資料６－２

政府機関等における
情報システム運用継続計画
ガイドライン
～（第３版）～

令和３年４月

内閣官房 内閣サイバー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例一覧等を追加
3	令和3年4月	第3版作成 ・「技術動向の変化」及び「感染症の流行」に係る内容を追加 ・利便性向上を目的にガイドラインの構成を改善 ・政府機関等の情報セキュリティ対策のための統一基準群に基づきガイドラインの対象組織を見直し

目次

1 はじめに 4
1.1 ガイドラインの位置づけ 4
1.1.1 ガイドラインの目的 4
1.1.2 ガイドラインの構成と利用方法 5
1.1.3 ガイドラインの適用範囲 5
1.1.4 参考資料について 5
1.1.5 策定した計画の取扱いについて 6
1.2 情報システム運用継続計画の策定・運用の流れ 7
2 各作業の進め方及び留意事項 9
2.1 基本方針の決定 9
2.2 策定・運用体制の構築 10
2.3 危機的事象の特定 12
2.4 被害想定 14
2.5 情報システムの復旧優先度の設定 17
2.5.1 非常時優先業務と情報システムの関連整理 17
2.5.2 情報システムの復旧優先度の設定 18
2.6 情報システム運用継続に必要な構成要素の整理 20
2.6.1 情報システムを支える構成要素の明確化 20
2.6.2 情報システムを支える構成要素ごとの目標対策レベルの設定 22
2.7 事前対策の計画とその実施 25
2.7.1 現状の対策の確認及びリスクの評価 25
2.7.2 事前対策計画の策定とその実施 28
2.8 危機的事象発生時の対応計画の検討 30
2.8.1 危機的事象発生時の体制構築 30
2.8.2 危機的事象発生時における対応計画 33
2.9 教育訓練・維持改善の計画とその実施 35
2.9.1 教育訓練の計画とその実施 35
2.9.2 維持改善の計画とその実施 38

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

「政府機関等における情報システム運用継続計画ガイドライン」は、ガイドライン（以下「本書」という。）、付録で構成される。本書は、政府機関等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、計画の実施と継続的維持改善を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、大規模災害、情報セキュリティインシデント及び感染症の流行（以下「危機的事象発生時」という。）による影響等によって情報システムの運用が中断又は途絶するときに、情報システムを継続又は復旧させることにより、その利用に係る影響を最小限に抑えるために必要な計画群の総称を指し、政府機関等の業務継続計画における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]。情報システムが機能しない場合の業務における代替策の実施については、政府機関等で定められた業務継続計画に策定されている等、業務継続計画と情報システム運用継続計画の整合性を確保することが重要である。

近年の業務においては情報システムの利用が必須であり、何らかの危機的事象を原因として情報システムの停止や誤作動が生じた場合、非常時優先業務 [2]の継続が困難となり、初動対応業務にも深刻な影響が生じることとなる。政府機関等の業務継続計画に定められている非常時優先業務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、必要な計画を事前策定し継続的に維持改善を行うこと、危機的事象発生時に同計画に沿って適切に対処することは、情報システム担当者の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）」において、「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。」旨が示された。このような背景を鑑み、本書は政府機関等の情報システム運用継続計画に含めるべき事項を具体的に示し、政府機関等がその組織の経済活動において国民の安全や利益に重大な脅威をもたらす「情報システム停止」から「その事後対応」までを考慮した、適切な計画を整備できるようにすることを目的とする。

本書は、第2版における首都直下型地震を想定した対策として追加・拡充された内容に加え、情報セキュリティインシデント発生時の対応やクラウドサービス等の外部サービスの技術動向に係る内容及び新型コロナウイルス感染症の流行を踏まえ、感染症の流行を想定した対策に関する内容を追加・拡充している。首都直下地震に係る検討に際しては、内閣府（防災担当）が公開している「中央省庁業務継続ガイドライン第2版（首都直下地震対策）」（平成28年4月）を、感染症対策に係る検討に際しては、内閣官房新型コロナウイルス感染症対策推進室が公開している「新型コロナウイルス感染症対策の基本的対処方針」（令和2年3月28日）（令和2年5月25日変更）、及び内閣官房新型インフルエンザ等対策室にて公開している「新型インフルエンザ等対策ガイドライン」（平成30年6月）、「新型インフルエンザ等対応中央省庁業務継続ガイドライン」（平成26年3月）等も併せて参考にされたい。

---

[1] 本書で策定を推奨する情報システム運用継続計画は、政府機関等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（不正プログラム感染やサービス不能攻撃による情報セキュリティインシデント）への計画も含むものであり、政府機関等の業務継続計画より広い範囲を対象としたものとなる。

[2] 本書における「非常時優先業務」とは、危機的事象発生時において組織が優先的に実施する業務を指す。「中央省庁業務継続ガイドライン」における非常時優先業務及び「新型インフルエンザ等対応中央省庁業務継続ガイドライン」における発生時継続業務等も該当する。

1.1.2 ガイドラインの構成と利用方法

本書は、政府機関等の担当者が情報システム運用継続計画を作成する際の検討手順や留意点を取りまとめた文書である。策定の流れに則り、別冊「付録」を参考に追記・修正することで同計画をスムーズに策定できるような構成となっている。

また、政府機関等に既に同種の計画が存在する場合には、本書内容を確認の上、既存計画の不足点や改善点等について追加修正すればよく、新たに情報システム運用継続計画については策定し直す必要はない。

なお、本書の記載内容全ての遵守を求めるものではなく、検討事項の目的を鑑み、情報システムの運用継続に必要な対策を実施されたい。

1.1.3 ガイドラインの適用範囲

本書では、危機的事象発生時における政府機関等の内外との連絡手段の確保を最低限実施する事項ととらえ、政府機関等の担当者がメールやWeb、SNS等の情報収集・共有・伝達手段、基幹LANや外部サービス及びこれらにアクセスするための認証基盤等についての運用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、記載し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、本書を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、非常時優先業務を支える全情報システムにおいて、要否を含めて整合性が図られている必要がある。

1.1.4 参考資料について

本書の利用に当たっては下記の資料を事前に確認しておくことが望ましい。

表 1.1-1 ガイドライン利用にあたっての参考資料一覧

文書名	発行年月	発行者	備考
中央省庁業務継続ガイドライン（第2版） http://www.bousai.go.jp/taisaku/chuogyoumukeizoku/index.html	平成28年4月（最新版を参照とする）	内閣府防災担当	遵守事項
○○業務継続計画 （※○○には政府機関等の名称が入る）	（政府機関等の取組時期による）	政府機関等	遵守事項
政府機関等の情報セキュリティ対策のための統一基準群 https://www.nisc.go.jp/materials/index.html	平成30年7月（最新版を参照とする）	サイバーセキュリティ戦略本部	遵守事項
○○情報セキュリティポリシー （※政府統一基準群に準拠して策定した政府機関等基準の文書名を記す）	（政府機関等の取組時期による）	政府機関等	遵守事項
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） https://www.nisc.go.jp/inquiry/	平成24年3月	内閣官房情報セキュリティセンター	推奨事項
政府情報システムにおけるクラウドサービスの利用に係る基本方針 https://cio.go.jp/guides	平成30年6月（最新版を参照とする）	各府省情報化統括責任者（CIO）連絡会議決定	推奨事項
IT-BCP 策定モデル https://www.nisc.go.jp/active/general/pdf/IT-BCP.pdf	平成25年6月（最新版を参照とする）	内閣官房情報セキュリティセンター	参考資料

文書名	発行年月	発行者	備考
東日本大震災を踏まえた政府機関における情報システムの運用継続に向けた対処要件等に係る調査　対処要件の一覧と個別対策例 https://www.nisc.go.jp/active/general/pdf/kobetu-taisaku.pdf	平成25 年6 月（最新版を参照とする）	内閣官房情報セキュリティセンター	参考資料
新型インフルエンザ等対策ガイドライン https://www.cas.go.jp/jp/seisaku/ful/keikaku.html	平成30 年6 月	新型インフルエンザ等及び鳥インフルエンザ等に関する関係省庁対策会議	参考資料
新型インフルエンザ等対応中央省庁業務継続ガイドライン https://www.cas.go.jp/jp/seisaku/ful/keikaku.html	平成26 年3 月	新型インフルエンザ等及び鳥インフルエンザ等に関する関係省庁対策会議	参考資料
JIS Q 22301:2020（ISO 22301:2019） セキュリティ及びレジリエンスー事業継続マネジメントシステムー要求事項 https://www.jisc.go.jp/app/jis/general/GnrJISSearch.html	令和2 年11 月	経済産業省 日本産業標準調査会	参考資料

本書では、「中央省庁業務継続ガイドライン（第 2 版）」を、以下「中央省庁業務継続ガイドライン」といい、「政府機関等の情報セキュリティ対策のための統一基準群」を、以下「政府統一基準群」という。

1.1.5 策定した計画の取扱いについて

策定した情報システム運用継続計画は、計画の管理部署、担当者及び保管先を事前に決定し、政府機関等及び国民の安全や利益に重大な脅威をもたらす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できるようにする。また、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ため、保管先を複数箇所とすること（電子媒体と紙媒体の両方による保管、複数箇所への保管、及びクラウドサービス等の外部サービス [1]を利用した保管等）も検討することが望ましい。

なお、情報システム運用継続計画の検討に当たっては、適宜政府機関等の情報セキュリティポリシーを参照するとともに、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。

また、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] クラウドサービス等の外部サービスを利用する際には、政府機関等の対策基準策定のためのガイドライン（平成30 年度版）4.1.4(1)「クラウドサービスの利用における対策」遵守事項、基本対策事項及び解説を参照されたい。
※今後、廃止又は変更される可能性があるため、最新版を確認した上で利用すること。

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・運用の流れの例を以下に図示する。

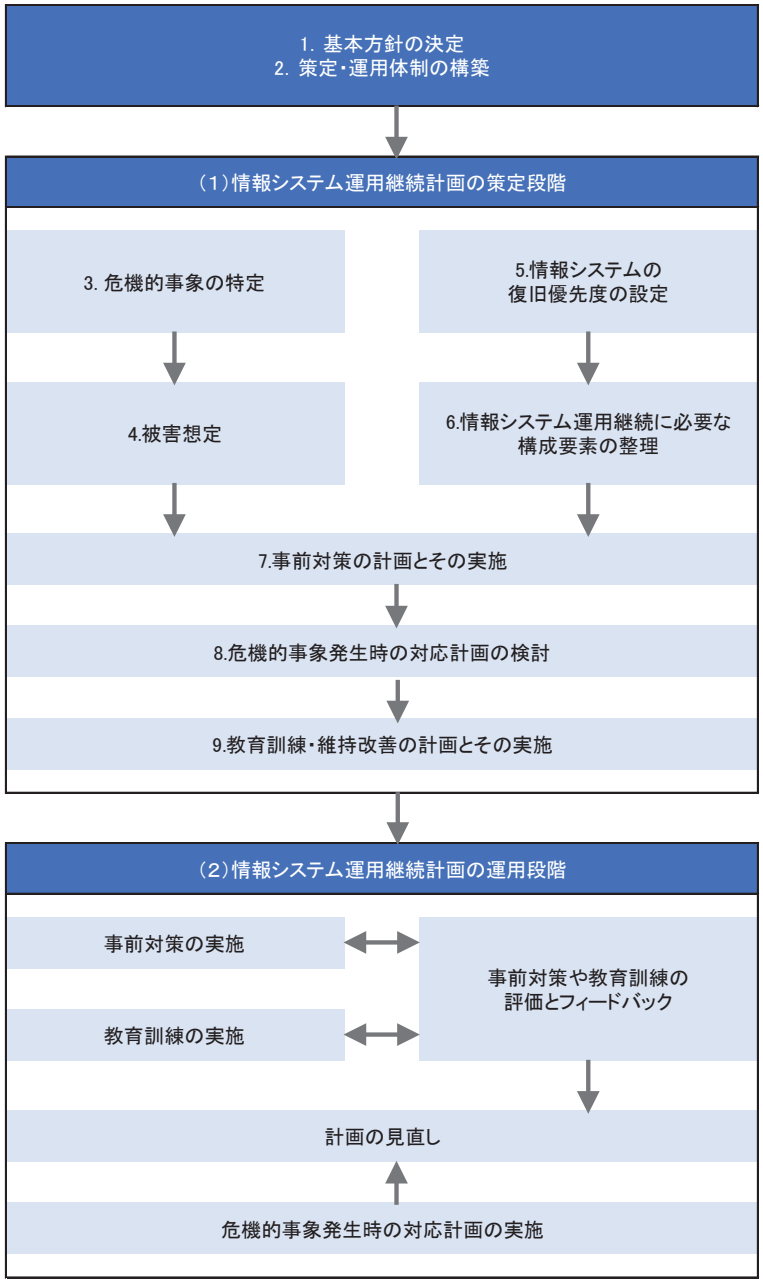

図 1.2-1 情報システム運用継続計画策定・運用の流れ

情報システム運用継続計画の策定段階

本書の「2 各作業の進め方及び留意事項」以降では図 1.2-1 の（1）情報システム運用継続計画の策定段階について記載する。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	本書の項番
1	基本方針の決定		計画の適用範囲及び基本方針を定める。	2.1
2	策定･運用体制の構築		計画の策定・運用に係る体制を構築する。	2.2
3	危機的事象の特定		計画の対象とする危機的事象を調査・検討し、特定する。	2.3
4	被害想定		危機的事象が発生した場合の情報システムの被害状況を想定する。	2.4
5	情報システムの復旧優先度の設定			2.5
	①	非常時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の関連性を整理する。	2.5.1
	②	情報システムの復旧優先度の設定	非常時優先業務の目標復旧時間と、情報システム停止時の影響や代替手段を踏まえ、情報システムの復旧優先度を設定する。	2.5.2
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	危機的事象発生時に必要な情報システムを支える構成要素を整理する。	2.6.1
	②	情報システムを支える構成要素ごとの目標対策レベルの設定	情報システムを支える構成要素ごとに、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。	2.6.2
7	事前対策の計画とその実施			2.7
	①	現状の対策の確認及びリスクの評価	情報システムの構成要素ごとに、現状の対策を確認し、リスクの評価を実施し、情報システムの運用継続に係るリスクを整理する。	2.7.1
	②	事前対策計画の策定とその実施	リスクの評価を踏まえ、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。	2.7.2
8	危機的事象発生時の対応計画の検討			2.8
	①	危機的事象発生時の体制構築	危機的事象発生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体制・役割を決定する。	2.8.1
	②	危機的事象発生時における対応計画	情報システムの運用を継続させる具体的な対応方法を対応計画として整理する。	2.8.2
9	教育訓練・維持改善の計画とその実施			2.9
	①	教育訓練の計画とその実施	事前対策や危機的事象発生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。	2.9.1
	②	維持改善の計画とその実施	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。	2.9.2

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「教育訓練計画」及び「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、危機的事象の発生を踏まえ、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において、適宜各種計画（図 1.2-1 の（1）情報システム運用継続計画の策定段階で策定した各計画）の見直しを行う。

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・運用の流れに沿って、以下に各検討の目的・趣旨、検討事項、考え方について例示を交えて記載する。例示を参考に、各政府機関等での検討を実施されたい。

2.1 基本方針の決定

目的・趣旨

政府機関等は情報システム運用継続計画の基本方針・適用範囲を決定する。

検討事項

(1) 情報システムの運用を継続する最高責任者[1]及び責任者[2]は、情報システム運用継続計画の適用範囲、優先的に対策に取り組む情報システム等、基本方針について定める。

(2) 新規に情報システムを導入する際は、情報システム運用継続計画の策定を検討する。

【考え方】

<2.1(1)関連>

2.1(1)-1 情報システム運用継続計画の適用範囲の決定に際しては、国民の生命、身体、財産の保護を最優先に考慮した上で、政府機関等の個別の事情（例えば、経済活動等に密接に関連する重要な情報システムが多い、利用頻度の高い情報システムであるために独自の方法での計画及び検討が必要等）を考慮する。

2.1(1)-2 各政府機関等で定める業務継続計画との整合性確保の視点から、情報システム運用継続計画の適用範囲には以下の点を含めるよう留意する。

a) 危機的事象発生時に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、代替拠点から各政府機関等の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こと。

b) 代替拠点に設置されている情報システムを活用する場合は、業務を実施するためにそれらが危機的事象発生時に利用可能であること。

2.1(1)-3 情報システム運用継続計画の適用範囲には、政府機関等の業務継続計画に定められた非常時優先業務を支える情報システムである、メールやWeb、SNS等の情報収集・共有・伝達手段、基幹LANやクラウドサービス等の外部サービスにアクセスするための認証基盤等を含める。基幹LAN及び認証基盤等が政府機関等において共用されている場合は、業務連携、影響度及びパフォーマンスについても考慮する。

2.1(1)-4 情報発信、共有を行っている情報システムが利用できなくなった際には、テレビやラジオ等のメディアといった手段も政府機関等の業務継続計画に定められた非常時優先業務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る。

<2.1(2)関連>

2.1(2)-1 新規の情報システム導入時には、情報システム運用継続計画作成の必要性を検討し、作成する場合には本書の検討プロセスを実施し、検討結果を調達仕様書に盛り込むことに留意する。また、危機的事象発生時に情報システムの運用を継続する担当者が対応できない場合を想定し、情報システムの運用業務の遂行手段の多様化（オンサイト、オフサイト）及び自動化も考慮する。

---

[1] 情報システムの運用を継続する最高責任者とは、情報システムの運用継続計画の策定及び運用に関する事務を統括する者をいう。組織全体での業務継続と優先順位の観点から、情報システムの運用継続に関する意思決定ができる者を充てること。

[2] 情報システムの運用を継続する責任者とは、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。本書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場合は、当該体制・枠組みにおいて該当する者を充てること。

2.2 策定・運用体制の構築

目的・趣旨

情報システム運用継続計画の策定及び運用を推進する体制を整備する。

検討事項

(1) 情報システムの運用を継続する最高責任者は、情報システム運用継続計画の策定及び運用を推進する体制を整備し、策定の検討及び運用において監督及び指示等を行う。

(2) 情報システムの運用を継続する責任者は、情報システムの運用継続に必要な担当者を定める。

(a) 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、政府機関等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。

(3) 情報システムの運用を継続する最高責任者及び責任者は、政府機関等の業務継続計画と情報システム運用継続計画との整合性を考慮する。また、情報システムの運用継続計画及び情報セキュリティ関係規程のそれぞれで定める対策に矛盾があると、危機的事象発生時に職員等は一貫性のある行動をとることができないため、情報システムの運用を継続する最高責任者及び責任者は、情報セキュリティ管理の観点からも検討する。

【考え方】

<2.2(1)関連>

2.2(1)-1 情報システムの運用を継続する最高責任者は、情報システムの運用を継続する責任者及び担当者に対して、組織全体及び業務継続の観点から監督及び指示等を行う。

<2.2(2)関連>

2.2(2)-1 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適用範囲を踏まえて必要な担当者を定める。また、各部署との連携体制を構築する。

2.2(2)-2 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。

a) 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・運用に幹部層を含めた必要な要員を定めること。各部署のシステム担当者が検討に加わる場合には、判断基準や指示命令系統の調整等や委託先等の関係者との連携方法を調整すること。

b) 危機的事象発生時の情報システム運用継続に当たって、担当者が対応できない場合を想定し、担当者の代行要員（必要な人数及び必要な経験・資格等所持者の確保を含む）、交代勤務を考慮したチーム編成等を含めた体制を検討すること。

c) 政府機関等の業務継続計画の推進体制がある場合、情報システムの運用を継続する責任者は参画すること。

<2.2(3)関連>

2.2(3)-1 情報システム運用継続計画を策定・運用する上で、政府機関等の業務継続計画との整合性を確保する。

2.2(3)-2 危機的事象発生時においては、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ることから、両者の間では特に事前の整理と、危機的事象発生時における情報セキュリティに係る対策事項[1]を検討することに留意する。

2.2(3)-3 危機的事象発生時に情報システムの運用を継続させるために適用する例外措置があることを想定し、平常時の情報システム運用手順において確認するプロセスを盛り込む等、例外措置が常態化しない仕組みを導入する。

[1] 危機的事象発生時における情報セキュリティに係る対策事項については、政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）5.3.1(1)「情報システムの運用継続計画の整備・整合的運用の確保」遵守事項、基本対策事項及び解説を参照されたい。※今後、廃止又は変更される可能性があるため、最新版を確認した上で利用すること。

(例示)

<2.2(1)関連>

- 情報システムの運用を継続する最高責任者が情報システム運用継続計画の策定及び運用において監督及び指示等を行う際は、下記を例とする観点を考慮することが重要である。
  - 国民の生命、身体、財産への影響
  - 政府機関等の個別の事情（経済活動等に密接に関連する重要な情報システムが多い等）
  - 政府機関等の業務継続計画との整合性
  - 政府機関等の人材、財源等の資源等（策定及び運用に利用できる人材及び予算の確保等）

<2.2(2)関連>

- 情報システム運用継続計画の策定・運用推進体制及び各担当の役割の例を下記に示す。政府機関等の組織構造等に応じた体制構築や役割分担を実施されたい。

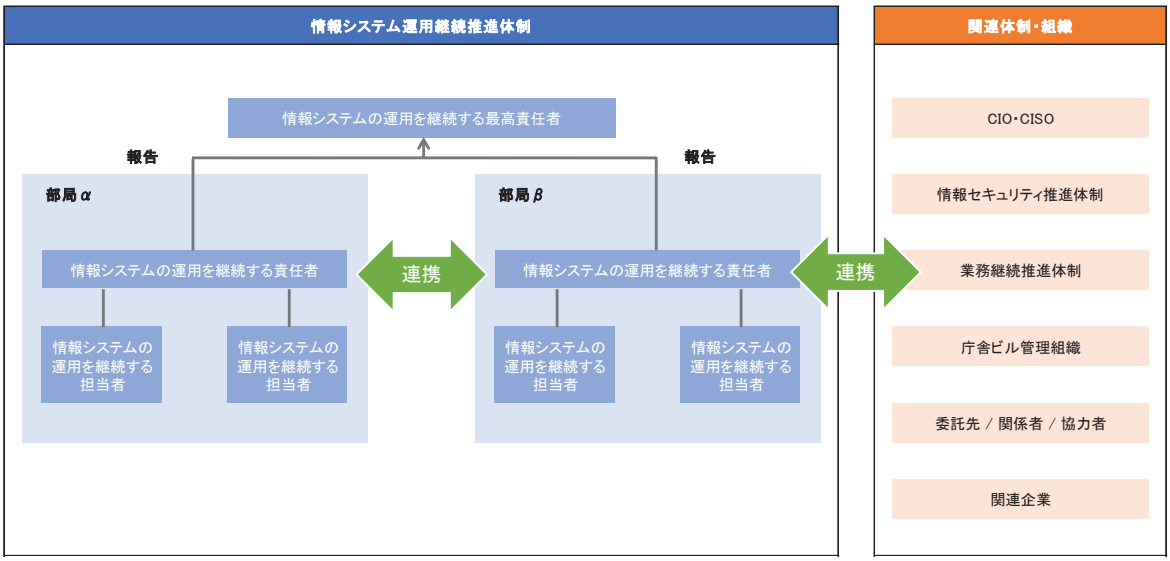

図 2.2-1 情報システム運用継続計画の策定・運用推進体制（例）

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	情報システム運用継続計画の策定・運用全般を統括し、最終的な責任を負う。
情報システムの運用を継続する責任者	所管する情報システムに係る情報システム運用継続計画の策定・運用を統括する。
情報システムの運用を継続する担当者	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。

<2.2(3)関連>

- 情報システムの運用を継続する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。

2.3 危機的事象の特定

目的・趣旨

情報システムが曝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危機的事象を特定する。

検討事項

(1) 情報システムの運用を継続する最高責任者及び責任者は、情報システム運用継続計画の対象とする危機的事象を特定する。
  (a) 対象とする危機的事象は、発生時の影響の大きさ、発生の確率、政府機関等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する。
  (b) 危機的事象発生時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。

(2) 情報システムの運用を継続する最高責任者及び責任者は運用継続を脅かす危機的事象を定期的に見直す。
  (a) 政府機関等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。
  (b) 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る危機的事象は変化することを考慮する。

【考え方】

<2.3(1)関連>

2.3(1)-1 本書では、情報システムの可用性に影響を与える事象を、危機的事象の対象とする。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、まずは大規模災害や情報セキュリティインシデント等といった情報システムのハードウェア・ソフトウェアに影響を与える事象に加え、感染症等の発生等といった情報システムの運用業務に影響を与える事象を対象範囲に含める。
  a) 情報システムのネットワーク・ハードウェア機器等の物理的な故障により、情報システムの可用性に影響を与えるインシデントが発生する可能性も考慮する。
  b) 感染症発生時は、情報システム運用担当者や委託先担当者の不足に起因する情報システムの停止を想定する。また、情報システムに対する物理的な被害は発生しないが、感染症の流行が国内全域、全世界的となる可能性及び長期化する可能性も考慮する。

2.3(1)-2 物理的な情報システムへの被害が想定される場合は、情報システムの耐障害性や可用性を高めるために、代替の情報システムを遠隔地に設置する又はクラウドサービス等の外部サービスの利用を考慮する。なお、クラウドサービス等の外部サービス[1]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。

2.3(1)-3 政府機関等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（不正プログラム感染やサービス不能攻撃による情報セキュリティインシデント）も考慮する。

[1] クラウドサービス等の外部サービスを利用する際には、政府機関等の対策基準策定のためのガイドライン（平成30年度版）4.1.4(1)「クラウドサービスの利用における対策」遵守事項、基本対策事項及び解説を参照されたい。
※今後、廃止又は変更される可能性があるため、最新版を確認した上で利用すること。

（例示）

<2.3(1)関連>

- クラウドサービス等の外部サービスの利用においては、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、確認することが重要である。

<2.3(1)(b)関連>

- 業務時間外（政府機関等においては閉庁時）や休日夜間における危機的事象の発生や建物・施設（政府機関等においては庁舎等）の管理システム停止等を前提におくことによって、発生時における職員の自宅からの参集、関係者との対応まで検討する。
- 長期休暇中を含めた対応についても検討する。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、委託先への連絡等において、平日では発生しない課題が発生する場合がある。
- 基幹 LAN 等、組織情報システムの運用を継続する共通（連携）システムへの依存性や、自組織外が管理する管理システム（空調、ビル管理システム等）の非常態勢についても事前に確認し、被害想定、現状の確認とリスク評価の検討時に考慮する。
- 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。交通機関・電力・水道等の重要インフラが停止した際の影響調査等も検討の対象とすることが望ましい。
- 危機的事象として、業務や関係者へ大きな影響を与える情報セキュリティインシデントの発生を想定する。例として、重要システムの不正プログラム感染や不正侵入等が考えられる。また、平日の始業時間前の不正プログラム感染や不正侵入の発覚も業務開始の直前であることから影響が大きいと考えられる。

2.4 被害想定

目的・趣旨

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を想定し、情報システムの抱えるリスクを明らかにする。

検討事項

(1) 情報システムの運用を継続する最高責任者及び責任者は、危機的事象が発生した際の情報システムに係る下記の被害を想定に含める。
  (a) 大規模災害発生時の被害想定
  (b) 情報セキュリティインシデント発生時の被害想定
  (c) 感染症発生時の被害想定
  (d) その他危機的事象発生時の被害想定

(2) 政府機関等として取組の整合性を確保するため、業務継続計画の被害想定を活用する[1]。

(3) 情報システムの抱えるリスクの算定が複雑となることから、細かすぎる被害想定を避ける。

【考え方】

<2.4(1)関連>

2.4(1)-1 情報システムの設置拠点が複数存在する場合は、拠点ごとに環境が異なることを考慮し、拠点ごとの被害を想定する。なお、クラウドサービス等の外部サービス[2]を利用している場合は、外部サービス事業者のサービス提供環境も考慮する。

2.4(1)-2 情報システムの運用継続対応に当たっては、対応期間中に担当者に必要となる備蓄品等（トイレ、飲料水、食糧、休眠スペース、マスク、手指消毒液、体温計、サーモグラフィ等）を整備する。備蓄品は政府機関等の定める業務継続計画等を参考にする。

<2.4(1)(b)関連>

2.4(1)-3 情報セキュリティインシデントの発生時の被害は、例えば不正プログラム感染やサービス不能攻撃等の直近の情報セキュリティインシデント事例を参考にして、ある程度重大な被害を受ける前提で想定することに留意する。

<2.4(1)(d)関連>

2.4(1)-4 その他の危機的事象については、2.3(1)で特定した危機的事象に応じて検討する。検討の際には、2.4(1)(a)から(c)の危機的事象と同様に被害を想定することに留意する。被害想定は、ある程度幅を持たせた被害を想定し、前提条件から多少外れても対応可能な計画とすることに留意する。また、既に存在する公表資料の情報を基に、定期的に大まかな予測として整理することに留意する。なお、軽微すぎる被害を想定すると、本来必要な事項の検討に抜け漏れが生じるおそれがあることに留意する。

---

[1] 情報システム運用継続計画による検討で、業務継続計画の被害想定の詳細の見直しの必要性が判明することもありうる。

[2] クラウドサービス等の外部サービスを利用する際には、政府機関等の対策基準策定のためのガイドライン（平成30年度版）4.1.4(1)「クラウドサービスの利用における対策」遵守事項、基本対策事項及び解説を参照されたい。
※今後、廃止又は変更される可能性があるため、最新版を確認した上で利用すること。

(例示)

<2.4(1)関連>

- 情報システムの運用を継続する最高責任者及び責任者は、下表を例とする被害を想定する。なお、他組織と合同で利用する建物の場合は、建物を管理する組織と調整の上推進が必要な項目もあることに留意する。

表 2.4-1 大規模災害発生時の被害想定例

被害想定対象		被害想定の概要
人的資源	情報システム運用業務に従事する要員	情報システム運用業務に従事する要員（責任者及び担当者）の被害を想定する。また、参集可能な要員の把握をする。
建物・設備	情報システムの設置場所	情報システム設置場所の地理的距離や建物の構造を考慮し、被害を想定する。最悪の事象では建物が被災をする場合も想定する。
	交通インフラ	情報システムの運用継続に必要な職員や委託先が参集するための交通機関の被害を想定する。
	電力	政府機関等の電力被害を想定する。非常時の電源復旧計画確認や送電網及び発電機の被災や冗長化が未実施であることも想定する。
	水道	水冷式の空調を利用している場合は、水道復旧まで空調が停止するため、水道の被害を想定する。
情報システム	情報通信ネットワーク	音声通話、メール、アプリ（通話・チャット等）のサービスの停止・中断及び政府機関等の情報通信ネットワークの被害状況を想定する。情報通信ネットワークの切断等によるテレワーク環境への被害も想定する。
	情報システム機器	サーバ等の情報システム機器の被害を想定する。
	データ	情報システムの OS・アプリケーションのデータ、クラウドサービス等の外部サービスを含めた業務データの被害を想定する。バックアップデータがある場合、被害を想定する。
外部組織	委託先	委託先担当者及び協力者等の被災を想定する。委託先の業務提供の縮退を想定する。

表 2.4-2 情報セキュリティインシデント発生時の被害想定例

被害想定対象		被害想定の概要
人的資源	情報システム運用業務に従事する要員	情報システム運用業務に従事する要員（責任者及び担当者）が対応できない場合の被害を想定する。
建物・設備	情報システムの設置場所	クラウドサービス等の外部サービスにおける被害を想定する。
	交通インフラ	影響はない。ただし、情報システム運用継続を担当する要員の移動手段として、深夜、交通機関マヒ等の際の被害を想定する。
	電力	影響がないため、想定の必要なし。
	水道	影響がないため、想定の必要なし。

被害想定対象		被害想定の概要
情報システム	情報通信ネットワーク	不正プログラム感染やサービス不能攻撃を受けた場合には可用性の低下に伴う被害を想定する。 音声通話、メール、アプリ（通話・チャット等）のサービスの停止・中断及び政府機関等の情報通信ネットワークの被害状況を想定する。
	情報システム機器	不正プログラム感染の際に起こりうる障害、サービス不能攻撃による可用性の低下等の被害を想定する。
	データ	不正プログラム感染やサービス不能攻撃等に加えて、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を想定する。
外部組織	委託先	委託先が対応できない場合を想定する。

表 2.4-3 感染症の流行時の被害想定例

被害想定対象		被害想定の概要
人的資源	情報システム運用業務に従事する要員	情報システムの運用業務に従事する要員（責任者及び担当者）の感染症への罹患又は濃厚接触者となることによる一定期間の隔離及び濃厚接触の疑いのある者の自宅待機を想定する。情報システムの運用を継続する要員の通勤時の感染リスクを想定する。また、時差出勤やテレワークによる情報システム運用を担当する要員の減少を想定する。
建物・設備	情報システムの設置場所	作業環境の三密（密閉、密集、密接）、作業者が共同で利用する機器の汚染による感染リスクを想定する。
	交通インフラ	政府行動計画における対応方針により、運行本数の削減や運行時間の短縮を想定する。
	電力	影響がないため、想定の必要なし。
	水道	影響がないため、想定の必要なし。
情報システム	情報通信ネットワーク	テレワークの増加によりアクセスが集中し回線の帯域の不足やテレワーク用ソフトウェアのライセンス不足が発生することを想定する。
	情報システム機器	感染症の流行の影響により輸出入が滞り、新たな機器調達や既存機器の故障に際して交換が必要な部品調達等に時間を要することを想定する。
	データ	影響がないため、想定の必要なし。
外部組織	委託先	委託先の担当者及び協力者の感染症への罹患又は濃厚接触者となることによる一定期間の隔離を想定する。 委託先の業務提供の縮退を想定する。

2.5 情報システムの復旧優先度の設定

2.5.1 非常時優先業務と情報システムの関連整理

目的・趣旨

業務継続計画に定める非常時優先業務を踏まえ、優先する業務と情報システムの関連性を明らかにする。政府機関等が代替拠点に移転する場合における非常時優先業務を支える情報システムの運用継続についても本整理に含める。

検討事項

(1) 情報システムの運用を継続する最高責任者及び責任者は、既存の業務継続計画に定められている非常時優先業務を確認し、対象となる情報システムとの関連性を整理する。

(a) 情報システムの運用を継続する最高責任者及び責任者は、政府機関等の業務継続計画を確認し、情報システム運用継続における非常時優先業務の洗い出しを行う。

(b) 情報システムの運用を継続する最高責任者及び責任者は、各非常時優先業務がどの情報システムを利用しているかを明確化する。必要に応じて、各非常時優先業務所管部署や委託先に非常時優先業務と情報システムとの関連性について確認するよう指示する。

【考え方】

<2.5.1(1)関連>

2.5.1(1)-1 政府機関等においては、国民の生命、身体、財産の保護に関する業務の復旧優先度が高くなる。また、社会不安を解消し、国民の理解と協力を確保するため、危機的事象の発生による被害状況、これに対して採られた措置の概要等の正確かつ迅速な情報提供に努めるとともに、国内外に向け、的確に情報を発信する役割がある。これらを踏まえ、既存の業務継続計画に定められている非常時優先業務を確認し、対象となる情報システムとの関連性を整理する。

2.5.1(1)-2 検討に当たっては、業務継続計画に定められている非常時優先業務で利用する情報システムが洗い出されていれば、その情報を活用することに留意する。なお、個々の業務、情報システムごとに対応を考えるのではなく、情報システムの運用において非常時優先業務をどのように継続させるかの検討を行う。

2.5.1(1)-3 情報システムの運用を継続する最高責任者及び責任者は、対象とする情報システムを以下の観点で洗い出すことに留意する。

a) 情報システムの単位は物理的なサーバの単位ではなく、業務側で把握している情報システムの単位（例：メール、ホームページ等）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。

b) 業務側で把握している情報システム以外に、これらの情報システムが稼働する前提となる基盤系システム（例えば、認証、ドメインネームシステム（DNS）等）についても、運用を継続する情報システムとして明確化する。

c) クラウドサービス等の外部サービスの利用状況も整理する。

2.5.1(1)-4 情報システム担当部署は各部署や関係者へのヒアリング等を定期的に実施し、業務継続計画に定められている非常時優先業務と情報システムの関連付けが適切であること、情報システムの抜け漏れが無いことを確認する。

2.5.2 情報システムの復旧優先度の設定

目的・趣旨

非常時優先業務で利用する情報システムに対し、当該システムをどのくらいの時間で復旧させるかというRTO(目標復旧時間)及びどの水準まで復旧させるかというRLO(目標復旧レベル)を定め、復旧優先度グループに分類する。業務の復旧目標における優先順位や代替手段の有無を考慮したRTO及びRLOを設定する。

検討事項

(1) 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 非常時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 RTO 及び RLO を設定する。

(2) 情報システムの運用を継続する責任者及び担当者は、RTO及びRLOの検討結果より、情報システムをRTO及びRLOの時間帯・対象による復旧優先度グループに分類する。復旧優先度グループの分類は以下に留意し、政府機関等の個別の環境を考慮して定める。

(a) 復旧優先度の高い情報システムをできるだけ絞り込むこと。

(b) 委託先と、業務の復旧目標における優先順位や代替手段の有無を連携すること。

(3) 情報システムの運用を継続する責任者及び担当者は、時間の経過とともに対象の情報システムの重要性が変わる可能性があることから、復旧優先度は定期的に見直す。

【考え方】

<2.5.2(1)関連>

2.5.2(1)-1 業務に関係する情報システムが複数ある場合は、復旧順序と復旧に要する時間を考慮した上で、業務のRTOを達成できるようにする。

2.5.2(1)-2 業務の RTO 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を検討する。業務部門において政府機関等の業務継続計画を踏まえて情報システムが停止している間の業務側の代替手段を講じる際、RTOを達成できない場合があることについて業務部門に理解を求め、その場合を含めた代替業務手段の策定が業務部門側で実施されていることを確認する。RTOを短く設定するほど、情報システムに必要な対策費用は高額になるため、業務側で代替手段があるかを考慮する。なお、代替手段をとる場合、情報システムを用いた手段より作業負荷が増す可能性もあることに留意する。また、危機的事象発生時の業務部門側との情報システム運用状況のタイムリーな情報連携（業務側の迅速な代替策への切替や戻しに寄与）を検討することに留意する。

2.5.2(1)-3 一つの情報システムが複数の業務で利用されている場合は、各業務の RTO を一覧にし、RTOが最も短い業務に合わせて情報システムのRTOを設定する。

2.5.2(1)-4 情報システムの RTO 及び RLO の設定結果を踏まえ、基盤系システムも含めた RTO 及びRLOを設定する。基盤系システムのRTOは、原則として非常時優先業務を支える情報システムのRTOより短時間に設定する。

<2.5.2(2)(a)関連>

2.5.2(2)-1 優先度が高い情報システムが多くなると効率的な運用継続が不可能となるため、優先度が高い情報システムの対象数はできるだけ厳選する。

<2.5.2(2)(b)関連>

2.5.2(2)-2 危機的事象発生時には委託先が通常のサービスを提供することが難しいことが想定されるため、委託先との間で予め危機的事象発生時に提供可能なサービス内容を確認し、サービス品質保証(以下「SLA[1]」という。）として合意する。

[1] SLA：アプリケーション・サービス・プロバイダ等のIT アウトソーシング会社がその顧客に提供するテクニカルサポートや保証基準を定義する契約を言う。Service Level Agreement の略。

（例示）

<2.5.2(1)関連>

- 情報システムの停止や業務用のパソコン等のデータが使用できなくなる等、手作業で業務を実施せざるをえない状況を想定し、危機的事象発生時における情報システムへの被害想定を踏まえた代替手段等の対応について、政府機関等の業務継続計画に基づき平常時から業務部門と調整しておくことが考えられる。
- 情報システム本体だけではなく、情報システムの運用管理業務にも被害が及ぶ可能性を想定し、ファイルサーバや電子メール等の電子的手段が利用できない場合、あるいは被災等により一部の運用業務を通常とは異なる方法で実施する必要が生じた場合における手順書の整備や障害対応訓練等も検討することが考えられる。

<2.5.2(2)関連>

- 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ある。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おそれがある。これを回避するため、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行い、個々の情報システム責任者と調整をすることが望ましい。
- 情報システムの復旧優先度の例を下記に示す。政府機関等の個々の環境により、RTO 及び復旧優先度を定めることが望ましい。また、下記の例は RTO に基づき復旧優先度を定めているが、RLO も検討する場合には RLO 及び RTO の両方を考慮して復旧優先度を定める。

表 2.5-1 情報システムの復旧優先度の例

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

- RLO は設定対象に応じて、通常レベル（100%）、通常時における処理能力の 50%等、平常時を 100%としたときの処理量や稼働率等をパーセントで示すこともある。また、業務の性質によって、利用者数 500 人等のように示すこともある。また、RLO の値については政府機関等の個々の状況及び対象とする情報システムの重要性に応じて検討する必要がある。

<2.5.2(3)関連>

- 政府機関等は新型インフルエンザ等の発生に備え、『新型インフルエンザ等対策特別措置法（平成 24 年法律第 31 号）』第 6 条に基づく新型インフルエンザ等対策政府行動計画等を踏まえ、感染拡大の各段階（国内発生早期、蔓延期等）に応じた具体的な対応を盛り込んだ業務継続計画をあらかじめ策定することとされている。これに倣い、各段階に応じた情報システム運用継続を検討する必要がある。
- 時間の経過や状況の変化による情報システムの変更や設定の変更、人事異動による担当者変更や将来の見直しを見越し、情報システムの変更と復旧優先度設定の根拠を確実に記録しておく必要がある。

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

目的・趣旨

危機的事象発生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情報システムを支える構成要素を明確にし、対策を実施する。

検討事項

(1) 情報システムの運用を継続する責任者及び担当者は、次の情報システムを対象として、情報システムを支える構成要素を明確化する。
  (a) 非常時優先業務を支える情報システム
  (b) 部署横断で連携する重要な情報システム
  (c) メールやWeb、SNS等の情報収集・共有・伝達手段、基幹LANや外部サービス及びこれらにアクセスするための認証基盤

【考え方】

<2.6.1(1)関連>

2.6.1(1)-1 情報システムの運用環境を踏まえて情報システムを支える構成要素を検討する。対象となる情報システムがクラウドサービス等の外部サービスの場合は、自組織で所有する場合と同様に検討する。

2.6.1(1)-2 情報システムを支える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作業量が増えるため、対象とする情報システム数によっては、復旧優先度が高いグループに限定して進める等の柔軟な対応をする。

2.6.1(1)-3 情報システムの運用を継続するためには利用者の端末からサーバまでエンドツーエンドでの稼働が求められることを考慮し、情報システムを支える構成要素において単一障害点を明確化して代替の確保を検討する。

(例示)

<2.6.1(1)関連>

- 情報システムを支える構成要素には、情報システムの運用継続の対応手順書や緊急連絡先リスト、情報通信ネットワーク設定情報等の情報、運用継続のために必要なソフトウェアやデータ等がある。

表2.6-1.情報システムを支える構成要素の整理の例

情報システムを支える構成要素		説明
人的資源	情報システム運用業務に従事する要員	情報システムの運用を継続するために必要となる要員（情報システムの運用を継続する責任者及び担当者）、必要な人数及び経験・資格、交代勤務を考慮したチーム編成
	情報システム運用体制	情報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体制と役割分担、手順書の整備及び連絡体制の確保

情報システムを支える構成要素		説明
建物・設備	施設	情報システム機器の設置環境（建物やデータセンターの立地条件及び堅牢性、作業場所の安全性、自家発電設備の有無、施設維持管理システムの多重化・冗長化、電力系統の多重性、上下水道、備蓄品の整備等）、複数拠点の代替環境（バックアップサイト）確保
情報システム	情報通信ネットワーク	情報システムを利用するために必要な情報通信ネットワークの通信回線の帯域及び敷設状況（電気通信事業者の通信回線サービスの種類・ルート分散等）
	周辺機器	複合機やプリンター等の設置状況、外付 HDD/SSD、NAS 及び USB メモリ等の管理状況（データの暗号化等）、ウェブカメラ、ヘッドフォンマイク、モバイル通信網接続装置等のテレワーク用機器の管理状況
	ハードウェア	サーバ、ルータ、端末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）、テレワーク用の端末数
	ソフトウェア	テレワークを想定した際に必要となるソフトウェア（VPN ソフトウェア、ウェブ会議用アプリケーション等）のライセンス
	システム領域	アプリケーションやシステム認証・設定情報等の情報システムの運用継続に必要なデータの所在及び管理状況（同時被災しない外部に保管しているバックアップ媒体、データ暗号化及びデータ改ざん防止措置等）、複数拠点の代替環境（バックアップサイト）確保
	データ領域	重要なデータの所在及び管理状況（同時被災しない外部に保管しているバックアップ媒体、データ暗号化及びデータ改ざん防止措置等）、クラウドサービス等の外部サービスを利用する場合、サービス事業者との責任分界点の明確化、複数拠点の代替環境（バックアップサイト）確保
外部組織	委託先	危機的事象発生時における委託先の支援・協力体制、委託先の事業継続能力の把握、SLA の締結、クラウドサービス等の外部サービス提供事業者との責任分界点の明確化、複数拠点の代替環境（バックアップサイト）の確保

2.6.2 情報システムを支える構成要素ごとの目標対策レベルの設定

目的・趣旨

政府機関等の固有の環境に応じ、RTO（目標復旧時間）及びRLO（目標復旧レベル）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。

検討事項

(1) 情報システムの運用を継続する責任者及び担当者は、政府機関等の現状を踏まえて、情報システム復旧の目標水準をRLOとして設定し、段階的な復旧を検討する。

(2) 情報システムの運用を継続する責任者及び担当者は、RTO及びRLOを達成するために必要となる対策の実施方針を定める。「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に応じた目標対策レベルを整理する。

(3) 情報システムの運用を継続する責任者は、現状の情報システムの設置環境や利用している通信回線、情報システムの利用特性（政府機関等内に限定した利用か、不特定多数が利用するものか等）を考慮し、データセンターの利用、中長期の情報システム化推進計画、対策に要する費用等を踏まえて対策を決定する。

(4) 情報システムの運用を継続する責任者及び担当者は、目標対策レベルを設定する上で他部署と調整を要する事項は課題として記録しておく。

【考え方】

<2.6.2(1)関連>

2.6.2(1)-1 情報システムのRTOが短く、RLOが高いと、必要となる費用及び資源（リソース）が増大する可能性があるため、費用及び資源（リソース）と重要システムの中断・停止による影響とのバランスを確保することに留意する。

2.6.2(1)-2 情報セキュリティインシデントへの対策の内、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、政府機関等の情報セキュリティポリシー等に則った運用が求められる。情報システム運用継続計画内では、「情報システム運用業務に従事する要員」、「情報システム運用体制」、「委託先の事業継続能力」について、目標対策レベルを設定する。

2.6.2(1)-3 感染症の発生時は情報システム自体に直接的な被害は発生しないが、感染症の罹患やその疑いにより出勤抑制を求められることもあるため、係る事態を想定して「情報システム運用業務に従事する要員」、「情報システム運用体制」、「委託先の事業継続能力」について目標対策レベルを設定する。情報システムの運用継続を担っている担当職員や常駐の委託先担当者が現場で作業を実施できなくなる可能性があることから、情報システムの運用規模を縮小して継続することや、現場における交代制勤務又はテレワークの実施を考慮する。

<2.6.2(2)関連>

2.6.2(2)-1 情報システムをRTO内に復旧させるためには、情報システムを支える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ことに留意する。

<2.6.2(3)関連>

2.6.2(3)-1 危機的事象発生時には通信回線帯域が不足する可能性があるため、それらを考慮しRTOを満たす対策を決定する。

2.6.2(3)-2 RLOを達成するために必要な対策の目標を設定し、目標と現状との乖離を把握し、今後実施する対策を明確化する。

2.6.2(3)-3 情報システムの運用継続能力を向上させるため、短期的に実現することが難しいと考えられる目標対策レベルであっても設定し、中長期的にどのような対策を実施するかを現状からのギャップと合わせて管理する。

<2.6.2(4)関連>
2.6.2(4)-1 例えば自家発電装置等、情報システム運用継続計画の適用範囲と異なる部署が管理している構成要素については、当該部署に現状及び今後の対策計画を確認し、目標対策レベルを整理することに留意する。対策計画が不足と考えられる場合、政府機関等の業務継続の事務局と連携して別途対応し、適切なタイミングで対応ができるよう記録を残すことに留意する。

(例示)
<2.6.2(1)関連>
- 復旧優先度が最も高いグループの情報システムは、即時の復旧が必要となる。危機的事象の発生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、以下の対応を検討する。
  - データセンター等の被害を受け難い場所に情報システムを移設する。
  - 被災しても即時に切り替えて利用できる冗長化システムの環境を同時被災しない場所に構築しておく。
  - 情報システムの設置環境への被害の集中によるリスクを避けるためクラウドサービス等の外部サービスを利用する。
- 復旧優先度が最も低いグループの情報システムは、重要なデータの保護対策が実施されていることに留意する。

<2.6.2(2)関連>
- 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]を利用した情報システムの復旧優先度に応じたハードウェアにおける対策レベルの例を記載する。

表 2.6-2 情報システムの復旧優先度に応じたハードウェアにおける対策レベルの例

情報システムの復旧優先度	対策（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、現在の拠点と同時に被害を受け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、冗長化システムによる復旧を行う。※1	4
A	**ウォームスタンバイ用ハードウェアの確保** ・現在の拠点と同時に被害を受けない拠点にOS、アプリケーションをインストールし、起動している状態の予備機を準備する。被災時には専用の代替機として利用することにより、冗長化システムによる復旧を行う。※1	3
B		
C	**コールドスタンバイ用ハードウェアの確保** ・現在の拠点と同時に被害を受けない拠点に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
D		

[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。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。

情報システムの復旧優先度	対策（例）	対策レベル
E	**遠隔地にバックアップ用ハードウェア準備なし（被害拠点での復旧）** ・販売が終了しており、保守契約の締結や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。生産年数、在庫の保管年数等も確認する。	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。

- 情報システムを堅牢なデータセンターに設置することで可用性を確保しながら被害を極小化する予防的対策、遠距離拠点に冗長な環境を設置することで早期復旧を実現する対策、又はこれらを組み合わせる対策等が考えられる。外部サービス（データセンター及びクラウドサービス）を利用した対策レベルの例を記載する。

表 2.6-3 外部サービス（データセンター及びクラウドサービス）を利用した対策レベルの例

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	**外部サービスへバックアップ（又は移行）する** ・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する。 ・地理的距離が十分に離れた場所にデータを保存しているクラウドサービスを利用する。 ・SLA の内容を予め確認しておくことが重要である。	2
D E	**外部サービスへバックアップしない** ・販売が終了しており、保守契約の締結や再調達が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。生産年数、在庫の保管年数等も確認する。 ・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・水害対策を実施することで、損壊する可能性を低減させる。	1

- 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」で特定した、情報システム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。

<2.6.2(3)関連>

- 耐震性の高い拠点への移設、代替環境の構築をする際には次の点に留意する。
  - 費用対効果の観点から、復旧優先度の高い情報システムを明確化し代替環境設置対象のシステムを絞ることが望ましい。
  - 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、本番サイトと同時被災しない地域が望ましい。
  - 危機的事象発生時に代替環境へ情報システム担当者が駆けつける必要がある場合は、駆けつけ可能な距離であることが求められる。
  - 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。

2.7 事前対策の計画とその実施

2.7.1 現状の対策の確認及びリスクの評価

目的・趣旨

情報システムの現状の対策を、前項で設定した目標対策レベルに基づき把握する。

検討事項

(1) 情報システムの運用を継続する責任者及び担当者は、以下の手順により、目標対策レベルの実現に向けたリスクを評価する。

(a) 現状の対策の確認

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を評価する。

(b) リスクの評価

情報システムの運用を継続する責任者及び担当者は、現状の対策を踏まえ、目標対策レベルの実現に向けた情報システムのリスクを定期的に評価する。

【考え方】

<2.7.1(1)(a)関連>

2.7.1(1)-1 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。

<2.7.1(1)(b)関連>

2.7.1(1)-2 情報システムの運用継続作業を困難とさせるリスクについて評価しておく。

(例示)

<2.7.1(1)関連>

- 現状の対策の確認及びリスク評価の際に注意する例を示す。これらの対策は一例であるため、各政府機関等での現状を踏まえて検討を実施されたい。
  - 危機的事象発生時の対応体制及び連絡方法の整備
    - ・システム運用体制を確保するための対策として、代替要員（所持する経験・資格を含む）の確保や役割分担を定めておく等があるが、特定の要員に依存した運用により当該要員が業務遂行不可の場合の代替要員が確保できない等、情報システム運用を継続する体制の検討が不十分である。
    - ・必要な要員や委託先に緊急連絡を行い、必要に応じて参集を求めるため、最新の連絡先（休日・夜間を含む）を常備するとともに参集方法を事前に定めておく等の対策があるが、連絡先を入手していない又は最新情報に更新していない、参集方法が明確ではない、安否確認の方法が整備されていない等、緊急時の連絡方法が整備されていない。
    - ・情報システムの運用を継続するための対策として、必要な情報（LAN 構成図・ホームページ更新手順・復旧マニュアル等）や別拠点への機能移転等の手続きを整備しておくこと等があるが、それらが整備されていない。
    - ・情報システムの運用を継続する要員が不足するおそれがある場合の対策として、遠隔にて月次処理、バックアップ処理、システム改修業務、情報通信ネットワーク監視等の情報システム運用業務を実施する等があるが、テレワークに関連した規程や手順が未整備である、又は遠隔で運用業務が実施できるようにシステムが設計されていない。
    - ・既存の情報伝達・情報共有のためのシステムが利用できない場合の対策として、Web 会議や TV 会議の活用、クラウドサービス等の外部サービスを利用した電子メールシステムの活用等があるが、それらを活用した情報伝達・共有のための仕組みが構築されていない。

- 電力の対策状況

・自家発電装置や無停電電源装置（UPS）を利用している場合の対策の例として以下が挙げられるが、これらを実施していない。

  - 電力節約のため危機的事象発生時に継続する重要な情報システムを絞り込み、必要な電源容量、連続稼働可能時間を明確にする。
  - 自家発電装置の有無、装置の起動時間、装置が稼働する間の電力供給、長時間停電に備えた装置の燃料補給の体制の整備、復電後の切り戻し時の装置の再始動時間を考慮する。また、自家発電装置を利用した情報システム運用を一定時間に限る等の対応を考慮する。
  - 無停電電源装置（UPS）の動作を定期的に確認する、無停電電源装置（UPS）が機能している時間内で情報システムが正常終了できるよう自動シャットダウン設定を施す、また、復電後の切り戻し時の無停電電源装置（UPS）の電力量を確認する。

- 空調の対策状況

・空調を利用している場合の対策の例として以下が挙げられるが、これらを実施していない。

  - 危機的事象発生時にも空調が稼働するよう考慮する。
  - 被災時の電力抑制に配慮し、扇風機や送風機をサーバ熱源付近に設置し、空気を攪拌する。
  - サーバ室に個別空調を導入し、当該空調に自家発電装置を繋げる。
  - 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、適切に補強をする（天井埋め込みのケースについても同様）。

- 情報通信ネットワークの対策状況

・危機的事象発生時に情報通信ネットワークを確保するための対策として、LAN の冗長化（LAN 敷設経路の分散を含む）、モバイル通信網を経由して端末等をインターネットに接続させる装置（モバイル通信網接続装置）の利用、複数のキャリアの利用等が考えられるが、LAN や情報通信ネットワーク回線の不通に備えた冗長化や代替手段確保等の対策の検討が実施されていない。

- ハードウェアの対策状況

・ハードウェアの利用不能を想定した対策の例として以下が挙げられるが、これらを実施していない。

  - 情報システムが停止する可能性や復旧に要する時間が長期化することを想定し、非常時優先業務で利用するサーバを二重化する（ハードウェア故障時に予備サーバに切り替わる等）。
  - ハードウェアを利用する情報システムや業務について、同様のサービスを提供する外部組織への委託や、危機的事象発生時のみ業務を委託する事前契約を検討する。
  - 代替拠点や代替委託先を活用する局面の要件定義を業務部門と協議し、必要なハードウェアを確保する。

- 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

・危機的事象発生時における重要なデータを保護するための対策の例として以下が挙げられるが、これらを実施していない。

  - 各種情報通信ネットワーク設定情報を含む重要なデータのバックアップを取得する。データの更新頻度とバックアップの頻度は同等とする。
  - バックアップ用の媒体が適切に挿入されている等、運用ミスによりバックアップが取得できていない事態がないよう確認をする。
  - 正常にバックアップが実施されているか確認し、バックアップしたデータの復元テストを実施する。
  - バックアップ媒体は、損壊や紛失を避けるために適切に保管し、資産管理も行う。
  - 情報システムの設置場所又は冗長化システムと同じ場所にバックアップ媒体が保管されていないようにする。

- 情報通信ネットワークを介して、バックアップを取得している場合、バックアップデータが一斉に暗号化され使用できなくするサイバー攻撃により、バックアップデータとして利用できなくなるおそれがあることを考慮する。バックアップデータからの復旧時間については、通信回線帯域の利用状況により変化することを想定する。

- 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

・危機的事象発生時に調達が困難になる場合の対策として以下の例が挙げられるが、これらを実施していない。

- 予備品を適切な保管場所に保管する。(耐震固定された什器を使用する、壁際等の崩れやすい場所を避ける等)
- 販売が終了しており再調達困難なハードウェア・ソフトウェアや、再調達に極めて時間を要する機器類の利用を可能な限り避ける。(ホストコンピュータ[1]やオフィスコンピュータ[2]、特殊な仕様で発注した特注品等)
- 感染症の流行等により輸出入が滞る、又は政府機関等又は地方公共団体によりテレワークが推奨される場合において、テレワーク用のソフトウェアの需要が増加し、迅速な調達が一時的に困難になることを想定して調達を計画する。

- クラウドサービス等の外部サービスの利用の検討

・クラウドサービス等の外部サービス[3]を利用する場合の対策として以下の例が挙げられるが、これらを実施していない。

- 「SaaS」[4]「PaaS」[5]「IaaS」[6]等のクラウドサービスの仕組みを理解し、保存領域及び責任分界点について、サービス事業者に確認及び把握をする。
- クラウドサービスも SLA が未達となる可能性があるため、その場合の代替業務手順を確立するよう業務側に促す。
- クラウドサービスの利用中断・途絶を防ぐ手段として、サービス事業者の二重化や、サーバ設置場所の二重化等を考慮する。
- データ運用・管理における運用継続の管理策の確認をする。
- クラウドサービス等の外部サービスにて取得しているバックアップデータについて、復元が自動で実施される仕様となっているかを確認する。
- 第三者によるセキュリティ評価を受けている事業者を選定する。[7]
- クラウドサービス等の外部サービス提供事業者の運用・管理体制を定期的に確認する。
- 不正プログラム感染の検出等に対する機能が標準化されていることを確認する。

---

[1] ホストコンピュータ：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。

[2] 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。

[3] クラウドサービス等の外部サービスを利用する際には、政府機関等の対策基準策定のためのガイドライン（平成30年度版）4.1.4(1)「クラウドサービスの利用における対策」遵守事項、基本対策事項及び解説を参照されたい。
※今後、廃止又は変更される可能性があるため、最新版を確認した上で利用すること。

[4] SaaS「Software as a Service（サービスとしてのソフトウェア）」

[5] PaaS「Platform as a Service（サービスとしてのプラットフォーム）」

[6] IaaS「Infrastructure as a Service（サービスとしてのインフラ）」

[7] 政府情報システムのためのセキュリティ評価制度（ISMAP）、国際規格（ISO27017）の認証取得、SOC 等。
ISMAP：政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的とした制度を言う。Information system Security Management and Assessment Program の略。
JIS Q 27017：2016 (ISO/IEC 27017：2015)：情報技術ーセキュリティ技術ーJIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範を言う。
SOC：業務受託会社における内部統制保証報告やサイバーセキュリティに関する内部統制保証報告の枠組みを言う。SOC2 は、アウトソーシング事業者(受託会社)が委託されている業務で、セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに関連する内部統制を対象として保証を行う報告書である。System and Organization Controls の略。

2.7.2 事前対策計画の策定とその実施

目的・趣旨

前項で把握した現状のリスクに対応し、情報システムの運用継続能力を強化するために、事前対策計画を策定する。

検討事項

(1) 事前対策方針の検討

情報システムの運用を継続する責任者及び担当者は、現状の対策を目標対策レベルに近づけるための方針（事前対策実施方針）を情報システムごとに定める。

(2) 事前対策計画の策定及び実施

(a) 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事前対策計画に定め、計画を実施する。

(b) 調達仕様書を作成する際には、情報システム運用継続計画を確認し、事前対策を仕様書に盛り込む。

【考え方】

<2.7.2(1)関連>

2.7.2(1)-1 事前対策方針の作成に当たっては、以下を検討・実施する。

a) 国民の生命、身体、財産の保護を最優先に考え、国民への影響が大きいと思われる情報システムは停止した際の影響も考慮し方針を定め「業務影響度分析(BIA)」を実施する。

b) 他の情報システムとの依存関係も含め分析を行う。

c) 必要に応じて段階的に継続能力を強化できる方針とする。

d) 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利用方法を検討する。

e) 政府機関等の業務継続計画との整合性を確保する。

2.7.2(1)-2 事前対策は復旧優先度の高い情報システムを優先する。また、様々な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。

<2.7.2(2)(a)関連>

2.7.2(2)-1 事前対策計画に盛り込むべき内容として以下の事項に留意する。

a) 予算等の関係から対策をすぐに実施することが難しい場合には、業務影響度分析の結果等を考慮し、各政府機関等の実状に合わせて優先順位を定めて対策を実施する。優先順位により対応がとられていない対策は明示し、順次対応を行う必要がある。

b) 必要に応じ、危機的事象発生時のセキュリティレベル低下をどこまで許容するか関係者と事前調整し、政府機関等の情報セキュリティポリシーに基づき、危機的事象発生時における情報セキュリティに係る対策事項を検討しておく。

c) 情報セキュリティインシデント等によるシステム停止の事前対策については、情報システムで既に実施されている場合もあるため、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。また、被害想定・現状のリスク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。

d) 感染症の流行が発生した場合、影響が長期化する可能性も踏まえて、情報システムの運用を継続するために必要な要員（職員、委託先）を確保するための情報システム運用体制及び委託先の継続能力を確認する。人との接触削減が求められた場合に備えたテレワークの実施可能性についても確認する。

<2.7.2(2)(b)関連>
2.7.2(2)-2 重要な情報システムにおける対策では、クラウドサービス等外部サービスの利用を検討する。外部サービスの利用に際しては運用やサポートにおいて必要な情報セキュリティレベルが確保されるよう、調達時に適切な要求事項及びSLAについて契約書や仕様書に盛り込むことに留意する。

(例示)

<2.7.2(1)関連>

- 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の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。

<2.7.2(2)関連>

- 段階的に実施する場合には概算費用も考慮しながら、各段階でどのようなリスクを解決できるか（期待効果）、並びに実施後に残存するリスクを整理し、計画を更新する。
- システムが全停止した際に、復旧までの間に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、ローカルPC等を利用した簡易システムによる業務を代替する等の復旧戦略を検討する。

2.8 危機的事象発生時の対応計画の検討

2.8.1 危機的事象発生時の体制構築

趣旨・目的

政府機関等の業務継続計画による業務継続体制と連携して情報システムの運用継続活動を効率的に実施できるよう、情報システムの運用継続に係る危機的事象発生時の体制を構築し、役割分担を定める。

検討事項

(1) 情報システムの運用を継続する最高責任者は、危機的事象発生時の情報システム運用継続計画の発動に係る体制を構築し、役割分担を定める。情報システムの運用を継続する責任者は、危機的事象発生時において情報システム運用継続計画の発動に伴う作業を実施する責任者、担当者及びそれぞれの代行者を定める。

(a) 情報システム運用継続計画の発動に伴う作業を実施する責任者には、情報システムの継続に係わる具体的な判断・指示を行うことが可能な者が就任すること。

(b) 情報システム運用継続計画の発動に伴う作業を実施する担当者が対応できない場合も考慮した代行要員（必要な人数及び経験・資格保持者）を確保すること。

(c) 情報システム運用継続計画の発動に伴う作業を実施する担当者の作業負荷を考慮した体制（交代勤務を考慮したチーム編成等）や仕組みを構築すること。

【考え方】

<2.8.1(1)関連>

2.8.1(1)-1 危機的事象発生時に最高責任者、責任者及び担当者に連絡がとれない可能性を考慮し、代行者を定める。

2.8.1(1)-2 情報システム運用継続計画の発動に伴う作業を実施する責任者及び担当者は、危機的事象発生時における委託先との協議、情報システムの復旧作業の実施、運用継続の判断及び報告を実施する。

<2.8.1(1)(a)関連>

2.8.1(1)-3 情報システム運用継続計画の発動に伴う作業を実施する責任者は、情報システムの運用継続に係る具体的な判断・指示を行うことが想定されるため、平常時の情報システムの運用を継続する責任者が就任することを考慮する。

<2.8.1(1)(b)関連>

2.8.1(1)-4 危機的事象発生時においては、知見を有している前任者等による応援も考慮する。

<2.8.1(1)(c)関連>

2.8.1(1)-5 情報システム運用継続計画の発動に伴う作業を実施する担当者と、情報システムに関する各部署からの連絡窓口を分離することに留意する。特定の担当者に作業が集中しないように配慮し、危機的事象発生の影響が長期化することが想定される場合は、担当者が交代で勤務ができるようなチーム編成による交代制勤務等を考慮する。

2.8.1(1)-6 情報システム運用継続計画の発動に伴う作業を実施する担当者が現場における作業を実施すること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の構築を検討する。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検討する。

(例示)

<2.8.1(1)関連>

- 下表は、危機的事象発生時の情報システム運用継続計画の発動に伴う体制・役割の例である。政府機関等の業務内容やCSIRT[1]を含む組織構造等に応じ、体制・役割の追加や変更をする。

表 2.8-1 危機的事象発生時の情報システムの運用継続体制（例）

担当	役割	役割の内容
情報システムの運用を継続する最高責任者	最高責任者	• 政府機関等の対策本部への参画及び報告 • 情報システム運用継続計画の発動に係る意思決定
情報システムの運用を継続する責任者	責任者	• 政府機関等の対策本部への参画及び報告 • 情報システム運用継続計画の発動に伴う対応方針の検討及び報告
情報システムのインシデント対応担当者	CSIRT	• 報告管理、監視、分析の対応 • 被害の最小化、原因解析、再発防止策の対応 • 各組織との情報共有
情報システム運用継続計画の発動に伴う作業を実施する責任者	作業実施責任者	• 被災時の情報システム運用継続の作業実施責任者 • 情報システム運用継続方針の検討 • 情報システム復旧完了の利用者への通知 • CSIRT との連携
情報システムの運用を継続する事務局（情報システムの運用を継続する担当者）	情報収集・共有	• 被害状況／情報システム復旧状況の取りまとめと関係者への情報伝達 • 情報システムの運用を継続する責任者の支援
	各部署との連絡窓口	• 要員参集状況の確認と報告 • 情報システム利用者からの問合せ対応
情報システム運用継続計画の発動に伴う作業を実施する担当者	被害状況の確認	• 被災拠点における情報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
	情報通信ネットワークの復旧	• 被災拠点における情報通信ネットワーク復旧・動作確認 • 委託先への対応指示
	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 • 委託先への対応指示

[1] CSIRT：機関等において発生した情報セキュリティインシデントに対処するため、当該機関等に設置された体制をいう。Computer Security Incident Response Team の略。

担当	役割	役割の内容
情報システム運用継続計画の発動に伴う作業を実施する代替拠点の担当者	情報通信ネットワークの切り替え	• 代替拠点における情報通信ネットワーク切り替え作業 • 委託先への対応指示
	情報システムの切り替え	• 代替拠点における情報システム切り替え作業 • 委託先への対応指示
委託先	情報システム、情報通信ネットワークの復旧	• 担当者の指示又はSLAに基づいた作業 • 担当者の支援、報告

2.8.2 危機的事象発生時における対応計画

趣旨・目的

情報システムの運用を継続する最高責任者、責任者及び担当者は、危機的事象発生時に必要な実施手順を含んだ計画を作成する。

検討事項

(1) 情報システム運用継続計画の発動に係る判断基準の作成
情報システムの運用を継続する最高責任者及び責任者は、情報システム運用継続計画の発動に係る意思決定の判断基準（要員参集基準、情報システム切り替え基準、テレワーク実施基準等）を定める。

(2) 情報システムの運用継続業務の全体の流れ（全体フロー）の作成
情報システムの運用を継続する最高責任者及び責任者は、危機的事象発生から対応完了までの全体フローを政府機関等の業務継続計画を踏まえて作成する。

(3) 全体フローを踏まえた対応手順書の作成
情報システム運用継続計画の発動に伴う作業を実施する責任者及び担当者は、情報システムの運用継続業務の全体の流れを踏まえ、危機的事象発生時の体制で定めた各責任者及び担当者が採るべき対応を明確にした手順書を作成する。

(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
情報システム運用継続計画の発動に伴う作業を実施する担当者は、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、システム停止を伴わない活性保守等）に関する方式についても検討する。

【考え方】

<2.8.2(1)関連>

2.8.2(1)-1 情報システム運用継続計画の発動に係る判断基準の作成にあたっては、政府機関等の業務継続計画の基準と整合をとることに留意する。判断基準には、情報システム運用継続計画の発動基準に加え、発動に伴う各種作業の実施判断を下すために必要となる基準も含める。

<2.8.2(2)関連>

2.8.2(2)-1 全体フローには、危機的事象発生時の情報システム運用継続計画の発動に係る各種判断を下すために必要となる情報、意思決定者、発動時に必要となる実施事項の概要を記載することに留意する。詳細が記載される規程類・個別手順・チェックリスト等は、参照資料として資料名を全体フロー内に記載しておくことに留意する。

<2.8.2(3)関連>

2.8.2(3)-1 対応手順書の作成に当たっては、情報システムの運用継続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、国民への説明責任を果たすための情報公開手順も含める。

2.8.2(3)-2 情報システム運用継続計画の発動に伴い情報システムの運用継続に必要な例外措置を適用した場合は、その実施状況を管理し、不適切な例外措置が常態化しないようにすることに留意する。また、適用した例外措置は情報システム運用継続計画の発動解除後も管理し、平常時の情報システムの運用として恒常的に実施する内容と、危機的事象発生時に対応する内容を整理し、平常時又は危機的事象発生時の手順書及び業務フローへの反映を検討する。

<2.8.2(4)関連>

2.8.2(4)-1 代替拠点における通常時の運用計画は、本番サイトにおける政府機関等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。

（例示）

<2.8.2(1)関連>

- 情報システム運用継続計画において、危機的事象発生時の情報システム運用継続計画の発動に係る判断基準や対応手順が不明確であるために意思決定ができず、その間に情報システムが停止に陥る事態も想定されるため、発動のタイミング、発動に係る意思決定の権限者及び代行者等を含めた手順を策定する。
- 情報システムの運用を継続する最高責任者及び責任者は、情報システムの運用継続に必要な要員が不足する時には他部署から人的支援を確保するための施策を行うことが望ましい。
- 危機的事象発生時には、委託先による SLA に基づくサービスの提供が難しくなることも想定される。予め委託先との間で危機的事象発生時に提供可能なサービス内容について確認・合意しておくことが望ましく、委託先との合意事項は政府機関等の業務継続計画に反映されていることを確認する。

<2.8.2(2)関連>

- 情報システムの運用を継続する最高責任者及び責任者は、外出先等で被災することもありうるため、危機的事象発生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、常に携行しておくことが望ましい。

<2.8.2(3)関連>

- 危機的事象発生時には、混乱に乗じた政府機関等の建物へ侵入等が発生する可能性もある。情報システムの運用上、入退室管理等について適切な情報セキュリティレベルが確保されるよう配慮する。被災時には、建物内に関係者以外の人々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、関係者以外の人々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や、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。
- 委託先が運用継続の作業を遂行する場合、委託先の運用継続体制を事前に確認しておく。
- 危機的事象発生時の事後対応に係る手続きや予算の確保について、対応手順書を作成する際に確認する。

2.9 教育訓練・維持改善の計画とその実施

2.9.1 教育訓練の計画とその実施

趣旨・目的

危機的事象の発生に対する情報システムの運用を継続する最高責任者、責任者及び担当者の理解や対応力を向上させるとともに、事前対策の有効性を確認し、気づきや反省をもとに改善することを目的とする。

検討事項

(1) 情報システムの運用を継続する最高責任者及び責任者は、年間で取り組む教育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）。

- (a) 手順書の確認を優先的に計画する
- (b) 情報システム復旧訓練を実施するよう計画する
- (c) 教育訓練は段階的に高度化するよう計画する
- (d) 訓練の実施に当たっては、予め計画・準備をした上で実施する
- (e) 業務部門が参加する訓練を実施する

【考え方】

<2.9.1(1)関連>

2.9.1(1)-1 教育訓練の目的は以下の 3 つに分類されるため、それぞれの内容を踏まえ訓練を計画する。

- a) 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
- b) 危機的事象発生時対応計画の理解と対応能力の向上
- c) 事前対策内容の確認と検証

2.9.1(1)-2 情報システムの運用を継続する最高責任者及び責任者は、危機的事象発生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。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。情報システムの運用体制に委託先が含まれる場合には、教育訓練計画の実施対象者として委託先を含めて検討する。また、情報システムの復旧及び運用継続を実施する過程に業務部門が関与する場合には、業務部門を含めた教育訓練計画の実施を検討する。

2.9.1(1)-3 取得したバックアップからデータを復旧できるか否かを検証していないケースが多いため、情報システム復旧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に留意する。

2.9.1(1)-4 訓練を計画する際には対象とする危機的事象・情報システム・危機的事象発生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み、危機的事象発生時の対策事項の理解と対応能力の向上の他、対策事項の有効性の確認も目的とすることに留意する。

2.9.1(1)-5 テレワークの実施に係る規程を整備している場合、訓練時にその運用の有効性を検証し、改善点を明確化することに留意する。改善点については関係者で協議し、整備している規程や実施手順書等を修正する。

(例示)

<2.9.1(1)関連>

- 平常時の情報システム運用継続計画の維持改善
  - 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、情報システムの運用を継続する最高責任者及び責任者が、業務継続に関する十分な知識と経験を身につけておくことが重要である。新規配属や人事異動等の際には情報システム運用継続計画に関する基礎知識を習得させ、人事異動に伴う情報システム運用継続計画の引き継ぎを確実に実施する。情報システムの運用を継続する最高責任者及び責任者は、業務継続に関する十分な知識と経験を身につけられるように規程や実施手順書等の整備・共有を行う等、特定の職員や委託先に過度に依存しないことが重要である。
  - 情報システムの運用を継続する責任者及び担当者は、政府機関等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。

- 危機的事象発生時対応計画の理解と対応能力の向上
  - 危機的事象発生時対応計画に定められる実施手順については、情報システムの運用継続をする責任者及び担当者が内容を熟知しておくとともに、計画の内容に不備や改善点がないか事前に検証し、情報システムの運用継続をする最高責任者の承認を得ておくことが必要である。
  - 危機的事象発生時には、計画や訓練で扱ったとおりの事態が発生するとは限らないため、どのような事態が発生しても対応できるように、情報システムの運用を継続する最高責任者、責任者及び担当者は、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。
  - 教育訓練の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。
  - 緊急連絡時に利用する日常的に使用しない連絡手段（衛星電話や広域無線等）について、操作担当者交替や機材更新においては速やかな教育訓練及びマニュアルの整備により、連絡手段を維持する。また、定期的な訓練により操作練度を維持するとともに、電波状況、機材動作、バッテリー等消耗品についての確認を実施する。

表 2.9-1 危機的事象発生時の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
手順書 確認訓練	作成した危機的事象発生時対応計画を読み合わせ、業務継続計画に定められた非常時優先業務の担当者及び委託先を含む関係者間で危機的事象発生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。	業務継続計画に定められた非常時優先業務の担当者及び委託先を含む関係者が計画の内容を熟知できるとともに、手順の内容の抜け漏れを確認できる。
シナリオ 非提示型訓練	参加者に訓練シナリオ（危機的事象発生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。

- 事前対策内容の確認と検証
  - 事前対策として実施されたバックアップや代替環境が期待どおりに機能するか、定期的に訓練を通じて確認をしておくことが必要である。

- 法定点検の際等に、定期的に自家発電装置が重要な情報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。
- 電源容量が適切に確保されているか、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が確保されているか、無停電電源装置（UPS）のバッテリー寿命や性能劣化の有無を、定期的に確認する。
- 情報システム導入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、情報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等が挙げられる。
- 危機的事象発生時に情報システムの復旧が長期化する、復旧ができない事態となら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、情報システムの運用を継続する担当者の復旧作業の習熟も同時に図ることができる。実施時期の例としては、定められた各訓練実施時期や過去のインシデント発生日に合わせることが考えられる。

表 2.9-2 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	実施時の留意点
情報システム復旧訓練	実機を用い、バックアップしているデータから実際に情報システムを復旧する訓練。	訓練実施に当たっては、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。
情報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。

● 初期に実施する訓練としては、危機的事象発生時の対応体制に定められる担当者が手順書の読み合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、担当者の不在を想定し、危機的事象発生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、業務継続計画に定められた非常時優先業務の担当者や委託先等との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。

● 計画・準備に必要となる事項は教育訓練の内容によって異なるが、例えば以下の要素等が挙げられる。
  - 教育訓練実施体制（教育訓練推進リーダー・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）
  - 教育訓練シナリオ（危機的事象や被害の発生時点を想定して検討）
    ※被害状況によっては人員や設備が利用できないことを留意して、シナリオを策定することを考慮する。
  - 対象者（業務継続計画に定められた非常時優先業務の担当者及び委託先の参加の有無等）
  - 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 維持改善の計画とその実施

趣旨・目的

維持改善においては、計画の各情報が古くなることに起因する継続力の劣化を防ぐことが不可欠であることから、事前対策計画、危機的事象発生時対応計画、教育訓練計画を定期的に見直し、情報システム運用継続計画の実効性の維持又は向上を目的として検討する。維持改善計画を着実に実施し、改善活動を行うことが重要である。

検討事項

(1) 情報システムの運用を継続する最高責任者及び責任者は、情報システム運用継続計画の見直し時期・内容を定める。
  (a) 見直し時期は予算編成の検討時期を踏まえ設定する。
  (b) 危機的事象発生後には見直しを実施する。

(2) 情報システムの運用を継続する最高責任者及び責任者は、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。

(3) 情報システム運用継続計画に基づいた対策の有効性を確認するため、自己点検、内部監査等の定期的な実施や、必要に応じて、外部専門家による第三者監査等を実施して外部の見識を活用する等により、情報システム運用継続計画の継続的改善を図る。

【考え方】

<2.9.2(1)(a)関連>

2.9.2(1)-1 情報システム運用継続計画の定期的な見直しの結果、新たな事前対策の実施等により予算要求の必要性が生じる可能性もあるため、見直し時期は予算編成の検討時期を踏まえ設定することに留意する。

2.9.2(1)-2 危機的事象発生時に情報システムの運用を継続させるために例外措置を適用した場合は、情報システム運用継続計画の見直し時に、例外措置の対応内容を確認し、情報システム運用継続計画への反映を検討する。

<2.9.2(2)関連>

2.9.2(2)-1 政府機関等において、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ことに留意する。これにより、情報システムのライフサイクルの各段階において、情報システム運用継続計画の視点でも必要な検討が漏れなく行われるようになる。

<2.9.2(3)関連>

2.9.2(3)-1 新しいシステムの導入、扱う情報の変化、利用環境や利用方法の変化、各政府機関における業務継続計画の更新等のタイミングで、リスク評価、復旧優先度、対策の妥当性等の見直しが必要となることに留意する。自己点検、内部監査、外部の専門家による第三者監査等を実施することにより、情報システム運用継続計画に基づいた対策の有効性を確認することを考慮する。

(例示)

<2.9.2(1)関連>

- 見直し内容としては以下の例が考えられる。

表 2-9-3 情報システム運用継続計画の見直しの例

見直し事項	見直し内容（例）
事前対策計画	• 事前対策計画に基づき、対策は実施されたか。 • 実施した事前対策を踏まえて内容を更新したか。（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。 • 教育訓練の結果を踏まえて事前対策の見直しを行ったか。
危機的事象発生時対応計画	• 担当者や連絡先は最新化されているか。 • 実施した事前対策がある場合、対応手順を適切に見直したか。 • 教育訓練の結果を踏まえて対応手順の見直しを行ったか。
教育訓練計画	• 教育訓練計画に基づき、教育訓練は実施されたか。 • 教育訓練の結果を踏まえて対応手順の見直しを行ったか。
情報システム運用継続計画の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適用範囲を検討したか。 • 外部環境の変化、社会的な要求の高まり、危機的事象の発生等により、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、情報システム復旧優先度の設定や必要な事前対策計画、危機的事象発生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を検討したか。 • 業務部門及び政府機関等の業務継続計画事務局を交えて業務継続計画との整合性を確認したか。

参考：JIS Q 22301:2020（ISO 22301:2019）セキュリティ及びレジリエンス－事業継続マネジメントシステム－要求事項を利用した第三者認証の仕組みがある。