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

令和６年３月２９日

目　次

第１章　はじめに

1.1　本ガイドラインの目的

わが国は、その位置、地形、気象等の自然的条件から、これまでに多くの地震、水害等の災害に見舞われてきた。特に地震については、マグニチュード 6.0 以上の大地震の 20%以上が、世界のわずか 0.3%に過ぎないわが国の国土の中で起きている。近年では、平成７年（1995 年）に 6000 人を超える死者・行方不明者を出した阪神・淡路大震災（兵庫県南部地震）を始め、新潟県中越地震、能登半島沖地震、新潟県中越沖地震、岩手・宮城内陸地震といった大規模な地震が多数発生している。最近では、平成 23 年３月にマグニチュード９．０の未曽有の規模で起きた東日本大震災による津波被害や、平成２８年４月の熊本地震、令和 6 年１月の能登半島地震においても多くの犠牲者が出たところは記憶に新しいところである。

ビルの倒壊（阪神・淡路大震災　平成７年１月 17 日）

鹿島建設（株）ホームページ　http://www.kajima.co.jp/tech/seismic/higai/030604.html

家屋の倒壊・大規模な土砂崩れによる阿蘇大橋の崩落（熊本地震　平成 28 年４月 14 日）

内閣府 Web サイト（防災情報のページ 特集１　平成 28 年熊本地震）
https://www.bousai.go.jp/kohou/kouhoubousai/h28/83/special_01.html

また、地震や水害だけではなく、火災、感染症の蔓延等により、地方公共団体の施設、要員、依存するライフライン等が大きな被害を受けることも考慮しなければならない。ほぼすべての地方公共団体は地域防災計画等をはじめとする災害時の対応計画を策定しているが、地方公共団体自体の施設や要員、依存するライフライン等がこのような被害を受ける可能

性を認識し、必要な対策が取られているか、定期的に確認しておく必要がある。

大地震が発生した場合、過去の大地震の事例や公表されている被害予測データ等から、以下のような状況に陥ることが予想される。

（１）庁舎が使用できない

過去の大地震では、いずれの場合も多くの建物・家屋が倒壊している。各地方公共団体の庁舎の中には老朽化が進み、倒壊する危険のある建物も数多く存在するはずである。また、倒壊までは至らなくても、火災、天井の崩落、水漏れ等によりフロアが当面使用できなくなる可能性もある。さらに、勤務時間中において庁舎に被害が出て、来庁者等にけが人が多く発生した場合、救出活動等に専念せざるを得ず、業務の継続・復旧の大きな制約となることも考えなくてはならない。

（２）情報通信の設備、機器が損壊

情報通信機能を担う重要な設備や機器等が転倒しないよう固定されていなければ、設備・機器等は転倒し、故障して使用できなくなることも想定される。最悪の場合は新規に調達する必要が生じることもある。新規調達が必要となる事態に陥った場合、再調達費用がかかるだけではなく、最低でも１ヶ月程度はサービスが停止する可能性もある。基幹システムが１ヶ月停止した場合の影響は甚大である。

（３）必要な職員が参集できない

夜間や休日等勤務時間外に災害が発生した場合、復旧に必要な職員が直ぐに参集場所に集まることのできない可能性は高い。大地震の場合は、鉄道は脱線等により長期間停止し、また道路は車両が通行できなくなる事態も懸念されるほか、例え通行できたとしても主要道路は緊急車両通行のため一般車両通行止めになる可能性がある。徒歩や自転車しか移動手段がなく、さらに都市部では建物の倒壊や帰宅困難者が道にあふれること等から、歩行等の速度は大幅に低下する。その結果、遠隔地に居住している職員が参集できない可能性がある。また、職員が死亡や大けがをする可能性もあるほか、家族に被害がでればその職員の出勤を期待することは難しい。

（４）電力供給が停止

電力の供給が停止すれば、サーバやネットワーク機器等（以下、「情報通信機器」という。）の稼動ができず、さらに地方公共団体の業務遂行全体に大きな影響を与えるはずである。過去の大地震においても、電力は、水道・下水道・ガス等他のライフラインに比べて復旧は早いものの、供給停止の影響は広範囲にわたる。

非常用の電源を用意することで、このような事態をある程度は防ぐことが可能となるが、過去の事例でも、非常用電源設備が立ち上がらなかった例は多い。また、非常用電源は、通常の電力使用量の数分の一程度の容量しかないのが通常であり、必要な情報通信機器やそれを支える空調機器のすべてが非常用電源によってまかなえないことも想定される。

（５）空調設備が損壊

過去の事例では、天井カセット型のエアコン室内機が宙吊りになった事例やダクトの脱落・破損等が起きている。情報通信機器が無事であっても、空調設備が長期間機能停止した場合、温度・湿度の異常により情報システムが停止することとなる。

（６）必要な外部事業者と連絡が取れない、対応準備がとられていない

情報システム（ネットワーク回線・設備を含む。以下同じ。）の復旧や設備の修理等、外部事業者の協力が必要なことは数多くある。また、日常の管理運営を外部事業者に依存している場合も少なくない。大地震発生時は被災地へ安否確認等の通話が集中し、一般電話や携帯電話は通信規制によりほとんど通話できない状態が丸１日から数日間続くことが多い。さらに、外部事業者が同じ地域にある場合には事業者自身も被害を受けているため、連絡がついても早急に対応できない可能性もある。

このように、大地震等の大規模な広域災害が発生した場合、普段当然のように使用している施設、要員、依存するライフライン等が使用できず、これまで予期してこなかった機能不全の状態に陥る可能性がある。

また、特に対象を情報システムに限定した場合は、大規模なネットワーク障害を引き起こすコンピュータウィルスの蔓延やサイバー攻撃、情報システム障害等の事故が発生して、情報システムがほとんど使用できなくなる事態に陥る可能性等もある。さらには、新型コロナウイルス感染症や新型インフルエンザ等世界的に流行する「パンデミック」が発生して、多くの職員が庁舎に出勤できない事態、さらにはライフライン、物流などの社会機能が維持できない事態に陥る可能性もある。

地方公共団体は、災害時において、地域住民の生命、身体の安全確保、被災者支援、企業活動復旧のために、災害応急業務、復旧業務及び平常時から継続しなければならない重要な業務を実施していく責務を負っている。これらの業務の継続を確保するためには、近年において情報システムがまさに不可欠であり、災害時に情報システムが稼働していることは極めて重要である。

情報システムは、平常時からの業務継続の備えがないと、被害を受けてからの事後的な復旧に時間がかかる特性が強い。また、住民情報等を失った場合、その回復に時間を要すると、甚大で回復困難な影響を住民・企業に生じさせてしまう。そのような意味から、業務継続計画の策定の必要性が高い典型的な部門であり、業務継続力をつけることの価値は大きい。

以上の問題意識から、総務省では、平成 20 年度に情報システムを所管するＩＣＴ部門の業務継続計画（ＢＣＰ）策定に向けた地方公共団体の取組を支援するため本ガイドラインを作成し、令和５年度に、最近のＩＣＴ利活用の技術、環境を踏まえ、時点更新をしたところである。

■業務継続計画／ＢＣＰの名称について

緊急時の重要業務の継続を目的とした計画は、民間企業では「事業継続計画」、行政では「業務継続計画」とされる場合が多い。また、米国、英国等における英語名では、ＢＣＰ（Business Continuity Plan）と呼ぶ場合が多い。

本ガイドラインにおいては、本文中では「業務継続計画」という名称を使用し、各章、各部及び各ステップの表題においては業務継続計画の略称である「ＢＣＰ」を使用することとする。

1.2　本ガイドラインの基本的考え方について

（1）ＩＣＴ部門を対象とする

本ガイドラインは基本的には地方公共団体の情報システム・ネットワーク等に関する企画や統括管理をする部門が使用することを想定している。このような部門は地方公共団体によって情報システム課、情報政策課、情報管理課等名称は様々であり、本ガイドラインでは「ＩＣＴ部門[1]」と呼称する。

まずはＩＣＴ部門が主管する情報システムに関する業務継続を中心に検討する。他方、それぞれの業務担当課が個別に管理している情報システムについても、重要なものであれば業務継続のための計画を検討する必要性が高い。本ガイドラインの利用に当たって、ＩＣＴ部門以外が管理する情報システムであっても同様の手法で業務継続を検討することが可能である。重要な情報システム（例えば、消防、防災に関する情報システムのように地震、風水害等の広域災害において早急に必要となる情報システム等）について、それらを管理する部門もＩＣＴ部門と同様の検討体制を作り、ＩＣＴ部門と連携して検討すべきである。

早急に他の部門を含めた検討体制が作れない場合は、まずはＩＣＴ部門のみでも検討を開始すべきである。その後、他の部門に対して検討結果を積極的に公表して、他の部門が管理する情報システムに対する対策を進めるように促すことが望ましい。

（2）大地震を主たる対象事象とする

業務が停止する原因としては、地震、風水害等の自然災害のほかにも、テロ等の事件、火災や長時間の停電等数多くある。また、特に対象を情報システムに限定した場合は、サイバー攻撃や大規模なネットワーク障害を引き起こすコンピュータウィルス等の情報システム関連の事故の影響も多大である。以下、業務継続に影響を与える可能性がある大規模災害や事故、事件等を「災害・事故」と表記する。

しかし、最初から様々な事象を盛り込んで検討しようとすると、情報システムを利用する各業務部門に情報システムが停止した場合の影響を照会しても、どのような事態による停止なのかの想像がつかなければ質問に答えられない可能性が高い。そこで、特定の被害想定[2]を前提とした状況を想像してもらい検討することがまずは有効である。

なお、最初の検討においては、発生懸念が大きく、かつ、最大の被害になり得る事象を対象として検討することで、他の事象への対策もある程度は包含した対策とすることができる。この点、日本ではどの地域でも発生の懸念のある大地震を前提とした場合は、火災等の二次災害及び電力途絶等事態も想定して対処することが求められることや、施設・設備の損壊が他のテロ等の他の原因であっても対応が類似のため、応用が容易である。したがって、本ガイドラインでは「大地震」を対象事象として検討を始めることを基本としている。

---

[1] ＩＣＴ(Information Communication Technology)：情報及び通信に関する技術の総称。わが国では同様の言葉としてＩＴ(Information Technology：情報技術)の呼称が普及しているが、国際的にはＩＣＴの方が使用される。

[2] ただし、最初の想定であっても、過度に被害想定を絞り込みすぎない方がよい。例えば地震であれば、発生をある時間に限ったりすることでなく、勤務時間内と夜間・休日の両方を一度に考えるべきであるし、震源地も一つに限らなくてよい。

（３）あらゆる規模の地方公共団体を対象とする。

業務継続計画の目的は、前述のとおり、災害発生等非常時においても、平常時と可能な限り同等のレベルで業務を継続することにあり、それはいかなる地域、いかなる規模の団体においても基本的には変わらない。

本ガイドラインでは、多数の対応可能な職員がいる大規模な団体だけではなく、小規模な団体も実際に活用できるようにするという現実的な要請から、比較的容易な取組から作業を進めるステップアップ方式を採用している。具体的な構成については、第２章「2.2 本ガイドラインの構成」で説明する。

1.3　業務継続計画とは

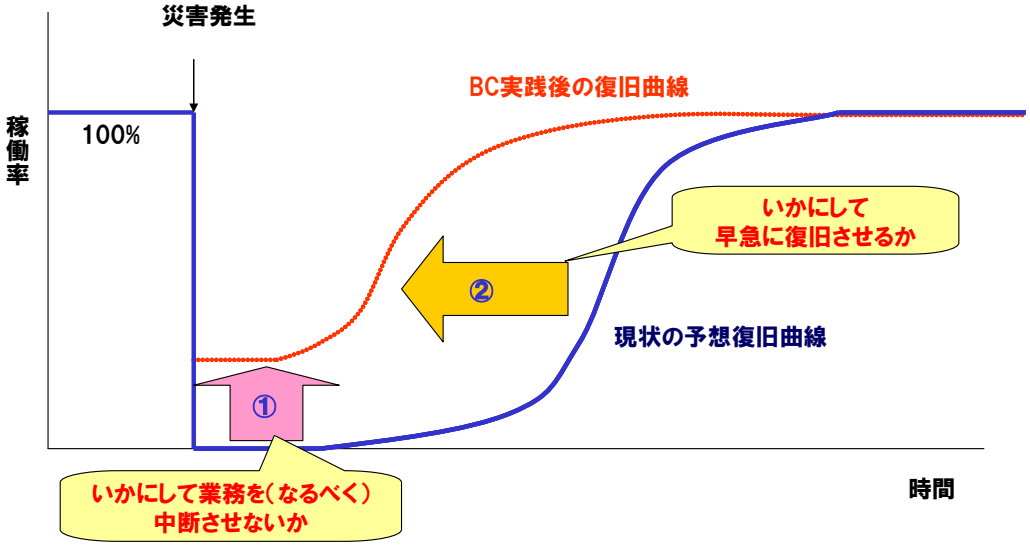
「業務継続計画」とは、災害・事故で被害を受けても、重要業務をなるべく中断させず、中断してもできるだけ早急に（あるいは、許容される中断時間内に）復旧させる「業務継続」を戦略的に実現するための計画である。

大規模な災害・事故が発生した場合、組織及び周辺地域の被害によりヒト、モノ、情報、資金、公共インフラ等利用できる資源に制約がある状況に陥ることが予想される。このような状況においても中断させることができない、あるいは復旧を優先すべき重要業務を事前に特定しておき、事前のバックアップ準備やリスク軽減、事後の災害時応急対応、復旧手順の明確化、指揮命令系統の確保等の計画をあらかじめ立案し、被災の影響を最小限にとどめることを目的とする。また、その実現を容易にするための事前対策（投資、体制整備等）を計画して着実に実施すること、そして、平常時から、常に業務継続が可能な体制を維持改善するための活動も計画に含まれるものである。

例えば、阪神・淡路大震災や東日本大震災のような震度６強以上の大地震やそれに匹敵する災害・事故等が発生した場合、地方公共団体の業務はどのような状況になり、どういう対応が必要になるだろうか。図 1-1 は、大規模災害や事故等の発生から復旧までの時間と業務の稼働率の関係を模式的に表したグラフである。何も対策を講じていない状況で被災した場合、図の実線のように稼働率はゼロ近くまで落ち、回復にはかなりの時間を要する。

このため、事前対策の実施や災害時の応急・復旧計画の策定、訓練等により、大規模災害や事故等が発生した場合に、図の点線のように復旧曲線を改善することが業務継続計画を策定し、それの実施・定着していく目的である。

【図 1-1】復旧曲線



業務の中断の未然防止及び早期復旧を実現するためには、同時被災しない遠隔地に業務継続に必要不可欠な代わりの設備、物品・サービス・情報、人員等の資源（代替リソース）を事前に準備しておき、被害が発生した場合にスムーズに運用を切り替えるようにすることが、理想的な解決方法である。

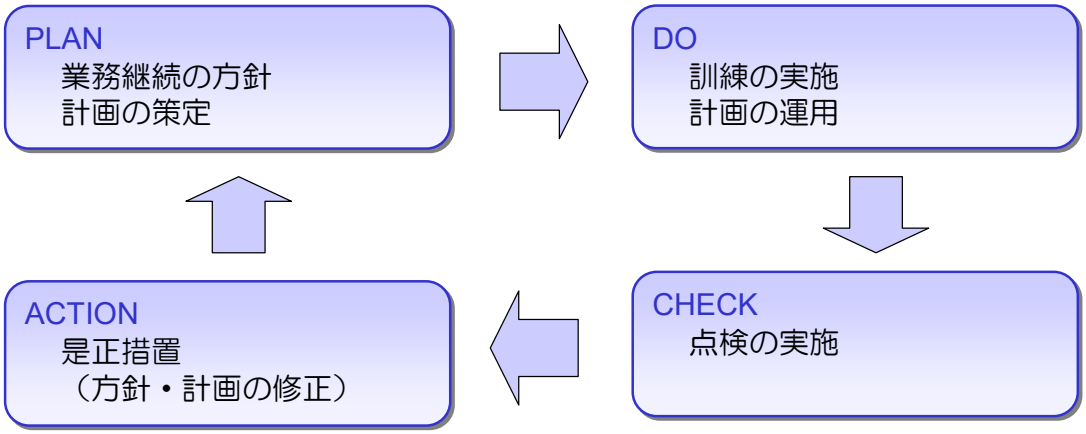
しかし、すべての業務において代替リソースを保持することは、代替調達先がない（あるいは少ない）物品・サービス・情報については実質的に不可能であるし、費用の観点から不可能に近いものも多い。そのため、代替リソースをあらかじめ確保すべき最低限の対策をすべき業務や情報システムの絞り込みを行う。また、平常時に業務で使用しているリソースに対して耐震補強等の補強措置を行うことも、すべての災害・事故に共通に有効とはならないが、想定した種類の災害・事故にはもちろん有効となる。

また、現時点では実施できない投資等の抜本的な対策は将来的な課題として認識しておき、環境が整ってから実施するということも考えられる。首長や首長に準じた役職にある者（以下「首長等」という。）が、対策がいまだ不十分であるというリスクを、担当の管理職・職員と課題として明確に共通認識を持つだけでも一定の効果がある（首長等が課題を認識していれば、災害が発生した場合に迅速に対応することができる）。これらのリスク認識の共有や投資判断のためには、首長等の参画が必要不可欠である。

＜計画の継続的改善＞

最初から完璧な業務継続計画を策定しようとしても困難である。まずは対象範囲を限定して、可能な範囲で検討することが重要である。そして、図 1-2 にあるように、職員への訓練を実施して問題点を見出し、さらに、点検作業等を通じた課題の洗い出し等により継続的な改善のための取組を実施することが必要である。このような運用を行うことを含めた業務継続の取組の全体を「ＢＣＭ（Business Continuity Management：業務継続管理）」という。

【図 1-2】業務継続計画のマネジメントサイクル



また、マネジメントサイクルを繰り返す中で、事業継続計画の実効性の向上を図っていくことが重要である。

前述のとおり、業務継続は、あらゆる災害・事故の被害を受けても達成されるべきである。しかし、実務的には、特定の被害想定をまずは前提とすることで策定作業を円滑に進めることができる。わが国では、地震の発生率が諸外国に比べて多く、その被害の懸念がどの地域でもあるため、地震を対象リスクとする業務継続計画を策定することは有効である。もちろん、地方公共団体の災害リスクとして風水害の方が大きいと判断するならば、それを最初の対象リスクとする。とはいえ、行政が対応しなければならない事態は数多くある（表 1-1 参照）ため、地方公共団体の業務継続計画は特定のリスクのみを対象とし

て策定すれば十分であるわけではないこと認識すべきである。

策定を進めた段階で、対象とした事象以外にも業務継続に影響を与える懸念が大きいリスクがあるかぎり、対象を拡大すべきである。特に、ＩＣＴ部門の業務継続計画においては、コンピュータウィルスの蔓延やハードウェアの故障等、情報システムの停止原因とその影響については様々存在する。自然災害に関係する状況だけを検討するものではないことを認識すべきである。

ただし、存在する数多くのリスクをすべて、ＩＣＴ部門の業務継続計画の検討対象とするということではない。業務継続計画が検討対象とすべきリスクは、「（ある程度）突発的に広範囲に人の生命・健康が脅かされる、庁舎・設備等の庁内インフラや交通・電気等公共インフラに多大な悪影響を及ぼすことにより、業務の継続に支障を来たすおそれのあるリスク」に絞られる。業務継続計画と別の手法により平常時の着実な取り組みで対処するしかないリスクも多数存在するからである。

【表 1-1】ＩＣＴ部門の業務継続における代表的なリスク

１．広域に被害を及ぼす事象
- 地震、津波
- 大規模風水害
- 疫病

２．局所（庁舎及び周辺）に被害を及ぼす事象
- 火災
- 停電
- 爆破テロ

３．情報システム単独の障害
- サイバー攻撃
- ハードウェア故障
- アプリケーション障害
- コンピュータウィルスの蔓延

1.4　業務継続計画の必要性

（１）地方公共団体の責任

地方公共団体が平常時に提供している行政サービスが停止した場合、住民生活や企業活動に大きな影響を及ぼす。また、災害・事故時には地方公共団体は救助・救援活動の主役であるが、自らが大きな被害を受けたからといってこの責務を果たさないわけにはいかない。このため、地方公共団体の業務継続は社会的責任が特に重いと言える。

災害時においても、地方公共団体の職員が自らの職責に基づき庁舎に参集することは責務である。しかしながら、やむをえない事情により参集できない場合もあり、そのため、特定の要員が参集できない状況においても、必要な業務を継続できるようにするための体制を整備することが求められる。

（２）危機管理に対する意識の高まり

危機管理に対する市民の意識向上により、災害等が発生すると、当該地方公共団体の対応が全国的に注目され、その対応の良否により対応者、さらには首長等の責任が厳しく問われる地方公共団体の対応者及び首長等は非常時にもなるべく迅速かつ的確な対応が取れるよう、平常時からの準備が求められる。

（３）業務継続計画と地域防災計画との関係

ほぼすべての地方公共団体は、災害対策基本法により、防災のために処理すべき業務等を具体的に定めた地域防災計画を定めている。また、災害対策基本法に基づき、内閣府中央防災会議で定められた防災基本計画においては、公的機関等の業務継続性の確保がうたわれており、合理的に自らの深刻な被害を想定して対応を考える業務継続計画を策定することが重要である。ただし、地域防災計画と別の計画と位置付けることが必要なのではなく、その中に溶け込ませて充実を図るという考え方が望ましい。

（４）リスクの発生懸念の増加

近年、地震が活動期に入ったという指摘もある。地球温暖化の影響で、台風、水害等が増えているとの議論もある。事業・業務の中断をもたらす感染症については、新型コロナウイルス感染症で経験したところであり、今後、新たな感染症も懸念される。一方、地方公共団体の業務の ICT への依存が高まる中で、サイバー攻撃、大規模システムのプログラムミスによるシステムダウンなど、従来なかったリスクの種類が増加している。したがって、業務継続のためには、包括的な行動計画がますます必要となっている。

1.5　地方公共団体におけるＩＣＴ部門の取組のあるべき姿

地方公共団体によって災害・事故時に情報システムの機能を継続、早期復旧するための条件・環境は相当多様であるが、どのような条件・環境であっても、首長等、あるいはＩＣＴ部門長は、以下の事項については何らかの取組をしていくべきである。

（１）最低限のバックアップの実施

いかなる理由があっても、住民・企業の納税や支援の情報、許認可に関わる情報をはじめ、地方公共団体のみが保有する住民、企業に関する情報を消失させることは、影響の大きさから必ず回避すべきことである。消失した場合に元の状態に戻すことが不可能な情報にどのようなものがあるかを把握し、最低限のバックアップをすることは、業務継続以前のＩＣＴ部門としての責務である。

また、バックアップが同時に被害を受けては意味がないため、県外等同時に被災しない場所に保管することが推奨される。遠隔地で保管することが難しい場合は、最低限、出先機関等で本体とは別に保管するべきである。さらに、データを通信回線で結んだ遠隔地に設置したストレージ（外部記憶装置）にコピーするなど、より信頼性の高い高度なバックアップの実施も検討すべきだが、多額の経費が必要となることも想定されるため、将来の取組の段階で予算化に向けた検討を実施する。

（２）ＩＣＴ部門としての緊急時対応体制の検討

担当者の参集の遅延のために業務が長時間停止したというような事態に陥った場合、住民やマスコミから危機管理意識の欠如を問われ、多くの社会的非難を浴びることが予想される。

全庁的な対応がすぐには取れない場合でも、ＩＣＴ部門だけでも先行して緊急時の体制や行動を計画することは可能である。必要な職員が緊急時に参集できるよう計画し、訓練を行って習熟することが重要である。

さらに、特定の要員が負傷等で参集できなくても業務が遂行できるように、要員の多重的な育成方針を考えたり、平常時からなるべく多くの要員でノウハウを共有したり、不慣れな担当者でも対応できるわかりやすい復旧手順書を準備する等の対策が強く推奨される。

（３）災害時の行動を指揮できる管理者の育成

災害時において、要員、機材等の資源及び情報が十分でない中でも適切な対応を取るためには、迅速な情報収集と意思決定ができる体制を構築しなければならない。このためには、緊急時における対応策を熟知してそのノウハウを駆使しながら指揮命令できるオールラウンドな管理者がいることが望まれる。ＩＣＴ部門長として、業務継続を統制することができる管理者を、自らを含め、育成・確保することが望まれる。

（４）外部事業者との連携・協力関係の構築

情報システムに関して外部事業者への依存度が高い地方公共団体はほとんどといってよい状態であるが、そのような場合でも、情報システム停止による業務停滞の責任は地方公共団体が負うことになる。「外部事業者が来ないから復旧できなかった。」という説明は対外的に理解を得ることができない。

したがって、外部事業者についても役所と同様の初動行動の計画を立てるよう連携・協力を求める必要がある。ただし、あらかじめ連携・協力関係を構築していても、道路の被災により早急には参集できない事態や、復旧担当者の確保を巡り同時に被災した他の地方公共団体等と競合し対応不能となる事態も考えられる。このため、恒常的に緊急時の対応について訓練を行うことや情報交換を密にしていくことが重要であり、必要に応じ、災害時の参集や復旧担当者の確保等を契約事項とすることも検討すべきである。

（５）情報通信機器の固定措置の実施

災害により建物が無事であるにも関わらず情報通信機器の固定措置をしていなかったために情報システム等が使用できない事態は、建物への多大な投資が活きないという結果でもあるので、是非とも回避しなければならない。情報システムがどのような設置環境にあるかを把握し、ＩＣＴ部門の予算内でできることをすることはＩＣＴ部門長としての責務であると考えるべきである。ＩＣＴ部門の予算を超える対策に関しては、全庁的な対応の必要性を訴え、実現可能な段階で具体化していく必要がある。

（６）地方公共団体間の協力関係の構築

重要な業務の中断を防ぐためには、同時被災しない遠隔地に必要不可欠な代替リソースを事前に準備しておき、非常時に運用を切り替えることが理想的な解決方法である。しかし、自らが代替資源を用意するのは費用の面で困難な場合が多い。そこで、他の地方公共団体との間の協力関係の構築により類似の効果が確保できれば費用面において効率的であろう。

現時点では、技術的要因等により、異なる外部事業者を情報システムの契約先とする地方公共団体間での協力は難しい。しかし、業務継続性を考慮した最終的な情報システム運用の形態として、多くの地方公共団体や事業者と共同して、解決方法を考えていくことが重要であり、早い段階で検討を開始すべき事項である。

（７）既存のマネジメントとの整合

業務継続計画の策定・運用は、前述のようにマネジメントシステムを導入することである。その導入に当たっては、情報セキュリティ対策や防災関係の対応等、既存の関連する取組との整合を図り、矛盾がないようにしなければならない。

特に、情報セキュリティ対策については対策面において相反する性格を持つ部分もあるが、両者の間での均衡が必要である（表 1-2 のとおり、両者の取組には共通する部分もある。）既存の情報セキュリティマネジメントと情報システムの業務継続のマネジメントはできるだけ同じ要員が担当して共通して管理し、セキュリティを軽視した対策や業務継続が過度に実施しにくくなる運用がなされることがないように注視する必要がある。例えば、業務継続上、機密性の要件の緩和が必要な対策について例外的扱いを認めるかを判断することが推奨される。

【表 1-2】情報セキュリティ対策とＩＣＴ部門における業務継続計画の比較

	情報セキュリティ対策	ＩＣＴ部門の業務継続計画
活動視点	機密性、完全性、可用性	可用性、継続性
管理対象	保護資産 （電子的記憶媒体上のデータ、通信回線上のデータ、プログラムコード、利用主体（ユーザ）、情報処理システム、ネットワークシステム、情報機器等）	重要業務と重要資源（建物、要員、データ、設備、電気、備品等）
活動目的	対象資産の保護	業務継続とそのための重要資源の確保
想定脅威	サイバー攻撃、情報システム障害、人為的な犯罪行為、オペレーションミス等（周辺のリソースは平常どおり使用できる状況を想定）	地震、水害、感染症、情報システム障害等 （周辺のリソースに被害がある状況）
主要活動領域	防犯領域	防災・危機管理領域

（8）クラウドサービスの利用

クラウドサービスを利用する形態が、近年、増加している。ＩＣＴ部門の業務継続の視点で考えると、自らの地域が被災しても、ネットワークや端末さえ利用可能であれば当該サービスを利用することが可能なため、自らの庁舎が被災した場合の業務継続に関するリスクの軽減を図ることができる。また、これらサービスの提供事業者がサービスを運用している地域が被災した場合でも、事業者として災害・事故対策を当該サービス拠点に集中的に投入すると期待できるので、被害は軽微で済む可能性が高い。したがって、各地方公共団体で分散して運用されているよりは早期復旧が可能と考えられる。一方、そのサービス拠点の被害が軽微に抑えられなかった場合、その影響がサービスを受ける多数の地方公共団体に及ぶというリスクもある。また、ネットワークの途絶の影響が大きくなるリスクもある。

以上より、業務継続の確保の観点からも、クラウドサービスを利用することは検討に値する。費用対効果、リスクの特性を総合的に判断して導入を検討することが必要である。

【表 1-3】クラウドサービスの長所と留意事項

長所	・サービス提供事業者の情報通信機器設置環境は一般的には堅牢であり、地方公共団体が通常負担できるレベルを上回る。 ・地方公共団体の庁舎内で、設備の耐震性の確保などの業務継続上の対策の必要性が少ない。 ・外部のリソースを活用するため、要員増大の抑制が可能である。
留意事項	・ネットワークが切断されるとサービスが停止するため、ネットワーク機能の継続ができる仕組みも検討していく必要がある。 ・クラウドサービスに障害が発生した場合のサービスの継続性もしくは代替手段を確認しておく必要がある。 ・地方公共団体の庁舎内での端末の稼働は不可欠なので、庁舎の耐震性、電力確保の対策などの必要性はあまり変わらない。 ・堅牢とはいえ、事業者の拠点の災害リスクを考慮する必要がある。 ・サービス内容によっては外部のサーバに重要な情報を保存することとなるため、導入に当たっては機密保持契約、情報漏洩対策等セキュリティ面での対策を実施する必要がある。

第２章　本ガイドラインを利用するに当たって

2.1　ＩＣＴ部門の業務継続計画策定に当たっての留意点

事業継続計画の策定は、首長等のリーダーシップのもと、各部局の主体的な取組が必要であり、計画の対象範囲が広くなる分、計画策定の事務局も各部局も相当の労力と時間を要する。そこで、ＩＣＴ部門がいきなり全庁を主導しようとしても容易ではないと予想される。しかし、ＩＣＴ部門は、災害・事故時の行政の業務継続を支える情報システムを管理する立場として、また、事前準備がなければ業務継続が大変難しい部門である特性からして、一刻も早く業務継続の取組が望まれているのも明らかな事実である。このため、本ガイドラインではＩＣＴ部門における業務継続計画を策定することを目的としている。

地方公共団体においてＩＣＴ部門の業務継続計画の策定を検討するに当たっては、以下の点に留意することが必要である。

（１）地域条件

情報システムを立ち上げるに当たり必要となる電力、通信（電話）等の公共インフラ復旧には地域差があり、事前対策や復旧対策の検討において考慮する必要がある。過去の地震における事例から見ても、山間部では都市部に比べて復旧に当たる供給事業者の担当者等の参集が難しいため、電力や通信の復旧時間が長くなる傾向がある。復旧に要する時間を事前に詳しく把握することは難しいが、電力、通信等の供給会社と連携して、早期復旧を阻害する要因を把握することが重要である。

また、情報システム復旧に当たる職員や要員の参集に必要な交通機関、道路や橋の被害発生予測を考慮する必要もある。

（２）外部への依存

情報システムに関して外部事業者への依存度が高い地方公共団体においても、情報システム停止による業務停滞の責任は当該地方公共団体が負うことになる。外部事業者との十分な連携・協力を考慮することが重要であり、必要に応じて外部委託契約のあり方を見直すことが考えられる。

（３）災害対策実施状況の格差

同時被災しない場所で情報のバックアップが保管されている場合、バックアップはないが耐震補強等の減災対策は取られている場合、何の対策も取られていない場合等、それぞれ地方公共団体により災害に対する対策状況は大きく異なっている。

同じ震度６強の状況を想定するにしても、このような事前の対策の実施状況により、情報システムの予想被害は大きく異なるため、まずは現状の災害・事故に対する脆弱性を明確にすることが重要であり、その上で、それぞれの状況にあった最低限必要な事前の対策（耐震補強やデータの外部保管等）を検討していくべきである。

（４）サーバ設置場所

情報システムの運用方法により、重要なサーバを庁舎内又は近隣に設置している場合とデータセンター等遠隔地に設置している場合がある。

重要なサーバが庁舎内又は庁舎が所在する地域と同時に被害を受ける場所にある場合は、災害・事故により、情報システムのサービスが停止するとともに、庁舎や地域住民も同時に被害を受ける。一方、重要なサーバをデータセンター等遠隔地に設置しており、そこが被災した場合は、庁舎等は無事であるにも関わらず、停電やネットワークの断線(および可能性は低いがデータセンターの被害)等により情報システムのみが使用できない状況になる可能性がある。

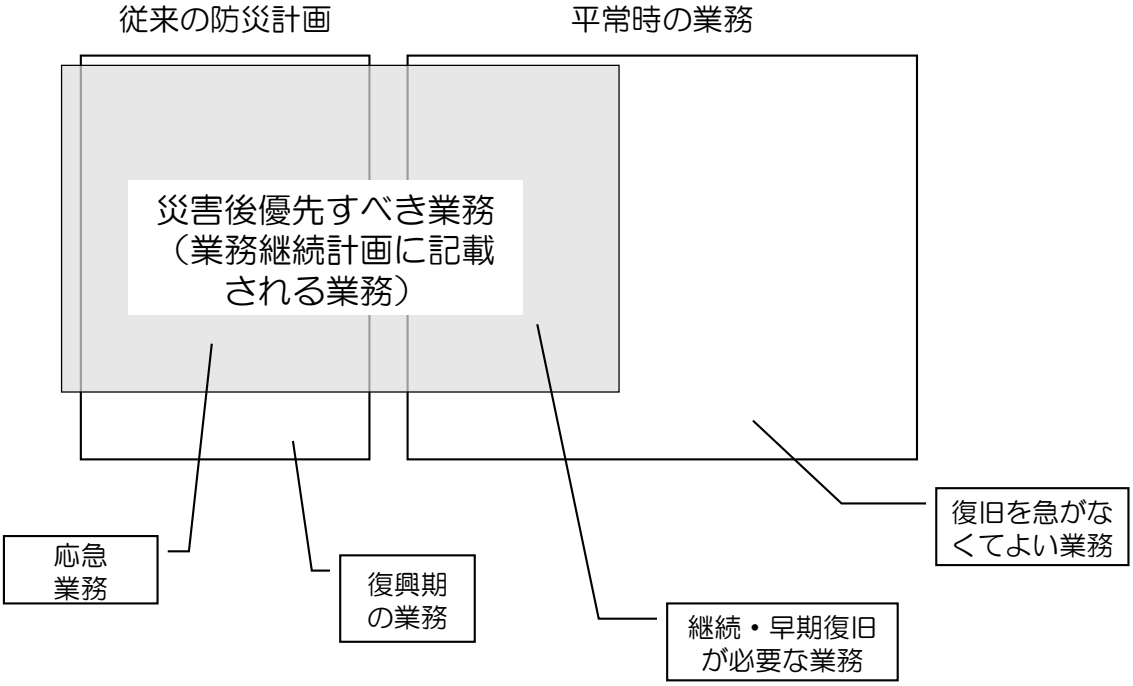
まずは、現状の情報システムの運用方法を確認し、何と何が同時に被災し得るかを検討する必要がある。

（5）業務視点での整理

第 1 章で述べたとおり、全庁的な業務継続計画ではなくＩＣＴ部門の業務継続計画と限定したとしても、目的は地方公共団体としての業務の継続・早期復旧であり、業務に関する視点なしでは検討はできないのは当然である。地方公共団体における災害後の業務範囲のイメージは図 2-1 のとおりである。

【図 2-1】行政機関の防災計画、平常時の業務

出典：丸谷浩明著「事業継続の意義と経済効果」



ＩＣＴ部門の業務継続計画の検討においては、図２-１の業務継続計画の範囲である「応急業務」及び「継続・早期復旧が必要な業務」に必要不可欠な情報システムを優先的な対象と考える。多くの地方公共団体の現状では、平常時の業務のうち「継続・早期復旧が必要な業務」と「復旧を急がなくてよい業務」の区別を明確にしていないため、まずは業務部門と共同してこれを選別するか、若しくは業務部門に可能な限り選別を求め、その作業を支援する等の対応を行うことが必要となる。

なお、「応急業務」に関しては、どのような業務があるかは従来から検討されてきているため、本ガイドラインによる検討ではこれを選別することは主要な検討課題とはしないが、前述のとおり、自ら被害にあってリソースに制約が生じている中で実際に実施ができるのかという観点での検討が現状では不十分であると考えられるため、この点の追加的な検討を業務継続計画では重視すべきである。

2.2　本ガイドラインの構成

前述の通り、本ガイドラインではＩＣＴ部門における業務継続計画を策定することを目的としている。このため、本ガイドラインでは３部構成のステップアップ方式を採用し、ＩＣＴ部門として無理なく業務継続計画の策定に着手し、着実に進め、改善を継続するとともに、全庁的な判断が必要な投資等の抜本的な対策の提案・実施に進むことが可能となるような工夫をしている。

第１部　ＢＣＰ策定の基盤づくり

ＩＣＴ部門が主導して検討や実施が可能な範囲での課題を取り上げ、各種の対策の実施計画及び災害時の行動計画を策定する。

非常時対応体制の整備や行動手順の整理、簡易かつ費用がかからずに（若しくは少ない費用で）実施できる業務継続に不可欠な基本的対策等、ＩＣＴ部門として最低限行わなければならない事項を実施することが目的である。

第２部　簡略なＢＣＰの策定

第 1 部を発展させて、業務部門（情報システムを業務で利用する各部門をいう。以下同じ。）を含めた検討体制を構築し、業務部門の意向も踏まえた簡略な業務継続計画を策定することを目的とする。

業務部門に対するヒアリングを通じて、ＩＣＴ部門における重要業務を選定し、業務の中断の原因となりかねない要素・資源の抽出や事前対策（多大な投資が必要なものを除く。）計画の策定とその実施、業務継続・復旧に関する行動の具体化を図る。

第３部　本格的なＢＣＰの策定と全庁的な対応との連動

本格的なＩＣＴ部門の業務継続を追求するためには多額の投資判断を要する事項も検討し、業務継続計画に位置づけ、着実に実施していく必要があり、そのような本格的な業務継続計画の策定を目的とする。多額な投資の判断が必要となるので、全庁的な業務継続計画でなくても首長等までを含んだ全庁的な検討体制が必要となる。

【参考】小規模団体向け ICT-BCP チェックリスト

ICT-BCP 策定の進まない小規模団体向けに、内閣府（防災担当）「市町村のための業務継続計画作成ガイド」[3]を元に ICT の最低限の備えとして、本ガイドラインと紐づけたチェックリストを新たに策定した。このチェックリストを用いて、最低限の不足している対策を確認、補うことで、業務継続計画と整合させた ICT-BCP としてのスモールスタートが図れるようにしているため、参照されたい。

[3] 内閣府（防災担当）「市町村のための業務継続計画作成ガイド」（平成 27 年５月）

2.3　本ガイドラインの利用方法

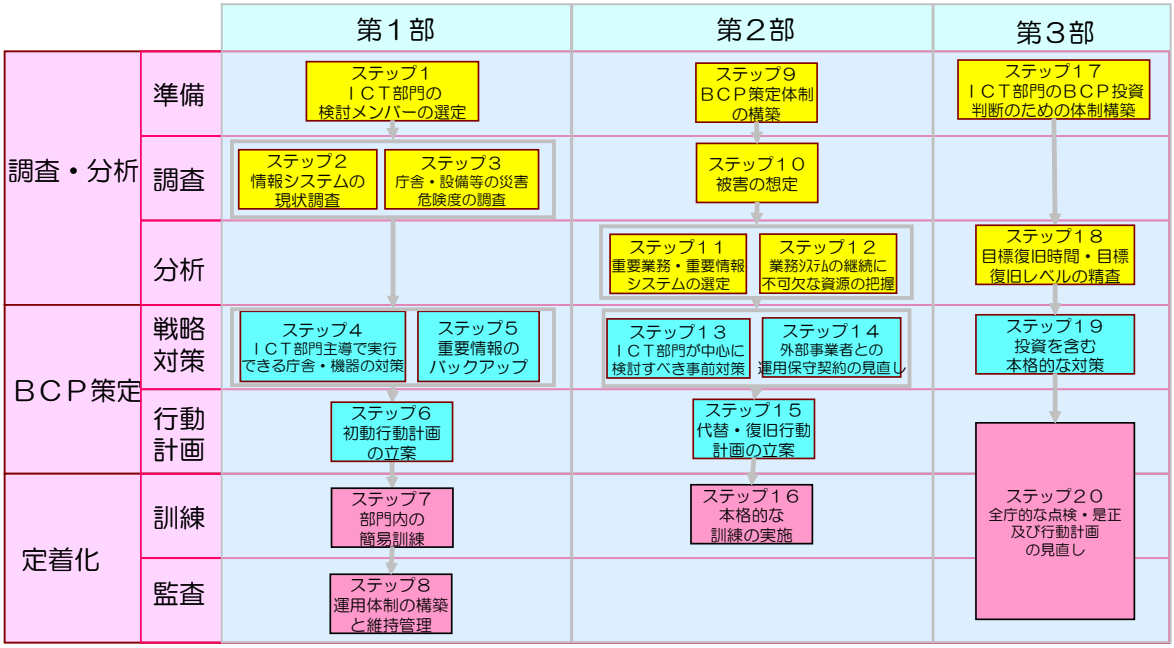
本ガイドラインの第１部は基本的にすべての地方公共団体のＩＣＴ部門において実施が望まれる範囲であり、また、第２部及び第３部も可能な限り実施していくことが望まれる。

図 2-2 において各部ごとに同列に並んでいるステップに関しては互いの検討に影響するため、同時並行して検討することを推奨する。また、同じ部の中であれば必ずしもステップの番号どおりに検討しなくてもよく、各ステップが完全に完了していなくても次のステップに進んでよい（例えば、ステップ４，５で決定した対策が完了しなくてもステップ６を検討してよい）。

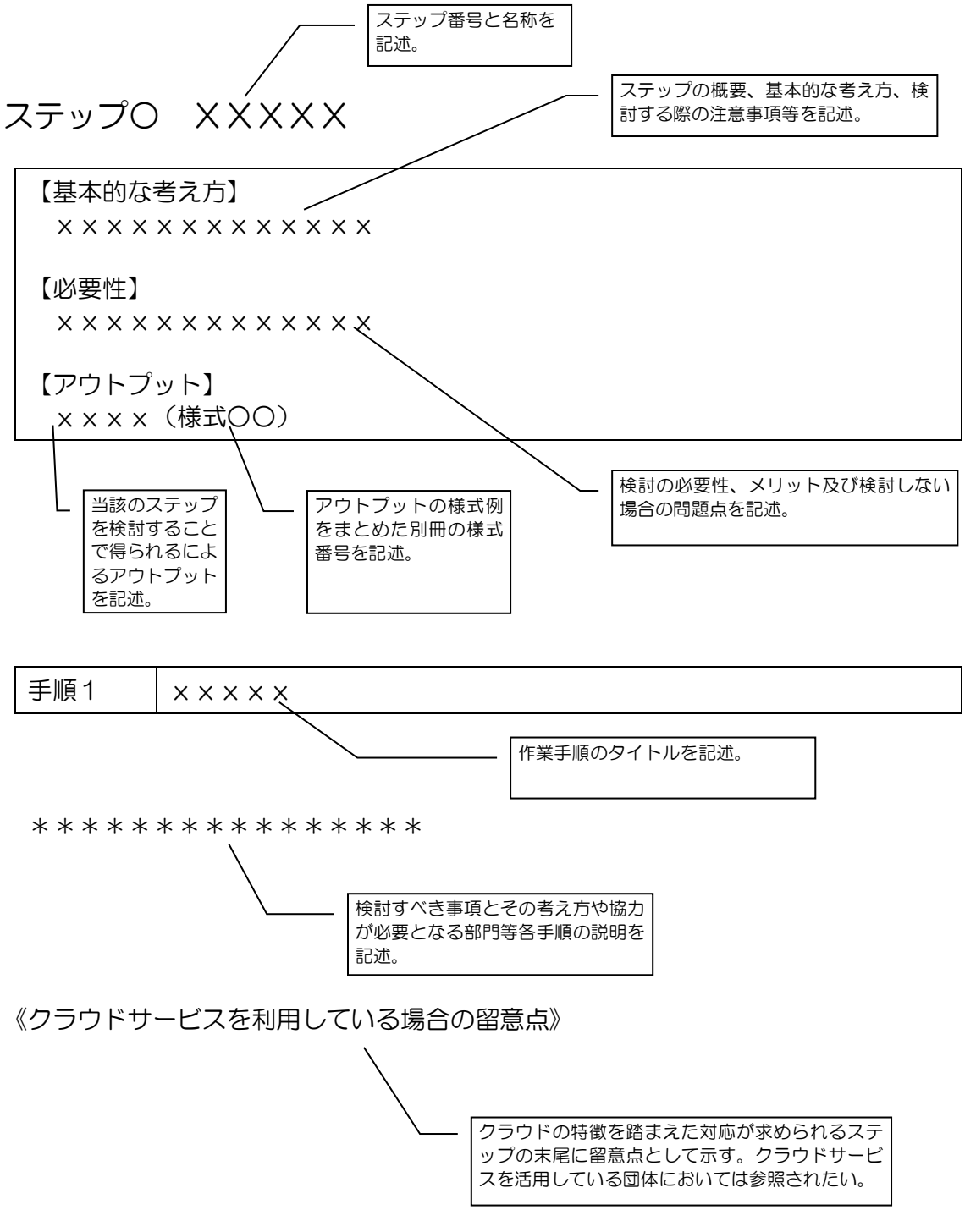
第２部や第３部の検討過程において、以前の検討結果の変更が必要な場合も多くある。関連する部分については、以前の検討内容を確認し、適宜修正しながら進めることが必要である。例えば、ステップ４，５の対策についてはステップ１１，１２で重要情報システムを決定した後には対策内容を変更する必要性が生じる可能性がある。このため、ステップ１３の検討時にステップ４，５を振り返って内容を確認する。

各部の検討終了時には、それまでの検討内容を検証し、かつ、定着を図ることを強く推奨している。本ガイドラインに記載された内容を検討し、決定・文書化することのみで業務継続計画の策定が完了するのではなく、定期的に訓練・見直し等を行い、維持更新活動を行い、職員に定着させ、またそれを劣化させないというマネジメントを実践することが重要である。

【図 2-2】本ガイドラインのステップ構成



■各ステップの構成
各ステップは以下のとおり文書が構成されている。

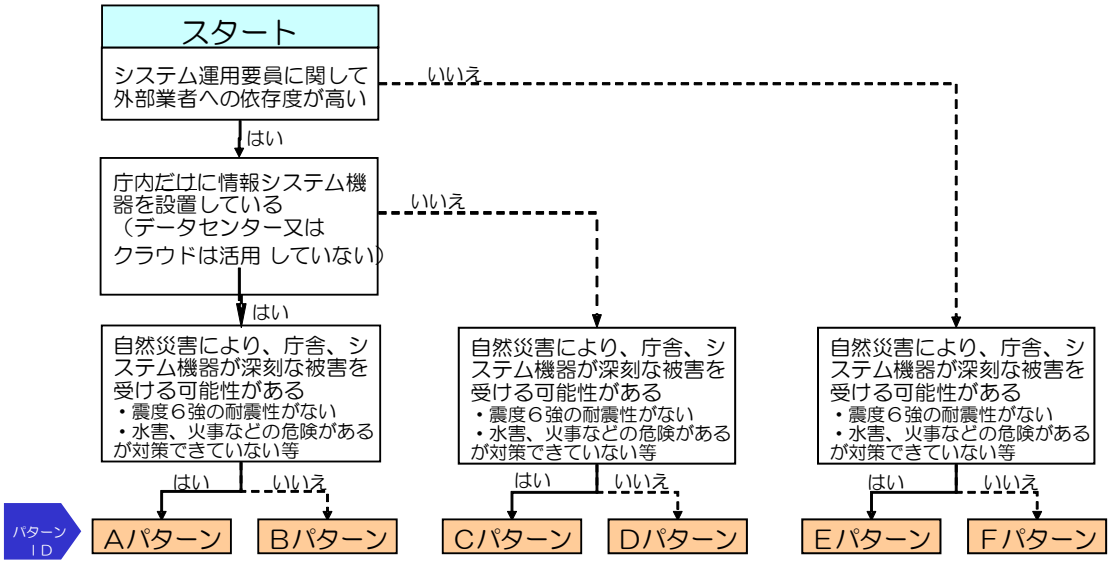


《クラウドサービスを利用している場合の留意点》

2.4　自らの状況の理解

地方公共団体によって、災害・事故時に情報システムの機能を継続、早期復旧するための条件・環境は多様であるため、各々の状況にあった業務継続計画を検討することが必要である。まずは、図 2-3 の分岐フローで自らがどのパターンにあるかを把握し、どういった事項を中心に検討すべきかを理解することが必要である。パターンによって検討内容が大きく異なる場合や検討を省略してもよい場合があり、それは本文中に注記する。したがって、策定作業を説明する第３章は、各地方公共団体自らが該当するパターン（ＡからＦまで）を十分に頭に置いて、検討を進める構成となっている。

【図 2-3】パターン把握



以下の表では、各パターンについて、以下の３点を説明している。

(1) 被災した場合の実態を把握すべき範囲
(2) 最優先して実施すべき対策
(3) その次に実施すべき対策

	中心的に検討すべき項目
A	(1)被災した場合の庁舎、情報システム、要員（外部事業者を含む)の実態を把握する。 (2)大きな物理的被害が懸念されるので、早急に低コストの減災対策及び情報システムの機能の継続対策を実施する。 (3)(2)と同時並行的に、外部事業者のシステム運用要員を含めた緊急連絡手段、参集、安否確認等の初動計画も策定する。その終了後、外部へのバックアップの搬送や代替設備の利用等の検討を行う。
B	(1)被災した場合の庁舎、情報システム、要員(外部事業者を含む)の実態を把握する。 (2)災害時の情報システムの被害は比較的軽微とみられるため、外部事業者のシステム運用要員を含めた緊急連絡手段の整備、参集、安否確認等の初動計画を整備する。 (3)外部へのバックアップの搬送や代替設備の利用等の検討を行う。
C	(1)被災した場合の庁舎、外部データセンター（クラウド含む)、情報システム、要員(外部事業者を含む)の実態を把握する。 (2)大きな物理的被害が懸念されるので、早急に低コストの減災対策及び情報システムの機能の継続対策を実施する。 (3) (2)と同時並行的に、外部データセンター（クラウド含む）についても、災害体制を確認し、外部事業者のシステム運用要員を含めた緊急連絡手段の整備、参集、安否確認等の初動計画を整備する。その終了後、外部へのバックアップの搬送や代替設備の利用等の検討を行う。

	中心的に検討すべき項目
D	(1)被災した場合の庁舎、外部データセンター（クラウド含む)、情報システム、要員(外部事業者を含む)の実態把握を実施する。 (2)災害時の情報システムの被害は比較的軽微の可能性があるため、外部事業者のシステム運用要員を含めた緊急連絡手段の整備、参集、安否確認等の初動計画を整備する。 (3)外部へのバックアップの搬送や代替設備の利用等の検討を行う。
E	(1)被災した場合の庁舎、情報システム、要員の実態を把握する。 (2)大きな物理的被害が懸念されるので、早急に低コストの減災及び情報システムの機能の継続対策を実施する。 (3) (2)と同時並行的に、職員の緊急連絡手段、参集、安否確認等の初動計画を策定する。その終了後、外部へのバックアップの搬送や代替設備の利用等の検討を行う。
F	(1)被災した場合の庁舎、情報システム、要員の実態を把握する。 (2)災害時の情報システムの被害は比較的軽微の可能性があるため、職員の緊急連絡手段の整備、参集、安否確認等の初動計画を整備する。 (3)外部へのバックアップの搬送や代替設備の利用等の検討を行う。

第３章　ＢＣＰ策定の手引き

第１部：ＢＣＰ策定の基盤づくり

ステップ１：ＩＣＴ部門の検討メンバーの選定

【基本的な考え方】
　第１部の検討メンバーを選定する。本来、業務継続計画策定に当たっては全庁を挙げた取組体制を策定すべきである。特に、首長等が積極的に参画して、全庁的な意思決定や予算配分判断をする仕組みを決める必要がある。しかしながら、それを待っていては迅速な対応ができないのであれば、ＩＣＴ部門は先行すべきである。そこで、第１部に関しては、ＩＣＴ部門単独でも十分に検討可能である課題を取り上げることにした。首長等や他の部門との協力体制を構築できない場合でも、最低限必要となるメンバーを選定して検討を始めることが可能であり、そのような取組を積極的に行うべきである。

手順１	検討メンバーの選定

業務継続計画策定のために、ＩＣＴ部門内で以下の検討メンバーを選定する。

（１）業務継続計画策定プロジェクト運営責任者（１名）
　プロジェクトとしての意見統一や首長等への報告を担当する。
　ＩＣＴ部門長が望ましい。

（２）担当者（最低限、１～２名）
　各種の調査や文書作成段階における文書化作業等の中心的な担い手あるいは作業の発注者の役割を行う。作業量が多いため、策定時における他の業務の負荷状況を勘案して適当な要員を任命する。情報システム全般に対して深い知識を持っている必要性はないが、ＩＣＴ部門の業務に対して一定程度理解している要員であることが望ましい。
　一般的には、第１部で策定した成果をまとめた文書の維持管理の中心的な作業も担当することになる。

　なお、業務継続計画による取組が、既存の情報セキュリティ方針に矛盾したものであってはならない。機密性を軽視した対応や対策が取られることがないように注視し、かつ、機密性の要件の緩和が必要な対策について例外的な取扱いを認めるかどうかを判断するためにも、既存の情報セキュリティマネジメントがある場合は、これを熟知した要員を検討メンバーに含めることが求められる。
　既存の情報セキュリティマネジメントを熟知した要員が参画することで、ステップ２の情報システムの状況調査等において、情報セキュリティにおける取組に関する情報を参考とすることができるというメリットもある。（本来、あってはならないことであるが、）その情報が陳腐化してしまっている場合は、 最新の状態に更新する必要はあるが、新規に調査するよりは必要な時間を短縮できると考えられる。

ステップ２：情報システムの現状調査

【基本的な考え方】
ＩＣＴ部門が主管する既存の情報システムの概要を調査し、問題点を把握するとともに情報システムの運用・保守を支える外部事業者との関係も整理する。また、ＩＣＴ部門以外が主管している情報システムについても、必要性に応じて調査・把握する。

【必要性】
ＩＣＴ部門の業務継続計画の検討を進める上での基礎的な情報として不可欠である。ここで調査した情報をもとに、本ステップ以降の検討を行う。

【アウトプット】
１．情報システム一覧（様式０１）
２．ネットワークの災害危険度（様式は自由）
３．外部事業者との関係の整理（様式０２－１）
４．クラウドサービス事業者との関係整理（様式０２－２）

手順１	情報システム一覧の作成

既存資料等を参考にして、情報システムごとに表 3-2-1 の事項を調査する。ＩＣＴ部門以外が主管している情報システムについて、どこまでを調査範囲とするかは各団体が個別に判断して決めることとなるが、消防、防災に関する情報システムについては、大地震等の広域災害においては早急に必要となる場合が多いため、調査対象として捉えるべきである。これ以外の情報システムについては、調査が可能な限り対象とすべきであるが、作業可能な範囲を考慮した上で範囲を限定して検討するのが現実的と考えられる。

【表 3-2-1】情報システム調査項目

対象情報システム	名称
	情報システムの概要（使用している業務）
	主管部門
ハードウェア	機種名
	設置場所
	保守事業者
ソフトウェア	ＯＳの名称・バージョン、インストールされているアプリケーション →故障した場合にすぐに再インストールできるか否か（特にレガシーシステム[4]か否か）を確認する。
	アプリケーションのバックアップの有無
	アプリケーションのバックアップ形態
	アプリケーションのバックアップ保管場所
代替機器	ハードウェアの損壊時に代替機として使用できる機器があるか →市販されているＯＳ（Windows11 等）で動作しており、どのような機器でも直ちに再インストールして動作するものは、代替機器があると同等に考える。

[4] レガシーシステムとは、時代遅れとなった古いシステムのことである。

	代替機の設置場所
クライアントＰＣ	クライアントＰＣの特殊性の有無 →市販されていない特殊なソフトウェアのインストールが必要か否かで判断する。

手順２	ネットワークの整理

当該情報システムに関するネットワークの全体像を把握する。ネットワーク構成図等があればそれを利用する。不明の場合は、ネットワークの運用保守を委託している外部事業者等に相談し、情報の整理を行う必要がある。

確認すべき情報としては、庁舎内のネットワーク及び各庁舎と支所や関連施設等を接続している庁舎外のネットワーク（ＷＡＮ）が二重化されているか否か、庁内のネットワーク機器が故障した場合に迂回経路があるか否かが重要である。特に、クラウドサービスを利用している場合は、ネットワークケーブルやネットワーク機器の対策は非常に重要である。サービスを運用しているサイトに接続する複数の手段があるか否かについては必ず確認する必要がある。

また、ＦＴＴＨ事業[5]のように地方公共団体が整備、運営管理している光ファイバー網等がある場合は、それも調査対象とし、ネットワーク機器類の災害対策状況や二重化の有無等を把握する必要がある。

手順３	外部事業者との関係整理

深刻な災害・事故の発生時において適切な対応をするためにも、主要な外部事業者（保守事業者等）について、表 3-2-2 の事項について確認することが必要である。情報システム、ネットワークの運用において外部事業者への依存度がほとんどない場合（パターンＥ、Ｆ）は、本手順を実施する必要は高くない。

【表 3-2-2】外部事業者との関係整理項目

契約事項	災害・事故時を含むサービス稼動率に関する取決め事項があるか。
	一定の被害が起きた場合に、担当者の参集時間に関する取決め事項があるか。
	災害によるサービス提供停止や被害が免責事項となっているか否か。
	一定以上の被害が起きた場合に、代替機器や場所を提供するなどのサービス継続に関する取決め事項があるか。
同時被災する可能性	地震等の広域災害において、事業者の事務所が同時被災する地域内にあるか。 →同時被災する地域内の判断がつかない場合は、地震を念頭に数十㎞離れているかどうかで判断する。
	事務所が同時被災する地域内にあっても、より遠隔に別の支援の拠点があるかをチェックする。
契約以外の協力関	一定以上の被害が起きた場合に、担当者が自動で参集する取決めが

[5] ＦＴＴＨ事業とは、光ファイバーによる家庭向けのデータ通信サービスである。

係について	あるか。
	電話が繋がらない場合に備えて、他の拠点の電話番号、衛星電話番号、メールアドレス等の代替連絡先を把握しているか。
	複数の担当者に直接連絡できるように、電話番号、メールアドレス等を把握しているか。

《クラウドサービス活用の場合の留意点》

手順１：情報システム一覧の作成においては、クラウドにてサービス利用しているシステムも対象にすること。ただし、オンプレと同様な調査項目の情報は得られない可能性が高いため、地震等の有事の際に、クラウドを運用する外部事業者がどこまでサポートするのかをSLA 等で確認することが考えられる。

手順３：外部事業者との関係整理においては、有事の際のサポート範囲に加え、平常時において、適正な取扱いが行われていることを定期的に委託先より報告を受け、確認できるようにしていることが重要である。

【表 3-2-3】クラウドサービス事業者との関係整理項目

契約事項	災害・事故時を含むサービス稼動率に関する取決め事項があるか。
	クラウドサービス事業者との責任分界点（データの管理責任の範囲や情報セキュリティ管理策等）を明確にし、それらについて合意しているか。
同時被災する可能性	地震等の広域災害において、クラウドサービス事業者のリージョンが同時被災する地域内にあるか。
	クラウドサービス事業者のリージョンが同時被災する地域内にあっても、より遠隔に別の支援の拠点があるかをチェックする。
契約以外の協力関係について	契約しているクラウドサービスの稼働状況や障害発生の有無を確認する手段があるか。

ステップ３：庁舎・設備等の災害危険度の調査

【基本的な考え方】
庁舎及び情報通信機器が、地震や水害等が発生した場合に、どのような被害を受ける可能性があるかを把握する。

【必要性】
現時点での課題を把握するためにも、可能な範囲で必ず実施する。

【アウトプット】
１．建物（庁舎・システム設置場所を含む）の状況把握結果（様式０３）
２．システム機器設置場所の状況把握結果（様式０４）

手順１	建物（庁舎・システム設置場所を含む）、設備等の脆弱性の点検

情報通信機器が設置されている庁舎、情報通信機器及び空調設備の地震・水害等に対する脆弱性を把握するため、庁舎、設備等について耐震性能や対水害性能を調査する。

庁舎以外に情報通信機器を設置している場合（パターンC、D）では、情報通信機器を設置している建物とＩＣＴ要員が通常作業をしている庁舎の両方について調査する必要がある。外部事業者のデータセンター等に設置している場合は、基本的には防災性の確保は外部事業者が契約責任を負っているが、不十分で業務継続ができない場合の住民や社会への責任は地方公共団体が負わなければならないので、状況を確認することが必要である。

（１）地震（震動）への対処

ア．庁舎

震度６弱から６強程度の地震が発生した場合に庁舎が機能を維持できる程度の耐震性を備えているかどうかを評価する必要がある。この震度を推奨するのは、震度６程度の地震が、日本全国のあらゆる地域でいつ発生するか分からない[6]とされていることに基づく。

まず 1981 年（昭和 56 年）６月から実施された新耐震基準で建築確認を取って建てられた建物か否かの確認については必ず実施する必要がある。新耐震基準以前の基準で建てられた建物については、耐震診断を実施しているか否か、耐震補強をしているか否かを管轄部門に確認し、耐震補強済みである庁舎は震度６弱から６強の揺れにも耐えられるレベルかどうかも確認する必要がある。

ただし、庁舎の耐震性が新耐震基準を満たしている場合であっても、強化ガラスや網入りガラスでない場合はガラスの飛散等の被害が発生する可能性があり、また、建物付帯設備も震度に耐えられるかは別途確認する必要がある。第２部以降でより詳細な評価をする場合は、建設会社又は設計事務所や設備会社等に相談する必要がある。

イ．情報通信機器

庁舎は十分な耐震対策が取られている場合でも（あるいは、耐震性が不足していても建物が運良く倒壊を免れることもあり、その場合でも）、サーバ、パソコン、プリンタ、ネットワーク機器等については、転倒により故障する可能性がある。何らかの被害を受けた

[6]首都直下地震対策専門調査会報告（中央防災会議「首都直下地震対策専門調査会」、平成１７年７月）では、活断層が地表で認められない地震規模の上限としてマグニチュード 6.9 の地震を「すべての地域で何時地震が発生するか分からない」として想定している。

場合、調達先が被害を受け再調達ができないかもしれず、調達先が被害を受けていないとしても再調達するには多くの時間を要する。

震度６強の地震にも耐え得る対策が実施されているかどうかの判断としては、パソコンやプリンタ等比較的小さな機器については、耐震マットや高強度のプラスチックベルト等で固定されていれば、概ね問題ないと考えられる。サーバ等の比較的大きな機器については、アンカー等で固定されているか否かを確認する必要がある。

ウ．空調設備

空調設備が故障した場合は、情報通信機器自体に被害がなくても、温度・湿度の異常により情報通信機器が停止する可能性が高い。実際に、過去の地震災害では、天井カセット型のエアコン室内機が宙吊りになる、ダクトの脱落・破損等が起きた事例がある。空調設備の保守事業者は災害時にすぐに参集できない可能性があるため、長期間修理できない状況になることも想定しなければならない。地震発生時の空調設備の安全性の確認を行う必要がある。

（２）水害への対処

情報通信機器が設置された場所が水害の危険があるかを把握するために、公表されている水害や津波のハザードマップや過去の経験から水害の危険性が高いとされる地域にあるか否かを確認する必要がある。危険性が高いとされる地域でサーバが１階や地下に設置されている場合は、浸水により全滅する危険性が高いことをよく認識する必要がある。また、電力線や通信線の引き込みが地下や低部にある場合には、それが被災する可能性も考慮する必要がある。

（３）火災への対処

地震については火災を併発するケースも考慮する必要がある（単独の火災についてはそのための業務継続計画が必要である。）。情報通信機器の主要な設置場所について、ハロゲン化物消火設備[7]等消火対策が取られているかを確認する必要がある。スプリンクラーは水を使用するため情報通信機器の消火対策としては適さず、また、情報通信機器がスプリンクラーの下に設置していないかについても確認することが必要である。また、火災の発生が懸念され安全のためとりあえず避難する場合などについては、消火の放水(上層階からの流下を含む。)から情報通信機器を守る対策を考えるべき場合もあると考えられる。

手順２	庁舎・設備等の脆弱性以外に認識するべきリスク

地震や水害等広域災害においては、電力や通信等公共インフラが停止するおそれがある。地方公共団体の庁舎への供給の復旧が優先される場合が多いと考えられるものの、広域災害においては運営側の対応できる人員も限られるため、長期間の停止となる可能性も検討する必要がある。以下の事項については、最低限現在の準備状況を確認することが必要である。

（１）電力

情報システムの稼働維持のために非常用発電装置が用意されているかを確認する必要がある。非常用発電装置がある場合は、何時間稼動することができる燃料がタンク等に実際に用意されているか、作動訓練の実施状況はどのようになっているかも確認する必要が

[7]水や粉末ではなくガス（炭化水素のハロゲン化物）を消化剤として利用する消火設備。消火剤による消火後の汚損が相当程度少ないという利点がある。

ある。
　また、安全に情報通信機器がシャットダウンするためのＵＰＳ装置（無停電電源装置）があるかも併せて確認すべきである。

（２）固定電話、携帯電話

　固定電話、携帯電話による通話は、広域災害の後は通話集中による輻輳（ふくそう）により非常に繋がりにくくなるため、災害時優先電話又は衛星電話が準備されているかを確認する必要がある。ＩＣＴ部門として準備がない場合でも、役所として準備があるか防災部門等に確認すべきである。

　なお、携帯電話のメールは広域災害時においても比較的つながりやすいため、ＩＣＴ部門の要員同士や主要な外部事業者との間で携帯電話のメールでのコミュニケーションが可能な状態となっているかも併せて確認すべきである。

《クラウドサービス、外部ＤＣ活用の場合の留意点》クラウドサービスについては、サービスの稼働状況や利用可否を公表しているサイトを事前に把握しておくことが望ましい。クラウドサービス、外部ＤＣ活用のケースでは、庁舎が無事で電源が確保できても、ネットワークが停止して情報システムにアクセスできない状況がありえる。ネットワークの回線の冗長性や通信事業者の基地局までのラストワンマイルについて、平常時のうちに脆弱性の有無を事前に確認し、必要に応じて対策しておくことが望ましい。

ステップ４：ＩＣＴ部門主導で実施できる庁舎・設備等の対策

【基本的な考え方】
ステップ2、3で明らかとなった庁舎や設備、情報通信機器等の課題について、ＩＣＴ部門のみで対応可能なレベルの対応策を実施する。

【必要性】
現時点での問題点を少しでも解決するために、可能な範囲の対策を実施することは急務である。早急には対応が難しいものについては残課題として整理し、第２部以降で改めて対策の実施について検討する。

【アウトプット】
１．現状の脆弱性と対策の実施計画（様式０５）

手順１	庁舎の脆弱性への対策

通常の作業場所や重要情報システムを設置している庁舎が耐震性や耐水害性等の問題があると分かった場合に、耐震補強等の抜本的な対策をＩＣＴ部門が主導で行うことは難しいことが多いと考えられる。しかし、課題を認識して以下のような対応策を取ることにより相当程度災害対応力の向上を図ることが期待される。

（１）重要サーバ等の移設
複数の庁舎がある場合には、サーバ等を設置している庁舎の他に耐震性の高い別の庁舎等がないかを確認する必要がある。耐震性の高い庁舎があれば、サーバやバックアップ媒体等を移設・移動することが望ましい。特に、バックアップ媒体を耐震性の高い庁舎へ移動することは比較的簡単に実施できるため、直ちに実施することを強く推奨する。
また、脆弱な庁舎内でなく、免震措置又は耐震措置が取られたデータセンター等のより安全な建物にサーバ等を移設することも対策の一つである。この方法は費用負担が大きくなるため、この段階で実現できない場合は、第２部で重要業務を選別した段階において、重要業務に必要な情報通信機器のみを移設することも考えられる。

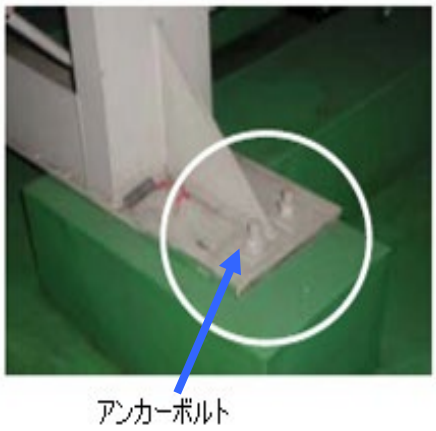
手順２	情報通信機器の脆弱性への対策

（１）ＯＡ機器等の対策
パソコンをはじめとしたＯＡ機器等比較的小さな機器については、安価で購入できる市販の耐震マットを底面に貼るだけで耐震や転倒防止に威力を発揮し、ある程度の震度まで対応が可能である。また、高強度のプラスチックベルトとロック部によってＯＡ機器等を固定できる商品もある。

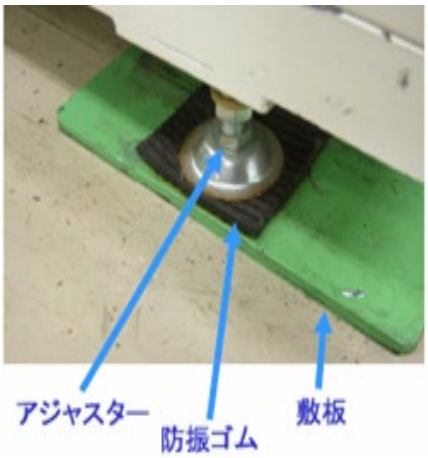
（２）サーバ等の対策
ラックに入ったサーバ等比較的大きな機器については、その性質・構造と設置する庁舎の壁・床構造にあわせて固定するか、あるいは免震対策を施して滑動防止措置を講ずるべきである。具体的な方法としては、アンカーボルト等による固定、アジャスター付設備や免震装置の導入、床全体を免震構造にする方法等が考えられる。施工した建設会社又はサーバ・機器等の供給元等に対して、より適切な対策を相談することが必要である。

【図 3-4-1】情報通信機器の耐震、免震対策例

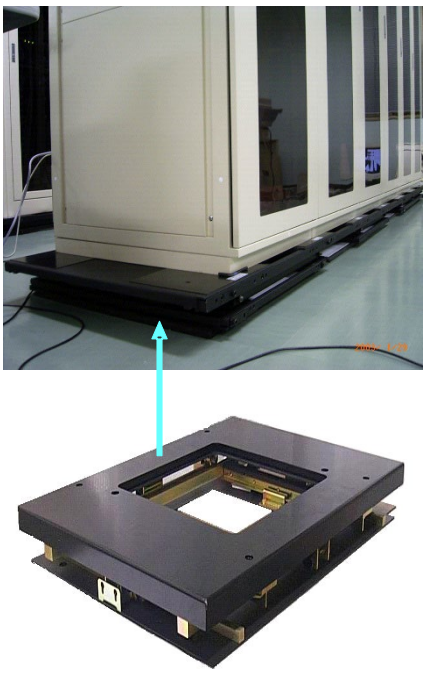
［a：固定的な耐震補強］



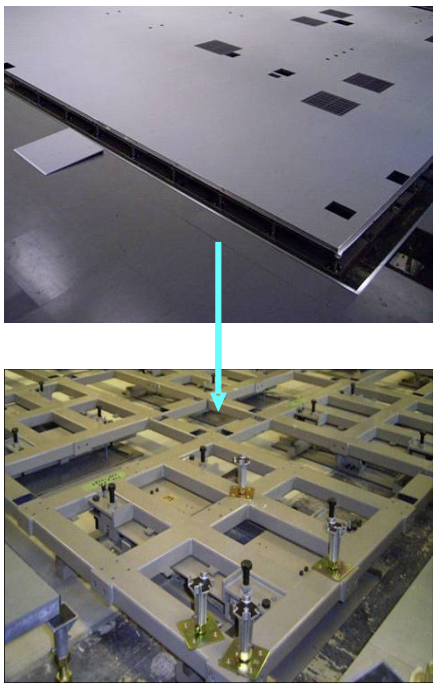
［b：防振ゴムによる免震対策］



［c：ＴＣＲ免震装置[8]による対策］



［d：床免震(床全体の免震対策)］



注：上記は対策の一例であり、導入に当たっては製造事業者や建設施工事業者に確認する必要がある。
出典：電機・電子・情報通信産業 BCP 策定・BCP 導入のポイント（電子情報技術産業協会・産業安全委員会情報通信ネットワーク産業協会）

手順３	ネットワークの脆弱性への対策

[8]TCR(Tuned Configuration Rail)免震装置：レールと車輪による振り子構造で地震の揺れを減衰させる装置

ネットワーク機器が損壊すれば影響が非常に大きいため、固定化等の措置を講じるほか、最重要のネットワーク機器（集積ハブ等）に関する安価な代替機器を準備することが必要と考えられる。

庁舎以外に情報通信機器を設置している場合（パターンC、D）では、ネットワークが切断されると庁舎が無事であってもサービスが停止する。ネットワークを停止しないように対策することが特に重要であり、サービスを運用している外部事業者の拠点に接続する手段を複数確保するなど手厚い対策を検討する必要がある。

ネットワークケーブルは、地震による揺れの影響で断線する可能性がある。庁舎内や庁舎間のネットワーク断線に備えて、予備用のケーブルを準備することが必要と考えられる。特に基幹の情報システムのサーバが設置されている庁舎と窓口業務等端末を数多く使用している業務を遂行している庁舎間のケーブルが断線した場合には、満足なレベルの窓口業務遂行が不可能になる可能性があるため、庁舎間を接続できる程度の長さのケーブルを事前に準備することが考えられる。
予備用のケーブルが被害を受けることを防止するため、地震による影響がないように保管手段を考えておくことも必要である。

庁外の通信事業者の責任範囲となる通信回線においては、通信事業者との災害協定等を行い、衛星通信や船上からの代替通信が可能な措置の検討も考えられる。外部との連絡はこれでよいが、行政システムの通信回線においては、閉域回線による外部拠点やクラウド接続が求められる場合もあるため、代替通信を用意したとしても、外部拠点やクラウド側の閉域接続サービスとの接続が即可能となる訳ではない。事前の準備やテストが必要となることを留意しておきたい。

手順４	その他の脆弱性への対策

ステップ2，3で以下についての脆弱性が明らかになった場合について、この時点でできる限りの対策を実施することが求められる。

（１）各種設備
空調設備等の情報システムの運用に不可欠な各種設備の耐震対策の状態に問題がある場合には、耐震補強等を行うべきか庁舎管理部門、防災部門等と調整する必要がある。

（２）電力
情報システムのサービス維持のために電力途絶に対する対策が十分ではない場合には、非常用発電装置の導入を検討すべきである。非常用発電装置があるなら、燃料の状態を確認し、燃料の量が不足である場合にはタンクの拡充が必要となる。また、非常時の際に優先的な燃料の補給が可能となるよう近隣の事業者と事前に取決めをすることも対策の一つである。

また、万一、安全に情報通信機器をシャットダウンするＵＰＳ装置がない場合は、直ちに装備する必要がある。

（３）固定電話、携帯電話
固定電話、携帯電話による通話が広域的な災害・事故等の後で非常に繋がりにくくなることへの対策として、災害時優先電話の導入を要請するか、衛星電話を準備するか検討す

る。ＩＣＴ部門としての確保ができない場合でも、役所として準備するか、あるいは役所として持っているものをＩＣＴ部門に割り当てるか防災部門等と相談する。

また、災害時優先電話や衛星電話を準備することが難しい場合でも、ＩＣＴ部門の要員間や主要な外部事業者との間で携帯電話のメールでのコミュニケーションが可能となるように、あらかじめメールアドレスを相互に把握するべきである。

《クラウドサービス活用の場合の留意点》

クラウドサービスを活用している場合は、かなりの部分を外部事業者に依存するため、外部事業者によるＢＣＰの取組みの確認を通じて、脆弱性が無いかを評価する必要がある。確認すべき内容として、総務省から発行している「ASP・SaaS の安全・信頼性に係る情報開示指針（ASP・SaaS 編）」[9]において、開示が求められる項目が参考になる。この中から、対象とするリスクに対し、必要な項目を選択して、新規契約時、契約更新時に確認していくことが考えられる。

[9] 総務省「ASP・SaaS の安全・信頼性に係る情報開示指針（ASP・SaaS 編）」（平成 30 年 10 月改訂）

ステップ５：重要情報のバックアップ

【基本的な考え方】
重要な情報が格納されたサーバやパソコンが破損し、バックアップも取っていない場合には、喪失したデータを復旧することは不可能になる。重要な情報については、最低限の対策としてバックアップを実施し、さらに、そのバックアップが同時に被災しないように対策を考える必要がある。

【必要性】
重要情報のバックアップをすることは必須事項であり、早急に対処すべきである。

【アウトプット】
１．重要情報のバックアップ状況と対策計画（様式０６）

手順１	重要情報の把握

まず、行政として、どんな場合にも失ってはならない情報や文書、業務の継続に不可欠な情報や文書としてどのようなものを保有・蓄積しているのかを調査することが必要である。

以下の２つのいずれかに当てはまる情報は、最低限守るべきものとして扱うことが重要である（第２部で重要業務を選定した場合には見直すこと）。

（１）大地震等災害・事故が発生した場合にすぐに使用するデータ、復旧に不可欠な図面や機器の仕様書等の書類
- 住民記録～住民の安否を確認するためなど
- 外国人登録～同上
- 介護受給者情報
- 障害者情報
- 道路その他の復旧に重要なインフラの図面又はそのデータ
- 情報通信機器等の重要機器の修復に不可欠な仕様書

（２）地方公共団体のみが保有しており、喪失した場合に元に戻すことが不可能あるいは相当困難なデータ
- 税金や水道料金等の収納状況
- 許認可の記録、経過等の情報
- 重要な契約、支払い等の記録の情報

手順２	重要情報の喪失危険性の把握

把握した重要情報がどのように管理されているかについて、以下の項目を調査する必要がある。
- どの場所、どの機器に情報が格納されているか
- バックアップを実施しているか
- バックアップをしている場合は、バックアップ媒体がどのように管理されているか（別拠点に定期的に移動しているか、耐火金庫等に格納されているかなど）
- データの復旧に外部のデータを利用できるのかどうか

各人のパソコンに重要情報があり、バックアップを定期的に行っていない場合、パソコンの転倒、滑落しただけでも重要情報を喪失する可能性があることを認識すべきである。

バックアップを定期的に行っている場合でも、同じ庁舎のサーバにのみ写しが保管されている、別の庁舎内であってもバックアップ媒体が無造作に置かれているような状況であれば、地震をはじめとする災害・事故に対する対策として十分とは言えない。

また、バックアップ媒体を耐火金庫等で保管している場合には、災害に対する危険度は比較的低いとは言えるが、庁舎に入れないレベルの被害を考慮すれば、対策としてはまだ不十分である。

手順３	重要情報の保護に関する脆弱性への対策

手順２で整理した重要情報の保管、バックアップ状況により、どのような対策を取るべきかを決定する。

（１）バックアップの実施

現時点で重要情報のバックアップが取られていない場合、情報通信機器が損壊するとデータを復旧させることが不可能となり、業務の継続が著しく困難となる状況が予想される。まずは初歩的な方式でも定期的なバックアップを実施することが不可欠である。

一般的にはテープ媒体によるバックアップが考えられる。より簡易な方法としては、定期的にデータが蓄積されている機器とは異なる機器にリモートコピーをすることがある。さらに、定期的に紙媒体に印刷することも最低限の対策としての一案である。

作業中の重要なデータが各人のパソコンの中にのみ保管されている状態にあることは、かなり多いのが現状とみられる。全庁的にこの傾向が見られる場合には、ＩＣＴ部門が率先してバックアップを実施しているサーバで重要情報を保管するように運用方法を変更し、そのノウハウを蓄積し、それを活用して他部門へも働きかけることが有効な一案である。

（２）バックアップ媒体の保管について

庁舎内に入れない被害状況となれば、同じ庁内でいくらバックアップを取っておいても意味がない。バックアップ媒体を定期的に異なる庁舎等に移動させることでリスクは大幅に減少する。可能であれば県外等遠隔地に定期的に移動させておくことが望ましいが、同じ地域内の耐震性の高い別の庁舎に移動させるだけでも重要情報が情報通信機器と同時被災するリスクは軽減される。

【参考】「非機能要求グレード（地方公共団体版）利用ガイド」[10]を活用したバックアップの外部保管方法等について、「非機能要求グレード（地方公共団体版）利用ガイド」において、業務・情報システムの分類のグループ単位で、「媒体による保管」、「同一システム設置場所内の別ストレージへのバックアップ」、「DR サイトへのリモートバックアップ」とレベルの指標を設定しているので参考にされたい（ガバメントクラウドにおける標準準拠システムについては、「地方公共団体情報システム非機能要件の標準【第 1.1 版】」[11]に記載）。

[10] 財団法人地方自治情報センター「非機能要求グレード（地方公共団体版）利用ガイド」（平成 26 年３月）
[11] デジタル庁・総務省「地方公共団体情報システム非機能要件の標準【第 1.1 版】」（令和４年８月）

ステップ６：初動行動計画の立案

【基本的な考え方】
実際に災害が発生した場合の行動計画を策定する。各種リソースが使用できなくなる状況を考慮して、可能な限り代替の作業手順も記述する。

復旧過程は以下の３つのフェーズに分けられる。本ステップでは必要性が特に高い初動フェーズにおける行動手順及びその実施担当者を整理する。復旧フェーズ、復帰フェーズについては、専門性がより高いため、第2部（ステップ１５）で検討する。
各フェーズは以下のような作業群から構成される。
（１）初動フェーズ：緊急事態発生の確認・連絡、被害拡大の防止、安否確認、被害情報の収集と被害評価の実施等
（２）復旧フェーズ：重要業務の仮復旧
（３）復帰フェーズ：本番環境への復帰

【必要性】
初動行動計画が不明確な場合は、例えば就業時間外に災害が発生したとすると対応要員が行動開始すべきか否か、どう行動すべきかなど判断が分かれたりして、業務継続活動が遅れる可能性が高い。簡略なものでも手順を整理することにより、復旧時間の短縮や誤った手順による手戻りの回避を実現できる。

【アウトプット】
１．緊急時対応体制（様式０７）
２．緊急連絡先一覧（様式０８）
３．緊急時における行動計画（様式９）
４．被害チェックシート簡易版（様式１０）

手順１	ＩＣＴ部門としての行動開始基準の設定

ＩＣＴ部門の職員が、どの程度の災害・事故が発生した場合に業務継続の対応を開始するかの基準を設定する。既にＩＣＴ部門の職員に対して「震度〇以上の場合は〇〇に参集する」等の一定ルールがある場合には、それで十分かどうかを再検討する。

大地震等の広域的な災害・事故の発生時には、通話集中による輻輳（ふくそう）により固定電話、携帯電話が非常に繋がりにくくなるため指示が伝達できない可能性が高い。そこで、ＩＣＴ部門としての行動開始基準の設定に当たっては、可能な限り客観的・定量的であり、かつテレビ・ラジオ等の公共放送から入手できる情報で判断できる基準とすることが有効である。

一般に、震度６弱以上の地震ならば、何らかの被害があることが予想されるため復旧要員全員が直ちに行動を開始すべきである。しかし、例えば震度５弱程度の地震でも、庁舎等に被害があるかないか現場に行かなければ判断できないことが多い。このような場合、最初からすべての要員が対応を開始するのではなく、まず特定の要員（本項では初期対応要員という）が状況を確認するために参集して、被害状況の調査し、責任者への報告を行い、部門全員による業務継続の対応を開始するかどうかを判断することが考えられる。

ただし、場合分けをあまり細かく設定しすぎると、どのケースに該当するか判断に迷いが

生じ、初動行動の遅延や行動ミスの発生の原因ともなる。行動開始基準としては震度等客観的に判断できる情報を判断基準として、以下の２段階か、あるいはこれに少数の段階を加える程度で設定することが望ましい。

（１）ある程度大きな被害が予想されるため最初から多くの要員が行動を開始すべき基準
（２）被害状況を確認するため初期対応要員のみが行動すべき基準

庁舎以外に情報通信機器を設置している場合（パターンC、D）は、設置している建物が被災した場合と、庁舎が被災した場合の両方について初動行動を検討する必要がある。なお、遠隔地の拠点に情報通信機器を設置している場合、当該遠隔地で災害が発生した場合の初動行動は担当者による電話等による情報収集から始まると考えられるが、その機器の管理者が別主体の場合、先方から自動的に迅速な連絡が入るような取決めもすることが望ましい。

手順２	ＩＣＴ部門としての緊急時対応体制

まず、ＩＣＴ部門の緊急時対応の指揮統制を取るための責任者を決定する。基本的にはＩＣＴ部門長がこれに当たるが、地方公共団体ごとの事情を考慮して決定する必要がある。広域災害時等には参集できず、通信も途絶えて連絡もできない可能性があるので、責任者と連絡が取れなくても復旧行動が遅延することのないように、代理（２人以上）を定めておく必要がある。

次に、初期対応要員を決める。責任者と同じく、特定の者が参集できないために復旧行動が遅延することのないように、必ず２名以上（できれば対象設備を考慮して必要な数）を指名する必要がある。当然ながら被害状況を評価するスキルを持つ要員を指名することが求められる。

情報通信機器を設置している建物がＩＣＴ部門の拠点と別に存在するなど（パターンC、D）、情報システムを運用する拠点が複数存在し同時に被災する可能性がある場合は、同時に初動行動を開始する必要があるため、拠点別に参集する要員を決定する必要がある。

外部事業者等の要員が初動対応要員として必要不可欠な場合（パターンA、B、C、D）は、あらかじめ当該事業者と協議して当該事業者側での対応要員も決定する必要がある。

手順３	緊急連絡先の調査

就業時間外に災害が発生し、必要な要員が参集できない場合でも連絡が取り合えるように、ＩＣＴ部門の要員や必要な外部事業者の要員の連絡先を事前に調査し、一覧にまとめるとともに、常に更新していくことが必要である。

様式０８「緊急連絡先一覧」を参考に必要事項を調査する。携帯電話、固定電話、携帯電話のメール等複数の手段を記録することが望ましい。特に、携帯電話のメールは広域災害時においても比較的つながりやすいため必要不可欠である。

なお、個人で契約している携帯電話等の連絡先の調査に当たっては、プライバシーの問題も考慮する必要があり、一般論として強制は難しいと考えられる。把握した情報の一覧表の取扱いについても、個人情報保護の観点から注意する必要がある。「緊急連絡先一覧」の作

成は災害・事故時における円滑な連絡に不可欠との認識を部門メンバーで共有し、加えて、収集した情報の取扱いについても同意が得られるような工夫をして、自発的な情報提供が得られるよう努める必要がある。

手順４	緊急時の行動手順検討

災害発生直後から迅速に行うべき行動をあらかじめ検討する。検討項目としては次のようなものが挙げられる。それぞれについて行動計画を整理する。

- 緊急事態発生の確認と連絡
- 情報通信機器の被害拡大の防止
- ＩＣＴ部門及び連携が不可欠な外部事業者の安否確認
- 被害情報の収集と被害評価の実施

初動対応については、就業時間内と夜間・休日など、災害発生時間により要員等の所在の状況や、周辺の負傷者等の支援の必要性などが大きく異なる。また、事態や被害の深刻さによっても初動対応すべき要員の範囲も変わってくるため、フロー図や場合分けの表などを作成して状況による対応の流れを整理する。

検討項目についての考え方は以下のとおりである。災害・事故等の発生が勤務中で建物が堅牢な場合（パターンB、D、F）は、所在地にとどまり状況を確認した上で、火災の発生や予想外の建物被害がない限り、情報通信機器の被害が拡大防止のための対応策を実施する。勤務中で建物が脆弱な場合（パターンA、C、E）は、現場（庁舎）に要員がいれば、まずは避難をしなければならない可能性が高い。情報通信機器の被害が拡大しないための行動は、建物や火災の安全が確認された後に取ることになると考えられる。
何をすべきか迷わないように、それぞれの状況に応じて、あらかじめ行動事項を整理することが必要である。

（１）緊急事態発生の確認・連絡

緊急事態を把握した場合に、その旨を報告すべき連絡先を優先順位付きのリストとして整理する。連絡できない場合を考慮して、連絡先は１か所当たり複数名（できれば３名以上）を設定するべきである。緊急事態を把握する役割を果たす要員、連絡先の相手について、具体的氏名又は具体的役職名で把握する。

就業時間内と夜間・休日での状況は大きく異なるが、特に夜間・休日に緊急事態が発生したことを想定して、緊急連絡の手段(通信の方法など)や、連絡事項をさらに別の者に伝達していくのであれば、その伝達の手順と手段を決めておくべきである。

なお、地方公共団体の部署によっては、関係先から被害状況の問合わせの電話が殺到して無用の負荷がかかってしまう場合がある。ＩＣＴ部門にそれが当てはまるかどうかわからないが、情報連絡は基本的に現場(庁舎)から発信することを原則とするルールを定め、各要員から職場に電話することを抑制することも一つの案である。ただし、情報連絡の妨げになる可能性もあり得るため、このようなルールを定めるかどうかは、各地方公共団体でそれぞれ判断することが必要である。

（２）被害拡大の防止

現場（庁舎）に要員がいる場合、情報通信機器への被害の拡大防止のための対策を取ることが求められる。何をすべきか迷わないように、取るべき行動をあらかじめ整理することが必要である。なお、外観上は軽微な被害のようであっても、内部は相当な被害を受

けており立ち入ることが危険である可能性もある。従って、被災した建物（庁舎）に立ち入る際には、建設会社又は資格を有する要員による安全性の確認をすべきことを明記することが重要である。

情報システムにおける二次災害防止措置としては、以下のようなものが挙げられる。各地方公共団体の特性を踏まえ、地震、火災、水害等様々な場面においてどのような対策を取るべきかを検討することが重要である。

ア．電源が落ちている機器は、以下の３点のすべてに該当する場合には電源を入れる。ただし、安全や状態について疑いがある場合は、事業者の技術者、電気技師等が機器と配電システムを点検するまで機器に通電しない。
- 物理的損害や浸水被害がみられない場合
- 外部電源が安定していると判断される場合
- UPS が機能する場合

イ．電源が入っている機器は、以下のいずれかに該当する場合は機器の電源を切る。ただし、機器のディスクランプが点滅しデータバックアップやシャットダウン処理等行っている場合等、電源を切るかどうかの判断がつかない場合は、即時の安全上の理由がある場合を除いて、事業者の技術者に相談するまで電源を切るべきではない。
- 公共の電源供給が途絶しており、UPS 電源による給電である場合
- 公共の電源供給が途絶しており、非常用電源による給電であり、十分な非常用電源の燃料が用意されていない場合
- 浸水被害、不安定な電源供給、埃、煙、塵その他の破片による汚染によってショートする可能性がある場合

ウ．庁舎から煙が出ている等、庁舎の被害が大きくなる可能性がある場合は、避難の緊急度の観点から許されれば、重要情報、文書、バックアップテープ等の持ち出しを行う。

エ．庁舎内の被害拡大が懸念される場合には、避難の前に、被害拡大の抑制のため、電気、ガス、水道の栓止めや防火扉の閉鎖等を実施する。

オ．配水管等の配置状況により、情報通信機器類に浸水の可能性がある場合は、ビニールシートを被せるか、軽量のものは設置場所を移す。

（３）安否確認

災害・事故の発生直後、人命救助や二次災害の防止措置を一応終えたら、復旧要員の確保のため、職員の安否を速やかに確認する必要がある。就業時間内に発生した場合は点呼により負傷者や閉じ込められた者等がいないかの確認を兼ねて行うこととなるが、夜間・休日に発生した場合を考えてあらかじめ、安否確認の連絡方法を決めておく。

ア．安否確認方法について

既に自宅電話や携帯電話等の緊急連絡網を作成している地方公共団体は多いと考えられるが、これは、電話が通常どおり使える場合には、有効な安否確認手段の一つとなる。災害・事故時においても確実に利用できるように、要員や連絡番号の更新状況、また緊急連絡網の保管状態を再確認する。

広域災害時には、通話の集中で固定電話・携帯電話はつながりにくくなる状況が予想されるため、電話より使用できる可能性が高い携帯電話のメールアドレス（携帯電話がない場合は自宅ＰＣのメールアドレス）も代替手段として追加登録することが必要である。

安否確認の手段としては、民間企業が提供している安否確認システムを導入することも考えられる。あらかじめ各要員が携帯電話等のメールアドレスを登録することで(同僚にアドレスが知られずに登録できるプライバシー保護に優れた種類もある)、発災時に自動的に（システムによっては手動で）メールが発信され、当該要員が安否情報を返信することで当該要員の安否情報を集中管理することができる。ＩＣＴ部門だけを対象として導入することには費用対効果を確認する必要があるが、全庁的に導入することも含め、対策として検討する価値はあると考えられる。

安否確認システムを全庁的に既に導入している場合の注意点としては、ＩＣＴ部門の管理職又は担当者が管理者として設定されていないと、非常時にＩＣＴ部門として安否情報を確認できない可能性があることである。これを契機に確認し、ＩＣＴ部門として活用ができるよう必要な処置を講じることが考えられる。

イ．職員以外の安否確認について

外部事業者等の職員以外で業務継続に必要な要員も安否確認の対象範囲に含めるべきである。役所の安否確認システムに登録することまでは難しいとしても、当該企業と協議し、必要な要員の連絡先を把握するとともに、企業側で適切に安否確認を行いその結果を早急に連絡するよう求めるべきである。

（４）被害情報の収集と被害評価の実施

緊急事態の際には、被害状況を確認して、業務継続の可否や業務復旧までの予想所要時間(とりあえずわかる範囲内でよい)等をＩＣＴ部門の責任者に早急に報告する。混乱状態の中で状況把握の漏れがないようにするために、あらかじめ被害評価チェックリストを作成し、これに基づいて情報収集することが望ましい。様式１０を参考として、サーバ室の環境及びステップ２で調査した情報システムごとの稼動確認のチェックリストを作成するだけでもまずは十分である。本格的なチェックリストの作成はステップ１５で行うこととする。

ステップ7：ＩＣＴ部門内の簡易訓練

【基本的な考え方】
　職員等関係者が計画どおりの行動がとれるようにするためには訓練の実施が不可欠である。また、計画の実効性の確認や改善のためにも実施する。本ステップではＩＣＴ部門単独でも可能な訓練を紹介する。全庁的な訓練計画との調整はステップ１６で説明する。

【必要性】
　策定した初動計画をはじめとした計画が非常時に有効に機能するためには、定期的に訓練を実施して、職員等関係者が計画どおりに行動できるようすることが必要不可欠である。また、計画の実効性の確認や改善のためにも必要である。

【アウトプット】
　１．訓練計画（様式１１）

手順１	訓練計画の策定

　業務継続のための訓練には、組織全体の参加が必要なものもあるが、ＩＣＴ部門単独でも実施することが可能なものもある。出来るものだけでも実施することで、情報システムに関わる業務の継続能力は大きく向上する。
　ＩＣＴ部門の業務継続に関連する訓練形態は、大きく分けて、机上での訓練（内容確認と役割分担の認識向上）と、対応要員が計画で定めている復旧行動を実施してみる実地訓練の２種類がある。訓練の目的によって、参加要員や訓練の進め方が異なる。必要な訓練をうまく組み合わせて、訓練計画を立てていくことが必要である。

手順２	訓練の実施

　以下の訓練については、ＩＣＴ部門単独で実施可能である。

（１）ＩＣＴ部門における机上訓練
　ステップ６で緊急時対応体制のメンバーとした要員が全員参加し、行動計画をまとめた文書を読み合わせて、各要員が緊急時に実施すべき行動の順を追って確認する。例えば、ある役割を任された要員が参集できない場合に、他の要員が代理してその役割を果たすことによって支障なく初動行動が実施されるかどうか、またその代理によって、本来その要員が行うべき役割が誰かによりカバーされるかなど、スキル要件等から実施が難しい行動がないかどうかを含めて確認する。

　なお、机上訓練では、リソースや公共インフラ等が一定期間使用できなくなる状況を想定して計画の妥当性までを検証することもある。これはステップ１０の被害想定の検討作業をした後の方が効率的であるため、ステップ１６で紹介することとする。

（２）緊急連絡、安否確認訓練

固定電話及び携帯電話が通話集中による輻輳（ふくそう）等でほとんど使用できなくなった事態を想定して、これらを使用せずに、緊急連絡及び安否確認を実施する訓練である。全庁的な訓練を実施しない場合であってもＩＣＴ部門内での緊急連絡、安否確認を実施する。多くの場合、携帯電話のメールなどを使うことが有効と考えられる。

なお、電話が使いにくい状況の中では、伝言型の連絡網は有効でないことが多いと考えられる。携帯電話等のメールを、システムが許容する相手方数の範囲内で同報発信し、それに個々のメンバーが返信する形の連絡方法が有効である。

（３）災害時用の情報システムや非常時用装置の点検

災害時用の情報システム（安否確認システム等）、非常時用装置（非常用電源や衛星電話等の非常用通信装置等）は普段使用しないため、必要になったときに使用方法がわからない場合や、故障や電池切れ等の状況になる可能性がある。また、安否確認システムについては、管理者権限が最新の状態になっていない場合や必要な要員に権限が付与されていない状況も考えられる。使用する可能性のある要員が定期的に使用訓練をしておき、機器の使用方法に習熟することが重要である。

（４）情報システム復旧訓練

情報システム停止を想定して、一度停止した（停止させた）情報通信機器の復旧作業の実地作業を実施する。また、代替システムを持つ場合には、切り替えの作業を実地に実施する。非常用電源等の使用を想定している場合は、災害時においても確実に使用できるか確認する。

このような復旧訓練は、非常用電源などの全庁的な設備は除き、ＩＣＴ部門が単独で実施することが可能である。ただし、その場合でも、情報システムの運用を外部事業者に依存していない場合（パターンＥ、Ｆ）を除き、外部事業者との協力が欠かせない。このため、外部事業者との協力関係を本格的に構築する第２部（ステップ１６）において、事業者も含んだ訓練について紹介することとする。

ただし、第２部の検討が直ちに開始できない場合は、ステップ１６を参照して、外部事業者も含んだ訓練を実施していく必要がある。

手順３	訓練結果の業務継続計画への反映

訓練を実施することで、様々な課題が発見されると考えられる。訓練実施のたびに、これらの課題の検討を行い、対応策を決定し、速やかに業務継続計画に反映することが必要である。

ステップ８：運用体制の構築と維持管理

【基本的な考え方】
検討した計画及び対策について必要な更新ができる体制を構築する。実際にどのような維持管理活動をしていくかを決定し、実践していく。

【必要性】
各ステップで検討した結果は、放置すれば内容が古くなり、非常時に役に立たなくなることも考えられることから必ず実施する。

【アウトプット】
１．業務継続計画の運用体制（様式１２）

手順１	運用体制の決定

第１部で検討した対策が計画どおりに遂行されているかを監督し、また作成した文書の更新を行うために、維持管理の責任者及び担当者を決定する。特段の事情が無い限り、策定体制の責任者（ＩＣＴ部門長）及び担当者が、そのまま維持管理における責任者及び担当者となることが望ましい。また、地方公共団体の災害対策の責任者が別に決められている場合には、従来の災害対策との整合を図る観点から、可能であれば責任者と副責任者を設定し、ＩＣＴ部門長は副責任者とすることも考えられる。この場合には、その責任者に、ＩＣＴ部門の業務継続の目的と策定した計画や文書の維持管理の重要性を理解してもらうことが必要であることは言うまでもない。
人事異動に備えて、役職で規定したほうがよい場合は役職で規定してもよいが、その場合には役職の重要な引き継ぎ事項として盛り込むことが不可欠となる。

情報セキュリティマネジメントシステム（ISMS）が既にある場合は、新たに業務継続計画の運用体制を作成せずに、既存マネジメントシステムと連動させれば、別々に運用することより生じる矛盾がなくなり、維持更新も確実に行われるようになると考えられる。例えば、ISMS の事務局の役割に、ＩＣＴ部門の業務継続計画の維持管理を追加することが考えられる。

検討メンバーではない職員を維持管理担当者として指名した場合は、これまでの策定プロセスを十分理解してもらうとともに、第２部以降の検討に参加させるべきである。

手順２	見直し時期と内容、承認ルールの決定

業務継続計画の見直しについては、策定済みの業務継続計画の最新性や正確性を維持するために１か月から長くても３か月程度の周期で見直すべき項目と、年に１回程度の周期で定期的に見直す項目がある。

見直すべき項目はそれぞれ以下の事項が挙げられる。見直しの際に見落としを防止するため、実施すべき作業項目を洗い出し、見直すべき項目のチェックリストを作成するべきである。

（１）１か月から長くても３か月程度の周期で見直すべき項目
- 人事異動、組織の変更による業務継続要員(多くの場合、ＩＣＴ部門全員が含まれ、業務継続に不可欠な外部事業者の担当者も含まれる。)の変更の有無
- 各要員や外部事業者等の電話番号やメールアドレスの変更の有無
- 復旧用の媒体、復旧手順書等、必要とする資源やマニュアルが予定どおりに準備されているか（破損等がないか）の確認
- 非常用電源(庁舎全体のものは除く。)や非常用通信手段の定期点検
- 取引関係の変更等により、協力関係を構築すべき外部事業者の変更の有無
- 机上訓練、連絡・安否確認訓練等の計画的な実施の有無
- 訓練実施結果の業務継続計画への反映状況
- 印刷された計画書の最新版への更新の有無

（２）年次で見直すべき項目
- 新たな情報システムの導入による計画の変更の必要性
- 点検等により洗い出された課題に対する対策の確実な実施（責任部門や対応スケジュールが未定のものは予算編成時に予算化するとともに、上位者、上位組織との相談が必要な案件については上位者等と対応を相談）
- 重要な外部事業者の業務継続（協力体制の構築）への取組の進捗確認
- 庁舎全体の非常用電源の稼働訓練に合わせた非常用電源の点検、その他の役所全体の防災訓練や設備点検に合わせた電気、通信、空調等のインフラの点検

年次見直しの時期については、定期人事異動後のある程度落ち着いた時期に設定すれば、人事異動による対応要員の変更にも速やかに対応することが可能である。

そのほか、予算編成時期や防災訓練実施時期等を意識して設定することが重要である。

また、定期更新と重ならない時期に新しい情報システムの導入、電気、通信、空調等のインフラの変更、業務の変更、組織変更、拠点の移動等があった場合は、早急に業務継続計画を見直す必要がある。定期更新以外の見直し要因を洗い出す必要がある。

なお、計画を改定した場合は、責任者の承認を得て、関係者に周知することが必要である。組織内の文書管理規程があればそれに従う。

■第１部のまとめ

この段階で策定した「業務継続計画」は、まだ、標準的に求められるレベル・内容のものとは言えない。しかし、ＩＣＴ部門が主導してできる基礎的な業務継続対策に取り組み始めており、緊急時に必要な職員が参集する仕組みや計画や文書について必要な更新ができる体制を構築できたことから、業務継続力は相当高まっているはずである。

これが時間の経過とともに劣化しないように、ステップ８の運用体制により、きちんと維持・点検といった管理がなされているかを確認し、その定着を見極めることが重要である。

策定した結果の文書は一冊の文書（加除式など、綴じ方は自由）にしてまとめておくとともに、検討経過の文書も見やすくファイルする。

（１）検討結果の首長等や関係部局への説明や開示について

ここまでの検討によって達成した情報システムの業務継続能力、対策レベルを首長等に報告し、併せて他の関係部局に積極的に説明していくことが重要である。取組内容を説明することで当該取組が評価され、全庁を挙げた協力体制構築に役立ち、第２部以降の検討を有利に運ぶことができる。また、他部局からの要請や未調整事項の課題が発見される可能性もある。

また、このような業務継続計画に関する地方公共団体の取組については、住民等の安心や信頼を確保するため、ホームページ、広報誌等を通じて、住民等に周知・広報することも重要なプロセスである。

（２）維持・更新、訓練に関して

第２部の検討に入る前に、ここまでの検討内容を再度確認する。

重要なのは策定成果の周知、維持・更新、訓練である。第１部で策定した内容について、ＩＣＴ部門の全員に十分周知し、特に、策定に中心的に関わっていない要員に自ら活動・作業を担う立場で意見を聞き、それが反映されているだろうか。また、必要な維持・更新ができる体制がＩＣＴ部門で取られ、それが定着しているかを再度チェックすることが必要である。また、ＩＣＴ部門内での訓練は不可欠であるが、その結果明らかになった問題点の解決を図ったであろうか。

これらの対応が完了するまでは、直ちに第２部に入ることは推奨しない。また、この後のステップでの精査の作業、訓練などの過程で問題点が明らかになった場合には、第１部で策定した計画や文書を早急に修正すべきである。修正は随時行い、その全体点検を年次の定期点検で行うと考えるべきである。

なお、訓練について、第２部の検討がすぐに開始できない場合には、第１部では詳細に説明しなかった初動訓練や情報システムの復旧訓練を、ステップ１６を参照して実施していくことが必要である。

第２部：簡略なＢＣＰの策定

ステップ９：ＢＣＰ策定体制の構築

【基本的な考え方】
第２部以降は、地方公共団体における災害・事故発生時の重要業務を選定して、自らの施設・要員等の資源に相当被害を受けている中でも、その重要業務だけは中断させず、あるいは必要な時間までに実施・復旧させるという、メリハリのある対応を実施するために、業務部門を含めた横断的な検討体制を構築する。

【必要性】
第２部以降はＩＣＴ部門だけでは検討できない事項が多い。業務部門を正式に検討体制に組み入れることが業務継続計画の策定に向けて必要である。

手順１	ＩＣＴ部門の検討メンバーの選定

第２部においても、ＩＣＴ部門の検討体制は、基本的に第１部での検討メンバーはそのまま引き継ぐ。ただし、検討メンバーが第 1 部で策定した計画の運用の担当となっていることが多いため、維持管理における負荷も想定して、メンバーを補充する。

ＩＣＴ部門としては、最低でも以下の役割は決めておく必要がある。

（１）業務継続計画策定プロジェクト運営責任者（１名）
検討プロジェクトとしての意見統一や首長等への報告・相談については、引き続きＩＣＴ部門長が行うことが見込まれるので、ＩＣＴ部門長が責任者となることがまず考えられる。ただし、第 1 部の運用体制で述べたように、全庁的な防災・危機管理計画の整合の観点などからすれば、すでに全庁的な防災・危機管理の責任者としてＩＣＴ部門長より上位者が決まっている場合には、その者を責任者とし、ＩＣＴ部門長が副責任者になる体制も考えられる。
本ステップ以降では業務部門との協力体制の構築が必要不可欠である。この点については、担当者レベルでの協力関係の構築に任せるのではなく、部門長間で協力体制を構築することが不可欠である。なお、ＩＣＴ部門長が責任者となり、ＩＣＴ部門長からの協力要請では業務部門から十分な協力を得ることが難しい場合は、首長等の強力な支援や指示が得られる体制作りが必要である。

（２）調査・文書作成担当（数名）
各種の調査や文書作成段階における文書化作業等を行う。作業量が多いため、策定時における他の業務の負荷状況を勘案して適当な要員を任命する。全員が情報システム全般に対して深い知識を持っている必要性はないが、ＩＣＴ部門の業務に対して一定程度理解している要員であることが望ましい。また、他部門や外部事業者との調整も本格化するため、深い知識を持つ者を１名以上当てるべきである。
第２部以降では業務部門との協力体制の中で、プロジェクトの対全庁的調整の事務局としての働きも必要となる。

手順２	ＩＣＴ部門以外の検討メンバーの選定

災害・事故時の発生時において、優先して実施すべき重要業務を選定するために、各業務部門の代表を検討メンバーに入れる。特に、防災・危機管理を担う部門（総務部門、福祉部門、建設部門など）の参画は不可欠であると言えるが、これだけではなく財政、人事、企画、住民窓口部門等も密接に連携することが必要なため、なるべく関係するすべての部門の代表を検討メンバーに含めることが必要である。

各部門の代表は、必ずしも部門長である必要はないが、各部門の業務内容を詳細に把握している幹部とする。

理想としては、全部門を含めた協力体制の構築が望まれる。しかし、これでは対象範囲が広すぎるならば、情報システムの利用の観点から明らかにＩＣＴ部門としての重要業務にならないと考えられる業務部門を対象外とする等の絞り込みを行う必要がある。対象外とした業務部門については、第 2 部での策定が終了した後の維持管理の段階で、検討すべき重要業務として抜け漏れがないかを改めて検証することが不可欠となる。

ステップ１０：被害の想定

【基本的な考え方】
　業務継続計画の策定に当たって対象とする事象（災害・事故リスク）を特定する。さらに対象とする事象によって業務に与える影響を想定する。

【必要性】
　被害想定を検討しない場合は、実際に災害・事故時に機能する計画であるのか判断ができないこととなる。また、ありえないリスクに対する過大な投資を防ぐためにも不可欠な作業である。

【アウトプット】
　１．被害想定の整理結果（様式１３）

手順１	対象とする事象の特定

これ以降のステップでは、対象とする災害・事故の事象を特定して、当該事象によりどの程度の被害を受けるかを想定した上で、実施すべき具体的な対策を検討する。対象とする事象を特定することで、各業務部門とともに重要業務を選定する場面で具体的なイメージを持って検討を進めることができる。また、現実的には起こる可能性が極めて少ない被害に対する対策の検討を省くことができ、過大な投資を防ぐことにも役立つ。

事象の特定は、最大の被害になり得る事象を選ぶことで、他の事象への対策もある程度は包含した対策とすることができる。例えば、「大地震」を前提とすると、震動による被害がテロなどの破壊活動と共通性があるほか、津波や火災等の二次災害及び電力途絶等の事態にも対処することが求められるため応用が利きやすい。このため、水害の危険性が高いなどの事情がない限り、まずは大地震を前提とすることを推奨する。

次に、特定した事象について、どの程度の規模を想定するかについても決定する。その災害・事故の規模に幅があると考える場合には、原則としては、より厳しいケースを想定することが必要である。
地震を前提とする場合は、いかなる地域でも震度６弱以上の直下型地震が発生し得る可能性があるとされていることから、震度６強、少なくても震度６弱以上の地震を想定することを推奨する[12]。

[12] わが国ではプレートや断層帯等の状況から地震が発生する可能性が高いとされる地域、その発生の可能性及び予想震度等が公表されているが、これらの地震の予想被災圏内にない場合でも、現状ではどこで発生するかの予想は難しく、マグニチュード 6.9 クラスの地震は国内すべての地域で何時発生するか分からないためである（マグニチュード 6.9 の震源付近では、震度６強～７の震度となることが想定される）。なお、平成２０年６月の岩手・宮城内陸地震ではプレートや断層帯等の状況から地震が発生する可能性が高いとされる地域外においてマグニチュード 7.2 の地震が発生した。

■参考：震度６強以上の地震により想定される二次災害例
- 津波、堤防決壊による河川氾濫等の水害
- 火災
- 土砂崩れ
- 電力、上下水道、ガスの途絶
- 通信途絶（音声、データのネットワーク）

特定した事象について、既存の防災計画等で被害想定が明記されていれば、この情報を活用することで作業を効率化することができる。防災計画等の被害想定で、原則として最も被害程度が大きい条件を採用する。

また、発生時間についても考慮する必要がある。ただし、前提条件を基本に据えながらも、あまり前提条件にとらわれることなく、他の条件に設定した場合の課題も合わせて検討することが重要である（例えば、要員の参集を考慮すると夜間・休日に発災した場合は条件が厳しいが、建物の倒壊までを考慮すれば平日夕方に発災した場合の方が条件設定として厳しいとも考えられる。夜間・休日の発災ケースのみを考えるのではなく、平日のケースも考慮に入れることが必要である）。

■地震の場合の条件設定項目
１．地震発生時期　　休日　冬、夕方６時　及び　平日　冬、午前１１時
２．震　源　地　　ＸＸＸＸ
３．規　　模　　マグニチュード６．９
４．庁舎付近震度　　６強
５．風　　速　　１５．０ｍ／sec

※発生時期を冬としているのは、暖房使用のために火災の発生確率が高いからであり、風速は、関東大震災時の強風と同様の風速 15m としている。これらの想定は、政府・地方公共団体の被害想定で多く使用されている。既存の被害想定で使用されている条件を使用すると、被害想定の作業の一部が省略できる。

情報通信機器を設置している建物が別にある（パターンC、D）など、情報システムを運用する拠点が複数ある場合には、まず、同時被災する可能性がある場合は、双方の被害を調査することになり、また、遠隔地にある場合には、情報通信機器を設置している建物が被災する場合と、庁舎が被災する場合の両方について調査する必要がある。

手順２	被害状況の想定

手順１で特定した事象について入手可能な情報を収集して、実際に当該事象が発生した場合に、自らの庁舎や関連施設、職員その他の要員、地域社会や公共インフラ等にどのような被害が発生するかを想定する。これにより、想定した状況下において業務実施に制約となる条件を把握するとともに、個々の具体的な対策の必要性を判断する際の基準とすることができる。

現実の被害は様々な要素が複雑に関係して発生する。そのため、正確に予測することは不可能であるので、ある程度幅を持たせた予測とする。あるいは平均的にはこの程度の被害であろうが最大ではこの程度の被害になる、といった予測とする。被害想定の精緻さは過度に追究せず、被害想定の困難さで立ち止まらないようにすべきである。必要ならば継続的に改善するものという姿勢で取り組むことが重要である。

以下の項目について、被害状況を想定することが望まれる。

（１）公共インフラの被害

広域災害においては、電力供給や交通手段の停止等が予想される。また、電話については、物理的な断絶に加え、安否確認や支援の要否の確認などで通話量が増加し、機器のパンクを防ぐため通話制限がかけられ、発災後しばらくは携帯電話及び固定電話ともに通話は輻輳によりつながりにくい状況となることが多い。復旧における制約条件を知るために、これらの被害の程度及び復旧見込みについて、大まかでも予測を立てておく。

被害の程度・復旧見込みは、特定の大災害に対して地域で既に発表されているものがあればそれを活用する。そうでなければ、過去の事例等をもとに推測するのが有効である。地域性によって公共インフラの復旧要員の参集に要する時間等の条件が異なるため、公共インフラの供給主体からの情報入手が必要である。その際、平均的な復旧スピードのイメージと、条件がかなり厳しい場合の復旧スピードのイメージの両方を把握して検討することが重要である。

ＩＣＴ部門としては、以下の公共インフラの被害について考えておくことが必要である。

- 電力の供給
- 通信インフラ（固定電話、携帯電話、電子メール等）の使用可否
- 公共交通機関の稼働状況（ＩＣＴ部門の要員の出勤可能性の観点）
- 道路の状況（ＩＣＴ部門の要員の出勤可能性、外部事業者や支援者の参集の観点）
  →防災部門に照会すべき内容であるが、交通規制の対象となる道路等は前もって決められており、橋の強度等も事前に調査されていれば途絶の可能性がわかる。
- 水道の供給（冷却水の観点、ＩＣＴ部門の要員の飲み水の観点）
- 下水道の被害（ＩＣＴ部門のトイレ使用の可否の観点）

（２）施設、要員等の被害

自らの庁舎をはじめ、学校、病院等の関連施設の被害について想定し、職員等の自らの要員の被害、裏を返せば出勤可能性についても想定する必要がある。

まず、情報システムを設置している拠点の庁舎の被害、次に役所機能の中枢を担っている庁舎の被害を調査する。関連施設は、必要性に応じて可能な範囲で検討対象とする（複雑になることを避けるため対象外としてもよい。）。

被害状況の設定が必要な主な項目は以下のとおりである。

- 庁舎の被害（庁舎の継続使用の可能性、庁舎への一時入館の可否）
- 職員の被害・出勤可能状況（ＩＣＴ部門は詳細に、他は概略で可）
- 施設への電力、水道の供給
- 施設内の設備（空調、電源設備等）
- 機器（サーバ、端末、ネットワーク機器等）の損害状況

ア．庁舎

ステップ３で調査した内容を参考にして、「倒壊の危険があり、即座に避難が必要」「倒壊はしないが継続使用は困難(一時入館の可否も想定)」「補修は必要だが継続使用できる(主な補修の種類も想定)」「ほぼ無傷」等の段階で推定する。判断のポイントは、その場で業務ができるか、災害直後に少しでも庁舎に立ち入ることができるかである。庁舎に対する電力、通信、水道、ガス、等の供給は優先的に復旧される可能性があるので、災害時の復旧の取決めを確認するなど、供給主体からの情報入手を強く推奨する。さらに火災が起これば全館避難となるので、火災発生の危険度にも考慮が必要である。

イ．要員（ＩＣＴ部門は詳細に、他は概略で可）

広域災害においては、夜間や休日に被災した場合は鉄道、バス等の公共交通機関の運行停止や道路の通行止め等により、要員が容易に参集できない可能性がある。職員の居住地を調査して徒歩や自転車等の手段でどの程度の要員が参集可能かを確認する必要がある。遠距離通勤をする職員が多い都市部の地方公共団体は注意が必要である。道路の陥没、建物の倒壊等による通行不能、避難者による混雑、停電等の原因により、平常時よりも多くの時間・体力を要することも考慮に入れる必要がある。

なお、ＩＣＴ部門の要員が多数でない限り、ＩＣＴ部門の参集可能性については、要員の対応可能性、代理の可能性などの検討で、既に第 1 部である程度把握されているはずである。また、ＩＣＴ部門に常駐する外部事業者の担当者なども、参集可能性の確認が必要な要員に含まれることは第 1 部で述べたとおりである。この段階ではそれらの再整理となる。

ＩＣＴ部門以外については、業務部門のコンタクトパーソンの参集可能性の把握は重要であるが、ＩＣＴ部門の業務継続を確保する観点からの作業であるので、役所全体としては概略の想定で足りる。

ウ．関連外部組織

情報システムの一部の運用をアウトソーシングしている事業者等の重要な関連外部組織は、業務継続計画を策定する上で必要不可欠な資源の一つである。

広域災害において、関連外部組織が同時に被災するかどうかは、その立地条件に影響される。庁舎の近隣にその拠点があれば、同程度の災害・事故にあうことになる。また関連外部組織の要員についても、近隣に居住又は勤務する要員については、職員と同様の被災程度と考えるのが妥当である。

また、関連外部組織が複数箇所に拠点を持ち、被災現地の要員が参集できない場合でも、同等のスキルを持った要員が別の拠点から参集可能な体制となっていれば、地方公共団体としての影響は軽減されるので、被害想定は異なったものとなる。

【留意事項】

個別の施設、機器、要員等の被害に関しては、個々の脆弱性をある程度判定できたとしても、様々な要素が複雑に絡み合うため、実際にどの機器、どの要員がどのような被害を受けるかを、事前に正確に予測することは困難である。したがって、個別の被害条件をできるだけ詳細に仮定して対応・対策を詳細に詰めることに精力を費やしても、前提条件から少しでも外れた事象には対応できないような業務継続計画を策定するのでは意味がない。むしろ、強い仮定を置かずに、被害程度に幅を持たせて設定し、それに合わせて対応・対策についていくつかの（少数の）選択肢を用意するという業務継続計画とする。ただし、少数の選択肢を用意するということは、災害後に一から対応・対策を考えることとは全く異なり、復旧の速度が格段に速くなることが期待できる点に留意が必要である。

《クラウドサービス活用の場合の留意点》

クラウドサービス等の外部サービスを利用している場合は、クラウドサービスの被害想定も考慮しておく。外部サービス事業者のサービス提供環境（災害対策、リージョン内の相互補完、リージョン間のバックアップの備え等）がわかれば、想定リスクに対する被害を評価し、整理しておく。

ステップ１１：重要業務・重要情報システムの選定

【基本的な考え方】
　業務部門と共同し、業務が停止した場合の住民や企業への影響を検討して、発災後において優先的に継続・早期復旧すべき「重要業務」を選定し、その復旧が望まれる時間を確認する。その後、重要業務の遂行に不可欠な重要情報システムを決定し、目標復旧時間と目標復旧レベルも定める。
　理想的な目標復旧時間・目標復旧レベルを目指すことは中期的なスパンで業務継続計画の達成目標を考える上で重要ではあるが、現実的な災害後の対応策を考えるという意味では、最低限達成しなければならず、かつ達成できる根拠がある目標復旧時間・目標復旧レベルとする必要がある。なお、本ガイドラインには、業務影響分析を行い、目標復旧時間と目標復旧レベルを求める手順を、手順１から５に示しているが、「非機能要求グレード（地方公共団体版）利用ガイド」[10]に基づき、業務・情報システムの分類のグループ単位に設定する方法も考えられるため、参考まで示しておく。

【必要性】
　重要業務・重要情報システムを選定して集中的に対策を講じることは、自ら相当の被害を受け、投入できる人員・資源が限られる中での対応であるため、不可欠な作業である。また、事前対策の費用対効果を上げるためにも重要である。地域住民や企業への影響を考えて目標復旧時間・目標復旧レベルを定め、その前までに復旧できるように努力することが必要である。

【アウトプット】
　１．重要業務一覧（様式１５）
　２．重要情報システムとその目標復旧時間（様式１６）
　３．重要情報の目標復旧時点（様式０６に追記する）

手順１	業務影響分析

　重要業務を選定するに当たっては、対象とする事象によって発生する地域社会における被害を想像しながら、様々な行政対応がどの程度の期間中断すればどの程度の影響が発生するかを見極め、地方公共団体に求められる個々の行政対応のレベルや実施・復旧の時期を見極める必要がある。これを業務影響分析(ビジネスインパクト分析)という。業務影響分析を行うに当たっては業務部門の担当者にインタビューやアンケートによる調査を行うことが必要である。以下にその手順[13]を説明する。

（１）インタビュー等の調査方式の決定について
　具体的には、直接インタビューする方式、アンケートを配布する方式などが考えられる（表 3-11-1 参照）。回答者数等を考慮して適した方式を選択する。

[13]本手順の中で業務の開始・再開が遅れることの評価は、内閣府（防災担当）「中央省庁業務継続ガイドライン第３版（首都直下地震対策）」（令和４年４月）の「3.2 非常時優先業務等の検討」の考え方を基本に、ＩＣＴ部門における業務継続計画の検討のために一部を変更している。

【表 3-11-1】業務影響分析の調査方式

	インタビュー方式	アンケート方式
方式	各個人と直接に面談してヒアリングする。	アンケート形式にして回答を求める。
長所	業務継続計画の概要や必要性を直接説明できるため、的外れの回答結果にはなりにくい。	アンケートを一斉配布すればよいため、回答者数が多いほど聞き取り時間を短縮できる。
短所	回答者の時間調整が必要であり、回答者が多い場合には適さない。	的外れの回答が返ってくる可能性や返答がない可能性があるため、回答者に対して質問の趣旨を説明する会合を開いたり、回答の趣旨や意図を確認したりする作業が必要。 個人回答とならないように、部門長の承認欄を経て提出するよう求めることが必要。

（２）調査内容について

ＩＣＴ部門の業務継続計画の範囲となる業務は、本ガイドライン１５ページの図 2-1 にあるとおり、「応急業務」及び「継続・早期復旧が必要な業務」に必要不可欠な情報システムに関する業務となる。そこで、この作業においては、非常時に優先されない業務や、全く情報システムに依存しない業務については対象外とする。ただし、業務継続計画で定める代替拠点（情報システムの代替拠点ではない）に移動した際に、代替拠点から情報システムへのアクセス、通信環境、情報セキュリティの確保ができるようにすることもＩＣＴ部門の業務継続計画の適用範囲として留意すること。

ア．業務の仕分け

部門ごとに担当する業務は数多くあるため、業務を一定のくくりで区分して整理することが必要である。区分の目安を示して（例えば、課単位で概ね数個の区分にすることを求める等）、業務部門と議論しながら整理する。例えば、窓口部門であれば、住民票発行業務、罹災証明発行業務等の提供しているサービス単位に整理する。

イ．業務ごとの調査項目

以下の項目を仕分けした業務ごとに調査する。アンケート方式で実施する場合は様式１５「業務影響分析　ワークシート」を使用する。

（ア）業務を継続・復旧するために必要な情報システム

対象となる業務の遂行に使用する情報システムをすべて挙げる。

（イ）復旧の目標とする時間とレベル（目標復旧時間、目標復旧レベル）

非常時において情報システムが停止した場合、いつまでに復旧する必要があるかと、その時点で完全な機能の復旧でなく部分的な機能だけでも何とか足りるなどの判断を求めること(双方の組合せとなる場合もある)が合理的であり、必要である。目標復旧レベルとしては、通常の何割の処理ができればよいのか、情報システムが動かなければ全く仕事にならないのか、どの程度の期間ならば代替方法（手作業で証明書発行業務を行う等）で乗り切れるかを確認する。

なお、回答の際には、回答内容の誤りの有無の確認や、後日の見直し等に使用するために、回答の理由まで記述してもらうことを推奨する。

（ウ）使用している情報システムのデータの目標復旧時点

情報システムに登録しているデータについて、最大で過去何日間あるいは過去何時間程度データが喪失しても許容できるかを確認する。

例えば、夕方にデータを喪失するような事態になった場合は、毎晩バックアップを取

っている場合でも当日分に登録した情報は失われる。帳票等から情報システム復旧後に再入力できれば問題ないが、例えば、住民の納税データがマスタからの消し込み処理前に喪失し復旧する手段がないような場合は、大きな混乱を招く可能性がある。

上記の検討により、このデータについては、過去この時点までのものを災害・事故により失わせない、あるいは迅速に復旧させるという時点を決めるが、これを「目標復旧時点」といい、ＩＣＴ部門の業務継続計画においては特に重要性が高い指標である。

確認した結果は様式０７の所定の欄に追記する。現時点のバックアップ状況では目標復旧時点でのデータ復旧ができない場合は、課題と認識して対策を検討する必要がある。

（エ）各業務の開始・再開が遅れることによる影響の大きさ

適切な時間区分を設定し、どの時間区分までに各業務を開始・再開すべきかを検討する。例えば、１時間、３時間、６時間、12 時間、１日、２日、３日、・・・といった区分が考えられる。また、業務影響度分析を行う際には、それぞれの業務について、実施できる業務量や段階的な到達点等の観点から目標レベルを設定する。これらは、情報システムの復旧の優先順位を決めるのに必要な範囲内で把握する。

検討にあたっては、「中央省庁業務継続ガイドライン第３版（首都直下地震対策）」[14]と同様に以下の観点から検討する。

- 社会への影響（地域住民、地域の企業への影響から深刻なものを考慮する）
- 法令、規則、契約義務、信義則等への違反の有無
- 地方公共団体内の他の業務への影響（〇〇業務が実施困難になる）

各業務の開始･再開が遅れる場合の発災後の経過時間ごとの影響の重大性を評価する。図 3-11-2 の「影響の重大性の評価基準」を基本として、影響の重大性がⅡ、Ⅲ、Ⅳ、Ⅴのそれぞれのレベルになる時間を評価する。

【図 3-11-2】影響の重大性の評価基準
（出典：中央省庁業務継続ガイドライン第３版（首都直下地震対策）[14]）

影響の重大性		各業務の開始・再開が遅れることに伴う代表的な影響の内容
Ⅰ	軽微	〇社会的影響はわずかにとどまる。 〇ほとんどの人は全く意識しないか、意識をしてもその行政対応は許容可能な範囲であると理解する。
Ⅱ	小さい	〇若干の社会的影響が発生する。 〇しかし、大部分の人はその行政対応は許容可能な範囲であると理解する。
Ⅲ	中程度	〇一定程度の社会的影響が発生する。 〇社会的批判が一部で生じ得るが、過半の人はその行政対応は許容可能な範囲であると理解する。
Ⅳ	大きい	〇相当の社会的影響が発生する。 〇社会的批判が発生し、過半の人はその行政対応は許容可能な範囲外であると理解する。
Ⅴ	甚大	〇甚大な社会的影響が発生する。 〇大規模な社会的批判が発生し、大部分の人はその行政対応は許容可能な範囲外であると理解する。

[14] 内閣府（防災担当）「中央省庁業務継続ガイドライン第３版（首都直下地震対策）」（令和４年４月）

（３）調査内容の再確認（アンケート方式の場合）

アンケート方式の場合は、質問の意味が十分に伝わっていないことを考慮しなければならない。集まった回答は、内容に不備がないか、質問の意図に沿った回答となっているか、個人の主観による回答となっていないかなどを確認することが必要である。回答内容に問題があると感じる場合は、回答者に再確認する。

特に、影響の重大性については、各部門の担当者は自らの業務やそれに関係する情報システムをなるべく重要業務・重要情報システムとして位置づけようと考えるおそれもある。すべての情報システムが短期間で復旧するに越したことはないが、緊急時には使用できるリソースが限られることや事前対策の費用による制約を考慮して、まずは必要最低限しなければならない対策は何なのかを確認することが重要である。

同様に、データ喪失許容度の回答についても障害が発生する直前の状態に戻ることが最も望ましい。しかし、データの損失ゼロを自動的に達成するためには、レプリケーション（ステップ１９参照）等の大規模な投資が必要となる。データ損失を最大限度で許容できる期間を回答しているかどうかを判断し、疑問がある場合には、回答者と調整して内容を修正することが必要である。

手順２	重要業務の選定

手順１によって調査した結果をもとに、優先して継続・復旧すべき重要業務を選定する。

基本的には、長期間停止していても影響の重大性が軽微な業務を重要業務（災害時優先業務）から除外をする。また、情報システムに依存していない業務も対象外である。基準としては、例えば発災後２週間～１ヶ月以上業務が停止していても影響の重大性がⅢ（中程度）以上の支障が生じない業務は重要業務から除外する。発災後の制約が厳しい場合はさらに重要業務を絞り込んでいく。なお、「非機能要求グレード（地方公共団体版）利用ガイド」[10]において、業務・情報システムの分類例として、グループ①からグループ④のグループを設定しているので参考にされたい。

なお、ＩＣＴ部門ではなく各業務部門が個別に管理している情報システムを重要情報システムとして選定した場合、次のステップ（ステップ１２）以降の検討について、どの程度まで行うか判断が必要である。必要があればＩＣＴ部門と同等の検討体制を構築して、ＩＣＴ部門と一緒に検討する。すぐには体制を構築することが難しい場合には、まずは現状の体制で検討可能な範囲での業務継続計画を策定することを目指す。

手順３	重要な共通情報システムの選定

手順１では、個別業務部門へ調査して必要な情報システムを明らかにした。しかし、個別業務部門への調査からでは重要性が明らかにならない重要な情報システム及びネットワーク等の情報インフラも数多くある。これらの整理は、ＩＣＴ部門の要員が中心となって、考えられるものを挙げていくことが必要である。

選定した重要業務の遂行に不可欠な情報システムと、ここで抽出する共通情報システム・情報インフラ及び災害・事故時にのみ必要とする情報システムを合わせて、ＩＣＴ部門における業務継続計画の目的である重要情報システムとなる。

（１）全業務で共通的に必要となる情報システム
　個別業務部門に対する調査では抽出されにくい、全業務で共通的に使用している情報システムを確認する。災害時に職員の安否を確認する安否確認システムや電子メール、庁内の電子掲示板機能等が該当する。

（２）重要情報システムを稼動するために不可欠な情報インフラ
　重要情報システムを稼動するために不可欠な情報インフラを整理する。利用部門には見えないバッチ処理システムやセキュリティ関連システム、ネットワーク、サービスを利用するために必要な端末等が該当すると考えられる。

（３）災害・事故時にのみ必要とする情報システム
　災害・事故時における適切な意思決定や資源配分のためには、迅速な情報の収集と集約が不可欠である。また、罹災証明発行業務等、災害時にしか実施しない業務もある。これらを遂行するために必要な情報システムがないかを確認し、不足していればあらかじめ導入を検討することを推奨する。
　以下は、無償で手に入れることができるプログラムを紹介するものである（ただし、事業者に導入の支援を依頼する場合は費用がかかる。）。例えばこれらのプログラムを使用するならば、それを運用できる情報システムを災害・事故の直後に確保することが必要となる。

　地方公共団体情報システム機構の被災者支援システム
　https://www.j-lis.go.jp/rdd/hisaisyasiensys/cms_9098.html

（４）他の組織・地方公共団体と連携した情報システム
　住民基本台帳ネットワークシステムのように他の組織や地方公共団体と連携している情報システムについては、関連する組織や地方公共団体と調整のうえ、重要情報システムとするかを判断する。

手順４	目標復旧時間・目標復旧レベルの決定

　手順３までで選定した重要情報システムごとに目標とする復旧時間と復旧レベルを決定する。手順１，２で選定した重要業務の遂行に不可欠な情報システムと手順３で選定した共通的情報システムで設定方法が異なる。

（１）重要業務の遂行に不可欠な情報システムについて
　重要業務の遂行に不可欠な情報システムは、その重要業務の目標復旧時間・目標復旧レベルを達成することができるよう復旧させる必要がある。

ア．重要業務の目標復旧時間・目標復旧レベルの把握
　重要業務の目標復旧時間の簡易な定め方としては、アンケート結果から影響の重大性がある一定のレベルに到達する直前を目標復旧時間として仮に設定することが考えられる（例：影響の重大性がⅣになる前に復旧することをメドとするなど）。
　そして、望まれる目標復旧時間ではなく現実的に対応可能な目標復旧時間としなければ業務継続計画として達成できるものとはならないため、各業務部門と協議する。
　さらに、その目標復旧時間について業務量の復旧レベルが 100%である必要がなければ、時間とレベルの組合せと理解して、どの時間ではどのレベルの業務量の復旧が必要かを把握して、双方を組み合わせて設定する（例えば、1 日後には 30 パーセント、3 日後

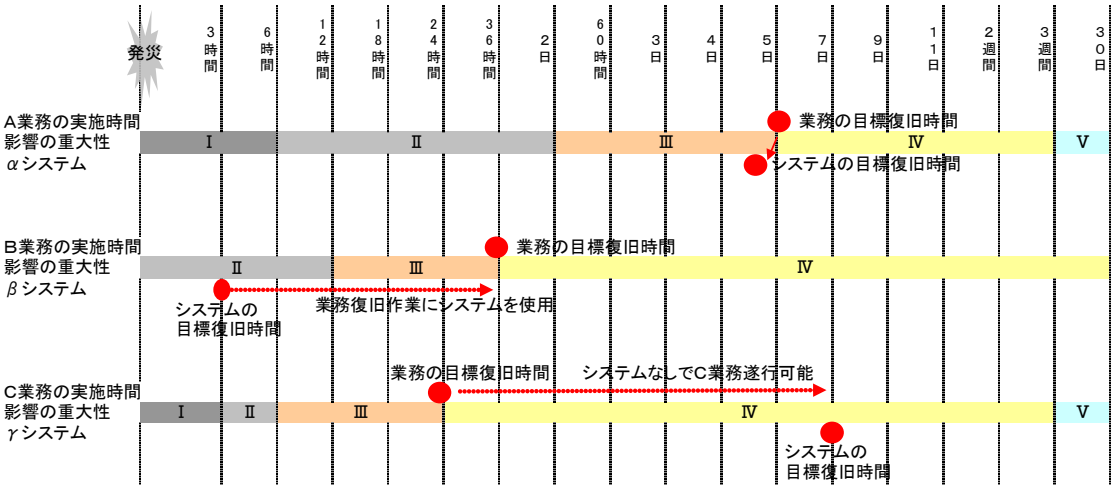
には 100 パーセントなど）。
　なお、この目標復旧レベルと組み合わせた検討は、検討作業としては目標復旧時間だけの検討よりも煩雑になる。組み合わせて検討を行う理由は、業務を支える情報システムの必要な稼働水準を見極めるためである。したがって、情報システムの稼働水準の高低に関わりの薄い業務については、目標復旧レベルの検討は省略して差し支えない。

イ．情報システムの目標復旧時間の設定
　重要業務の目標復旧時間・目標復旧レベルを定めた後に、情報システムの目標復旧時間と目標復旧レベルを設定する。情報システムの目標を設定する際には、以下の２点に注意する。

（ア）業務に対して必要になる時期の見極め
　各重要業務のある復旧レベルを達成させるべき目標復旧時間と同じ時点に情報システムが必要な水準で稼動してれば十分なのか、それとも、その準備の過程において既に情報システムの稼働が必要なのかを見極めなければならない。後者であれば、どの時点で情報システムがどの程度復旧していなければならないかを確認し、情報システムとしての目標復旧時間と目標復旧レベルを決めることが必要である。
　例えば、窓口業務に使用する情報システムは、窓口再開の少し前の時期に稼動していればよいことが多いため、業務の目標復旧時間の少し前を情報システムの目標復旧時間としてよいであろう（図 3-11-3 のＡ業務、αシステムを参照）。一方で、被害情報の把握に使用する情報システムや連絡用の情報システム等は、例えば災害状況の集約と発表の目標時間に復旧するのでは遅く、情報収集の作業の過程においても必要となる（図 3-11-3 のＢ業務、βシステムを参照）。

（イ）代替手段による業務遂行
　大地震等の災害時においては、現行の業務プロセスをそのまますべて復旧しなくても済むのならば、それによって節約できるリソースを他に回すべきである。情報システムに関して言えば、稼動していなくても手作業やネットワークに接続しないパソコン上で管理して、後日事態が沈静化してから結果を再登録すればよいものもある。このような情報システムについては、当面、重要情報システムから除外してよい。ただし、手作業等で代替するにしても、「数日間ならば持ちこたえられる」といった期間限定の代替手段もあるので、重要業務について前述の目標復旧レベルという概念を用いることが必要となる。業務部門に確認し、臨時代替手段で対応することが可能な期間についても確認をして、業務ごとの目標に合うように重要情報システムの目標復旧時間と目標復旧レベルを設定する（図 3-11-3 のＣ業務、γシステムを参照）。

【図 3-11-3】業務の目標復旧時間と情報システムの目標復旧時間



（２）共通情報システムの目標復旧時間と目標復旧レベルについて

全業務で共通的に必要となる情報システムや重要システムを稼動するために不可欠な情報インフラ等の目標復旧時間と目標復旧レベルについては、（１）で決定した重要業務の遂行に不可欠な情報システムの目標復旧時間・目標復旧レベルの設定を参考にして、ＩＣＴ部門が中心となって決定する。

手順５	重要情報の目標復旧時点の整理

重要情報の把握と対策についてはステップ５で整理したが、手順１の調査結果により、現状以上に保護が必要なデータが明らかになった場合は、現状の対策状況と目標とすべき保護範囲を、目標復旧時点を含めて整理する。

【参考】「非機能要求グレード（地方公共団体版）利用ガイド」[10]を活用した目標復旧時間・目標復旧レベル・目標復旧時点の設定

「非機能要求グレード（地方公共団体版）利用ガイド」[10]に地方公共団体における業務・情報システムの分類のグループ単位で、目標復旧時間・目標復旧レベル・目標復旧時点のレベル、大規模災害におけるシステム再開目標のレベルの指標を設定しているので参考にされたい。（ガバメントクラウドにおける標準準拠システムについては、「地方公共団体情報システム非機能要件の標準【第 1.1 版】」[11]に記載）。業務影響度分析の実施が困難な団体は、これらの基準を参考に定めることが考えられる。

《クラウドサービス活用の場合の留意点》

手順１で調査する情報システムに限らず、手順３の重要な共通情報システムの選定についても、「（１）全業務で共通的に必要となる情報システム～（４）他の組織・地方公共団体と連携した情報システム」はクラウドサービスとして活用しているケースも考えられるので、重要業務に利用される重要情報システムを選定する際はクラウドサービスを漏らさないように注意する。

ステップ１２：重要情報システムの継続に不可欠な資源の把握

【基本的な考え方】
災害・事故時において、重要情報システムの継続を確保するために、あるいは、優先的に復旧すべき重要情報システムを早期復旧するために、最低限必要となる資源（要員、庁舎、設備、備品、電力等）を把握し、これらの被害や既存の状態での代替策の有無等を検討して、重要情報システムの継続・復旧における課題を把握する。

【必要性】
上述の最低限必要となる資源を把握して、事前対策として、被害により失われ災害発生後に短い時間内で調達することが不可能な資源をあらかじめ代替資源として準備する、あるいは被害を受けないように補強するなどの対策を実施しなければ、重要情報システムの継続や早期復旧は達成できない。

【アウトプット】
１．必要最小資源の整理一覧（様式１７）

手順１	最低限必要となる資源の把握

情報システムを継続・早期復旧するために最低限必要となるヒト、モノ等の資源を把握する。実際に復旧作業を担当する要員が中心となって、現状の情報システム環境を基に、情報システムの継続・早期復旧に最低限必要と考えられる資源について、考え得るものをすべて挙げる。

日常何気なく使用しており、存在することが当然のものとなっている資産については見落としがちである。当然存在すると思い込んでいた資産が非常時において突然に利用できない状況にならないように注意が必要である。

具体例としては一般的に以下に例示されるようなものがある。表 3-12-1 を参考に、必要な資源を整理する。

（１）庁舎
情報通信機器が設置されている庁舎及びＩＣＴ部門の要員が作業する庁舎が使用可能なことが第一に挙げられる。通常どおり使用可能なことが必要不可欠な庁舎について、これまでの検討結果をもとに予想される被害（一切立入りできなくなる可能性、業務に使用できなくなる可能性、必要最小限のＩＣＴ部門の要員が作業できる環境スペースの確保可能性など）を整理する。

（２）情報通信機器
前ステップで選定した重要情報システムの継続のために必要で損壊を回避すべき情報通信機器（ハードウェア）を把握するために、重要情報システムごとに関係する機器を整理することが必要である。

（３）情報通信機器の稼動に不可欠な設備
情報通信機器に支障がなくても、非常用発電装置が稼働しない場合、電力が一時的にでも途絶すれば使用できない。また、空調設備が長期間機能停止した場合、温度・湿度の異常により情報システムが停止することとなる。

（４）重要情報システムの復旧に必要な機器、備品等

重要情報システムが被害を受けた場合を考慮して、復旧活動に必要となる資源を整理することが必要である。実際に情報システムが故障したことを想定し、復旧作業に必要となるものをーからシミュレーションするべきである。一般的には以下のものが挙げられる。

ア．故障した場合に代替機として考えている機器
イ．ソフトウェア、業務アプリケーション等のインストール、再セットアップ媒体
ウ．復旧手順書等の復旧に必要な文書類
エ．復旧作業に必要な情報通信機器（クライアントＰＣ等を含む）
オ．プリンタ、ＦＡＸ、事務用品等情報システムの復旧に関連する備品等
カ．ネットワーク断線に備えた予備用のケーブル

（５）要員

重要情報システムの継続、復旧に要するスキルを考慮して必要な要員をリストアップし、役割等に応じて整理する。具体的には、情報システム全体の統制をとる職員だけではなく、運用対応の職員のほか、派遣職員や外部事業者の保守要員等、確保できないことで目標復旧時間・目標復旧レベルの達成が困難になる要員はすべて整理しなければならない。また、出来る限り必要なスキル別に分けて整理することが必要である。例えば、メインフレーム、オープン系システムでそれぞれ復旧担当者が１名ずつ必要な場合に職員２名と整理していても実際にオープン系システム要員２名だけが参集しては、重要情報システムの継続運用・復旧作業は進まない。

必要な要員数をスキル別に把握した後は、夜間・休日に発災したことを想定し、スキル別にどの程度の要員確保ができるか分析するために、スキル別に分類した継続・復旧作業に必要な要員数と作業を遂行できる参集可能要員数（住所を調査して徒歩での参集可能性まで考慮）を比較する。要員不足となる作業については、次のステップで対策を検討する。

（６）公共インフラ

ステップ１０で検討した被害想定により途絶すると予想される公共インフラについては、代替手段（例：電力途絶については非常用電源）の準備の必要性を判断するために、使用できない場合の影響を把握する。

具体的には、以下の事項について検討する必要がある。

ア．電力

電力供給に関しては、庁舎内及び各施設の電力供給経路及び電源装置の状況について調査し、さらに、非常用電源装置の準備について確認する。

非常用電源を既に準備している場合でも、通常の電力使用量の数分の一程度の容量しかないのが通常であり、必要な情報通信機器やそれを支える空調機器が非常用電源に接続されているか、さらには、その稼動に十分な容量があるかどうかの確認も必要不可欠である。現状において容量が不足している場合は要検討課題として整理する。

イ．ガス

情報システムへの電源供給（非常用発電装置の稼働を含む）にガスを活用している場合もある。情報システムの継続・復旧においてガスの供給が必要な場合は、使用できない場合の代替手段を検討する必要がある。

ウ．上下水道

飲料水及びトイレは発災直後から作業する人数分の確保が必要である。上下水道が停止

する事態も想定し、停止が想定される期間中の飲料水の備蓄及び簡易トイレの備蓄状況を調査することが必要である。

水冷式の空調設備や機器等を使用している場合、水道水の供給停止により大規模な機能停止になる可能性もある。水冷式の空調設備や機器を使用している場合は、空冷式に変更する等の対策を検討することが必要である。

エ．電話（固定電話、携帯電話）

固定電話、携帯電話ともに１～数日間は通話集中による輻輳（ふくそう）によりつながりにくい状況になることが予想される。非常用通信手段について準備する必要の度合を検討する。なお、携帯電話のメールについては、輻輳の影響はある程度低いため、外部事業者を含めて各要員のメールアドレスの把握がされているかもあわせて確認する。

（７）要員の生活資源

復旧活動を行う要員の人数を踏まえて、必要な食料、生活必需品、医薬品等を把握する。職員だけではなく参集予定の外部事業者等の要員の分も計上しなければならない。これらについては、既に防災部門等により十分な備蓄品が準備されている可能性もあるので、まずは現時点で必要な備蓄品を確認する。

これらの準備は、一般的にはＩＣＴ部門が直接管轄する範囲ではないが、準備が十分ではない場合は、ＩＣＴ部門の業務継続・復旧に必要な分だけでも用意する必要がある。

（８）消耗品等

コピー用紙やプリンタのトナー等の消耗品は発災後しばらくの間調達できなくなることを考慮して、必要な量を保持することが必要である。窓口業務で使用するコピー、プリンタ等の管理もＩＣＴ部門が責任を負っている場合は、特に注意し必要な量を確認して管理することが必要である。

手順２	資源の準備状況の調査

手順１で検討した最低限必要となる資源が現状でどの程度準備されているかを確認する。また、機器や備品等に関しては被害を受けて使用不可能になることがないように、その保管状況についても併せて確認する。情報通信機器及びデータに対する対策は第１部で検討したが、重要情報システムの選定結果を踏まえて、改めて重要情報システムに関係のある機器や備品、備蓄について対策の妥当性と実施状況を詳細に確認する。

具体的には、現状の対策状況を確認した上で、ステップ１０で検討した予想被害の情報を参考に、各資源がどのような被害を受ける可能性があるかを把握する。正確な被害状況を予測することは容易でないため、予想被害については精緻に考えすぎないことも重要である。現状の耐震対策等の減災対策に不足があれば要検討課題として、次ステップ以降で対応策を検討する。

手順３	災害発生後に必要となる時期の見極め

復旧局面において必要な資源については、ステップ１１で定めた目標復旧時間・目標復旧レベルを達成するための重要情報システムの継続、早期復旧を実現するための各資源の必要数量及び必要時期を検討する。

必要数量及び必要時期を明らかにすることで、事前に資源を予備的に用意するなどの措置を講じることができる。また、災害時に必要となる資源が損壊した場合には、いつまでに代替の資源を調達しなければならないのかがすぐに判明する。
必要時期について正確に見極めることは難しく、おおよその目安としての算定でよいが、目安程度としても必要時期がわからない場合は、細かい時間単位での必要量は考慮せず発災後１週間以内で必要となる数量を考えるものとする。１週間以降については、自然災害やテロ等の事件であれば、徐々に新規調達が可能となると考えられるためである。

災害発生後直ちに使用する資材については、被害を受けることがないよう保管に注意することが必要であるが、万が一被害を受けた場合には、災害発生後に購入することも考慮しなければならない。方策として通常とは別の代替調達先を把握することが有効と考えられる。代替調達先からの調達も日常から一部でも行っておけばより確かであるが、代替調達先の情報を有するだけでも業務継続力は向上する。

《クラウドサービス活用の場合の留意点》
クラウド等外部サービスを活用している場合は、そのほとんどの資源を外部事業者に依存することになるので、外部事業者から提供されるサービスをひとまとめの資源として考え、対策状況を把握しておく必要がある。具体的な確認項目はステップ4，ステップ１４を参照。

【表 3-12-1】必要資源の整理例

必要最小資源 ｶﾃｺﾞﾘ		発災後必要数量			予想被害	既存の代替有無	
		即時	3日	1W			
庁舎	庁舎Ａ（ｻｰﾊﾞ設置施設）	現状と同等	ー	ー	倒壊はしないが、長期間使用できない可能性が高い	無	現状は代替ｲﾝﾌﾗ環境なし。30KM 南東のＢ事務所活用可能性あり
要員	情報システム統制者	１名	１名	１名	居住地が遠隔地のため、就業時間外は短期参集が困難	無	ｲﾝﾌﾗ対応メンバﾘｰﾀﾞが、訓練により対応の習熟可能性あり
	ｲﾝﾌﾗ対応者	１名	３名	３名	近隣居住のため、参集可能	有	複数メンバーが対応可能
	ﾎｽﾄ系運用担当者		２名	２名	近隣居住のため、一部参集可能	無	一部対応 AP により、代替不可
	ｻｰﾊﾞ系運用担当者		３名	３名	近隣居住のため、一部参集可能	無	一部対応 AP により、代替不可
庁舎内機器・設備・備品	空調機器		１台	１台	転倒、落下により 1W は機能停止	無	夏場の場合、代替不可能
	住基系ｻｰﾊﾞ	３台	３台	４台	免震床により稼動継続可能	無	代替サーバなし,
	介護保険用ｻｰﾊﾞ	１台	１台	１台	現状は、据え置きで転倒、１ヶ月機能停止の可能性	無	UNIX 系で、代替サーバとしての目処はたっていない
	職員用給与計算ﾎｽﾄ	１台	１台	１台	アンカーで固定したため転倒しないが、ﾃﾞｨｽｸ停止の可能性（３日間）	△	ホスト事業者と、隣接市町村とのホスト共有、協力の合意が書面で得られている
	事務用机、椅子		各７台	各７台	現状、強固な机、椅子	有	庁内での調達可能
	業務用ＰＣ		50 台	50 台	現状、地震用 PAD の貼り付けもされておらず、50%は転倒	有	Ｂ庁舎の PC100 台の活用
	プリンタ		５台	５台	現状、地震用 PAD の貼り付けもされておらず、50%は転倒	有	Ｂ庁舎のプリンタ 25 台を共有しての活用
データ	業務ｼｽﾃﾑﾊﾞｯｸｱｯﾌﾟ	１ｾｯﾄ	１ｾｯﾄ	１ｾｯﾄ	データ保管事業者の Daily 保管	有	データ保管事業者からの供給
	APﾊﾞｯｸｱｯﾌﾟ	１ｾｯﾄ	１ｾｯﾄ	１ｾｯﾄ	データ保管事業者の Daily 保管	有	データ保管事業者からの供給
	自治体 IT 継続計画書	12 冊	12 冊	12 冊	オフィス、自宅に設置完了	有	コア要員は活用環境が整備済
インフラストラクチャ	情報システム用電力供給	UPS	ﾒｰﾙｻｰﾊﾞ用	全面処理用	電力事業者の拠点が隣接していることによる電力供給の不足	無	終了処理用の UPS が整備済みであるが、代替供給機能はない 電力会社から早期復旧の可能性のコメントはあり
	庁舎Ａ内上水道		通常	通常	備蓄品５人３日分	無	備蓄飲料水の追加確保の必要有
	庁舎Ａ内下水道		通常	通常	備蓄トイレ３０回分	無	簡易トイレの追加確保の必要有
	電話：固定電話	通常	通常	通常	輻輳により、当日利用できない可能性あり	無	庁内に公衆電話が１台あり
	通信：NW(WAN)	通常	通常	通常	冗長化の構成ができているため、被害軽微	有	庁舎Ａからの外部へのアクセスラインは冗長化されている
	通信：NW(LAN)	通常	通常	通常	冗長化の構成ができているため、被害軽微	有	ルータも予備機が設置されている
	通信：地域防災無線	３台	３台	３台	主要拠点間での通信用に確保、訓練済み	無	何らかの理由で破損時は、利用不可能
	通信：衛星電話	１台	１台	１台	情報システム統制者用に一台確保済み。外部の電話、コミュニケーション確保が可能	無	何らかの理由で破損時は、利用不可能
	道路：交通規制		一部	解除	２週間程度は車での交通は困難	有	徒歩、マウンテンバイク整備済
	道路：近隣橋の強度	OK	OK	OK	強度に問題はないため、通行不可になる可能性は低い	有	橋の迂回路は２４H以上の距離となる

必要最小資源 ｶﾃｺﾞﾘ		発災後必要数量			予想被害	既存の代替有無	
		即時	3日	1W			
	鉄道：対象路線	ー	ー	ー	××線脱線、１ヶ月利用不可	無	代替策なし、バイク、徒歩

ステップ１３：ＩＣＴ部門が中心に検討すべき事前対策

【基本的な考え方】
ステップ１２で把握した業務継続にかかる課題を克服するために、取り得る対策を検討する。本ステップでは、主としてＩＣＴ部門が中心となって検討すべき対策を説明する。全庁的な予算計画の中で検討すべき課題については、第３部で検討する。

【必要性】
現時点での課題を解決するために、まずは出来る範囲の対策を実施していく必要がある。多大な予算が必要になるものについては検討課題として明確に記録しておき、第３部で改めて対策が必要かどうかを検討する。

【アウトプット】
１．課題克服のための事前対策（様式０５に本ステップでの検討結果を追記する）

手順１	事前対策の検討

この段階では各課題に関して、以下のような対策を取ることが考えられる。検討した対策については、実行責任者、スケジュールを決定して、業務継続計画書に事前対策の計画としてまとめて記録することが必要である。

（１）情報システムの継続・早期復旧のための対策
情報システムの継続・早期復旧のために必要な情報通信機器固定化や重要情報のバックアップ等基本的な対策は、ステップ４及びステップ５で検討したが、ステップ１１での検討結果を踏まえて、重要情報システムに関する対策に漏れがないかどうか検討する。第１部で検討した対策を精査し、追加すべき対策があれば、確実に本ステップで検討する。

また、生産停止や保守サポート切れ等により、故障した場合に代替品を再調達することが不可能な情報通信機器やアプリケーションを使用している場合(レガシーシステム)は、破損・故障すると元どおりに機能を復旧させることが困難となる。リスクをよく理解し、情報システム更新の優先順序の判断基準とすることが必要である。

（２）要員
情報システムの継続・早期復旧においては、特定の個人がいなければ活動が全く進まないという状況は避けなければならないが、実際にはそのようになっていることが多いとみられる。その改善には以下のような対策が考えられるが、あらゆる情報システムについてこれらの対策を取ることは困難であることが多いと考えられるため、基本的には目標復旧時間が短い情報システムから優先的に対策を行うことが重要である。

ア．代替要員の育成
特定の要員しか実施できない作業については、技術、専門知識を共有して、複数の要員で対応できるようにすることが重要である。
２名以上の要員が対応可能であればリスクは格段に低下すると言える。現状実施できる唯一の要員(以下「キーパーソン」という。)の働きはできなくとも、ある程度実施できる要員がいるだけで状況は大きく好転する。現時点においてＩＣＴ部門に適当な要員がいない場合でも、前任者やＯＢで対応可能な者がいれば、代替要員として事前に依頼し、訓練などに参加を要請して体制を整えることも考えられる。

イ．外部事業者における代替要員の確保

外部事業者に情報システムの継続や復旧を依存している場合は、委託先の代替要員の確保を求めることも必要である。外部事業者内においても、復旧作業が特定の個人に依存している状況は多いと考えられる。地震のような広域災害時には、そのキーパーソンが被害にあう、あるいは他の重要顧客の対応に取られてしまう可能性も考えなければならない。事業者と協議して、特定の個人に依存する状態から脱却するよう要求していくべきである。必要があれば、外部委託契約のあり方を見直すことが考えられる（ステップ１４を参照）。

ウ．作業手順やノウハウの文書化

情報システムの継続・復旧においては、読めば誰でも（若しくはある程度の知識を有する者ならば誰でも）作業できる詳細なコマンド（情報システムを継続・復旧させるために画面操作で入力する指示や命令文等）を記載した復旧マニュアルをあらかじめ作成することで、キーパーソンが参集できないリスクを軽減することができる。

特に、事業者に大きく依存している状況であれば、委託先の代替要員が参集できず、職員だけで対応しなければならないことも考慮し、詳細な復旧手順書を準備する必要がある。

エ．テレワークによる対応

ＩＣＴ部門の業務継続計画の発動に伴う作業を実施する担当者が現場での対応が困難な場合を想定し、リモートアクセス環境から作業が実施できるよう、テレワークの仕組みを構築することも考えられる。

オ．業務の自動化

現地で手動による対応を実施している作業は、可能な限り自動化を図っておくことも考えられる。

（３）文書、インストール媒体等

復旧手順書等の情報システム復旧に必要な文書やインストール用の媒体等が、保管している建物の被災、二次災害の火災による焼失等により使用できなくなる可能性を考えておく必要がある。

対策としては、なるべく複数の場所、複数の手段で保管することがある。例えば、復旧手順書ならば電子データで部門サーバ等に保管するほか、クラウド等のセキュアな外部サービスを利用して保管する、あらかじめ印刷しておいて耐火金庫等で保管する等の対策が有効である。保管場所については、ＩＣＴ部門のみで検討するのではなく、ＩＣＴ部門と他の業務部門との間で相互の協力体制を構築し、重要資源を相手先でも保管する工夫が必要である。

（４）電力

電力供給は電力会社によるところが大きく、地方公共団体による対策で供給事業者による復旧時間の短縮を実現することは難しい。目標復旧時間の短い情報システムや必要となる端末を維持するに足りるだけの非常用電源装置を用意することが強く推奨される。なお、非常用電源装置の不具合などの場合、電源車による供給を受ける手段もあるが、その場合には供給電源を受ける設備が必要であるので、必要な検討を行うことも推奨される。

（５）通信の途絶リスク

発災後 1 日以内程度で外部事業者等と連絡を取らなければならない依存関係がある場合には、固定電話や携帯電話に代わる通信手段を必ず用意する。衛星電話や災害時優先電話等非常用通信手段がこれに当たる。

非常用通信手段をＩＣＴ部門単独で用意することは費用面などから難しいのであれば、防災部門等と協力して、役所として準備しているものをＩＣＴ部門に割り当てる、あるいは、役所として整備あるいは増設することを検討する。ＩＣＴ部門が自由に使用できない状況であれば、必要な場合に使用できないことのないように事前に使用ルールについて協議が必要である。

連絡先も同じ地域内におり、先方からの発信に輻輳の影響を受ける場合には、相手方の対策も検討する必要がある。まずは関係事業者に対して、非常時の連絡手段について、その対策及び考え方を確認し、問題がある場合は改善を求めていく必要がある。

東日本大震災等、最近の震災のケースでは、比較的インターネットがつながりやすかったことから、インターネットを活用したコミュニケーションツールの活用も考えられる。

ステップ１４：外部事業者との契約の見直し

【基本的な考え方】
　これまでのステップでも、非常時における外部事業者との協力関係の見直しを検討してきた。本ステップでは、外部事業者との協力関係を再度見直し、最終的には契約内容の見直しを検討する。

【必要性】
　外部事業者の常駐要員が、被災、交通の途絶等により早急には参集できない事態や、復旧担当技術者の確保をめぐり同時に被災した他の顧客と競合し対応不能となる事態も考えられる。災害時における要員の参集を外部事業者が保証し、また復旧担当技術者の確実な対応や災害時におけるクラウド等外部サービスの一定の SLA の保証を契約事項とすれば、災害・事故対応力は向上する。ただし、契約事項の見直しには多くの費用がかかる可能性があるため、多大な費用がかかるのであれば首長等まで含めた検討体制を構築する第３部で検討することとし、この段階では可能な範囲内の対策を行う。情報システムの運用を外部事業者に依存していない場合（パターンＥ、Ｆ）では本ステップの検討は省略する。

手順１	必要不可欠な外部事業者の把握

　必要不可欠な外部事業者としては、機器担当者が参集できないあるいは代替要員が派遣されないと著しく早期復旧等に支障をきたす情報システムを担当している事業者やクラウド等外部サービス提供事業者が該当すると考えられる。特に、重要情報システムの中で目標復旧時間が短い情報通信機器の修理、点検等を担当する事業者や外部サービスは必要不可欠な外部事業者と言える。
　必要不可欠な外部事業者の範囲の設定については各地方公共団体の判断となるが、目安としては、大地震の場合でも１週間を経過すれば、ほとんどの地域で外部事業者とも自由に連絡することができると考えられるため、ステップ１１で検討した重要情報システムの目標復旧時間から考慮して、１週間以内に対応作業を実施してもらうことが必要不可欠な外部事業者に限定してよいと言える。

　必要不可欠な外部事業者を整理した後、改めてステップ２の手順３を確認して、委託先との災害・事故時の協力状況について把握する。

手順２	緊急時対応計画策定の要求

　ステップ６において行動計画を外部事業者と一緒に検討せず、あるいはステップ１３で必要と判明した外部事業者の対応についてまだ実施されていない場合など、外部事業者の緊急時の対応計画が未定の場合は、本ステップで改めて主要な外部事業者に対して、外部事業者における緊急時対応計画の策定や担当者の連絡先の通知等を要求する。

手順３	契約内容の見直し

　情報システムに関する外部事業者への依存度の高低に関わらず、情報システム停止による業務停滞の責任は、地域の住民・企業や地域社会に対しては地方公共団体が負うことになるため、最終的な対策としては、外部事業者との契約事項の一つとして災害・事故時の対応

を義務付けることが考えられる。
　なお、災害・事故時に外部事業者が必要な要員の参集を保証し、また復旧担当技術者の確実な対応を保証し、あるいは、災害時におけるクラウド等外部サービスの一定の SLA を保証することを契約事項として盛り込むことについては、本来は、事業者の保守サービスの一つとして提供されていてもよいと考えられるが、現状ではこのようなサービスを提供している事業者はほとんどない。このため、これを契約事項とするためには、基本的には契約金額の追加負担は避けられないものと考えるべきである。また、中期的な視点で見れば、地元の事業者の保守サービスの対応能力が増強されることにつながる。

　外部事業者との契約については、ＩＣＴ部門の予算内で判断できる可能性もあるため第２部で説明しているが、契約金額の追加負担が多大なものとなる場合は、第３部において首長を含んだ体制の中で検討すべきものとなろう。このように契約上の対応を先送りとした場合においても、外部事業者とは常に情報交換を密にして、必要な要員の参集及び派遣優先度の向上の働きかけや災害時におけるサービス提供維持の取組推進等をすることを推奨する。

《クラウドサービス活用の場合の留意点》
　クラウドなど外部サービスを利用する場合は、外部サービス事業者のサービス提供環境も考慮し、システムの重要度に応じて、以下の内容を契約事項として確認しておくことが望ましい。
・情報システムへの被害が極小化される堅牢なデータセンターを利用している（情報システムのハードウェアの設置場所に耐震措置や免震措置、火災・水害対策、停電対策を実施することで、損壊する可能性を低減させている）
・第三者によるセキュリティ評価を受けている
・SLA の内容が明確であり、自治体の運用に耐えうる仕様になっている
・地理的距離が十分に離れた場所にデータのバックアップを保存している。また、復元が自動で実施される仕様となっている
・システムの運用において、適正な取扱いが行われていることを定期的に委託先より報告を受け、確認できる
・危機的事象発生時における委託先の支援・協力体制及び、外部サービス提供事業者との（「SaaS」「PaaS」「IaaS」等のクラウドサービスの仕組みに応じた）責任分界点が明確化になっている）

ステップ１５：代替・復旧行動計画の立案

【基本的な考え方】
　これまでの検討結果をもとに、ステップ６で検討した初動フェーズの行動計画を修正するとともに、復旧フェーズ及び復帰フェーズにおける災害時対応業務や平常時業務の代替・復旧のための行動項目を整理する。誰が、いつ、何に基づいて、どう行動するのかを記述し、関係者間で合意を得る。
（１）初動フェーズ：緊急事態発生の確認・連絡、被害拡大の防止、安否確認、被害情報の収集と被害評価の実施等
（２）復旧フェーズ：重要業務の仮復旧
（３）復帰フェーズ：本番環境への復帰

【必要性】
　ステップ６の初動フェーズと同様に、復旧フェーズ及び復帰フェーズに関する具体的な行動手順を決めておかなければ災害・事故時の対応が遅れ、被災地域住民への対応や企業の復旧の遅れを招くこととなる。具体的な行動手順を明確にし、以後は、訓練もこれにしたがって行い、その有効性を確認していくことも必要である。

【アウトプット】
１．緊急時対応体制（検討結果により様式０７を適宜修正する）
２．代替・復旧行動計画（検討結果により様式９を適宜修正する）
３．被害チェックシート詳細版（様式１８）
４．参照文書一覧（様式１９）

手順１	既存の防災計画等との整合

　業務継続計画における災害・事故時の行動計画と、既存の防災計画や緊急時の行動規定等とを比較し、追加すべき内容は追加していく。既に詳細な緊急時の行動規定がある場合には、その内容をよく確認し、必要があれば修正することになるが、多くの場合、地方公共団体自らの設備・施設、要員等の資源には深刻な被害がないことを前提に既存の計画は策定されているので、自らの資源に相当の被害が発生していることを前提にした行動計画を追加することになるものと考えられる。

（１）行動開始基準について
　ステップ６で定めたＩＣＴ部門としての行動開始基準は、既存の緊急時の行動規定等と整合的なもので十分であるならば、それが望ましい。しかし、不十分な場合も多いと考えられる。その場合には、防災・危機管理部門と調整して、ステップ６で定めた行動開始基準に合うようにＩＣＴ部門の行動開始基準を追加していくことも必要である。

（２）対応者の検討
　既存の防災計画等において、重要情報システムの復旧に必要不可欠な要員が地区防災拠点応援要員や広域避難場所従事要員等に指名されている場合、これらの担当から外すなどの調整を行うことが必要である。特に、短期間で復旧しなければならない情報システムに関しては、その復旧作業に必要不可欠な要員が欠けることは極力避けるように対処すべきである。
　直ちに調整が出来ない場合でも、要検討課題として整理しておき、次年度以降に必ず調整を行う。

また、ＩＣＴ部門長が災害対策本部の要員となっている可能性がある。この場合、ＩＣＴ部門長が現場にいない時間が多いことも想定されるため、現場の指揮をするための代理要員の指名が特に重要となる。

手順２	ＩＣＴ部門内のチーム編成

重要情報システムを早急に復旧させるために、災害・事故時において重要情報システムの復旧活動を実施するチームを編成し、その役割を明確にする。

職員だけではなく外部事業者の要員等も含めて、重要情報システムを継続・復旧させるために必要な体制を構築することが必要である。外部事業者についても、職員と同様に緊急時に参集するようにあらかじめ定めておく。自動的な参集を求められない場合でも、緊急時に連絡するための連絡手段（できれば担当者個人の携帯電話や携帯メールアドレスも含む。）を把握することとすべきである。

チーム編成は必要とするスキル単位に分けることが必要である。例えばホスト系システム[15]とオープン系システム[16]をどちらも保持している場合は、それぞれ異なるスキルを必要とされる。ネットワークの復旧についても、情報システムの復旧とは異なるスキルが必要である。ホスト系システム復旧チーム、オープン系システム復旧チーム、ネットワーク復旧チームというように、スキル単位でチーム編成を行う。また、クラウド等外部サービスの提供維持の状況確認を主に行う要員をチーム編成することも考えられる。

チームごとに２名以上（できれば３名）を割り当て、代理要員が確保できる体制を構築することが重要である。チーム編成に当たって、以下の項目を検討する。

（１） 要員のスキル

現時点で特定の要員にしか実施できない作業がある場合は、平常時からなるべく作業を交替してもできるように訓練して、複数の要員で対応できるようにすることが必要である。

（２）参集可能性

要員の居住地を調査して、道路の途絶や公共交通機関等の停止を想定した上で、徒歩で参集できる可能性がある要員を最低１名選定する必要性が高い。

ただし、細かくチーム編成しすぎても組織として成立しない。各チームに複数名を割り当てても兼務が生じないくらいのチーム数とすることが望ましい。スキルから考えて必要な作業を完全には対応できない要員が割り当てられることになった場合には、その作業をある程度対応できるように訓練する必要がある。

（３）テレワークの実施

現場における作業を実施することが困難な場合は、リモートアクセス環境から作業を実施することも考えられ、行動開始基準と同様にテレワーク実施基準を定めておくことも考えられる。

[15]特定のメーカーの製品のみを組み合わせて構築されたコンピュータシステム。
[16]メーカー固有の仕様ではなく、様々なメーカーのソフトウェアやハードウェアを組み合わせて構築された情報システム。主に Windows や UNIX で構成された情報システムを指す。

手順３	被害チェックリストの作成

混乱状態の中で情報システムの状況把握に漏れがないようにするためには、被害チェックリストを作成し、これに基づいて情報収集することが望ましい。緊急時にすべての要員が参集できるとは限らないため、チェックリストは出来る限り多くの要員が状況を確認できるように、場所・確認方法等をわかりやすく記述する必要がある。

重要情報システムの被害状況及び業務継続に必要な資源に関する被害状況を、ステップ６で作成した簡易的なチェックシートに追記して、より精緻にチェックが可能なリストを作成する。チェックリストは全体的な事項、庁舎別に調査する事項、システム別に調査する事項等がある。ＩＣＴ部門が実際に調査する事項ではなくても、被害状況を確認すべき内容は、チェックリストとして整理することが必要である。

以下に調査事項の具体例を記載する。

（１）全体的事項
- 要員の安否
- 公共インフラサービス～電気・ガス・水道の供給状態、周辺道路・鉄道の被害、電話やＦＡＸ等の通話状態等（情報システムの稼動に必要な事項や要員の参集に関わる事項について調べる）

（２）庁舎（フロア）、データセンター別に調査すべき事項
- 入室可否（庁舎内で業務遂行可能か否か）
- 電源設備の状況～停電していないか。配電盤、ブレーカーの稼動状態に問題はないか UPS 装置の損害・故障はないか
- 空調設備の状況～冷却水の温度、圧力に異常はないか。空調システムの明確な物理的損害はないか。漏水していないか

（３）ネットワークの被害

ネットワークの稼動状況を調査すべき庁舎・主要拠点をあらかじめ列挙しておき、ＩＰアドレスを記述する。初動の時点では ping コマンドでの導通確認をして、異常がある拠点についてネットワーク機器や断線等の原因を調査する。

（４）情報システム別に調査すべき事項
- 機器が転倒、フリースペースの陥没により落下していないか
- 機器が大きく位置ずれしていないか
- 外観からわかる破損がないか
- 異常ランプが点灯していないか
- 水没や消火時の放水等による水濡れ被害、出火、発煙、塵等による汚染、異臭がないか
- （水冷式の機器の場合）機器から漏水していないか
- 電源が入っているか否か。
- 当該機器で提供するサービスが正常稼動しているか

（５）クラウド等外部サービス別に調査すべき事項　・サービス提供への影響はないか
- 被害を受けている資源はないか、被害を受けている場合、復旧の見込みはあるか
- サービスを停止している場合の復旧の見込みはいつか

手順４	復旧フェーズでの行動手順の検討

ステップ６では、初動行動計画として安否確認や庁舎への参集に関する行動計画をまとめたが、本ステップでは参集後の情報システムの復旧に関する行動計画をまとめる。

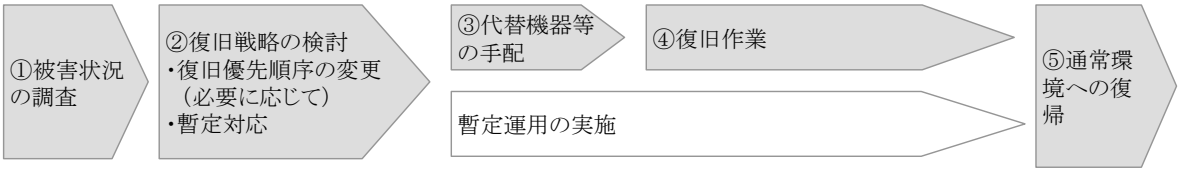
初動の段階では、あらかじめ定められた手順や行動基準どおりに機械的に行動することが多い。しかし、被災状況が明らかになるにしたがって、あまり想定していなかった事態も確認され、どのような行動や資源配分を行うべきか責任者が戦略的に判断しなければならないケースが増える。このため、以下のように様々なケースを想定して、適切な対応方法を検討することが必要である。例えば、手作業により代替的に業務を遂行するなど、実情に合わせて計画を作成する。

また、庁舎以外に情報通信機器を設置している場合（パターンC、D）には、情報通信機器を設置している建物が被災した場合と、庁舎が被災した場合の両方について代替・復旧行動を検討する必要がある。

【あらかじめ対応方法を考えておくべき状況の例】
- 庁舎が倒壊するなど使用できなくなった場合、庁舎に当面立ち入れない場合
- 情報システムの停止が長期間に及ぶ場合
- 電力供給が途絶した場合
- 輻輳により通信手段が使用できない場合
- 必要な職員や事業者の要員が参集できない場合

一般的には以下の復旧プロセスとなる。

【図３－１５－１】業務復旧プロセス



復旧手順は以下の点に留意して検討する。

（１）暫定運用による業務遂行

情報システムが停止しても手作業により当分の間対応が可能であり、かつその必要がある重要業務については、ＩＣＴ部門が情報システムの復旧に要する時間を早急に調査して、手作業による暫定的な業務を開始するかどうかの判断材料として各業務部門の責任者に知らせなければならない。そのためには、どのような行動をすべきなのか整理する。

手作業により業務を遂行する場合には、情報システム停止中の暫定的な業務遂行の内容をパソコンや紙に記録しておき、情報システム復旧時にその内容を反映しなければならないことを各業務部門に徹底する必要があり、業務継続計画書に明記する必要がある。また、復旧後の反映方法も検討して、それがやりやすいように暫定的な記録の方法を定める必要がある。

（２）データ保管事業者との連絡方法

バックアップ媒体をデータ保管事業者に預けている場合には、保管事業者への連絡方法を確実にする必要がある。また、保管事業者との連絡には暗証番号が必要となることがあるため、平常時にデータ保管事業者との連絡を担当していない要員でも緊急時に連絡でき

るよう備えておく必要がある（金庫等にデータ保管事業者との連絡手順を別途保管するのがよい）。その際、セキュリティに注意を払うことは重要である。

（３）関係者への連絡

情報システムが停止した際に、各業務部門などの関係者に対して情報システムが停止したことの連絡（暫定運用の開始の判断の材料として）、情報システムの被害調査結果の連絡、復旧完了の際の連絡などは、ＩＣＴ部門が責任をもって遅滞なく行わなければならない。このため、各業務部門との連絡役を指名し、連絡を徹底することを業務継続計画書に明記する。

（４）セキュリティポリシーとのバランス

災害・事故時においても、既存の情報セキュリティポリシーに則り情報を取扱うことは前提であるものの、特に人命に関する情報システムの維持・早期復旧のためには、一時的にセキュリティレベルを緩和することも必要である。その際は、緩和条件に時間設定等の制限を設けること、その間は、緩和によるリスクが伴う状況であることを関係者に周知徹底しておくこと、緩和条件を元に戻す際は、漏れが無いように確認することに留意したい。ただし、以下の点については、災害・事故時においても最低限守るべき事項として考慮しなければならない。情報セキュリティマネジメントを熟知した要員を検討に参加させ、機密性とのバランスをとった情報の取扱いが必要である。

ア．管理者権限の付与

災害・事故時においては、情報システム管理者が職務遂行できずに、別の要員が代替して作業することが起こり得る。作業時のＩＤや権限の付与について、以下のことをあらかじめ考慮しておかねばならない。

(ア)誰が参集しても作業可能にするために誰でもわかるようなログインＩＤとパスワードを設定しがちだが、セキュリティの観点からは非常に問題が多い。そこで、作業を行う可能性がある要員に、あらかじめＩＤとパスワードを割り当てておくこととし、誰でもわかるような設定は回避する。

(イ)ＩＤ、パスワード、権限情報等を管理する場合は、ファイルを暗号化した上で保存することが望ましい。

イ．通常とは異なる環境での業務遂行

災害・事故時においては、通常の拠点とは異なる場所で業務を遂行する状況も考えられる。このような状況においても、盗視による情報流出や非許可者による情報持ち出し等について、通常の拠点におけるセキュリティ対策基準と極力同等に対処しなければならない。

具体的には、以下のような点に関して考慮しなければならない。

(ア)一時的な利用端末においても、通常端末と同様に、離席時のスクリーンロックやロックをかける際のパスワード設定についても規定する必要がある。特に情報システム運用で利用する端末では必ず実施しなければならない。ＩＣＴ部門は作業環境の復旧だけではなく、これらの対策方針を他の部門に対して指導することも求められる。

(イ)非許可者による情報の持ち出し等に特に注意しなければならない。情報資産の分類に関する指針と手続を明示し、機密性の高い情報資産を機密性に沿ったアクセス管理の下で利用する。

(ウ)代替施設においても、できるだけ入退室時の記録を収集することが望まれる。台帳等によって手作業で収集してもよい。

ウ．代替機器等の接続について

サーバや端末が故障して新たな機器を導入する場合や復旧作業用に外部事業者の持ち込んだ機器を緊急で接続する場合等について、不正な機器の接続の防止のため、以下の対策を実施しなくてはならない。

(ア)緊急時においても、イントラネットに接続する端末がセキュリティ要求事項を極力満たすようにしなければならない。新たな端末をイントラネットに接続することに備えて、セキュリティ要求事項を満たした端末を早急に用意できるように、セキュリティ用のアプリケーションのインストール媒体を備える、他の端末からのセキュリティ機能をコピーできる仕組みを備えるなど、事業者と協力して予め用意するべきである。

(イ)緊急時においては、不正な機器の接続防止や、その前提となるマシン室等への入退室についてはより一層配慮すべきである。可能であれば監視員を付けることも検討する。

手順５	復帰フェーズでの行動手順の検討

緊急時体制から通常体制への復帰については、ＩＣＴ部門長が判断し、対応体制の復帰計画を実行に移す。復帰フェーズでの行動手順について、以下の事項を漏れなく業務継続計画書に記載する必要がある。

（１）決定事項の連絡

緊急時体制から順次、通常体制に戻すための時期や手順を決め、関係者に連絡しなければならない。

特に、緊急措置として職務代行措置や権限者の変更があった場合には、責任者、その指揮下の要員等の関係者へ速やかに連絡する必要がある。

（２）業務継続計画の検証

災害からの復興作業で多忙ではあっても、記憶が確かなうちに速やかに業務継続計画の有効性を、実施の経験を踏まえて検証すべきことを明記する。

具体的には、業務継続計画の記述の問題点を特定することが必要である。例えば、庁舎が被災して代替拠点で情報システムを暫定的に運用した場合、代替拠点に十分な資源が用意されていたかを現場担当者に確認し、問題があった場合には物資等の確保方法の改善が提案されなければならない。

手順６	参照する文書の整理

業務継続計画書として完成させるために、業務継続計画書の本体のほかに、参照すべき文書類を整理する。詳細なコマンド（情報システムを継続・復旧させるために画面操作で入力する指示や命令文等）を記載した復旧手順書やバックアップリストア手順書は業務継続計画書の中に含めると双方が見づらくなるため、別冊にすべきと考えられる。

また、要員個人の連絡先を記載したリストについても、個人情報保護の観点から別冊として厳重保管することも多いと考えられる。

参照すべき文書類は、保管場所を明確にして整理する。参照すべき文書類が災害・事故の被害で入庁不可能になる可能性のある庁舎のみに保管されている、焼失により使用できないようなことがないように、なるべく複数の方法（例：紙で保管するほか電子データでサーバ内に保管するかクラウド等の外部サービスを利用して保管するなど）で別の場所で保管するべきである。

ステップ１６：本格的な訓練の実施

【基本的な考え方】
業務継続計画が有効に機能するためには、定期的に訓練を実施して、職員等の関係者が計画どおりに行動できるようにすることが重要である。また、訓練の実施により、計画の中で整合がとれていない箇所、非効率な行動、最新性が保たれているか、など確認することにもなる。本ステップでは、ここまでの検討結果を活かした本格的な訓練について紹介する。

【必要性】
策定した業務継続のための行動計画や事前対策が非常時に有効に機能するためには、定期的に訓練を実施して、職員等関係者が理解を深め、計画どおりに行動できるようにすることが必要不可欠である。ステップ７で実施した訓練に加えて、より高度な訓練を実施する。

【アウトプット】
１．訓練計画（様式１１に本ステップでの検討結果を追記する）

手順１	訓練計画の策定

ステップ７で定めた訓練計画に加えて、全庁を挙げて実施される訓練等と連動した計画として、再度、訓練計画を作成する。例えば、初動訓練はＩＣＴ部門単独でも実施可能であるが、既存の災害時の行動計画がある場合は、他の部門と一緒に訓練を実施することでより大きな効果を期待できる。全庁を挙げた災害対策本部の設置や参集、安否確認に関する訓練が実施される場合、これと連動して重要情報システムの業務継続の訓練計画を策定する。

また、災害対応力をより向上させるために、訓練に慣れてきたら、以下のような訓練を実施していくことも検討する。

（１）平常時の要員（すなわち主たる作業予定者）以外による情報システム復旧訓練

（２）抜き打ちによる訓練

訓練の参加者に対して訓練日時を事前に通知せずに突然実施することで、災害対応力をより強化することを目的とする。

抜き打ちによる訓練の一案として、行動開始基準を一時的に低く設定して、小さい規模の災害の場合でも大地震の場合と同様に初動訓練をするように通知することも考えられる。例えば、同地域で震度４以上が発生した場合に震度６弱以上の行動計画と同様に行動することをあらかじめ通知することで、実際に震度４の地震が発生した場合には、あらゆる要員にとって完全に抜き打ちでの訓練とすることができる。

手順２	訓練の実施

これまでの策定作業により、災害・事故等での被害のイメージが固まり、また業務部門や外部事業者との協力関係が構築されていると考えられる。それを活かした本格的な訓練は以下のとおりである（業務継続計画における訓練の全体像は表 3-16-２を参照）。本格的な訓練を実施するには準備がかなり必要で、慣れない場合は戸惑うことが多いが、効果は大きい。代表的な訓練を自ら実施する場合の準備事項を以下で説明する。

（1）シナリオ提示型の机上訓練

ステップ6、１５で緊急時対応要員とした要員が全員参加し、行動計画をまとめた文書を読み合わせて、各要員が緊急時にすべき行動を確認する。本ステップではステップ7で紹介した内容に加え、リソースや公共インフラ等が一定期間使用できなくなるといった状況の前提条件（シナリオ）を提示し、参加者で計画書を読み合わせ、提示された制約のある状況下でも代替手段等で計画どおりに業務継続の活動が可能かどうかを検証する。例えば、ある役割を任された要員が参集できないといった前提条件が提示されたら、他の要員が代替してその役割を果たすことによって支障なく初動行動等が実施されるかどうか、代替要員のスキルの不足から実施が難しい行動がないか、などを確認する。

また、ステップ９で決定した各業務部門の代表者の参加も検討すべきである。

シナリオ（リソースや公共インフラの被害状況）は、ステップ１０で検討した内容（様式１４「被害想定整理」を参照）を使用する。具体的には、以下に挙げた項目について災害・事故発生後の時間ごとの前提条件を提示する（例：固定電話は２日間使用できない）。細かく考えすぎず、数時間～数日単位で区切る。

- 要員の参集～職員、外部事業者
- 庁舎の利用可能性
- 情報通信機器の損害の種類と程度
- 通信の利用可能性～固定電話、携帯電話、携帯電話のメール、電子メール
- ライフラインの使用可能性～電気、ガス、水道、下水道(トイレ)
- 交通インフラの使用可能性～道路、電車

（2）計画発動時の行動訓練・演習

(1)の机上とは異なり、できるだけ災害対策本部や復旧作業の拠点として使用する予定の場所で実施する。夜間・休日に被災したことを想定する場合（ほとんどの職員が職場以外にいる状況）や遠隔地の外部事業者等が同じ会場で参加する場合には、なるべく災害・事故時と同様の環境を設定する必要があることから、直接コミュニケーションを取ることのない要員間の接触を避けるよう仕切り等を用いるなど、部屋の配置を工夫する。

前提となる被害状況や制約条件を適時に映し出すために、モニターを用意する。

訓練参加者とは別に、進行役として以下の役割が必要である。ただし人数が不足する場合には、記録係は省略してもよい。

【表３－１６－１】行動訓練における役割分担

進行係	１名	司会進行、タイムキーパーを担う。訓練状況が停滞している場合には、必要に応じて手助けをするなど、訓練の進行を管理する。
コントローラ	２名程度	各業務部門や出先機関、事業者、住民等その場にいない役割の代行、公共インフラや道路状況等の社会状況全般についての情報提供などを行う。
記録係	数名	進行状況、問題点、気づいた点等の記録を行う（必須ではないが、第三者として気づいたことを記録することは有効である）。

訓練の事務局は事前に以下の用意する必要がある。

ア．前提条件（シナリオ）の作成
前提条件については、(1)の机上訓練のシナリオと同様の内容について検討する。

イ．追加要素
訓練に慣れてきたら、業務継続力をより向上させるために、理解度に応じて予期しない追加要素を準備しておき、訓練の場で制約条件として付加するべきである。ただし、初回の訓練では参加者に業務継続計画の内容を理解させることが重要なので、あまり複雑な要素は追加しない方がよい。
多くの要員に困難な状況をインプットし過ぎると誰も動けず訓練として機能しない可能性もあるが、障害が少なすぎても訓練としての意味が乏しい。訓練の目的により、適切な難易度となるように調節する。

・ 個人ごとの前提条件
出張や怪我により庁舎に参集できないなど、個人や部門ごとに災害時の居場所や状況等、異なった条件を設定する。復旧活動が特定の要員に頼った状況になりがちな場合、特定の要員が復旧活動に参加できない状況を設定して、残った要員で復旧活動をするなどそれぞれの特性によって条件を設定する。

・ 想定外情報
訓練の進捗状況により、参加者に事前に知らせていない条件を訓練の場で新たに追加する。地震を前提としている場合は余震が発生したことにして新たな対応をさせることや、職員からの出勤不可の連絡や住民からの被害問い合わせ等があったことを想定して適切な対応をする等が考えられる。

（３）重要情報システム復旧訓練
情報システムの早急な復旧のためには、バックアップ媒体からのリストアが本当にできるか、準備している代替機が予定どおりに稼動するのかなど、日頃から復旧作業を実践して訓練することが必要である。
なるべく多くの要員が対応できるようにするために、ＩＣＴ部門の要員は訓練に全員参加することが望ましい。また、実際に情報システムやバックアップ媒体を動作させるため、関係事業者の立会いも必要となる。
なお、訓練の内容によっては、通常時使用している情報システムを停止する必要があるため、休日等の業務停止時を利用して実施する。この場合、訓練実施中に情報システムの利用ができないことを予め通知することが必要である。

復旧訓練の準備事項として、以下の事項を事前に準備する。

ア．被害状況の想定
訓練の実施内容と範囲を決めるために、どのような状況を想定するかを大まかに決めておく。計画発動時の行動訓練・演習における前提条件（シナリオ）は精緻に決めておかなくともよいが、下記の例の程度のことは考えておく。
例）
- 広域災害により情報システムを運用している庁舎が倒壊した
- 広域災害により広域通信網（広域ＬＡＮ等）が寸断され、復旧の目処が立たない
- ミラーリングされたデータベースサーバが両系とも損傷し、復旧の目処が全く立たない
- 電力が停止している
- 固定電話、携帯電話が使用できない

イ．作業内容チェックリストの作成

訓練の目的が予定している復旧プロセスの遂行の確認であることから、実施すべき復旧プロセスを細かく業務継続計画かその下位の文書として定めておくことが必要である。また、訓練用のデータの消し忘れがないように、復旧訓練における手順だけではなく、データの削除等最終的な訓練完了までの手順を記述する。

表 3-16-2 の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）を参考に訓練内容のチェックリストとチェックの担当者を決めておく。作業に要する想定時間をあらかじめ記述することで、想定と実際の作業時間の差が明らかになり、問題点の抽出につなげることが可能である。

手順３	訓練を通した業務継続計画の課題の洗い出し・解決

訓練の実施に際しては、策定した業務継続計画に内在する課題の洗い出し及びその解決のため、計画どおりに業務継続のための作業が行われているか記録した上で、訓練後に分析を行い課題の洗い出しを行う。

課題の解決策には大きく分けて、行動計画を修正すればよいもの、何らかの投資を計画して事前対策を行うべきもの、早急には対応できず要検討課題となるものがある。早期に解決できる課題については速やかに解決することが望ましい。

【表 3-16-2】業務継続計画における訓練全体像

訓練の種類	参加要員	方法
机上訓練	緊急時対応要員	参加要員間で計画書を読み合わせ、各要員が緊急時にとるべき行動を確認する。 代替要員のスキル等から実施が難しい行動がないか確認する。
連絡、安否確認訓練	緊急時対応要員	固定電話、携帯電話を使用せずに緊急連絡及び安否確認を実施する。
災害時用の情報システムや装置の使用訓練	ＩＣＴ部門要員	安否確認システムや非常用電源、非常用通信装置等平常時は使用しない装置や情報システムの使用訓練を実施する。
シナリオ提示型の机上訓練	緊急時対応要員	リソースや公共インフラ等が一定期間使用できなくなる状況を想定する。参加要員間で計画書を読み合わせて、想定する制約がある状況下でも代替手段等により計画どおりに復旧作業が可能か否かを検証する。
初動訓練（ＩＣＴ部門の参集、連絡、安否確認等）	緊急時対応要員	リソースや公共インフラ等が一定期間使用できなくなる状況を想定する。シナリオの状況下で、参加要員が計画どおりに初動行動全般を実践する。
バックアップデータのリカバリ等の情報システム復旧／切り替え訓練	ＩＣＴ部門要員、事業者	情報システム停止時を想定して、復旧作業（代替システムを持つ場合は切り替え）の実地作業を実施する。

※緊急時対応要員とした訓練については、複数部門の一括開催が望ましいがＩＣＴ部門単独での開催も可能である。

【表 3-16-3】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を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を確かめる)		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けるようにする。

《クラウドサービス活用の場合の留意点》
地方公共団体における情報システムのクラウド依存が高い場合は、情報システムの復旧や運用継続は外部事業者の取組に影響されるため、地方公共団体の情報システムの運用継続方針について委託先と共有し、危機的事象発生時の対応について協議をしておくことが重要である。共同訓練を通じて、情報システムの運用継続の実効性について確認し、不足事項があればSLA の見直しや契約事項について見直しを検討する。

■第２部のまとめ

この段階までの検討と策定作業を着実に進めたのであれば、地方公共団体のＩＣＴ部門として最低限継続しなければならない業務が把握され、どのように災害・事故に備えるかといった対応の考え方が定着し、災害・事故にあった場合に重要業務が継続できる可能性が相当程度高まったと言える。

また、第１部のまとめでも述べたが、策定成果の更新と訓練が重要であることを強調したい。策定した成果を放置すれば内容はすぐに古くなり、万一の場合に役に立ちにくくなってしまう。平常時の維持・点検といった管理が定着しているかを見極め、また実際に訓練を行い、本当に機能するものかどうか確認することが重要である。

（１）検討結果の首長等や関係部局への説明や開示について
ここまでの検討によって達成したＩＣＴ部門の業務継続能力、復旧対策レベルを首長等や他の関係部門に積極的に説明していくことが必要である。ＩＣＴ部門の業務継続に関する考え方を鮮明にし、他の部門からの協力・理解を得るために、以下の事項については簡単に説明をするべきである。また、他部局からの要請や未調整事項の課題が発見される可能性もある。

- 業務継続計画の前提条件とした事象(災害・事故の種類、程度など)
- ＩＣＴ部門としての業務継続のための行動開始基準
- どのような状況・被害になると情報システムが使用できなくなるかの条件の概要
- 情報システム停止時に各業務部門が暫定対応を行う際、復旧に備えた要請の内容
- 実施済み、実施予定の対策

業務継続の取組の概要を議会や住民に公表するか否かについても考える必要がある。第１部のまとめでも述べたとおり、公表する場合は、その範囲を精査することが必要である。

（２）更新、維持・点検に関して
第３部の検討に入る前に、ここまでの検討内容を再度確認する必要がある。また、第２部での検討によって第１部での検討結果を修正する必要性が多いのは前述のとおりである。第１部での検討結果まで含めて検討結果を更新、維持・点検などの管理をしていくよう、着実な対応を進めていくべきである。

（３）定期見直し事項の拡充
また、第２部まで検討を進めたことによって、ステップ８で例示した年次で見直すべき項目について、以下の項目を追加しなければならない。見直し内容をチェックリスト化している場合は追記をする必要がある。

- 既に策定した業務継続計画で想定した事象とは異なる事象を前提とした計画を検討する必要性の確認
- ＩＣＴ部門以外で管理する情報システムなど、現状の業務継続計画で対象外とした情報システムがある場合、対象を広げる必要性の検討

（必要があれば、検討スケジュールを立案し、策定状況を継続的に管理する。）

- 外部環境の変化等による重要業務の変更の有無、重要業務の変更や情報システムの変更等による選定した重要情報システムの変更の有無、それらの目標復旧時間、目標復旧レベルの変更の有無

第３部：本格的なＢＣＰの策定と全庁的な対応との連動

ステップ１７：ＩＣＴ部門のＢＣＰ投資判断のための体制構築

【基本的な考え方】
　多額の投資判断等を含んだ本格的なＢＣＰを策定するに当たって、首長等を含んだ全庁的な検討体制を構築する。

【必要性】
　第３部では多額の投資判断を要する課題を扱うため、首長等を含んだ全庁的な検討体制が不可欠である。

手順１	首長等への報告とその参画

今後の検討については、首長自らが関与することが望ましい。首長に次ぐ立場の者の参画は不可欠である。首長等にこれまでの検討結果を報告して承認を得るとともに、今後の検討への参画を要請する。

手順２	業務部門長の参画

全庁的な検討体制への参画を要請すべき各業務部門や財政、人事、企画等の横断的な部門の長に対して、ＩＣＴ部門としてこれまでの業務継続計画の検討結果を説明する。
なお、情報セキュリティ委員会がある場合には、必要となる部門の長が参画することが多いと考えられることから、これを利用して(あるいは一部拡充して)連携して検討するのも一案である。

ここでの投資判断は、全庁的に見て高い優先順位の投資であるとのコンセンサスが得られなければ実現できないものであることを十分に認識して、全庁的な会議等を設定することが必要である。

全庁的な体制が整ったら、必要に応じて幹事会や実務レベルの会合も設定する。また、それら体制・会合の事務局におけるＩＣＴ部門の役割についても明確にする。ＩＣＴ部門がある程度先導できる体制が必要であるが、一方で、投資判断や人員・組織の充実などが必要となること、防災・危機管理の対策でもあることを踏まえ、それらに深く関係する部局との連携に十分な配慮をしていくことになるであろう。

ステップ１８：目標復旧時間・目標復旧レベルの精査

【基本的な考え方】
第２部までで検討した計画に盛り込んだ対策で本当に地方公共団体としての責任を果たすことができるかという全庁的な視点から、選定した重要業務及び重要情報システムに係る目標復旧時間・目標復旧レベルを精査する。

【必要性】
目標復旧時間を達成するためには、多大な投資や相当な準備・手間を要する施策の実施が避けられないこともある。また、復旧が必要な時点での業務実施の水準が１００%必要でなければ、投資や手間をその分、抑えることが可能になるはずである。この段階での投資等の多大な支出や労力を要する対策の実施判断に当たって、第２部での比較的簡易な分析だけでは不十分であるため、以降のステップを検討する前には必ず実施しなければならない。

【アウトプット】
１．重要業務、重要情報システムの目標復旧時間・目標復旧レベルの精査結果（様式１５．１６を変更する）

手順１	重要業務及び重要情報システムの見直し

ステップ１７で構築した首長等を含んだ全庁的な検討体制の中で、第２部で選定した重要業務及び重要情報システムが、地方公共団体の業務継続の面で重要であるか、さらに重要なものはないかについて確認する。

手順２	前提事象の再検証

これまで業務継続計画の前提としてきた事象よりも大きな被害が発生し、対応がより困難となる事象(その発生確率はより低いのが通例であることに留意)についても重要業務及び重要情報システムを継続させられるように、対策を実施しなければならないかを検証する。具体的には、例えば、震度７でも継続させる高度な対策レベルとするのか、震度６強でも継続させるレベルとするのか、震度６弱程度であれば継続させるレベルにとどめてよいのかを判断する。これは、重要情報システムの全体について一律に判断するという観点だけでなく、情報システムごとに別々に判断するという観点を含むものである。

もちろん、すべての重要情報システムに震度７でも継続できる高度な対策を実施できることが理想的であるが、被害が重大となる事象に対応するための費用は格段に大きくなるのが通常であることから、絞り込んでメリハリをつけた対策とせざるを得ないのが現実であろう。

その上で、第２部までに事前対策の計画に盛り込んだ対策のすべてが実施済みとなった場合に、ここで再検討して前提として定めた災害・事故の事象への対策として必要なレベルに到達できるのかを確認する。例えば、震度７でも継続しなければならないと判断した重要業務、重要情報システムについて、第２部検討時点における対策内容において震度６強までの対策しか実施していなかった場合には、ステップ１９において、震度７の場合にも継続させられるだけの追加対策を考えなければならない。

一方、第 2 部までの検討では要検討課題として対策案が暫定的に記述されているものについて、この段階でそこまでの対策は必要ないといった検討結果になる場合もあるので、留意が必要である。

手順３	復旧見込み時間の見積もり

災害時において、どの程度の期間重要業務の停止を許容できるのか(許容中断時間と呼ばれることもある)を再度確認し、設定した目標復旧時間内で復旧することで住民等の大きな支障が生じないか、あるいは理解を得られるかという視点から、重要業務の目標復旧時間の妥当性を確認する。

その際、特に情報システムに依存する業務については、業務の復旧が平常時の例えば何割かでも許容されるのであれば、その業務レベルも合わせて見極め、時間とレベルとの組み合わせで許容される水準を把握するのがより有効である。

次に、第２部までで検討した計画に盛り込んだ対策をすべて実施できた場合に、重要情報システムが使用可能になるまでに要する予想時間を見積もる(必要に応じて、その時間までに稼働可能となる情報システムの稼働レベルも合わせて見積もる。)。情報システムを使用する業務の停止が許容される時間と情報システムの現状での復旧見込み時間(必要に応じ手稼働のレベルを含めて)を比較して、現状の復旧見込み時間が十分に速いかどうかを分析する。問題があると判断される場合、手順２と同様に要検討課題として、ステップ１８で追加対策を考えなければならない。

この検討における復旧見込み時間とは、「現状の」復旧見込み時間ではない。投資判断を行う前提とする復旧見込み時間であるので、計画済みで実施が確実な近い将来の対策は実施済みと考える。双方を混同しないようにする十分注意する必要がある。

ここでの復旧見込み時間は以下のとおりに見積もる。

（１）検討基準時点

復旧見込み時間を算出するに当たって必要な検討基準時点を決定する。標準的には、中期的期間（数年間）で確実に実施できそうな対策（予算のめどが立っていることも条件）が実施された時点を基準として評価することが適当と考えられる。

（２）想定する被害状況

ステップ９で検討した被害想定をもとにして、対象とする情報システムやその継続運用・復旧のための作業に必要不可欠な資源がどのような被害を受けるか想定する。原則として、起こり得る一般的事象の中でより厳しい対応を迫られる条件とする。

情報通信機器についても、実際の災害によってどの程度の被害を蒙るかどうか確実にはわからない。情報通信機器の被害については、修理・調整で済む場合（３日～1 週間程度での復旧）と、機器の再調達が不可欠な場合（数カ月程度での復旧）の２段階での被害想定が必要であることが多い。例えば、震度７の地震が発生したとしても再調達が必要となる事態には陥らないほどの高度な対策をしている場合を除いて、この２段階での被害想定で分析することを推奨する。この場合、各段階のうちどちらの段階がより可能性として高いのかも十分考慮しつつ分析を進める。

（３）情報システムを復旧するまでの業務プロセスの分析

対象とする情報システムを復旧するまでに要するプロセスを整理する。情報通信機器の被害が修理・調整で済む場合と、機器の再調達が不可欠な場合では、復旧プロセスは大きくことなるため、２通りの分析を実施する。

業務プロセスの分析では、発災して庁舎に参集するところから情報システムのサービス提供が再開するところまでの作業手順を想定する。プロセスごとに必要不可欠となる資源を整理し、被害を受けると想定される資源については、代替品を確保するためのプロセスを追加する。また、全く異なる作業プロセスへの変更を要する場合には、代替業務プロセスとして位置づけて分析を行うことが必要になる。

職員だけでは作業が進められない業務プロセスも分析もある。例えば、外部から特定の機器を搬入するプロセスや、外部事業者の要員が参集するプロセスについては、それらを実施する主体に質問することにより、これらのインプットが確実に行われる時間を可能な限り把握する必要がある。

ステップ１９：投資を含む本格的な対策

【基本的な考え方】
ステップ１８で洗い出した、各重要情報システムについての復旧見込み時間（確実に実施される見込みの対策は実施済みと仮定）と、その重要情報システムの社会的に許容される停止時間の乖離を縮小する各種対策を検討し、必要な費用とそれにより達成される効果を議論して、首長等による投資判断を行う。

【必要性】
最終的には多額の投資をしてでも運用の継続、早期復旧を確保すべき情報システムが存在する。これまでの重要情報システム選定や代替手段の有無の検討結果をもとに、必要不可欠な投資に関する判断を首長等に求めることが必要不可欠である。

【アウトプット】
１．本格的な事前対策（様式０５に本ステップでの検討結果を追記する）

手順１	対策案の洗い出し

第２部までは、ＩＣＴ部門での予算内で判断できる比較的費用のかからない対策を中心に検討したが、建物の耐震補強、代替システムの確保、システム構成の変更等大規模な投資を行わなければ目標復旧時間（より厳密にいえば、その重要情報システムの社会的に許容される停止時間）を達成することが不可能なものもあると考えられる。本ステップでは、各種対策について必要な費用とそれにより達成される効果を、首長等まで含めた全庁的な議論を実施し投資判断を求める。

投資判断の際の方法論としては、本ステップの記述を参考にして、まずはＩＣＴ部門が中心となって、対策状況（既に計画済みで実施が確実な対策は実施済みと仮定する）をもとにした復旧見込み時間と社会的に許容される停止時間との乖離を埋めるための対策案を数種類列挙し、必要な費用とそれにより達成される効果を整理することが必要である。これをたたき台として全庁的な議論を行い、実施すべき対策を選択するというプロセスが有効である。

目標を高く設定し過ぎると、多額の投資判断を必要とする対策を数多く実施することとなり、結局投資自体を断念せざるを得ない事態となる可能性もある。それを防ぐためには、どのデータ、どの情報システムを守るか、早急に復旧させなければならないかを今までの検討結果をもとにして再度整理し、これらの点が不明瞭にならないように判断の根拠を明確に提示することが必要で、情報システムの復旧の優先順位も再度明確にする。災害時において制約された資源の有効利用の観点からも、すべての情報システムを一律に守るという結論になることは避けなければならない。

本ステップで検討すべき対策としては以下のものが考えられる（これまでのステップで紹介した対策もあるが、ここで総合的に判断するために再掲した）。各対策について事業者等と相談することが必要である。

（１）建物・設備の脆弱性に対する対策

地震を想定した場合、建物の耐震性が確保されているか否かで業務継続計画の内容は大きく変わる。ステップ３で調査した内容を再度確認して、昭和５６年 ６ 月以降の新耐震基準ではなく、それより前の旧耐震基準で建築確認を受けた建物を使用している場合には、耐震診断を行って危険度を把握することが必要である。耐震性に問題があると判断された場合には、職員や来訪者の安全確保の観点から耐震補強を行うことが必要であるが、情報システムが損壊して業務が長期停滞するといった観点を含めて、耐震補強に関してこの段階で正面から議論することになる。耐震補強が実施されれば、代替拠点の位置づけ、重要な情報の保管のあり方等にも変化が生じるため、業務継続計画の内容全体を根本的に見直す必要が生じるが、業務継続のための行動は非常に行いやすくなるはずである。

また水害の危険性がある場合は、情報システムの業務継続の観点からは、地下や１階に設置されている重要な機器・設備を高層階に移転することが検討対象になる。また、通常１階で行われる窓口業務を現場で支援する情報通信機器は移転が難しいため、代替機器の確保やその迅速な運用開始などの対策も検討されなければならない。

建物の脆弱性に対する対策は多大な投資を要する上、実現には数年以上を要することが多い。このような抜本的な対策実現までの間は、別の実施可能な（費用がかからない）対策を実施して、業務継続能力を高める必要がある。

（２）重要情報システムの早期復旧のための対策

重要情報システムの早期復旧のための対策としては、各重要情報システムの機能を踏まえて、外部データセンターの活用、他の地方公共団体との相互協力、冗長性の高いバックアップ方式の導入等、様々なものが考えられる。各種対策に係る費用対効果を全庁的に議論して、復旧に関する基本方針を決定する。

【案１】機器を設置する施設の堅牢化

耐震性、耐火性、耐水性等に問題がある庁舎で重要情報システムを運用している場合、優先する情報通信機器を他の堅牢な庁舎、関係団体の堅牢な施設、さらには事業者等が提供する堅牢なデータセンター等に移設することを検討する。庁舎が倒壊し、立入りができない被害となった場合でも、一般の業務は必要な要員と若干の機材さえ集まれば別の場所でも仮に運用できる可能性があるのに対し、情報通信機器に関しては機器が大規模に損壊すると少なくとも１ヶ月以上はサービス提供が停止する状況に追い込まれる。このため、情報通信機器だけでも堅牢な施設に移設することは有効な対策の一つである。

役所内でより堅牢な他の庁舎があれば、そこに情報通信機器を移設することで、データセンター等に移設するよりも低コストで対策を実施することができる。大規模なフロア配置の見直しを伴うことから全庁的な調整事項となろうが、業務継続の観点からは非常に有効な対策の一つであるため、優先して検討すべきである。

データセンターへの移設は、保管・運用コストが毎月発生するほか、データ転送に耐えられる高速ネットワーク等を必要とする。しかし、庁舎自体を堅牢化するよりも安価ですむ可能性もある。また、すべての機器を移設するのではなく、停止することが許されない情報通信機器のみを移設する等の取捨選択も可能である。ただし、重要な情報を外部に保存することとなるため、機密保持契約、情報漏洩対策等セキュリティ面での対策を実施する必要がある。

なお、例え堅牢な施設に移設したとしても、地震の二次災害を含む火災の発生、爆弾テ

口等による物理的破壊、大規模なネットワーク障害等などで業務が中断する可能性がなくなるわけではない。すなわち、施設の堅牢化だけでは、業務継続計画における対策として完全ではなく、代替施設の確保がより確実であることは理解しなければならない。

【案２】情報システム構成の変更

情報システム構成を変更することで業務継続におけるリスクを減少させることが可能な場合がある。業務継続上の必要性のみで情報システム変更を決断することは難しいかもしれないが、情報システム更新の検討時には、以下の事項について情報システム選定の判断基準に含めるべきである。

ア．代替品の再調達が不可能な情報通信機器等の更新

生産停止や保守サポート切れ等により、機器が故障した場合に代替品を再調達することができない情報通信機器やアプリケーションを使用している場合、サポート体制が整備されている他の情報通信機器やアプリケーションへの更新を検討することが必要である。ステップ１３で判断を先送りした場合は、この段階で必ず首長等を含めて検討し、必要な対策として認識することが必要である。

イ．クラウドサービスの利用

クラウドサービスの利用形態は、役所自体が被災しても、ネットワーク及び役所側の端末さえ利用可能であれば当該サービスを利用することが可能なため、業務継続に関するリスクの軽減を図ることができる。ただし、ネットワークの被災や、高度な対策が実施されているとはいえ事業者の拠点の被災のリスクがあり、また、情報セキュリティの面で追加的配慮が必要な面もあるので、これらの点も考慮する必要はある。情報システム更新の際に、業務継続性の観点を視野に入れて、クラウドサービスの利用を検討することが今後推奨される。導入の検討に当たっては、費用対効果を総合的に判断することが必要である。

【案３】情報システムの二重化による代替性確保の投資

重要情報システムについては、電力や空調設備等その稼働に必要な設備が整備されたスペース（代替拠点）を、平常時に情報システムを運用する拠点とは別に確保するとともに、同じ構成の情報システムを代替拠点にあらかじめ用意する必要性も出てくると考えられる。

このような代替拠点での運用においては、平常時の運用と同等のレベルで稼動する情報システムは必ずしも不可欠ではなく、発災後しばらくの間を乗り切るための縮退（スペックを下げたレベルで運用すること）の環境を用意するだけでもよい。情報通信機器が完全に破損し再調達する事態（庁舎内で復旧するには数ヶ月を要すると想定）において、どの程度の機能が必要となるかを考慮して代替拠点のスペックを検討するのが基本であるが、建物が堅牢であれば、情報通信機器が修繕で済むような被害における作動停止期間を想定する考え方もあろう。

また、代替拠点を設定する場合は、当該拠点で情報システムを立ち上げるために必要な要員の確保、移動手段についても考慮しておかなければならない。

ア．自らの施設を利用する場合

通常は地方公共団体が遠隔地に拠点を有する例は少ないと言えるが、地方公共団体が保有する別の拠点に予備用の情報通信機器を設置することが可能であれば、この可能性を検討する。

イ．他の地方公共団体が所有する情報システムの緊急時相互利用

他の地方公共団体とあらかじめ協定を結んでおき、緊急時に相互利用することも対策案の一つとして考えられる。すべての地方公共団体に共通的な情報システムだけでも地方公共団体間での相互利用を活用できるようになれば、各地方公共団体で固有に持つ情報システムのみを二重化等により手厚く保護することで済む。現状では、技術的要因により、異なる事業者が提供する情報システム間の代替は困難で、同じ事業者が提供する情報システムを利用する地方公共団体間でも情報システムの相互利用は難しいことが多いが、最重要の業務だけでも近隣の情報システムの利用が可能かどうか検討することが重要である。

ただし、同じ事業者を利用する地方公共団体間で協定を結ぶことによって、特定の事業者との結びつきが強くなり、システム更新時等に他の事業者へ移行したくてもできなくなる可能性があることは理解しておかなければならない。

また、ＩＣＴ部門に限定せずに全庁を挙げた検討体制において検討している場合は、例えば近隣の他の地方公共団体の庁舎において、窓口業務のみを実施できるように相互協定を結んでおくという対策案も考えられる。このような方針が立てられた場合、ＩＣＴ部門としてはスムーズに当該近隣地方公共団体でも業務が遂行できるように必要な対策を取ることが求められるであろう。

ウ．事業者等の提供する専門サービスの利用

事業者等の提供するサービスを利用し、データセンター等に予備の情報システムを準備することも対策案の一つとして考えられる。

まず、利用形態面では、情報通信機器の設置場所だけを賃借し情報通信機器そのものは地方公共団体が所有する形態と、設置場所の賃借だけではなく情報通信機器のリースまで行う形態、クラウドとしてまるごとサービス利用する形態がある。

また、情報通信機器の運用面では、予備の情報システムは動作させずに待機状態にしておき、本番の情報システムに問題が発生してから予備用情報システムを立ち上げる方式（コールドスタンバイ）と、予備用情報システムを常に動作させて本番の情報システムと同期させ、障害時に即座に切り替える方式（ホットスタンバイ）の二とおりの方式がある。コールドスタンバイはホットスタンバイに比べて費用は安いが、サービス提供の再開に要する時間は数日から１週間以上を要する。ホットスタンバイは、サービスダウンの時間を最小（数時間～数秒）にすることができるが、多額の費用が発生する。各情報システムの停止許容時間を考慮して、どの方式を選択すべきかを検討する。

なお、予備用情報システムを一つの地方公共団体が専用に準備するのではなく、同時に被害を受ける可能性が低い地域の地方公共団体間で共有する形態も考えられる。この形態では共有のため独自のカスタマイズを事前にはできないので、専用のシステムを利用するより再開に時間を要するが、費用負担を減らすことができる。今後、地方公共団体における ICT 部門の業務継続計画策定の取組が広く進めば、共有型のサービス提供は増えていくと予想されるため、現状では適したサービス提供がなくとも引き続きサービスの内容を確認していくべきである。

《クラウドサービス活用の場合の留意点》
クラウドサービス等の外部サービスの利用においては、危機的事象発生時の対応が適

正に行われていることを直接確認することが一般的に容易ではない点に注意する。また、複数の利用者が共通のクラウド基盤を利用することから、自身を含む他の利用者にも関係する情報の開示を受けることが困難である点にも注意する。

（３）重要情報の保護のための対策

重要情報の保護のためのバックアップの方式は、複数考えられる。データの重要性や必要となる時間、現在の環境、技術的制約要因、必要経費等を検討し、実現すべきバックアップ方式を決定する。

【案１】テープ等によるバックアップ

重要情報の保護については、定期的に（毎日あるいは毎週等）磁気テープ等にデータをバックアップして、遠隔地に保管することが基本な対策となる。また、アプリケーションのバックアップも遠隔地に保管するべきである。ステップ５でも検討すべきとしたが、まだ実施していない場合にはここで改めて検討する。また、紙媒体でのバックアップしかない場合、業務継続の観点で考えれば対策として著しく不十分であり、改善を考えるべきである。バックアップをするに当たっては、以下のような課題についての対策も必要である。

ア．バックアップのセキュリティ対策について

バックアップ媒体は、機器との同時被災を避けるため遠隔地に保管することが望ましいが、この場合には保管場所のセキュリティについてよく考えなければならない（【参考】バックアップにおける問題点と対策案を参照）。また、輸送時のセキュリティについても考慮する必要がある。

イ．地方公共団体間でのバックアップ媒体の相互保管について

バックアップ媒体の遠隔地保管については、事業者等が運営するデータセンターや運送事業者の倉庫に保管するサービスもあるが、保管費用がかかる。その額は保管するデータ量や保管場所との距離等により異なるが、月一回程度の運送や保管の安価なサービスもある（見積もりはサービスを提供する事業者に確認すること）。そこで、例えば数十キロ以上の遠隔地に相互協力関係を構築している地方公共団体がある場合には、相互にバックアップ媒体を保管しあうことで、事業者のサービスを利用するよりも搬送コストや保管コストを低く抑えることが可能となることもあろう。実現可能性を検討し、取り組んでいくことも一案である。保管する地方公共団体は、あまりに遠すぎると輸送コストも高くなることを考慮する必要がある。

相互保管に当たっては、バックアップ媒体が保管先で自団体のセキュリティポリシーに合致したレベルで厳重に保管されていることを定期的に確認しなければならない。逆に、自らが他の地方公共団体の媒体を保管する場合についても細心の注意を払わねばならない。

【参考】バックアップにおける問題点と対策案

バックアップに関する代表的な問題として、以下の機密性に関する問題、可用性に関する問題が挙げられる。それぞれ対策案を考えておくことが必要である。

＜機密性に関する問題＞

○バックアップ媒体の不正持ち出し

⇒バックアップデータの暗号化を実施する。

⇒保管場所への入退室について、そのデータのレベルに応じた認証を適用するとともに、ログ収集や監視カメラ等の設置をする。

⇒外部移管に対する手続きを明示する。
⇒バックアップのセキュリティ教育を定期的に実施する。

○廃棄したバックアップメディアからの情報漏えい
⇒不要なデータを識別して廃棄の可否について検討する。
⇒保有期間を定めていないデータに対しては、担当者任せとせず、管理責任者と共に保有期間を設定し、確実な廃棄ルールを確立する。

＜可用性に関する問題＞
○バックアップのリストアの所要時間
⇒定期的な訓練の実施、リストアにおける手順書の準備を行い、リストアに要する時間が長くならないように留意する。

○バックアップメディアからのリストアの失敗
・バックアップメディアが損傷していてリストアできない
⇒正副のテープをとっておく。
・メディアのドライブの読み込みが不良
⇒バックアップ訓練等に合わせて、定期的なクリーニングを実施する。
・最新版ではないバックアップ媒体を誤ってリストアする
⇒担当者を決め、メディアの世代管理を実施し、ラベルに世代情報等を記述する。
・異なるサーバで各々バックアップを取っており、バックアップソフトのバージョンが異なっていたためリストアできなかった
⇒リストアする可能性のあるサーバすべてでリストア訓練を実施するようにする。

【案２】レプリケーション（複製）

レプリケーションとは、通信回線で結んだ遠隔地に設置したストレージ（外部記憶装置）にデータのコピーを作成する仕組みである。テープバックアップと異なり直前の入力データまで保護することができる長所がある。ディスクベースでデータが保持されるため切替えれば直ちに使用可能であり、即時のサービス再開も可能である。

ただし、実用化にはデータ転送に耐えられる高速ネットワーク等を必要とし、費用負担は大きい。極めて重要度が高いと判断した情報システムに絞って導入を検討すべき方法といえる。

【参考】「非機能要求グレード（地方公共団体版）利用ガイド」[10] を活用した代替拠点の検討

「非機能要求グレード（地方公共団体版）利用ガイド」[10] において、レベルに応じた代替拠点の有り方が記載されているので参考にされたい（ガバメントクラウドにおける標準準拠システムについては、「地方公共団体情報システム非機能要件の標準【第 1.1 版】」[14] に記載）。

（４）職員による災害対応力の向上

外部事業者と協力関係を構築している場合でも、必要な要員が早急には来られない事態や同時に被災した他の地方公共団体と担当者や復旧技術者の奪い合いになる事態も考えられる。職員だけですべての復旧活動をできるようにすることが理想であるが、それは無理でも、最重要な情報システム等について、職員だけでも応急的な仮復旧が可能となっていれば災害対応力は飛躍的に向上する。また、職員で対応可能な作業でも特定の職員しか対応できないならば、他の職員でも対応可能となるように教育することも必要である。

これらの教育に関しては、ＩＣＴ部門の要員の確保や育成方針に関わるとともに、人件費や教育用の費用も必要となる。これまでのステップで費用面での問題等から検討が進んでいない場合、職員による対応をどこまで求めるのか首長等とも相談し、必要に応じて要員の確保・育成に必要な費用を予算化する。

（５）事業者との契約見直し

ステップ１４において、外部事業者に対する災害時の対応の義務付けに係る契約事項の説明をしたが、費用負担の観点から実施していない場合は、ここで実施しすることを推奨する。

ステップ２０：全庁的な点検・是正及び行動計画の見直し

【基本的な考え方】
業務継続のマネジメントサイクル（業務継続マネジメント：BCM）を定着させるために、定期的な点検及びそこで明らかになった問題の是正措置を首長等に報告し、さらに大きな改善点を洗い出して業務継続の取組全体を見直し、次年度以降の方向性を打ち出す必要がある。その際に、正しい現状認識を持ち、業務活動の変化を十分踏まえることも求められる。業務継続・復旧戦略の見直しを行った際には、行動計画も同様に見直すことが必要である。

【必要性】
災害・事故等のリスクに強くなるためには、計画の点検・是正、最高責任者による見直しを定期的に繰り返す必要がある。定期的な点検とともに必ず実施する。

【アウトプット】
１．代替・復旧行動計画　修正結果（検討結果により様式９を適宜修正する）

手順１	要検討課題の整理

首長等による見直しを行う前に、ＩＣＴ部門長が中心となって、定期的に実施している点検や訓練の実施により発見された問題点とその是正措置（容易に是正できない問題点は要検討課題として整理）、現時点での業務の継続・早期復旧を阻害し得る要検討課題、投資その他の対策実施計画の進捗状況、平常時の業務継続計画の維持・更新状況などを整理する。

手順２	首長等による見直し

業務継続計画の運用・管理の最高責任者である首長等は、策定した業務継続計画の点検と是正措置が十分に行われているかを確認し、要検討課題を認識し、業務継続の取組全体を見直し、次年度以降の方向性を打ち出していかなければならない。

（１）要検討課題の認識
現時点での業務の継続・早期復旧を阻害し得る要検討課題を把握する。首長等が課題を把握しているだけでも、把握していない場合に比べて災害が発生した場合の対応力は大きく変わる。
従来、予算や人事・組織上の都合などで対策を実施できていない課題について、改めて対策の必要性を見極め、対策が必要であると判断したものについては、予算化や人事・組織上の対処の判断をすることが求められる。

（２）環境の変化による見直し
地方公共団体を取り巻く環境は日々変化しており、それに合わせて重要業務も変化すると考えられる。首長等は、業務継続計画の全体を統括する視点で、策定時点や前回の見直しの時点からの環境の変化を踏まえて、必要があれば重要業務、目標復旧時間・目標復旧レベル、事前対策等の見直しを指示することが必要である。

（３）対象リスクの拡大
大地震を前提とした業務継続計画を策定したとすれば、火災等の二次災害や電力途絶、

交通機関停止等様々な事態にある程度対応できる計画となっているものの、それで十分ではない。

首長等には、懸念される事象の発生可能性や発生した場合の被害の甚大性などを踏まえ、必要に応じ、他のリスクを前提とした業務継続計画の検討を指示することが望まれる。

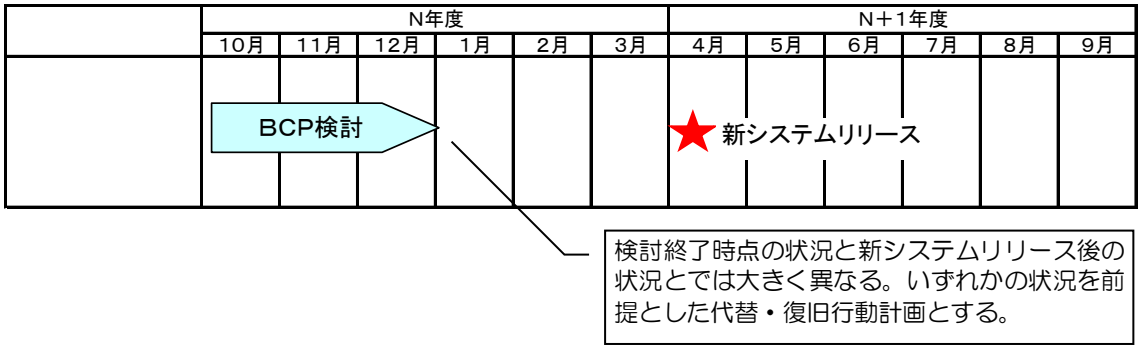
【参考】業務継続計画の点検方法について

首長を巻き込んだ点検の具体的な方法として、自己点検、内部監査、外部の専門家による第三者監査等の実施と組み合わせて実施し、結果を首長に報告することも考えられ、必要に応じて、業務継続のマネジメントサイクルに組み込んで実施することを推奨する。

手順３	本格的な事前対策の実施を踏まえた行動計画の修正

ステップ１９で多額の経費を必要とする本格的な事前対策（遠隔地運用サービスを利用した情報システム構成の変更、情報通信機器のデータセンターへの移設、代替拠点の設置、バックアップ媒体の外部保管、建物の堅牢化等）を実施した場合、実施前と実施後では災害・事故時における対応行動は大きく異なってくる。事前対策を実施した後は、実施後の状況に合うように対応行動の計画を修正する必要がある。また、事前対策実施前であっても、実施スケジュールを考慮の上、将来の状態を前提に代替・復旧行動計画の修正作業を開始するか否かを検討する。

【図３－２０－１】行動計画



将来の状態を前提に情報システムに関する対応行動計画を策定する場合は、その間に災害・事故等が発生した場合の暫定対応案も合わせて策定する必要がある。

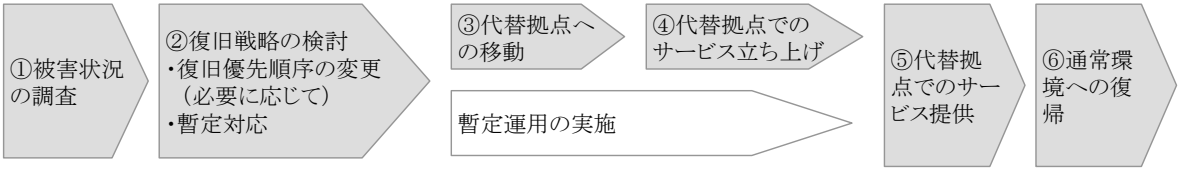
ただし、例えば３年後に完了する予定の代替拠点を存在するものとして対応行動計画を策定すると、完了するまでの間に災害・事故等が発生した場合、業務継続計画は役に立たないおそれがある。このため、前提条件の置き方については注意を要する。参考までに、前提条件の置き方を提示する。

- 事前対策実施のスケジュールが明確に決まっていない場合は、現在の状態を前提とした代替・復旧行動計画を策定する
- 事前対策実施のスケジュールが明確になっている場合、最長１年後までの状態を前提とした対応行動計画を策定する。それ以降に実施する予定ならば、年次ごとの見直しの中で、事前対策実施を前提とした対応行動計画の修正を行う

このように、対策実施前に業務継続計画の目標復旧時間等を変更し公表してはならない。行政の業務継続計画は、他の主体の事業継続の前提になる場合も多く、まだ実現できないレベルの業務継続を実現できると誤解されてはならない。その実現前に災害・事故が発生したら、取り返しがつかない。

ステップ１９で通常の情報システム運用拠点とは別に、代替拠点を設置することになった場合は、対応行動計画の大幅な修正が必要となる。

【図３－20-２】代替拠点を持つ場合の復旧プロセス



代替拠点を活用する業務継続計画では、以下の事項を決定し、対応行動計画に明記する。

（１）切替え基準

代替拠点における情報システム運用に切替えるかどうかの判断を行う者と、その判断の期限をあらかじめ決めておく。切替えの判断を行う場合、代替拠点で情報システムを立ち上げる範囲、代替拠点に移動する要員と残る要員の配分についても判断する必要があることを明記する。

切替え判断の期限については、代替拠点への移動時間と代替システム立ち上げに要する時間をあらかじめ見積もっておき、重要業務の目標復旧時間までに代替システムを稼働させるために、いつまでに判断しなければならないかを見積もっておく。

（例：移動に１２時間、機器の立上げに１２時間を要し、目標復旧時間が７２時間の場合、発災後４８時間以内に切替え判断をすることが求められる）

（２）代替拠点での機器の立上げについて

代替拠点にも、情報通信機器の立上げに必要な機材、文書などをあらかじめ用意するなど、代替拠点での立ち上げ作業が実際にできるかどうかを確認し、定期的に点検する。定期的に切替え訓練をすることが必要である。

バックアップ媒体等を代替拠点以外の場所で外部保管している場合には、本庁舎ではなく代替拠点に搬入することになる場合も多いであろう。代替拠点へのスムーズな搬入が可能であるか、契約している物流事業者との取り決め事項を確認する。

また、以下の手順書やツール等の準備が必要である。必要なものを準備し、あらかじめ保管場所を業務継続計画書に明記する。

・代替システムの構築に必要なツールや手順書
・ネットワークの切り替えに必要なツールや手順書

（３）代替拠点への要員の移動

本庁舎からの複数の移動ルートをあらかじめ調査する。特に公共交通機関が停止している状況が考えられるので、途中まで自転車や徒歩等で移動する場合のルートも考えておくことが必要である。事前に地図を余分に保持することも検討する。

（４）通常体制への復帰について

代替拠点等、通常時とは別の拠点で情報システムを運用した場合、通常拠点に運用を戻す際には情報システムを一旦停止することになるため、関係する業務部門と調整して影響の少ない時期に復帰作業を行うべきである。非常時体制から平常時体制への復帰について、その時期、考慮事項等を対応行動計画に追記する必要がある。

■第３部のまとめ

第３部まですべての検討及び策定作業を進めたことにより、首長等を含めた検討体制によってＩＣＴ部門としての業務継続計画がより本格的で精査されたものとなった。これにより、多額の経費を要する対策も含めて災害・事故に備えた対応の具体策が実施に移されていくことになり、本格的な業務継続計画を策定したということができる。一般に、行政の業務継続の内容は、他の主体の事業継続計画の前提となる場合も多いため、たとえＩＣＴ部門に特化したものであったとしても、その概要を市民に向けて公開していくべきかを検討することが望ましいであろう。また、市民の安全・安心に関わる情報であり、かつ、多大な費用を要する対策を含むものであるため、議会への概要説明も検討すべきこととなろう（公開範囲については第１部、第２部のまとめの記述と同様に、よく精査すべきである）。

第１部、第２部のまとめと同様に、策定成果の更新と訓練が重要であることを再強調したい。策定した成果を放置すれば内容はすぐに古くなり万一の場合に役に立ちにくくなってしまう。平常時の維持・点検といった管理が定着しているかを見極め、また実際に訓練を行い、本当に機能するものか確認することも重要である。さらに、対策が予定どおりに実施されているかその進捗を調査していくことも不可欠であり、構築した維持管理の体制が適切に機能するかどうかを確認することが何よりも重要である。

むすび

地方公共団体は、災害・事故時において地域住民の生命、身体の安全確保、被災者支援、経済活動復旧のために、災害応急業務、復旧業務及び平常時からの重要な継続業務を実施していく責務を負っている。これらの業務の実施・継続を確保するには、近年においては、情報システムの利用が不可欠となってきている。

そのため、本ガイドラインは、平成 20 年度の公開時点では、行政全体での業務継続計画を策定する動きがあまり進んでいない中でも、「ＩＣＴ部門における業務継続計画」を策定することを求めてきた経緯があり、ICT 部門で一定程度単独で進められる構成になっている（第 1 部の進め方等）。しかし、今日においては、行政全体での業務継続計画の取組も浸透してきており、必ずしもステップ通り進める必要性はなく、行政の業務継続計画との整合を図ることに重点を置き、必要なステップを適宜参考にして利用いただければと考える。