中央省庁における
情報システム運用継続計画
ガイドライン
～策定手引書（第２版）～

平成 24 年 5 月

内閣官房情報セキュリティセンター

改版履歴

版数	年月日	変更内容
1	平成23年3月	第1版作成
2	平成24年5月	第2版作成。優先的に取り組むべき対策一覧等を追加。

目次

1. はじめに

1.1. ガイドラインの位置づけ

1.1.1. ガイドラインの目的

本ガイドラインは、本書「策定手引書」、雛型及び雛型の別紙で構成される。本書は、中央省庁の情報システム担当者が、「情報システム運用継続計画」を策定し、計画を運用（計画の実施及び継続的維持改善）するための手引書である。

情報システム運用継続計画とは、災害・事故等の非常時に、情報システムを早期に復旧させ継続して利用するために必要な計画群の総称を指し、府省庁の業務継続計画の、情報システムの検討部分をより詳細化したものと位置づけられる。[1]

業務の情報システムへの依存度合いが急速に拡大している現状においては、首都直下型地震等の大規模地震からマルウェア感染（不正プログラム）まで多岐に渡る様々な危機的事象のうち、何らかの事象を原因として情報システムが停止した場合、重要な業務の継続に深刻な事態が発生することは否めない。また、非常時における情報システムの重要性という視点においても、メールや Web 等の情報収集・共有・伝達手段、基幹 LAN 及びこれにアクセスするための認証基盤等が利用不可能となった場合は、非常時の情報収集・共有・伝達手段が極めて限定され、初動の対応業務そのものに深刻な影響が生じることとなる。

このように、政府機関の果たすべき重要な役割（業務継続計画における非常時優先業務の実施・継続）が情報システムの停止を原因として遂行できなくなることを避けるために、必要な計画を事前に策定し、継続的に維持・改善を行い、危機的事象発生時に計画を適切に実施することは、情報システム担当者としての極めて重要な役割の一つである。

「第二次情報セキュリティ基本計画（平成 21 年 2 月 3 日情報セキュリティ政策会議決定）」における「各政府機関は保有する情報システムの災害・障害時対応の必要性・優先度について決定するとともに、必要なものについては業務継続計画を策定する。」との決定のとおり、情報システム停止に備えた必要な対策に取り組むため、本ガイドラインは、中央省庁の情報システム運用継続計画に含める事項を具体的に示し、適切な計画を整備できるようにすることを目的とする。

さらに、平成 23 年 3 月 11 日に発生した東日本大震災は、地震、津波等による大規模停電やネットワーク障害等、情報システムにも大きな影響を及ぼし、情報システムの運用継続計画の必要性が改めて認識された。本ガイドライン第 2 版では、震災の教訓から対策の有効性や留意点を取りまとめた「東日本大震災における政府機関の情報システムに対する被害状況調査及び分析（最終報告書）（平成 24 年 4 月、内閣官房情報セキュリティセンター）」で示された「優先的に取り組むべき対策一覧」を事前対策計画の検討の項目に首都直下型地震を想定した対策として追加・拡充した。今後、対策を検討するに当たっては、同最終報告書を含め、参考にされたい。

[1]本ガイドラインで策定を推奨する情報システム運用継続計画は、府省庁の業務継続計画が扱っていない情報システム特有の危機的事象（マルウェア感染や不正侵入等のネットワークを介した外部攻撃による情報システムの予期せぬ停止）への計画も含むものであり、府省庁の業務継続計画より広い範囲を対象としたものとなる。

1.1.2. ガイドラインの構成と利用方法

本書（策定手引書）は、情報システム運用継続計画を作成する上での検討手順及び検討時の留意点を取りまとめた文書である。本書に記載される策定の流れの順序に則り、別紙「雛型」を活用し追記することで、府省庁の担当者が情報システム運用継続計画を策定できることを目的としたものである。

「雛型」と、本書での策定の流れの対応関係については本書内の各関係項内に記載する。

また、府省庁に既に同種の計画が存在する場合には、本書内容を確認のうえ、既存の計画の不足点や改善点等があれば追加修正すれば足り、新たに情報システム運用継続計画を策定しなおす必要は無い。

なお本書と「雛型」の文書は、異なる目次構成をとっている。これは雛型においては、非常時の利用のしやすさを考慮し、非常時に必要となる箇所を優先的に記述していることによる。

1.1.3. ガイドラインの適用範囲

本書及び雛型では、非常時における府省庁内及び府省庁間の連絡手段の確保を最低限実施すべき事項ととらえ、メールやWeb等の情報収集・共有・伝達手段、基幹LAN及びこれにアクセスするための認証基盤の継続計画を優先的に作成できるよう記載している。ただし記載されている検討手法は汎用的なものであり、どのような情報システムを対象とする場合も、本書及び雛型は利用することができる。将来的には情報システム運用継続計画の対象範囲を、情報システムの重要度に応じて段階的に拡大し、全システムにおいて運用継続計画の検討を行うことが望ましい。

1.1.4. 参考資料について

本書では、以下の資料を参照するよう求めることがある。このため、本書の利用に当たっては当該資料を準備しておくことが望ましい。

文書名	発行年月	発行者
中央省庁業務継続ガイドライン（第1版） http://www.bousai.go.jp/jishin/gyomukeizoku/index.html	平成19年6月	内閣府防災担当
○○業務継続計画 （※○○には府省庁の名称が入る）	（府省庁の取組時期による）	府省庁
政府機関の情報セキュリティ対策のための統一基準群（最新版） http://www.nisc.go.jp/materials/index.html	第6版：平成24年4月26日 (毎年見直し)	情報セキュリティ政策会議
○○情報セキュリティポリシー （※統一基準群に準拠して策定した府省庁基準の文書名を記す）	（府省庁の取組時期による）	府省庁
東日本大震災における政府機関の情報システムに対する被害状況調査及び分析（最終報告書）	平成24年4月	内閣官房情報セキュリティセンター

本書では、「中央省庁業務継続ガイドライン（第１版）」を、以下「中央省庁業務継続ガイドライン」と言い、「政府機関の情報セキュリティ対策のための統一基準群」を、「政府機関統一基準群」と言う。

参考：政府機関統一基準群と情報システム運用継続計画の関係について

政府機関統一基準群には、不正プログラム、セキュリティホール、サービス不能攻撃及び踏み台攻撃を原因とするシステム停止を防ぐための、予防的対策が記載されている。本書では、これら予防対策が有効に機能せずシステムが停止する事態を想定した対応手順の整備を推奨するものである。対応手順の検討に当たっては、現状の予防対策の状況を踏まえる必要が生じる可能性もあるため、この場合は適宜政府機関統一基準群と府省庁の情報セキュリティポリシーを参照するとともに、府省庁の情報システムセキュリティ責任者に対して現状の取組状況を確認する必要がある。

1.1.5. 策定した計画の取扱いについて

本ガイドラインに基づき策定した情報システム運用継続計画は、保有者及び保管先を事前に決定し、危機的事象が発生した際に、必要な管理職及び担当者が確実に利用出来るようにすること。保管先の決定に当たっては、計画や手順書自体が被災し参照できなくなる可能性があることから、電子媒体と紙媒体の両方による保管、保管先を複数箇所とすることも検討すること。

なお、システムの設置拠点や代替環境の所在地、現状の情報システムの運用体制や環境、脆弱性等については、テロ等の攻撃の標的となりうることから、情報システム運用継続計画は、機密情報として取り扱い、原則として外部には公表しないこととする。ただし行政機関の責務として、外部に概要を説明する必要があれば、適宜問題が生じない範囲で対応する。

1.2. 情報システム運用継続計画の策定・運用の流れ

情報システム運用継続計画の策定・運用の流れの全体像を以下に図示する。

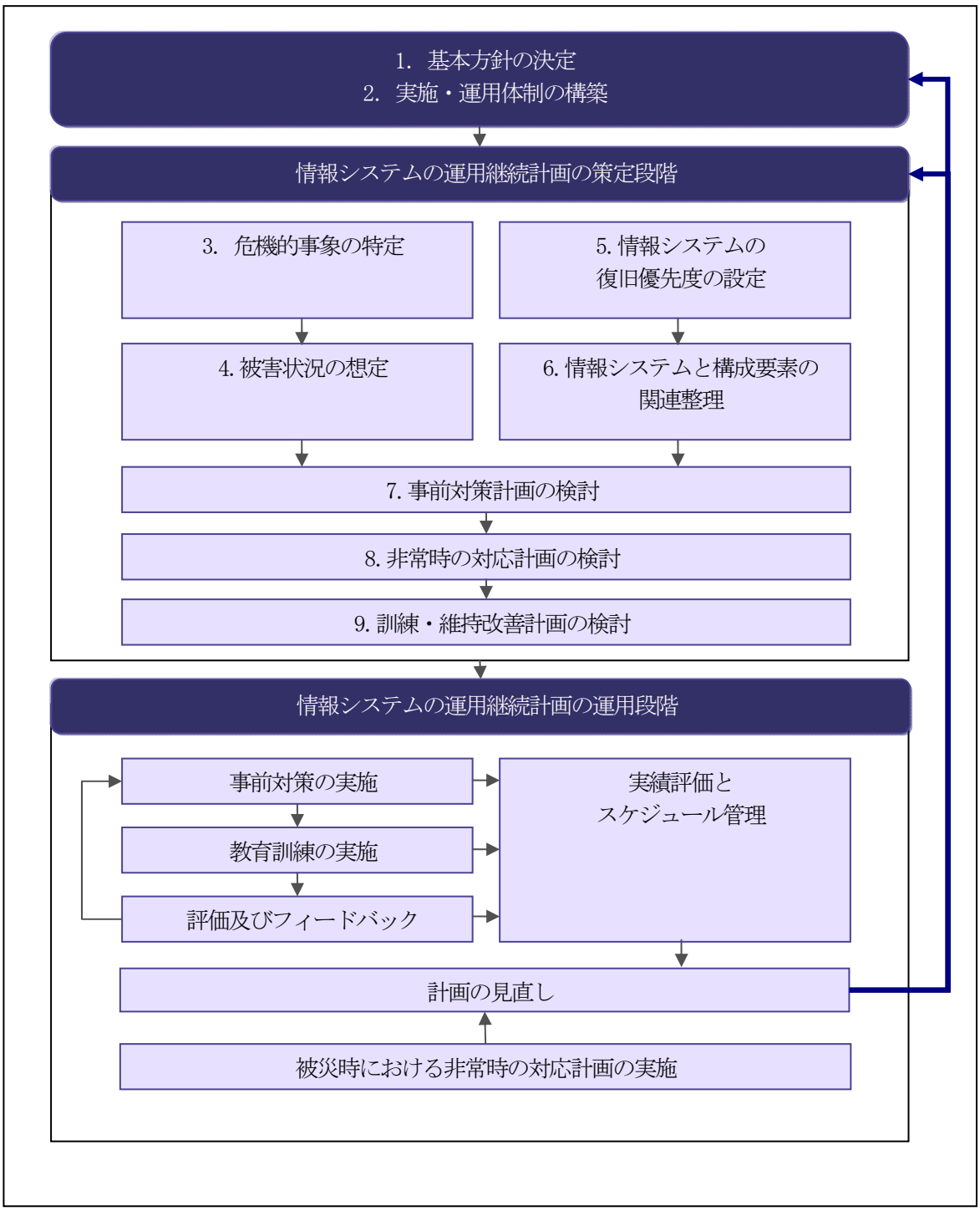

図 1.2-1 情報システム運用継続計画策定・運用の流れ

情報システムの運用継続計画の策定段階

策定段階の、各検討作業の概要を以下に記載する。

表 1.2-1 検討作業の概要

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

情報システム運用継続計画の運用段階

本段階では、策定した「維持改善計画」に基づき、計画の実施と維持改善を行う。また、事前対策計画に基づき事前対策を実施するほか、教育訓練計画に基づく訓練を行う。また事前対策の実施状況や訓練結果を評価の上、必要に応じ各種計画の見直しを行う。その他、実際の被災により情報システム運用継続計画の改善点が明らかになった場合も、各種計画の見直しを行う。

1.3. 文書構成例

本書に基づき策定される情報システム運用継続計画の構成の例を以下に示す。

1. 本書の目的と基本方針
    1.1. 本書の策定主旨
    1.2. 基本方針
    1.3. 本書の適用範囲
    1.4. 情報システム運用継続計画の実施・運用体制
2. 非常時の対応計画
    2.1. 非常時における基本方針
        2.1.1. 対象事象
        2.1.2. 参集基準
        2.1.3. 情報システム切り替え基準
        2.1.4. 対策本部機能の設置場所
    2.2. 非常時の対応体制
        2.2.1. 対応体制・指揮命令系統図
        2.2.2. 代行者一覧
    2.3. 非常時における対応手順（首都直下型地震）
        2.3.1. 全体フロー
        2.3.2. 対応手順
    2.4. 非常時における対応手順（予期せぬシステム停止）
        2.4.1. 全体フロー
        2.4.2. 対応手順
3. 事前対策計画
    3.1. 構成要素ごとの現状対策レベルと脆弱性
    3.2. 事前対策の実施計画の策定
4. 訓練・維持管理計画
    4.1. 教育訓練計画
    4.2. 維持改善計画
        4.2.1. 計画の実施に伴う維持改善
        4.2.2. 定期的な点検・是正による維持改善
        4.2.3. 被災経験に伴う維持改善
5. 計画策定の根拠とした調査・分析・検討
    5.1. 想定する危機的事象
    5.2. 想定する被害状況
    5.3. 情報システムの復旧優先度の設定
    5.4. 情報システムと構成要素の関連整理
        5.4.1. システム構成要素の整理
        5.4.2. 構成要素ごとの目標対策レベルの設定

2. 各作業の進め方及び留意事項

情報システム運用継続計画の策定・運用の流れに沿い、以下に各検討の目的・検討内容及び留意事項を記載する。

2.1. 基本方針の決定

雛型への反映先：「1.1 本計画の策定主旨」、「1.2 基本方針」、「1.3 本計画の適用範囲」

（1）検討の目的

情報システム運用継続計画策定の基本方針・対象範囲を、関係者間で合意形成する。

（2）検討内容

情報システムの運用を継続する責任者[1]は、情報システム運用継続計画策定の対象範囲を定める。また、優先的に対策に取り組むシステム等、関係者間で共有すべき基本方針について定める。

（3）検討に当たっての留意事項

ア）メールやWeb等の情報収集・共有・伝達手段、基幹LAN及びこれにアクセスするための認証基盤を対象範囲に含めること（最低限実施すべき事項）

情報システム運用継続計画における対象範囲の決定は、府省庁の個別事情（例えば既に計画がある、積極的に継続すべき重要システムが多い・少ない、極めて特殊性の高いシステムのため独自の方法での計画検討が必要、等）により判断するものとする。

ただし、メールやWeb等の情報収集・共有・伝達手段、基幹LAN及びこれにアクセスするための認証基盤は、災害発生時に省庁全体の非常時優先業務の活動を支える重要な資源となることから、情報システム運用継続計画の対象範囲に含めなければならない。府省庁は、検討した計画を基に、府省庁の判断で必要な対策を講じていくものとする。

イ）新規システム導入の際に、情報システム運用継続計画を策定すること

情報システム運用継続計画は、将来的には、府省庁の全てのシステムを策定対象とすることが望ましい。またこの中で、新しく導入するシステムについても、同様に情報システム運用継続計画を策定する必要がある。

新しく導入するシステムに対しては、導入時に情報システム運用継続計画作成の必要性を検討することが望ましい。また作成する場合は本書に記載のある検討プロセスを実施し、検討結果を調達時の仕様書に盛りこむことが望ましい。これによりシステム導入時から、災害対策の視点で必要な対策をとることができる。

---

[1] 情報システムの運用を継続する責任者は、所管する情報システムの運用継続に関し、計画の策定及び運用を統括する者をいう。各府省庁において、本ガイドラインで求める事項につき、情報セキュリティ推進体制等既存の体制・枠組みにおいて実施することと整理されている場合は、当該体制・枠組みにおいて該当する者を充てられたい。

2.2. 実施・運用体制の構築

雛型への反映先：「1.4 情報システム運用継続計画の実施・運用体制」

（1）検討の目的

情報システム運用継続計画の策定及び運用を推進するに当たって必要な体制を整備する。

（2）検討内容

それぞれの情報システムの運用を継続する責任者は、「2.1 基本方針の決定」で定めた情報システム運用継続計画の策定の対象範囲を踏まえつつ、必要な担当者を定める。また、関連部局との連携体制を構築する。

以下の図は、対象システムを限定し、関係部局間で適宜連携して検討を進める例である。府省庁全体として計画の策定に取り組む場合（例：全システムを対象とする場合等）は、部局間の調整を行う事務局を別途体制に定める等、適切な推進体制を構築することが必要である。

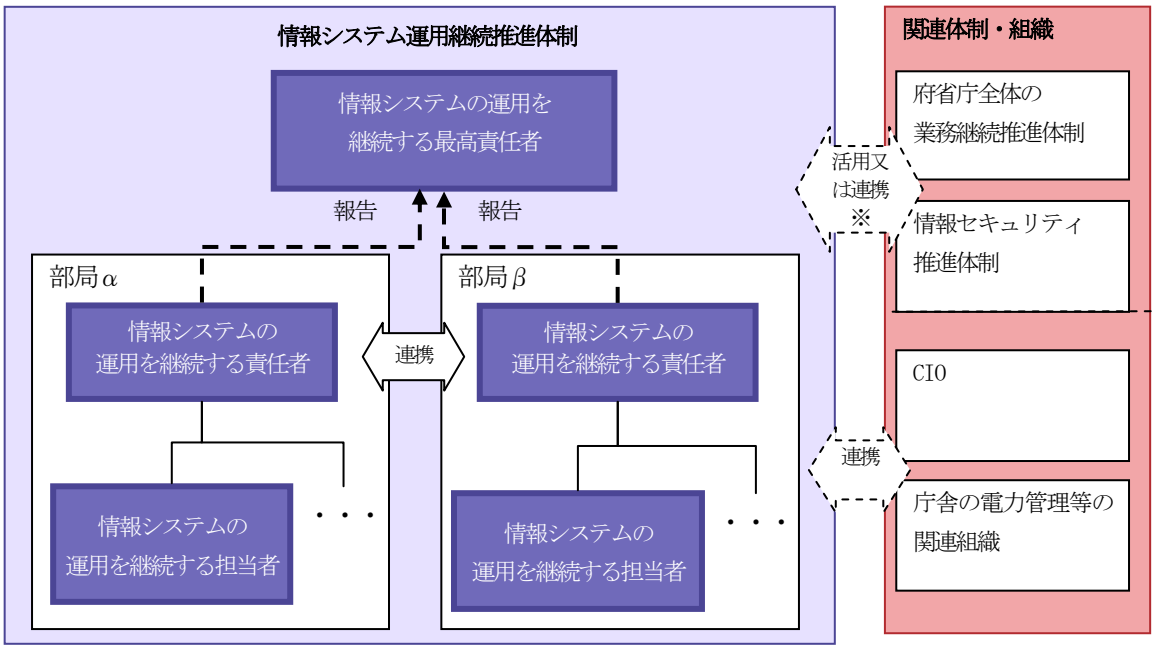

図 2.2-1 情報システム運用継続計画の策定・運用推進体制（例）

表 2.2-1 情報システム運用継続推進体制における各担当の役割（概要）

担当	役割の概要
情報システムの運用を継続する最高責任者	・対象システムの情報システム運用継続計画の最終責任者。
情報システムの運用を継続する責任者	・担当する情報システムの、情報システム運用継続計画の策定・運用全般を統括する。
情報システムの運用を継続する担当者	・担当する情報システムの、情報システム運用継続計画策定に関する各種検討作業を行う。

（3）検討に当たっての留意事項

情報システム運用継続計画推進体制を構築する際は、以下の点に留意する必要がある。

ア）情報システムの継続に必要な担当者を定めること（最低限実施すべき事項）

情報システムの運用を継続する責任者は、情報システム運用継続計画の策定・運用に必要な要員を定めなければならない。この時、他部局のシステム担当者が検討に加わる場合、指示命令系統の調整等、関係者との連携方法を調整しなければならない。

また、非常時のシステム復旧に当たって、情報システムの運用を継続する担当者以外が必要な場合（例えば、システムの担当者ではないが、ホームページのコンテンツを管理している利用者や非常時のシステムの復旧指示に当たって必要な担当者等）、同様に策定・運用のための要員に加えることが望ましい。

イ）業務継続計画との整合性を考慮すること

情報システム運用継続計画を策定・運用する上では、府省庁の業務継続計画との整合性を確保する必要がある。このため、情報システム運用継続計画の策定・運用に係る実施体制には、府省内の業務継続推進体制に参画している情報システム担当者を含めることを基本とする。

また、府省庁の業務継続計画の推進に当たり設置された推進会議等の体制がある場合、当該体制に加わることで情報システム運用継続計画との整合性をより確保できることから、情報システムの運用を継続する最高責任者、又は情報システムの運用を継続する責任者は、メンバー又はオブザーバーとして参画することが望ましい。

ウ）情報セキュリティマネジメントとの整合性を考慮すること

非常時においては、情報システム復旧作業のためのサーバルーム内への事前登録者以外の立ち入りや、保全のための重要データの外部持ち出し等、一時的に平常時の情報セキュリティポリシーの例外的な運用を求められる場合がある。このように、情報システム運用継続計画における対策と、情報セキュリティ対策は、状況によっては相反することもあり、両者の間では特に事前の整合性の調整と、非常時における判断の体制が必要である。したがって、既存の情報セキュリティマネジメントと情報システム運用継続計画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する体制とすることが望ましい。

例として以下のような体制が考えられる。

・情報システムの運用を継続する責任者・・・情報システムセキュリティ責任者
・情報システムの運用を継続する担当者・・・情報システムセキュリティ管理者

2.3. 想定する危機的事象の特定

雛型への反映先：「5.1.想定する危機的事象」

（1）検討の目的

情報システムがさらされている脅威を洗い出し、情報システム運用継続計画の前提となる原因事象を決定する。

（2）検討内容

情報システムの運用を継続する責任者は、情報システム運用継続計画の対象とする危機的事象を決定する。この場合、府省庁の業務継続計画で対象とした危機的事象だけでなく、情報システム特有の危機的事象も考慮する。

（3）検討に当たっての留意事項

ア）対象とする危機的事象決定の留意点（最低限実施すべき事項）

情報システムの運用を継続する責任者は、発生時の影響の大きさ、発生の確率、府省庁の業務継続計画で前提とする脅威との整合性等の要素を考慮し、対象とすべき危機的事象を決定しなければならない。

本ガイドラインでは、首都直下型地震及び、マルウェア感染や不正侵入等のネットワークを介した外部攻撃による情報システムの予期せぬ停止（以下「予期せぬシステム停止」）を対象の危機的事象として推奨する。

最初から全ての危機的事象を対象とすることは膨大な労力を要することから、まずは首都直下型地震及び予期せぬシステム停止を優先し、順次想定する危機的事象を増やしていくことが推奨される。

首都直下型地震は、業務継続計画の対象脅威とされる中央省庁が優先的に取組むべき危機的事象である他、予期せぬシステム停止は、他の業務に被害が無い状況で情報システムのみが長時間停止することから利用者への影響が大きいため、取組の必要性が高い。

また首都直下型地震等の大規模地震の想定は、広範囲な物理的被害の発生と、情報システム以外の電力・水道・交通ネットワーク等のインフラが利用できなくなる事態の発生が前提である。一方、マルウェア感染等による停止は、情報システムも含めて物理的な被害は発生しないが、情報システムのみが突然長時間停止する事態の発生が前提である。この２つの異なる事態を想定することにより、情報システム運用継続計画は、様々な危機的事象に対して概ね対応可能なものとなると考えられる。

なお、業務継続計画で首都直下型地震以外の事象を対象としている場合、情報システム運用継続計画においても、当該事象を対象とする必要がある。

イ）危機的事象発生時間等の前提条件検討における留意点

事象発生時間等の前提条件は厳しい条件を想定し、必要な検討に漏れが生じないようにすることが必要である。例えば、休日夜間の発生を前提におくことによって、発生時の職員の自宅からの参集が検討に含まれる。

首都直下型地震については、業務継続計画における前提条件を原則として利用する。また予期せぬシステム停止については、以下の考え方を参考に発生時の条件を想定することが望ましい。

- 想定する危機的事象は、重要な情報システムがマルウェア感染した場合や、不正侵入等が仕掛けられた場合とする。
- 厳しい条件の例として、平日の午前 9 時にマルウェア感染が発覚した場合や不正侵入等を仕掛けられるケースを想定する。平日の午前 9 時は業務開始の直前であることから、業務や関係者へ大きな影響が発生することが考えられる。
- また、土曜日 24 時（日曜日 0 時）にマルウェア感染の発覚や不正侵入等仕掛けられるケースについても検討することが望ましい。これは、業務への影響は限定されるものの、自宅からの職員の参集や、関係者への連絡、情報システム外部委託者への連絡等において、平日とは異なる課題が発生する場合があるためである。
- その他、情報システムによっては、情報システム運用継続の条件が著しく厳しくなる特定の時期、時刻、曜日等の条件があることも考えられる。このようなケースも検討対象とすることが望ましい。

ウ）環境変化に伴う、対象とする危機的事象の見直し

外部環境等の変化に応じ、情報システム運用継続計画が対象とすべき危機的事象は変化するため、情報システムの運用を継続する責任者は府省庁の情報システムの運用継続を脅かす危機的事象を定期的に見直すことが望ましい。

例えば、大規模水害や武力攻撃・テロ等、府省庁の業務継続計画等の他規程に対象とする危機的事象が追加された場合は、情報システム運用継続計画においても同様に危機的事象を追加する必要がある。

2.4. 被害状況の想定

雛型への反映先：「5.2.想定する被害状況」

（1）検討の目的

特定された危機的事象の発生時に、情報システムにおいて生じる被害状況を想定し、情報システムの抱える脆弱性（情報システムの運用継続を阻害する課題）を明らかにする。

（2）検討内容

情報システムの運用を継続する責任者及び担当者は、以下の手順によって対象とする危機的事象が発生した際の情報システムに係る被害状況を想定する。

①首都直下型地震発生時の被害状況の想定

情報システムの運用を継続する責任者及び担当者は、下表に示すそれぞれの単位で首都直下型地震の被害状況を想定する。情報システムの設置拠点が複数存在する場合は、拠点ごとに想定する。

省庁全体としての取組の整合性を確保するため、業務継続計画の被害状況の想定結果を活用することを基本とする[1]。

表 2.4-1 被害状況の想定

被害想定の単位	説明	参考にする業務継続計画の被害想定結果
情報システムの設置場所	情報システムの設置場所の被害状況を想定する。	庁舎
交通機関	IT 復旧に必要な職員や外部委託者が参集するための交通機関の被害状況を想定する。合わせて、参集可能な要員の把握等、要員の被害状況も想定する。	周辺環境
電力	電力の被害状況を想定する。	電力
水道	水冷式の空調を利用している場合、水道復旧までシステムが停止する。水道の被害状況を想定する。	上水道
電話	固定電話、携帯電話、携帯メールの被害状況を想定する。	電話、携帯電話
情報通信ネットワーク	府省庁内外のそれぞれの情報通信ネットワークの被害状況を想定する。また ASP 等の外部サービスを利用している場合は、その被害状況も想定する。	インターネット
情報システム機器（サーバ等）	IT 拠点に設置された設備機器の被害状況を想定する。	建物内部
データ	情報システムの OS・アプリケーションのデータ、また業務データの被害状況を想定する。またバックアップデータがある場合、バックアップデータの被害状況を想定する。	データ

[1] 注：本書による検討で、業務継続計画の被害想定の詳細を見直す必要があることが判明することもありうる。

その他、対応に当たる職員のために不可欠なトイレ、下水道、飲料水、食糧、休眠スペース等の状況も、業務継続計画等から想定しておく。

②予期せぬシステム停止発生時の被害状況の想定

情報システムの運用を継続する責任者及び担当者は、予期せぬシステム停止発生時の被害状況を以下の要領で想定する。情報システムの設置拠点が複数存在する場合は、拠点ごとに被害状況を想定する。

表 2.4-2 被害状況の想定

被害想定の単位	説明
情報システムの設置場所	影響が無いため、想定の必要無し
交通機関	影響が無いため、想定の必要無し
電力	影響が無いため、想定の必要無し
水道	影響が無いため、想定の必要無し
電話	IP 電話の場合には、被害発生の可能性があるため、被害状況を想定する。
情報通信ネットワーク	物理的被害は無いが、例えばマルウェア感染の場合は影響範囲、サービス不能攻撃の場合は想定をはるかに上回る急激な処理要求の増大が求められる事態が発生した場合の被害状況等を想定する。
情報システム機器（サーバ等）	物理的被害は無いが、例えばマルウェア感染の場合は起こりうる障害、サービス不能攻撃の場合は想定をはるかに上回る急激な処理要求の増大が発生した場合の被害状況を想定する。（極端な処理の遅延や停止の発生が考えられる）
データ	不正侵入による改ざんや消失、情報漏えいによる被害の可能性があるため、重要データを対象とした被害状況を想定する。

③その他危機的事象発生時の被害想定

情報システムの運用を継続する責任者及び担当者は、その他危機的事象について、上記の危機的事象と同様に被害状況を想定する。

（3）検討に当たっての留意事項

ア）細かすぎる被害状況の想定を避ける

実際の危機的事象発生時の被害状況は、正確に詳しく予測することは不可能である。一般に精緻に被害状況を想定すれば、想定どおりの被害状況が発生した際の実行性は向上するが、想定からずれた場合の実効性はかえって低下する。また、検討に多大な労力と時間を費やすこととなる。ある程度幅を持たせた予測として被害状況を想定することで、前提条件から多少外れても対応可能な計画とすることが重要である。したがって、被害状況の想定は、既に存在する公表資料の情報を基に、ある程度大まかな予測として整理することが望ましい。また、この際、軽すぎる被害状況を想定すると、本来必要な事項の検討に抜けの出る恐れがあるため、起こりうる状況を鑑み、ある程度重大な被害を受けることを前提とした被害状況を想定することが望ましい。

2.5. 情報システムの復旧優先度の設定

2.5.1. 優先業務と情報システムの関連整理

雛型への反映先：「5.3.情報システムの復旧優先度の設定」

（1）検討の目的

非常時優先業務を実施するために必要な対策を最適な範囲及び程度で行うために、非常時優先業務と情報システムの関連性を明らかにする。

（2）検討内容

情報システムの運用を継続する責任者及び担当者は、既存の業務継続計画に定められる非常時優先業務を確認し、対象システムとの関連性を整理する。本作業のワークシートのサンプルを別紙. 業務システム関連表に示す。

①非常時における優先業務の洗い出し

情報システムの運用を継続する責任者及び担当者は、府省庁の業務継続計画を確認し、非常時優先業務の洗い出しを行う。サンプルのワークシートを利用する場合、別紙. 業務システム関連表の横軸に業務名を記入する。

予期せぬシステム停止についても同様に業務と情報システムの関係を整理することが望ましい。予期せぬシステム停止については、情報システムのみの局所的な被害が発生するため首都直下型地震よりも非常時優先業務の範囲が狭く、基本的には平常時の重要業務が中心となる（原則災害被害対応に関わる業務は発生しないと考えられる）。このため、中央省庁業務継続ガイドラインの「1.はじめに 図1-1 応急業務と非常時優先業務の概念図」に示される非常時優先業務の「通常業務」のうち、業務継続の優先度が高いものが相当することを前提に、検討することを推奨する[1]。

②対象となる情報システムの洗い出し

情報システムの運用を継続する担当者は、今回対象とする情報システムを以下の観点で洗い出す。サンプルのワークシートを利用する場合は、洗い出し結果を別紙. 業務システム関連表の縦軸に記入する。

- 情報システム運用継続計画の対象システムを洗い出す。情報システムを洗い出す単位は、物理的なサーバの単位ではなく、業務側で意識している情報システムの単位（メールシステム、ホームページ管理等）とする。情報システムが複数のサブシステムによって構成され、サブシステム単位の復旧が可能な場合、それぞれを別の情報システムとして整理する。
- ユーザが直接利用する情報システム以外に、これらの情報システムを支える認証、ドメインネームシステム（DNS）等の基盤系システムについても、業務で直接利用する情報システムを洗い出した後、稼働の前提となる情報システムとして明確化しておく。

③非常時優先業務と情報システムの関連整理

情報システムの運用を継続する担当者は、非常時優先業務それぞれがどの情報システムを利用しているかを明確化する。本検討に当たっては、業務継続計画の中で、非常時優先業務で利用する情報シ

[1] ただし、大規模な自然災害の発生時には府省外の活動・移動も低下するのが一般的だが、予期せぬシステム停止ではこの稼動低下がないため、業務が増える可能性もある点に注意が必要である。

ステムが洗い出されている可能性がある。そのため、まず業務継続計画の内容を確認し、利用可能であれば検討結果を活用する。

サンプルのワークシートを利用する場合は、別紙. 業務システム関連表の該当する箇所に●印を記入する。

（3）検討に当たっての留意事項

ア）必要に応じ、各部局に確認をとること

情報システム部局で業務と情報システムの関連付けが不明なものがある場合には、各部局へのヒアリング等を実施し確認することが必要である。

2.5.2. 情報システムの復旧優先度の設定

雛型への反映先：「5.3.情報システムの復旧優先度の設定」

（1）検討の目的

非常時優先業務で利用する情報システムに対し、復旧の優先順位と、目標とする復旧時間（以下、IT-RTO[1]という。）を明確化する。更に、目標復旧時間の幅により復旧優先度グループに分類する。

（2）検討内容

情報システムの運用を継続する責任者及び担当者は、「2.5.1 優先業務と情報システムの関連整理」で洗い出した情報システムに対して、それぞれ IT-RTO を設定する。

本項では、情報システムを利用している業務の目標復旧時間と情報システム停止時の当該業務の実施における代替手段の有無を考慮した IT-RTO 設定方法を記載する。

① 業務の目標復旧時間の確認と情報システムに求められる目標復旧時間（IT-RTO）の設定

情報システムの運用を継続する責任者は、「2.5.1 優先業務と情報システムの関連整理」で整理した非常時優先業務それぞれの目標復旧時間を確認する。更に、その業務の実施の代替手段（すなわち、情報システムを使わない手段）の有無を考慮した上で、IT-RTO を設定する。以下に本作業の考え方と具体的な作業手順を記載する。

情報システムは業務を実施する前提条件であるため、IT-RTO の多くは当該業務の目標復旧時間よりも短く設定される必要がある。ただし、業務が情報システム以外の手段を用いて継続できるのであれば、必ずしも IT-RTO は業務の目標復旧時間より短い時間でなくてよい。例えば、システム停止時に職員が電話や FAX、パソコン内のデータの利用等の代替手段によって、1 週間程度なら暫定的な対応としてもさほど支障がないのであれば、その方法で１週間は業務を継続可能とみて、IT-RTO は、１週間程度と設定しても問題ないと考えられる。

このように、業務の目標復旧時間とともに、情報システムが停止した際の業務の代替手段の有無と、代替手段による業務継続時間（すなわち、さほど支障が出ない時間）を踏まえて IT-RTO を設定する必要がある。IT-RTO を短く設定するほど、情報システムに必要な対策は高額になるため、業務側で代替手段を取る余地がないかを入念に検討することが望ましい。

本作業の具体的な作業手順は、以下のとおりである。

- 情報システムの運用を継続する責任者及び担当者は、既存の業務継続計画を確認し業務の目標復旧時間を別紙. 業務システム関連表に記載する。
- 情報システムの運用を継続する責任者及び担当者は、雛型の「表 5.3-1 業務の目標復旧時間と情報システム停止時の代替手段分析結果（例）」を利用し、以下の検討結果を記載する。
  1．情報システムと業務の関連性
  2．業務の目標復旧時間の設定結果
  3．情報システム停止時の代替手段の有無及び代替手段により業務継続が可能な時間（すなわち、さほど支障が出ない時間）
- 情報システムの運用を継続する責任者及び担当者は、上記検討結果に基づき、IT-RTO の検討結果を雛型「5.3.情報システムの復旧優先度の設定」内の「(2) IT-RTO 検討結果」に記載する。この時、一つの情報システムが複数の業務で利用されており、それぞれの業務の IT-RTO が異なる場合は、最も短い IT-RTO を、当該システムの IT-RTO とみなす。

[1] RTO:Recovery Time Objective の略。

本作業では、代替手段の有無や代替手段によって業務継続が可能な時間を必要に応じて情報システムの利用者に確認する必要がある。

②基盤系システムの IT-RTO 設定

基盤系システム（DNS・認証システム等）は業務側で直接利用するものではなく、業務側で利用している情報システムの稼働の前提となるシステム群を指す。情報システムの運用を継続する担当者は、上記情報システムの目標復旧時間の設定結果を踏まえ、基盤系システムの洗い出しに検討漏れがないかを確認し、基盤系システムも含めた目標復旧時間を設定する。基盤系システムの目標復旧時間は、原則として基盤系システムが支える情報システムの目標復旧時間より短時間に設定する必要がある。

情報システムの運用を継続する責任者及び担当者は、基盤系システムの目標復旧時間設定結果を、雛型「5.3.情報システムの復旧優先度の設定」内の、「(2) IT-RTO 検討結果」に記載する。

③システム復旧優先度のグループ分け

情報システムの運用を継続する担当者は、IT-RTO の設定結果より、最終的に情報システムを IT-RTO の時間帯によるＳからＥまでの 6 段階のグループに分類する。

復旧優先度グループに分類する目的は、検討対象の情報システム全体を復旧優先度グループ毎で俯瞰し、検討の抜けがないかや優先順位の整合性に問題がないかを確認することと、今後必要な対策を検討する際の様々な技術的な対策手法パターンの適用単位を明らかにすることにある。

表 2.5-1 情報システムの復旧優先度ランク

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

情報システムの運用を継続する責任者及び担当者は、本復旧優先度ランクの設定結果を、雛型「5.3. 情報システムの復旧優先度の設定」内の、「（2）IT-RTO 検討結果」に記載する。

（3）検討に当たっての留意事項

ア）Ｓ又はＡランクの復旧優先度の情報システムを出来るだけ絞り込むこと

実際の被災時には、情報システム復旧に必要な要員、ベンダのサポート、機器等の必要資源が大幅に制限されることを考えると、被災発生当日内に復旧させなければならないＳ又はＡランクの情報シ

ステムの対象数は出来るだけ少なくすることが望ましい。さもないと、効率的な復旧活動が不可能となり、計画どおりの早期復旧の実現性が低くなる。また、早期の復旧を目指すほど、事前対策費用の高騰に直結することも考慮するべきである。S 又は A ランクの情報システムについては、本当にそこまでの時間内での復旧が必要なのか、当面の代替手段は存在しないのか、等の検討を何度も繰り返し実施し、可能な限り対象システム数を絞り込むことが望ましい。

イ）検討メンバーにてまずは検討し仮説を立案すること

システム利用者からは、業務の復旧優先度に関わらず、情報システムの可能な限りの早期復旧を求める要求が出される場合が多く、この要求どおりに復旧優先度を設定すると、情報システムの復旧優先度の要求が高止まりしてしまい、真に必要な対策の実施の遅延や、必要となる対策費用の増大を招く恐れがある。これを回避するため、本項の作業時には、情報システムの運用を継続する責任者と担当者との間で一連の検討をし、復旧優先度の仮説を立てたうえで、システム利用者と個別の調整をすることが望ましい。仮説を前提に調整の場を持つことにより、可能な限り復旧優先度の高止まりを防ぐことが望ましい。

ウ）設定方法と設定根拠を残しておくこと

上記で情報システム復旧優先度を設定する方法を例示したが、時間の経過や事情の変更により、設定の判断が変わることもありうる。また、府省庁の判断によりその他の方法を採用する場合もあろう。人事異動による後任の担当者であっても適切に理解し見直しできるよう、将来の見直しを見越して設定方法と設定根拠（どのように情報システムの復旧優先度を設定したか）を確実に残しておくことが必要である。

2.6. 情報システム運用継続に必要な構成要素の整理

2.6.1. 情報システムを支える構成要素の明確化

雛型への反映先：「5.4.1.システム構成要素の整理」

（1）検討の目的

情報システムの運用継続を実現するためには、非常時に情報システムの運用を継続させるために必要となる、人員・サーバ・情報通信ネットワーク・データ・手順書・外部委託者等の構成要素に対して網羅的に対策を実施することが重要である。そのためには、重要な情報システムを支える構成要素を明らかにせねばならない。

（2）検討内容

情報システムの運用を継続する責任者及び担当者は、下表の構成要素の区分を参考に、情報システムを支える構成要素を明確化する。現状の情報システムの運用環境を踏まえ、下表の構成要素以外に、情報システムの運用に必要な構成要素があれば追加する。

なお、対象となる情報システムがクラウドコンピューティングサービス、ASP サービス等の外部サービスの場合でも、自組織で所有する場合と同様に本構成要素を考慮する必要がある。これにより、サービス提供元に対して災害対策の内容を確認・調整する際の視点とすることができる。

表 2.6-1.情報システム構成要素の整理結果

構成要素	構成要素の説明
施設	情報システム機器の設置環境（庁舎、データセンタの場所・堅牢性・自家発電設備の有無・代替環境の有無、電力系統の多重性、上下水道等）
ネットワーク	情報システムを利用するために必要な情報通信ネットワーク（庁舎内及び拠点間等の外部）の敷設状況（利用キャリア・種類・ルート分散状況等）
周辺機器	複合機やプリンター等の設置状況、外付け HDD 等の管理状況（データの暗号化等）
ハードウェア	サーバ等のハードウェア機器の役割、台数及び所在（代替機がある場合はそれも含む）
システム領域	アプリケーションやシステム設定情報等の情報システム復旧に必要なデータの所在及び管理状況（バックアップ媒体の外部保管、データ暗号化及びデータ改ざん防止措置等）
データ領域	重要なデータの所在及び管理状況（バックアップ媒体の外部保管、データ暗号化及びデータ改ざん防止措置等）

システム運用体制	システムの被害状況の早期確認や適切な対応を実施するための運用の人的体制と役割分担、手順書の整備及び連絡手段の確保
ベンダの継続能力	非常時における情報システムベンダの支援・協力体制 （ベンダの事業継続能力把握、サービス品質保証契約の締結等）

（3）検討に当たっての留意事項

ア）構成要素を洗い出す対象システムの範囲

構成要素の洗い出しは、対象とする情報システム数が多いほど、膨大に手間のかかる作業となる。対象となる情報システム数によっては、調査対象の情報システムの範囲を、当初は復旧重要度ランクA以上あるいはB以上等に限定して進める等の柔軟な対応を考慮する必要がある。

イ）危機的事象発生時を想定し洗い出すこと

平常時における情報システム資産管理の観点とは異なり、危機的事象発生時に情報システムを復旧継続するための必要な要素の洗い出しであることに留意すること。例えば、平常時の情報システムの運用では利用しないが、危機的事象発生時には必要となる要素として、情報システムの復旧手順書や緊急連絡先リスト、ネットワーク設定情報等の文書情報、さらには復旧のために必要なソフトウェアやデータ等がある。雛型の「2.3 非常時における対応手順」や、府省庁の業務継続計画内で作成している非常時の対応手順、あるいは既に作成している情報システム復旧の対応手順（存在すれば）等を参考にしながら、首都直下型地震が発生した際の対応の流れをイメージし、必要な要素に漏れが無いように洗い出す必要がある。

2.6.2. 構成要素ごとの目標対策レベルの設定

雛型への反映先：「5.4.2.構成要素ごとの目標対策レベルの設定」

（1）検討の目的

本項の検討目的は大きく以下の２点である。

・情報システムを IT-RTO 内に復旧させるために、復旧優先度に対応して必要となる構成要素毎の対策の目標（以下、目標対策レベルと言う）を設定する。これにより、今後の対策計画を立案し、実行管理するための基準を作成する。

（2）検討内容

情報システムを IT-RTO 内に復旧させるためには、情報システムの構成要素それぞれに対し、復旧優先度に応じて必要となる対策を、現状の情報システム環境を踏まえながら実施していく必要がある。

例えば、復旧優先度グループがＳのシステムでは、ほぼ即時の復旧再開が必要となる。首都直下型地震による被害で利用できなくなる環境に情報システムが設置されている場合、復旧を再開するためには、被害を受けない場所（データセンタ等）に情報システムの設置環境を移設することや、被災しても即時に切り替えて利用出来るバックアップシステムの環境を同時被災しない場所に構築しておく、等の対策が必要である。

一方、復旧優先度がＥ等の復旧までに相当に時間をかけても構わない情報システムでは、現状が首都直下型地震で被害を受ける環境にあるとしても、重要なデータさえ消失しない対策が実施されていれば、被災時には必要な機器を再調達すれば良いため、情報システムの設置環境を移したりバックアップシステムを構築したりする必要はない。

このように、情報システムの運用を継続する責任者及び担当者は、情報システムの復旧優先度に応じた IT-RTO を達成するために必要となる対策の実施方針を決めた上で、「2.6.1 情報システムを支える構成要素の明確化」で定めた構成要素ごとに復旧優先度レベルに応じた目標対策レベルを整理する。

これにより、IT-RTO を達成するために必要な対策の目標（ゴール）が設定され、現在の状況との乖離及び今後実施すべき対策を明確化することができる。

以下に、ホットスタンバイ方式[1]、ウォームスタンバイ方式[2]、コールドスタンバイ方式[3]を利用し、現状の拠点と同時被災しない場所にバックアップシステムを確保することを想定した目標対策レベルの例と、現状システムのデータセンタへの移設を前提とすることを想定した対策レベルの例を、ハードウェアを例にとり記載する。

表 2-6-2　現状の拠点と同時被災しない場所にバックアップシステムを確保することを基本方針とする

[1] ホットスタンバイ：主システムと同じ構成や設定のシステムを設置し、OS・アプリケーションを起動させ、データの同期等主システムと同じ動作を絶えず行う状態で待機させている状態のこと。主システムが利用不可能になった場合、予備システムが処理を引き継ぐため、即座にシステムが利用可能となる。

[2] ウォームスタンバイ：主システムと同じ構成や設定のシステムを設置し、OS を起動させた状態で待機させている状態のこと（通常は開発環境として利用する、別アプリケーションを立ち上げている等）。主システムが利用不可能になった場合、必要なアプリケーションを起動し、各種設定作業をすることで、システムが利用可能となる。

[3] コールドスタンバイ：予備の情報システム機器を通常利用しない状態で待機させた状態のこと（OS・アプリケーションの未インストール、電源を入れない等）。主システムが利用不可能になった場合、必要な OS・アプリケーション・データをインストールし、各種設定作業をすることで、システムが利用可能となる。

対策レベル（ハードウェアの例）

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

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

表 2-6-3　データセンタへの移設を基本方針とする対策レベル（ハードウェアの例）

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

上記に例として挙げたハードウェア以外にも、「2.6.1.情報システムを支える構成要素の明確化」で

明確化した、情報システムの運用継続を支える構成要素それぞれに対して、同様に目標対策レベルを設定する必要がある。

また、表 2.6-2、表 2.6-3 ではホットスタンバイの技術等の採用を想定した例を記載しているが、府省庁固有の環境に応じ、IT-RTO を実現するための適切な目標対策レベルを設定する必要がある。なお、各情報システムの復旧優先度ランクに対応した IT-RTO を満たす対策であれば、必ずしも復旧優先度ランクと目標対策レベルを１対１に対応させる必要はない。

以上に留意し、情報システムの運用を継続する責任者は、雛型「5.4.2.構成要素ごとの目標対策レベルの設定」に、本検討結果を記載する。

（3）検討に当たっての留意事項

ア）府省庁の現状を踏まえ、対策の方針を決定すること

IT-RTO を満たすための対策には、現状の情報システム設置環境を極めて堅牢なデータセンタに設置することにより、情報システムの被災可能性及び被災時の被害を極小化する予防的な対策、また現状の設置環境に脆弱性があっても、同時被災しない場所にバックアップシステムを設置することにより早期の復旧を実現する対策、また両方を組み合わせて、現状の拠点の堅牢化をしつつ、代替拠点にバックアップシステムを持つ対策等、さまざまな方法がある。どのような対策方針を取るかは、現状の情報システムの設置環境や、情報システムの利用特性（府省庁内に限定した利用か、不特定多数が利用するものか等）から見たデータセンタ設置の可否、中長期の情報システム化推進計画、さらに最終的には対策にかかる費用を踏まえて決定する必要がある。

イ）目標対策レベルは、目標復旧時間を満たすための視点で作成すること

ここで設定する目標対策レベルは、あくまでも目標復旧時間を満たすために必要な望ましい対策手段であるため、現状の情報システム環境や予算からみた短期的な現実性とは乖離が生じる。しかしながら、情報システムの運用継続能力を向上するため、中長期的にどのような対策を実施すべきかを現状からのギャップと合わせて管理することは、今後の継続的維持改善における活動目標として必要である。従って、短期的に実現しそうにない目標対策レベルであっても設定することが重要である。

なお、対策レベル実現に向け、現状の情報システム環境からどのような対策を実施するかは、「2.7 事前対策計画の検討」において整理する。

ウ）対象部局と異なる部局が管理している構成要素のうち、要調整事項は課題として記録しておく

例えば自家発電装置の管轄等、情報システム運用継続計画の策定対象とした範囲と異なる部局が管理している構成要素については、当該部局における現状の認識と今後の対策計画を確認した上で、目標対策レベルを整理することとなる。ただし、当該部局の対策計画が不足と考えられる場合、府省庁全体の業務継続の事務局と連携した上で、別途対応することが求められる。 この場合、「2.7.1 現状対策レベルの確認と脆弱性の評価」の脆弱性欄等に状況を記載し、適切なタイミングで対応ができるよう記録を残すことが必要である。

エ）予期せぬシステム停止を想定した目標対策レベル

予期せぬシステム停止への対策については、ハードウェア、システム領域、データ領域、施設、情報通信ネットワークについては政府機関統一基準群内に実施基準及び対策内容が記載されているため、情報システム運用継続計画内で改めて基準となる目標対策レベルを設定する必要はない。情報システム運用継続計画内では、予期せぬシステム停止については「システム運用体制」と「ベンダの事業継続能力」について、目標対策レベルを設定することを基本とする。

2.7. 事前対策計画の検討

2.7.1. 現状対策レベルの確認と脆弱性の評価

雛型への反映先：「3.1.構成要素ごとの現状対策レベルと脆弱性」

（1）検討の目的

情報システム環境の現状を、前項で設定した目標対策レベルに基づき把握することで、目標とする情報システム運用環境と現状の情報システム運用環境のギャップを認識する。

（2）検討内容

情報システムの運用を継続する担当者は、以下の手順により、府省庁の情報システム環境の現状対策レベルを確認し、現状の情報システム環境を継続するための課題（脆弱性）を評価する。

①現状対策レベルの確認

情報システムの運用を継続する担当者は、情報システムごとに、前項で設定した目標対策レベルに対する現状の対策レベルを評価する。該当する情報システムが複数の設備機器で構成されており、それぞれの設備機器によって現状対策レベルが異なる場合は、最も対策レベルが低い設備機器のレベルを、当該情報システムの現状対策レベルとみなす。

②脆弱性の評価

情報システムの運用を継続する担当者は、現状対策レベルを踏まえ、情報システムの重大な脆弱性を評価する。

（3）検討に当たっての留意事項

ア）脆弱性の評価時の留意点（最低限実施すべき事項）

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

・危機事象発生時の対応体制及び連絡方法の整備状況

＜注意すべき例＞

- 情報システムの復旧と継続作業を行うための、体制、役割分担及び復旧の手順書が無い。
- 復旧継続に必要な要員（職員及び外部委託業者）の連絡先一覧表が最新のものに更新されていない。
- 復旧継続に必要な情報（府省庁内 LAN 構成図・ホームページ更新手順・復旧マニュアル等）が未整備である。
- 休日や夜間の連絡方法及び参集方法が明確になっていない。
- 特定の要員に依存しており、当該要員が不在の場合には復旧継続ができない（ホームページ更新、LAN の設定等）。

・同一拠点内でのハードウェアへの対策状況

＜注意すべき例＞

- 重要な業務で利用するサーバが二重化対応されていない（ハードウェア故障時に予備サーバに切り替わる等。平常時のハード障害でも業務に大きな支障をきたす恐れがあると共に、災害時にハードウェアの被災で停止する可能性や復旧にかかる時間が長期化する可能性が高まる）。

・重要なデータ（システム領域／データ領域）のバックアップ状況

＜注意すべき例＞

・重要なデータのバックアップを取得していない、あるいはバックアップの頻度がデータの更新頻度と比較して少なすぎる（毎日更新されるデータに対して、月１回程度等）。

・バックアップ媒体が無造作に置かれており損壊や紛失の危険性がある。

・情報システムの設置場所と同じ場所にバックアップ媒体が保管されており、情報システム設置場所に立ち入れない場合、利用できない恐れがある。

・バックアップしたデータを復元利用するテストを実施したことが無い。

・ハードウェアやソフトウェアの再調達が困難になる可能性の有無の把握

＜注意すべき例＞

・既に販売終了しており調達困難なハードウェア・ソフトウェアを利用している。

・再調達に極めて時間を要する機器類を利用している。

（ホストやオフィスコンピュータ[1]、特殊な仕様で発注した特注品等）

[1] ホスト：専用のハードウェアと専用のソフトウェアが一体となった、基幹業務システム等に用いられる汎用大型コンピュータを指す。
オフィスコンピュータ：専用のソフトウェアと専用のハードウェアが一体となった、事務処理に特化した比較的小規模のコンピュータを指す。

2.7.2. 事前対策計画の検討

雛型への反映先：「3.2.事前対策の実施計画」

（1）検討の目的

前項で把握した現状の脆弱性を解消し、情報システムの運用継続能力を強化するために、事前対策の実施計画を策定する。

（2）検討内容

①事前対策実施方針の検討

情報システムの運用を継続する責任者及び担当者は、目標対策レベルと現状対策レベルのギャップを解消し目標対策レベルに近づけるための基本方針（事前対策実施方針）をシステムごとに検討し、事前対策計画を作成する。

事前対策計画の作成に当たっては、必要に応じて幾つかのステップに区切り、段階的に継続能力を強化する計画とすることを検討する。雛型ではステップを２つに区切っているが、ステップ数は幾つに切っても構わない。

例えば、目標対策レベルどおりの対策を実施することを最終ステップに置き、その前には幾つか現実的に取り組める対策群を対策ステップとしてまとめることが案として考えられる。また、情報システムに対する各種対策は、一般に多くの費用が必要となるため、例えば情報システム更改のタイミング等で、復旧優先度の高い情報システムから順次対策を実施することが現実的である。

ステップを区切る際は、それぞれのステップでどのような脆弱性を解決できるか（期待効果）を整理する。また、ステップを実施しても残存する脆弱性（残存リスク）を整理する。これらとともに、概算費用も考慮し、それぞれのステップの実施計画を作成する。

②事前対策計画の具体化

情報システムの運用を継続する責任者及び担当者は、事前対策実施方針に基づき、事前対策の実施内容を具体化する。実際に事前対策を実施する際には、情報システム運用継続計画を作成している場合には調達時の仕様書作成時に情報システム運用継続計画を確認し、仕様書に必要な条件を盛り込むこと。

（3）検討に当たっての留意事項

ア）事前対策実施方針立案時のポイント

事前対策実施方針を立てる上では、復旧優先度の高い情報システムを優先して対策を実施することと、多くの情報システムや危機的事象に共通で必要となる対策（対応体制、役割分担及び行動の基準の明確化等）に早期に取り組むことにより、継続能力を早期に向上させることを目指すことが重要である。

イ）事前対策計画に盛り込むべき内容（優先的に実施すべき事項）

＜首都直下型地震に対する対策について＞

「2.6.2 目標対策レベルの設定」において、それぞれのシステムが目指すべき将来の目標の姿を整理したが、予算等の関係から、目標として定めた対策をすぐに実施することが難しい場合には、「別表 1. 優先的に取り組むべき対策一覧（首都直下型地震）」に示すような対策（現状運用しているシステムやネットワークへの被害を最小限に抑える対策や、速やかに被害の復旧を可能とするための対策）を優先して実施することが望ましい。

この他、非常時にシステムを利用するためには、利用者側のクライアント端末に対しても対策を行う必要がある。首都直下型地震に対してはパソコンに耐震固定を施す等、必要な対策に取り組むこと

が望ましい。またイントラネットに接続するクライアント端末は、非常時においてもセキュリティ要求事項を極力満たすようにしておく必要がある。セキュリティ要求事項を満たした端末を早急に用意できるように、セキュリティ用のアプリケーションのインストール媒体や他の端末からのセキュリティ機能をコピーできる仕組み等を、予め用意することが望ましい。また、必要に応じ、非常時のセキュリティレベルの低下をどこまで許容するか関係者と事前調整しておくことが望ましい。

＜予期せぬシステム停止に対する対策について＞

予期せぬシステム停止に備え優先的に実施すべき対策を下表に示す。予期せぬシステム停止を予防する対策については、政府機関統一基準群に基づき、検討・実施がされているため、下表の対策検討時に現状の対策内容の理解が必要であれば、必要に応じて情報システムセキュリティ管理者に対策内容を確認することが望ましい。また、被害状況・現状の脆弱性の評価結果等を踏まえ、必要に応じて情報システムセキュリティ責任者に対策を実施するよう促すことが必要である。

表 2.7-1.優先的に実施すべき対策一覧（予期せぬシステム停止）

構成要素	実施内容	対策例・留意点
ベンダの継続能力	早期にシステムを復旧するために、必要に応じベンダとの契約を見直すこと。	・情報システムベンダとの保守契約の見直し、非常時の対応内容の明確化等
システム運用体制	情報システム復旧のための体制と役割分担を整備すること。	（本手引書「2.8 非常時の対応計画の検討」を参照のこと）
	情報システム復旧のための手順を作成すること。	（本手引書「2.8 非常時の対応計画の検討」を参照のこと）

ウ）その他事前対策を検討する上での参考対策例

重要な情報システムに対する対策を検討する際は、例えばシステムベンダが提供する外部サービスの利用を検討することも考えられる。

外部サービスの利用時には、情報セキュリティが必要なレベルで確保されるよう、府省庁の情報セキュリティに係る基準に基づき、必要な要求事項を情報システムベンダに対する発注時の仕様書や契約に盛り込む必要がある。

2.8. 非常時の対応計画の検討

2.8.1. 非常時体制の構築

雛型への反映先：「2.2 非常時の対応体制」

（1）検討の目的

非常時に、既存の非常時体制と連携し情報システムの復旧継続活動を効率的に実施できるよう、情報システムの復旧に係る非常時の対応体制を構築し役割分担を定める。

（2）検討内容

情報システムの運用を継続する責任者は、平常時の情報システム運用継続体制を踏まえ、非常時において情報システムを復旧する責任者、担当者及びそれぞれの代行者を定める。下表は、情報システムの復旧対応に必要な体制・役割の例である。府省庁の業務内容や組織構造等に応じ、体制・役割の追加や変更をすること。例えば、情報システムの代替拠点が存在しない場合は、代替拠点の担当者を定める必要はない。

表 2.8.1 非常時の対応体制（例）

担当	役割	役割の内容
情報システムを復旧する責任者	責任者	• 被災時のシステム復旧対応の責任者 • システム復旧方針の決定 • システム復旧完了の利用者への通知
情報システムを復旧する事務局	情報収集・共有	• 被害状況／システム復旧状況の取りまとめと関係者への情報伝達 • 責任者の支援
	各部局との連絡窓口	• 要員参集状況の確認と報告 • システム利用者からの問合せ対応
情報システムを復旧する被災拠点の担当者	被害状況の確認	• 被災拠点におけるシステムの被害状況確認と、事務局への報告
	被害拡大の防止	• 被災拠点におけるブルーシートによる被覆、サーバ転倒防止等の被害拡大防止措置の実施、必要備品等の持ち出し
	ネットワーク復旧	• 被災拠点におけるネットワーク復旧・動作確認 • 情報システムベンダへの対応指示
	情報システムの復旧	• 被災拠点における情報システムの復旧・動作確認 • 情報システムベンダへの対応指示
情報システムを復旧する代替拠点の担当者	ネットワーク切り替え	• 代替拠点におけるネットワーク切り替え作業 • 情報システムベンダへの対応指示
	情報システム切り替え	• 代替拠点における情報システム切り替え作業 • 情報システムベンダへの対応指示

上記に加え、特に、予期せぬシステム停止に備えたメディア対応者を検討しておくことが望ましい。地震の場合、業務継続計画でメディア対応者が考慮されているが、予期せぬシステム停止の場合には、他の業務は正常に動いているので、メディア対応体制が不十分となる恐れがあるためである。

なお、雛型に例示するとおり、それぞれの担当については、連絡がとれない可能性を考慮し、必ず代行者を合わせて定めること。

（3）検討に当たっての留意事項

ア）情報システムを復旧する責任者には情報システムの運用を継続する責任者と同じ者が就任すること

情報システムを復旧する責任者は、情報システムの復旧に係る具体的な判断・指示を行うことが求められるため、原則として平常時の責任者である情報システムの運用を継続する責任者と同一であることが望ましい。

イ）担当者の負荷を考慮した体制を構築すること

情報システムを復旧する責任者・担当者は、非常時におけるベンダとの協議、情報システムの復旧作業を承認する役割を担うほか、各部局からの情報システムの復旧に関する催促及び問合せに対応し、報告も行わなければならない。

このため、復旧作業の担当者と各部局からの連絡窓口を分離したり、IT-RTO の短いシステムの担当が特定の担当者に集中しないようにしたり、それぞれの担当者が適宜交代で休憩が可能なように配慮する等、非常時における職員の負荷を考慮し、体制を構築する必要がある。また、被災者が出た場合の経験者（OB・OG）による部外からの応援も考えておく必要がある。

2.8.2. 非常時における対応手順の作成

雛型への反映先：
「2.1 非常時の基本方針」、「2.3 非常時における対応手順（首都直下型地震）」、「2.4 非常時における対応手順（予期せぬシステム停止）」

（1）検討の目的

復旧作業に当たる担当者が、非常時に必要な実施事項を確実に抜け漏れなく実施できるようにすることを目的とする。

（2）検討内容

①情報システム復旧に係る判断基準の作成

情報システムの運用を継続する責任者は、復旧対応に必要な判断基準を定める（要員参集基準や情報システム切り替え基準等）。

②全体フローの作成

非常時の初動から復旧までの大まかな流れを決めるために、危機的事象発生から復旧までの対応の全体フローを作成する必要がある。

情報システムの運用を継続する責任者は、要員参集から情報システム復旧作業を完了させるまでの非常時の一連の流れ（全体フロー）を作成する。

作成に当たっては、各担当間の指示・報告等の情報連携のタイミングに留意する。また、全体フローには、実施事項の概要を記載するに留めるが、詳細が記載される規程類・個別手順・チェックリスト等については、参照資料として資料名を全体フロー内に記載しておくとよい。

③全体フローを踏まえた対応手順の作成

情報システムを復旧する担当者は、全体フローを踏まえ、非常時の体制で定めた担当が、それぞれどのような対応するかをより明確にした、非常時における対応手順書を作成する。対応手順を作成するに当たっては、情報システムの復旧に係る技術的な手順だけでなく、初動時の対応や、関連組織への連絡（例：メールサーバ停止時に、メールによる情報連絡が現在不可能である旨を通知する等）も含め作成する。

④（代替拠点を設置する場合）代替拠点における運用計画の作成

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

（3）検討に当たっての留意事項

ア）情報システムの迅速な復旧に配慮した必要な対応を行うこと

メールやWeb等の情報収集・共有・伝達手段、基幹LAN及びこれにアクセスするための認証基盤の復旧は、省庁全体の復旧活動の前提条件ともなりうる。このため、復旧作業を円滑に進められるよう、復旧に必要な要員の不足時には他部局からの人的支援の獲得が得られるようにしたり、近郊の宿舎を利用できるよう規程の見直しを働きかけたりする等、情報システムの復旧に関わるメンバーには、当該情報システムの目標復旧時間に応じた待遇を確保することが望ましい。

イ）非常時の情報セキュリティに配慮すること（最低限実施すべき事項）

非常時には、混乱に乗じた府省庁内への侵入等が発生する可能性もある。情報システムの運用上、適切な情報セキュリティレベルが確保されるよう配慮した計画を作成しなければならない(不正な機器の接続防止やその前提となるマシン室等への入退室管理等。可能であれば、必要な箇所に監視員を付けることも検討する)。

ウ) 情報システムベンダにも復旧体制と復旧手順書の整備を促すこと

実質の復旧作業を遂行するのは、通常保守運用を担当している情報システムベンダであることが多い。府省庁は監督責任者としての立場から、各情報システムベンダに情報システムの復旧体制と復旧手順書の整備を促すことが望ましい。

エ) 携帯用カードを作成し、所持すること

外出先等、対応手順書を所持していない状況で被災することもありうるため、非常時の初期段階で必要となる行動と連絡先を記載した携行カードを別途作成し、財布や定期入れ等の中に入れて、常に携行しておくことが望ましい。携行カードの例は、別紙. 災害用携行カードに記載する。

2.9. 教育訓練計画・維持改善計画の検討

2.9.1. 教育訓練計画の検討

雛型への反映先：「4.1.教育訓練計画」

（1）検討の目的

訓練は、災害発生時に情報システムを復旧継続する計画行動に対する担当者の理解や対応力を向上させるとともに、実施した事前対策の有効性を確認し、これらの計画や対策に改善すべき点があれば、改善活動につなげることを目的とする。

（2）検討内容

情報システムの運用を継続する責任者及び担当者は、年間で取り組む訓練の内容と対象範囲を定める（年間の教育訓練計画を作成する）。

情報システムに関わる教育訓練は、目的を踏まえ大きくは以下の３つに分類される。それぞれの内容を踏まえ訓練を計画する必要がある。

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

以下に、それぞれの訓練の詳細と例を示す。

1．平常時の情報システム運用継続計画の維持改善活動への理解の向上

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

特に、新規配属や人事異動等による担当者の変更の際に教育訓練を実施し、情報システム運用継続計画に関する基礎知識を確実に習得させ、計画の引き継ぎを確実にすることが望ましい。このため実施時期としては、例えば人事異動の 2 ヶ月以内には実施されるよう、計画に定めておくことが望ましい。

実施する教育訓練の例としては、外部の専門団体が提供している研修の利用も検討に値する。なお、業務継続（情報システムに特化したものではなく業務継続マネジメント一般）の専門家資格が習得できるものとしては、例えば以下のものが挙げられる。

表 2.9-1 事業継続に関わる外部団体と専門家資格の例

外部団体名	資格名
特定非営利活動法人 事業継続推進機構（BCAO）	事業継続管理者資格（初級・准主任・主任）
Disaster Recovery Institute International (DRII)	DRII ビジネス継続プロフェッショナル資格
Business Continuity Institute（BCI）	BCI 認定資格

2．非常時対応計画の検証と職員の危機対応能力の向上

非常時対応計画に定められる実施手順については、関係者が内容に習熟しておくとともに、計画の

内容自体に不備や改善点がないか、事前に検証しておくことが必要である。

また実際の非常時には、計画や訓練で扱った被害状況どおりの事態が発生するとは限らないため、どのような状況が発生しても適切に対応できるような、職員の危機対応能力を高める訓練を実施することが重要である。

実施する訓練の例としては、以下に例示する、机上で実施する訓練が挙げられる。

表 2.9-2 非常時対応計画の検証と職員の危機対応能力の向上を目的とした訓練の例

訓練名	訓練内容	訓練の意義／実施時の留意点
手順書 確認訓練	作成した非常時対応計画を読み合わせ、関係者間で非常時における役割や行動について、机上で互いに確認する訓練。	関係者が内容に習熟できるとともに、手順の内容の抜け漏れを確認できることから、非常時対応計画を作成した後、関係者内で実施する必要がある。
シナリオ 非提示型訓練	参加者に訓練シナリオ（非常時において発生する被害状況と対応手順）を訓練前に通知せず、訓練時に発生した被害状況のみ提示し、参加者に対応させる訓練。	事前に訓練シナリオを通知し、定めた対応手順どおりの対応を促す訓練と比べ、発生する被害状況に対する能動的な意思決定を参加者に対して促すことが可能となる。

実施時期の例としては、防災週間や防災訓練実施日、大規模な自然災害・事故の発生日等に合わせることが考えられる。

3．事前対策内容の動作確認と検証

事前対策の一環として実施したバックアップや構築した代替環境については、被災時に期待どおりに機能・動作するか、定期的に訓練を通し確認・検証をしておくことが必要である。

初期に一度動作確認のテストを実施し、機能・動作することを確認している場合でも、年数の経過や情報システムを継続的に運用管理している中で、意図したとおりに復旧できなくなってしまうケースがある。例えば、システムの導入当初と比べ、扱うデータ量が増えたことで想定時間内にリカバリできなくなるケース、OS・機器構成の変更によりリカバリできなくなるケース、当該システムのリカバリ手順に詳しい要員の人事異動によって詳細なリカバリ手順が不明確になりリカバリできなくなるケース等が挙げられる。

以上のような原因がもとで、被災時に情報システムの復旧が長期化する、また最悪の場合には復旧ができない、ということがないように定期的に訓練を実施する必要がある。訓練の実施によって、担当者のリカバリ作業の習熟も同時に図ることができる。

実施する訓練の例としては、以下に例示する実機を用いた訓練が挙げられる。

表 2.9-3 事前対策内容の動作確認・検証を目的とした訓練の例

訓練名	訓練内容	訓練の意義／実施時の留意点
システム リカバリ訓練	実機を用い、バックアップしているデータから実際にシステムをリカバリする訓練。	訓練実施に当たっては、既存の開発機を活用したり訓練機を調達したりする等、本番環境での情報システム運用に影響が出ないよう配慮する必要がある。
システム 切り替え訓練	実際に本番機から代替機への切り替えが可能か確認する訓練。代替機が存在する場合に実施する。	訓練実施を休日に設定する等、訓練後の通常運用への切り戻し作業の時間も踏まえ、訓練の実施スケジュールを検討することが望ましい。

実施時期の例としては、防災週間や防災訓練実施日、大規模な自然災害・事故の発生日等に合わせることが考えられる。

（3）検討に当たっての留意事項

ア）手順書の確認訓練を優先的に実施するよう計画すること（優先的に実施すべき事項）

情報システムは特に短時間での復旧が求められることが多い。よって、非常時の各責任者・担当者は、非常時対応計画の内容を十分に理解し、迅速な対応を取れるようにすることは極めて重要である。

このため、手順書の確認訓練は定期的に実施されるよう、教育訓練計画に含めることが望ましい。

イ）システムリカバリ訓練を優先的に実施するよう計画すること（優先的に実施すべき事項）

平常時バックアップを取得していても、そのバックアップから本当にデータを復旧できるのかについては、検証がされていないケースが多い。非常時にバックアップからデータを復旧できない場合、システムが復旧困難となる恐れもあることから、バックアップからデータが復旧できることを確認する訓練（システムリカバリ訓練）は、定期的に実施されるよう、教育訓練計画に含めることが望ましい。

ウ）訓練は段階的に高度化するよう計画すること

非常時には様々な対応が求められる。このため、一度に全ての必要事項を網羅的に扱う訓練を実施することは不可能である。各年度の訓練を実施するに当たっては、府省庁の実力（理解度、対策の進捗状況等）をみながら、対象とする危機的事象・情報システム・非常時の対応事項等について、優先順位の高いものから段階的に取り組んでいくよう、計画を作成することが望ましい。

例えば、比較的初期に実施する訓練としては、非常時の対応体制に定められる担当者が手順書の読みあわせを行う訓練等が考えられる。より高度な訓練の例としては、非常時に対応可能な要員を増やすことを目的とし、非常時の対応体制に定められた以外の職員も訓練の対象者とすることや、各種訓練を組み合わせて、人の移動と情報システムの切り替えを組み合わせた総合訓練を実施すること等が考えられる。

エ）訓練計画時の留意点

訓練に当たっては、訓練内容について予め周到に計画・準備をした上で実施することが望ましい。必要な計画・準備すべき事項はそれぞれの訓練の内容によって異なるが、例えば以下の要素が計画・準備に含まれているか、確認することが必要である。

- 訓練実施体制（ファシリテーター・評価者等の運営側の体制）
- 目的と内容（実施する教育訓練の目的と内容）
- 対象範囲（対象システム、初動・復旧等の対象範囲）
- 訓練シナリオ（危機的事象や被災状況等）
- 対象者（情報システムベンダの参加の有無等）
- 評価指標と完了条件（結果評価のための指標と完了条件）
- 実施スケジュール（当日のタイムスケジュール）
- 実施方法（証跡取得方法、評価データの収集方法、トラブル発生時の対応方法等）
- 事前準備事項（教育訓練実施に向けて必要な準備事項、事前準備のスケジュール等）

2.9.2. 維持改善計画の検討

雛型への反映先：「4.2.維持改善計画」

（1）検討の目的

維持改善計画は、事前対策計画、非常時対応計画、教育訓練計画それぞれを定期的に見直し、情報システム運用継続計画の実行性を継続的に維持できるよう検討する。維持改善計画を着実に実施して、定期的に全体を確認できるようにすることが重要である。

（2）検討内容

情報システムの運用を継続する責任者は、情報システム運用継続計画の見直し時期・見直し内容・実施主体を検討する。

見直し内容としては以下の例が考えられる。

見直し事項	見直し内容（例）
事前対策計画	• 計画に基づき、事前対策は確実に実施されたか。 • 完了した事前対策を踏まえ、情報システム運用継続計画の見直しを行ったか（現状対策レベル、事前対策計画、その他計画については後述）。 • 事前対策計画に基づき、来年度予算で取り上げる対策を検討したか。また実施未定の対策について予算化を検討したか。 • 訓練の結果を踏まえて計画の見直しを行ったか。
非常時対応計画	• 連絡網や担当者は最新化されているか。 • 実施完了した事前対策がある場合、対応手順を適切に見直したか。 • 訓練の結果を踏まえて計画の見直しを行ったか。
教育訓練計画	• 計画に基づき、訓練は確実に実施されたか。 • 訓練結果を踏まえ、情報システム運用継続計画の見直しを行ったか。
計画策定の根拠とした分析・策定・検討	• 情報システム運用継続計画の策定対象範囲を広げることを検討したか。 • 外部環境の変化や社会的な要求の高まり等により、情報システム運用継続計画の見直しの必要性を検討したか。 • 新しい情報システムが追加された場合、システム復旧優先度の設定や必要な事前対策計画、非常時対応計画及び教育訓練計画を検討したか。 • 最新の技術動向に基づき、目標対策レベルの見直しの必要性を検討したか。

（3）検討に当たっての留意事項

ア）定期的な確認の時期について

見直しの結果、新たな事前対策の実施が必要となる等、予算要求の必要性が生じる可能性もある。このため、見直し時期としては、予算編成の検討時期を踏まえ設定することが望ましい（4月～5月等）。

イ）情報システム運用継続計画の策定・運用プロセスを、既存の情報システム企画開発・運用プロセス内に組み込むこと

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

別表 1. 優先的に取り組むべき対策一覧（首都直下型地震）

構成要素	実施内容	対策例	留意事項
施設	＜建屋＞ 重要システムの設置されている建屋の耐震性能を確保すること。	・耐震性能の高い拠点への移設、代替環境の構築	■代替環境設置対象のシステムを絞ること ・費用対効果の観点から、まずは復旧優先度の高いシステムを明確化した上で、該当システムを代替環境に設置することが望ましい。 ■代替環境設置時は、立地条件に留意すること ・代替環境の立地については、地震や津波等のリスクが低い地域、かつ、本番センタと同時被災しない地域が望ましい。 ・また、災害発生時に代替環境へシステム担当者が駆けつける必要がある場合は、本番サイトから駆けつけ可能な距離であることが求められる。 ■代替環境の平時の有効活用を考慮すること ・代替環境を採用する場合、平時の有効活用（メールやストレージのデータの保存先として利用する等）も考慮することが望ましい。
	＜電源＞ 非常時のシステム運用に必要な自家発電能力を確保すること。	・自家発電を管理する部局との間で、システム運用に割り当てられる自家発電能力を確認の上、必要な発電能力を確保	■管轄省庁と調整の上推進すること ・合同庁舎の場合は、管轄省庁と調整の上推進が必要である。 ■UPS との併用を検討すること ・（特に停止が許されないシステムについては）自家発電装置が稼働する間の電力供給を考慮すると、 自家発電装置と大型 UPS の併用が望ましい。 ■電力節約に係る事前検討をしておくこと ・自家発電による運用を可能な限り継続させられるよう、電力節約のため以下を考慮することが有効である。 －非常時にも継続すべき重要なシステムを絞り込むとともに、必要な電源容量、連続稼働可能時間を明確化する。 －上記重要システム以外については運用を停止することや、自家発電によるシステム運用を一定時間に限る等の対応を、運用計画内に考慮する。 ■定期的な訓練により状況確認すること ・運用計画では、法定点検の際等に、定期的に自家発電装置が重要システムに電力供給可能なことを確認することが有効である。

	＜電源＞ システムの電源に対する必要な措置をとること。	・自家発電装置への切り替えに備えた、無停電電源装置(UPS)の準備 ・無停電電源装置(UPS)の定期的な確認	■無停電電源装置の位置付け ・無停電電源装置(UPS)は本来、瞬電等のきわめて短時間の停電に対する対策であり、その際にシステムを正常にシャットダウンさせるための設備である。したがって、計画停電時にシステムを継続運用する目的において、単体で導入することは最適な対策とは言えず、自家発電装置との組み合わせ(自家発電装置の稼動までの短期間の対策)によって有効に機能する対策である点に注意すること。 ■適切なシャットダウン設定を確実に施すこと ・バッテリー消費後にシステムが異常終了しないよう、自動シャットダウン設定を確実に施すことが有効である。 ■定期的に、電源容量が適切に確保されているか確認すること ・正常なサーバシャットダウン処理に十分な時間の電源容量を確保するよう留意する。 ・無停電電源装置(UPS)のバッテリー寿命や100%放電による性能劣化に留意する。
	＜空調＞ システム運用用の空調が非常時にも稼働するよう考慮すること。	・空調の非常用電源との接続	■被災時における電力抑制に配慮すること ・最低限の電力使用とするため、扇風機をサーバ熱源付近に設置し、空気を攪拌する等の措置も有効である。 ・サーバ室に個別空調を導入し、当該空調に非常用電源を繋げる等により、非常用電源の電力消費を抑制するよう配慮する。
	＜空調＞ 空調本体の落下等、二次被害を低減するための対策を実施すること。	・空調本体の構造躯体に対する固定措置	■空調落下の危険性を十分認識し、固定措置を施すこと ・被災時の二次的被害を低減するため、空調本体を構造躯体でない壁に固定している場合は、適切に補強措置をすることが望ましい(天井埋め込みのケースについても同様)。
	＜セキュリティ＞ 非常時における不正な機器の接続防止やその前提となるマシン室等への入退室管理について適切なセキュリティ確保の対策を実施すること。	・情報セキュリティに係る府省庁の基準の改訂(非常時の対応を検討する)	■サーバ室の施錠管理(ラックの施錠を含む)徹底すること ・被災時には、庁舎内に民間人の一次避難受け入れをすることも想定される。こうした場合、民間人への個別かつ厳密なセキュリティ管理を実施するのは現実的ではない。そこで、最低限必要な措置として、予め受け入れエリアを確保(フロアを分ける等)した上で、執務エリアには侵入できないよう制限すること、また電力喪失時に電子ロックが機能しない場合も考慮して、サーバ室への施錠管理を徹底することが必要である。

ネットワーク	府省庁内 LAN を早期に復旧できる対策を実施すること。	・各種ネットワーク設定ファイルの定期的なバックアップ	
		・耐火性・耐震性のある保管庫への定期的保管や同時被災しない拠点への外部保管	
		・ルータやハブ等の予備品確保	■被災時の調達は困難なことに留意すること ・予備の LAN ケーブルやハブ等の保管に当たっては、その保管場所(耐震固定された什器や、壁際等の崩れやすい場所をさける等)を考慮することが有効である。
		・障害発見を迅速に行うためのネットワーク障害監視の仕組みを導入	■被災地の負荷低減に留意すること ・連絡手段の途絶により、被災地からは被害状況を確認することが困難な状況となる。このため、非被災地から各拠点のネットワークの被害状況を一括で確認できるような仕組み(ネットワークマネジメントシステム)の導入が有効である。
	被災時に LAN 切断の可能性を低減させる対策を実施すること。	・LAN の冗長化 ・冗長化した LAN の経路考慮(東回りと西回りで LAN を敷設する等)	
	被災時に LAN が不通になる可能性を低減させる対策を実施すること。	・無線 LAN の活用	■セキュリティの確保に考慮すること ・政府機関の情報セキュリティ対策のための 統一基準及び統一技術基準に遵守したルール作り(被災時に無線LAN利用をするためのルール)と環境構築(暗号化や接続制限等)が必要である。
	拠点間をつなぐアクセス回線やバックボーンの停止する可能性を下げる対策を実施すること。	・アクセス回線の冗長化 ・キャリアの分散	■ネットワーク回線の冗長化に当たっては、経路や引込口の冗長化を考慮すること ・キャリアを分ける(マルチキャリア化する)、又は異なる通信サービスを選択することが有効である。 ・ネットワーク回線を冗長化し、キャリアを分散していても物理的に同一のケーブルを通っていれば、災害時には両回線とも切断されてしまう可能性がある。ネットワークの冗長化に当たっては、物理的な経路や建屋への引込口を分ける等の対応が有効である。

周辺機器	周辺機器の被害を低減させる対策を実施すること。	・転倒防止措置の実施	■機器に転倒防止措置を施すこと ・サーバのコンソールPC等についても、落下防止措置をすることが有効である。 ・複合機等は重量も重く、地震の揺れによる倒壊やフロア内の移動等により、凶器になる。したがって、複合機やプリンター等についても固定措置しておくことが有効である。
	情報漏えいの可能性を低減させる対策を実施すること。	・データの暗号化 ・廃棄時の適切な処理	■外部損傷(水損含む)による故障の場合、データ復旧の可能性があることを考慮した措置をとること ・外付けHDD等については、日常からデータの暗号化を徹底することが望ましい。 ・外部損傷による故障の場合、データ復旧の可能性があるため、廃棄(リースの場合は返却)ルールに従って適切に処理すること。また、個別に廃棄する際には物理的措置(ドリルで穴を開ける等)が望ましい。
ハードウェア	再調達が不可能、もしくは長期間を要するハードウェアを確認し、必要な対策に取り組むこと。	・旧システム入替の検討	
		・ハードウェアを利用するシステムや業務について、同様のサービスを提供できる企業・団体へのアウトソーシングや、非常時のみ業務を委託する事前契約	
	地震発生時もハードウェアへの被害を最小限に抑える対策を実施すること。	・サーバラックの耐震補強・免震措置	■サーバラックが転倒しにくい措置をとること ・重い機器はラックの下層部におく、ラック同士を連結する等、ラックが倒れにくいように配慮することが有効である。 ・ラックに固定されていない機器については確実に固定し、ラックからの飛び出しによる損壊を防止することが有効である。 ■サーバラックの免震には対策の併用が有効である。 ・免震措置の際は、耐震架台との組み合わせが有効である。 ・また、免震ラックが正しく機能するように、免震装置の移動範囲を考慮し周囲を整理整頓しておくことが必要である。 ■自拠点に合わせた耐震強化策を検討すること ・フリーアクセスフロア自体の耐震強化でなく、サーバラックをビルの床スラブに固定することで、耐震性を強化することも可能なため、自拠点の状況に合わせた耐震強化策を検討することが有効である。

システム領域／データ領域	データ消失を回避するための対策を実施すること。	バックアップの取得	
		・耐火性・耐震性のある保管庫への定期的保管や同時被災しない拠点への外部保管	■ネットワーク経由での伝送も検討すること ・バックアップの手段は、外部媒体の輸送が安価ではあるが取り寄せ時に日数を要するため、ネットワーク経由での伝送を検討することが有効である。
	バックアップの適切な頻度を検討すること。	・各データの更新頻度に応じた現状のバックアップ頻度の適正化	
	バックアップのリカバリテストを実施すること。	・バックアップとして取得したデータを、実際に利用できるかリカバリテストの実施	
	バックアップの実施によって新たに発生する恐れのある情報セキュリティ上の脆弱性に対し、対策を実施すること。	・バックアップデータに対するデータ暗号化及びデータ改ざん防止措置 ・ネットワークの暗号化 （いずれも情報セキュリティに係る府省庁の基準に則り、適切に実施する）	
システム運用体制	担当者が出勤できない場合の対応手段を講じること。	・ネットワークの遠隔監視手段の整備	■非被災地からも被害状況を確認できるようにすること ・連絡手段の途絶、交通機関の停止により、被災地からは各地の被害状況を把握することは困難である。また、建屋に入館できない場合も考えられる。円滑な復旧対応のため、非被災地から被災地の被害状況を確認できる仕組みを導入することが有効である。
	迅速な安否確認を可能にするための対策を実施すること。	・緊急連絡網の整備 ・安否確認システムの導入	■安否確認システムは日頃から訓練すること ・安否確認システムについては普段より訓練と周知を繰り返し、登録者数を上げることが重要である。 ・被災時に円滑に安否を確認するためには、安否確認システムへの未登録者を一覧で整理しておくことが有効である。

迅速な情報共有のための対策を実施すること。	・Web 会議システム・TV 会議システム	■被災時に速やかに使用できるようにすること ・Web 会議システムは多地点同時接続による情報共有が可能であり、意思決定のスピードアップが見込まれる。留意事項として、被災時に速やかに使用できるように、システムを使った訓練(他拠点の接続テストや対策本部への設置練習等)を実施することが望ましい。 ・回線の冗長化(マルチキャリア化)についても考慮することが望ましい。
	・(クラウド等を利用した)待機系電子メールサービス	■被災時に速やかに使用できるようにすること ・システム障害や停電、災害等でメールシステムが運用できなくなった際に、クラウド等を利用した待機系システムに切り替えることでメールアドレスのドメインを切り替えることなく、職員用メールシステムの運用継続が見込まれる。自宅待機を余儀なくされた場合でもインターネット環境があれば利用可能であり、長期の災害時の連絡手段として有効である。 ・災害時の利用を許可するセキュリティポリシー等規定の整備が必要である。
	・ローカル PC 等を使った簡易システムによる業務代替戦略	■システムは止まるという前提のもと、全停止した際でも業務継続に寄与する、IT の利用方法を検討すること ローカル PC 等の表計算やデータベースソフトを使用した最低限の業務を代替する簡易システムが準備されていることにより、広い範囲に被害が及ぶ大災害時に、外部とのネットワークが遮断された状態においても、最低限の業務を継続することができる。 ・システムが全停止した際に復旧まで間、最低限必要な業務を効率的に継続させるといった観点から、範囲を絞り、シンプルかつ使いやすい仕組みを検討しいくことが望ましい。
情報システム復旧のための体制と役割分担を整備すること。	・非常時体制の整備	■参集不可と交替勤務に備え、必ず代行者を定めること ・連絡手段の途絶や交通機関の停止により、システム担当者と長時間連絡がつかない状況も予想されるため、代行者を必ず決めておくことが重要である。また災害時の対応は長期に渡ることが予想されることから、対応要員が交替で対応に当たることを考慮し、代行者の人数を定めることが有効である。
情報システム復旧のための手順を作成すること。	・非常時における対応手順書の整備	■非常時における対応手順書は定期的に最新化すること ・非常時における対応手順書は最新化しやすいよう、構造的に作成することが有効である(頻繁に更新の入る文書については添付資料にする等)。

	非常時に利用する備品類を確保し、迅速な対応を可能にすること。	・固定電話・携帯電話不通時の連絡手段の確保（衛星電話、広域無線）	■定期的にメンテナンスすること 緊急連絡時の固定電話や携帯電話以外の日常的に使用しない通信手段（衛星電話や広域無線等）については訓練を定期的に実施し使用方法や電波状況等を確認する他、バッテリー等の消耗品について定期的にメンテナンスしておくことが必要である。
ベンダの継続能力	早期にシステムを復旧するために、必要に応じベンダとの契約を見直すこと。	・情報システムベンダとの保守契約の見直し、非常時の対応内容の明確化等	■外部ベンダとの契約内容を把握しておくこと ・外部ベンダとのSLA契約を確認し、災害時の対応がオプションになっていないか、適切な参集時間が設定されているか等、把握しておくことが有効である。 ■外部ベンダとの連絡手段を定めておくこと ・緊急連絡網を整備する他、重要な外部ベンダについては広域無線や衛星携帯電話の相互確保による連絡も検討に値する。 ■外部ベンダの事業継続能力を確認しておくこと ・契約の見直しまで踏み込みが難しい場合は事業継続への取組について外部ベンダに質問するアンケートを配布する等して、ベンダ側の事業継続への取組を促すことが有効である（再委託しているケースについては、下請け先が漏れていないか注意すること）。