br>- システム運用要員<br>- 外部委託先（非常時の対応） | |
| | ② 運用を継続する対象の情報システムの対象目標対策レベルを決定していますか？ | |
| （7） 事前対策計画の検討（4 問） | ① 運用を継続する対象の情報システムの対象目標対策レベルに対する現状の対策の実施状況（ギャップ）を確認していますか？ | |

| | | |
|---|---|---|
| | ② 対策実施状況の確認結果から、重大な脆弱性の有無を評価していますか？ | |
| | ③ 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基本方針（事前対策実施方針）をシステムごとに検討していますか？ | |
| | ④ 事前対策基本方針に基づく対策の具体化を検討していますか？ | |
| （8） 非常時の対応計画の検討（3 問） | ① 非常時に対応する担当者として、できるだけ通常運用時の担当者を割り当てるよう考慮していますか？ | |
| | ② 非常時の対応計画において、担当者ごとの役割分担が明確にされ、負荷分散等復旧継続活動を効率的に実施できるよう考慮していますか？ | |
| | ③ 情報システムの復旧作業の担当者が、非常時に必要な実施事項を確実に実施できる手順書を整備していますか？ | |
| （9） 教育訓練計画・維持改善計画の検討（2 問） | ① 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、定期的に見直しを実施していますか？ | |
| | ② 情報システム運用継続計画の策定や改善の過程で新たな課題が確認されましたか？（あれば、以下の解答欄にご記入ください。）【解答を記入】 | |
| （10）東日本大震災の影響（2 問） | ① 東日本大震災により情報システムの停止や、利用の制限を経験されましたか？【解答を記入】 | |
| | ② 震災以降に対策の見直しを実施されましたか？（実施された場合にはその内容を、実施されなかった場合には理由を以下の解答欄ご記入ください。）【解答を記入】 | |

以下に、モデル省庁のアンケート調査に対するアンケートの回答結果をまとめる。調査対象のモデル省庁を、IT-BCP の策定状況により 2 つのグループに大別すると、首都直下地震発生等の非常事態に対する検討の度合いに顕著な差が見られた。

### 3.3.2. 文書収集の実施

モデル省庁における情報システム運用継続に関する体制の整備状況や、モデルシステムにおける対策検討状況を確認するために、アンケート調査の実施に合わせて以下の文書について提出を依頼した。

**表－ 24 収集文書の一覧**

| No. | 文書の名称 |
|---|---|
| 1 | システム構成図（全体、ヒアリング対象システムの概要） |
| 2 | ネットワーク構成図（全体、ヒアリング対象システムの概要） |
| 3 | 情報システム運用継続計画 |
| 4 | 全庁の事業継続計画 |
| 5 | 情報システム部門の組織図（人数入り） |
| 6 | 情報システム運用継続の体制図 |
| 7 | 全庁の業務継続推進体制図 |
| 8 | 全庁の情報セキュリティ推進体制図 |
| 9 | 情報システム環境の現状と運用継続に対する脆弱性に関する資料（調査報告書等） |
| 10 | 業務システム一覧 |
| 11 | 特定した非常時優先業務で利用する情報システムの構成要素別一覧 |
| 12 | 事前対策実施方針 |
| 13 | 事前対策実施計画 |
| 14 | 非常時対応計画<br>・ 情報システム復旧基準<br>・ 要員参集基準<br>・ 非常時の対応体制（対応体制図、指揮命令系統図、関係部局の連絡先一覧、関係企業の連絡先一覧）<br>・ システム復旧手順（全体フロー図）<br>・ システム復旧手順（個別手順書） |
| 15 | 情報システム運用継続に関する教育・訓練の計画、教材 |

収集結果から、全般的に文書の整備が遅れていることが確認された。特に、情報システム部門と組織の業務継続や情報セキュリティの推進体制との連携が不足していることは課題であると考えられる。

### 3.3.3. ヒアリング調査の実施

ガイドを用いてIT-BCPの素案を策定するために、現状の情報システム運用継続に関する管理態勢や対処の状況について聞き取りを実施した。

質問項目は、事前説の際の聞き取りや前項で実施したアンケート調査、文書収集の結果に基づき、情報システムの運用態勢や運用継続にかかわる対策を確認する内容で作成した。主に、前述のガイドに示した作業工程に沿って、事前の調査結果により確認された事項から質問内容を取りまとめた。(※　詳細な聴取結果については、各モデル省庁における固有の体制や対策の実施状況等が含まれるため、本報告書への掲載は行わない。)

表－ 25 ヒアリング項目の一覧

| No. | 質問項目 | 詳細 |
|---|---|---|
| ① | 基本方針の確認 | ■ 全省事業継続計画に規定された復旧目標<br>・ 対象業務<br>・ 対象システム<br>・ 目標復旧時間<br>■ 対象組織 |
| ② | 実施・運用体制の構築 | ■ 実施・運用組織<br>■ モデル省庁内の関連部局<br>■ モデル省庁外の関連府省庁<br>■ 外部の委託業者 |
| ③ | 想定する危機的事象の特定 | ■ 首都直下地震の想定<br>・ 発生時間帯<br>・ 震度<br>■ その他の危機的事象 |
| ④ | 被害状況の想定 | ■ 情報システムの設置場所<br>■ 交通機関<br>■ 電力<br>■ 水道<br>■ 電話<br>■ 情報通信ネットワーク<br>■ 情報システム機器<br>■ データ |

| | | |
|---|---|---|
| ⑤ | 情報システムの復旧優先度の想定 | ■ 復旧優先度を定めているか |
| ⑥ | 情報システム運用継続に必要な構成要素の整理 | ■ ハードウェア<br>・ サーバ<br>・ ストレージ<br>■ データのバックアップ<br>・ システム領域<br>・ データ領域<br>■ 施設・設備<br>■ 情報通信ネットワーク<br>■ システム運用体制<br>■ ベンダの事業継続能力<br>■ 情報システム停止時の業務代替方法 |
| ⑦ | 事前対策計画の検討 | ■ どのくらいの頻度で、何に基づき誰が検討しているか |
| ⑧ | 非常時の対応計画の検討 | ■ 非常時対応計画が策定されているか |
| ⑨ | 教育訓練計画・維持改善計画の検討 | ■ 年間の教育訓練計画が策定されているか<br>■ 過年度の年間の教育訓練の実施実績<br>■ 運用体制の維持改善計画が策定されているか<br>■ 過年度の年間の改善活動の実施実績 |

## 4. 参考文献

| 文書名 | 発行年月 | 発行主体 |
|---|---|---|
| 中央省庁業務継続ガイドライン（第 1 版）<br>（内閣府　防災情報のページのリンクから参照のこと）<br>http://www.bousai.go.jp/jishin/gyomukeizoku/index.html | 2007 年（平成 19 年）<br>6 月 | 内閣府防災担当 |
| ○○業務継続計画　　※ ○○には府省庁の名称が入る<br>（中央省庁等の業務継続計画に関するリンク集）<br>http://www.bousai.go.jp/jishin/gyomukeizoku/link_chuou.html | （府省庁の取組時期による） | 府省庁 |
| 政府機関の情報セキュリティ対策のための統一基準群（平成 24 年度版）<br>http://www.nisc.go.jp/active/general/kijun24.html | 2012 年 4 月 26 日 | 情報セキュリティ政策会議等 |
| ○○情報セキュリティポリシー<br>（※統一基準に準拠して策定した府省庁基準の文書名を記す） | （府省庁の取組時期による） | 府省庁 |
| 情報セキュリティ 2012<br>http://www.nisc.go.jp/conference/seisaku/ | 2012 年 7 月 4 日 | 情報セキュリティ政策会議 |
| 東日本大震災における政府機関の情報システムに対する被害状況調査及び分析（最終報告書）<br>http://www.nisc.go.jp/inquiry/index.html | 2012 年 3 月 15 日 | 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（第二版）<br>http://www.nisc.go.jp/active/general/itbcp-guideline.html | 2012 年 5 月 11 日 | 内閣官房情報セキュリティセンター |
| 大規模災害等緊急事態における通信確保の在り方について最終とりまとめ参考資料<br>http://www.soumu.go.jp/menu_news/s-news/01kiban02_02000043.html | 2011 年 12 月 | 総務省 |
| 「2011 年東日本大震災に際して提供されたクラウドサービスの事例」（震災時の緊急支援に役立てられたクラウドサービスの事例と、復旧・復興に向けたクラウドサービス安全利用に関する資料の公開<br>http://www.ipa.go.jp/security/cloud/cloud_sinsai_R1.html | 2011 年 12 月 19 日 | 独立行政法人情報処理推進機構（IPA） |

| | | |
|---|---|---|
| IT サービス継続ガイドライン　改訂版<br>http://www.meti.go.jp/policy/netsecurity/docs/secgov/2011_IoformationSecurityServiceManagementGuidelineKaiteiban.pdf | 2012 年 | 経済産業省 |
| 情報システム基盤の復旧に関する対策の調査報告書<br>http://sec.ipa.go.jp/reports/20120725.html | 2012 年 7 月 25 日 | 独立行政法人情報処理推進機構<br>（IPA） |
| 高回復力システム基盤導入ガイド（概要編、計画編、要件定義ワークシート）<br>http://sec.ipa.go.jp/reports/20120508.html | 2012 年 5 月 8 日 | 独立行政法人情報処理推進機構<br>（IPA） |
| 国、地方公共団体等公共機関における民間ソーシャルメディアを活用した情報発信についての指針<br>http://www.openlabs.go.jp/smp/guideline | 2011 年（平成 23 年）<br>4 月 5 日 | 内閣官房情報セキュリティセンター<br>（NISC）<br>総務省<br>経済産業省 |