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
付録
～（第２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
1.1	平成23年8月15日	「3.1.」、「3.2.」の目標対策レベルにおける記載を訂正
2	令和3年4月	第2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

付録の位置づけ

「政府機関等における情報システム運用継続計画」はガイドライン及び付録で構成される。付録は、政府機関等の情報システム担当者がガイドラインをもとに付録の活用により情報システム運用継続計画を作成することを目的としたものである。付録では情報システム運用継続計画に記載すべき事項について、主にメールや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例として記述している。なお、付録とガイドラインは異なる目次構成をとっている。これは付録においては、危機的事象発生時の利用のしやすさを考慮し、危機的事象発生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。

付録の利用方法

付録において想定する前提

付録は、以下を前提として記述している。また、政府機関等の業務継続計画や情報セキュリティポリシーを踏まえ、適宜変更する必要がある。

・「中央省庁業務継続ガイドライン 第2版（平成28年4月 内閣府防災担当）」等に基づき、政府機関等において、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対応した業務継続計画が策定されていること
・平時における情報セキュリティへの対応は、政府機関等の情報セキュリティポリシーに基づき行われていること

作成上のポイント

情報システム運用継続計画の策定にあたり、政府機関等における既存の情報システム環境や、中長期の業務計画や年度計画を踏まえて、以下のような方法で作成を進める。

- 付録において *[・・・]* 形式で示す設定値（組織名、期間等）は、政府機関等の定めに合わせる。
- 付録において点線枠の内容は留意事項及びガイドラインの参照先である。留意事項については、政府機関等の判断や固有の状況に基づき記載する。
- 既存の関連規程との関わりや整合性を考慮し、適切に相互参照する。
- 付録の図表は全てサンプルであり、政府機関等で定めた業務継続計画に基づき作成する。

付録とガイドラインの対応表

付録の各章における検討事項、考え方については、ガイドラインを参考にされたい。付録とガイドラインの対応について、以下に示す。

付録	ガイドライン
1.本計画の目的と基本方針	―
1.1.本計画の策定趣旨	2.1 基本方針の決定
1.2.基本方針	2.1 基本方針の決定
1.3.本計画の適用範囲	2.1 基本方針の決定
1.4.情報システム運用継続計画の策定・運用推進体制	2.2 策定・運用体制の構築
2.危機的事象発生時の対応計画	―
2.1.危機的事象発生時の基本方針	―
2.1.1.対象事象	2.8.2 危機的事象発生時における対応計画
2.1.2.参集要員	2.8.2 危機的事象発生時における対応計画
2.1.3.参集基準	2.8.2 危機的事象発生時における対応計画
2.1.4.参集場所	2.8.2 危機的事象発生時における対応計画
2.2.危機的事象発生時の対応体制	―
2.2.1.対応体制・指揮命令系統図	2.8.1 危機的事象発生時の体制構築
2.2.2.関係部局・関係企業連絡先一覧	2.8.1 危機的事象発生時の体制構築
2.3.危機的事象発生時における対応手順	―
2.3.1.全体フロー	2.8.2 危機的事象発生時における対応計画
2.3.2.対応手順	2.8.2 危機的事象発生時における対応計画
3.事前対策計画	―
3.1.情報システムを支える構成要素ごとの現状対策レベルとリスク	2.7.1 現状の対策の確認及びリスクの評価
3.2.事前対策の実施計画	2.7.2 事前対策計画の策定とその実施
4.教育訓練計画・維持改善計画	―
4.1.教育訓練計画	2.9.1 教育訓練の計画のその実施
4.2.維持改善計画	―
4.2.1.計画の実施に伴う維持改善	2.9.2 維持改善の計画とその実施
4.2.2.危機的事象の発生に伴う維持改善	2.9.2 維持改善の計画とその実施
4.2.3.定期的な見直しによる維持改善	2.9.2 維持改善の計画とその実施
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	2.3 危機的事象の特定
5.2.想定する被害状況	2.4 被害想定
5.3.情報システムの復旧優先度の設定	2.5 情報システムの復旧優先度の設定
5.4 情報システムを支える構成要素の関連整理	―
5.4.1.情報システムを支える構成要素の整理	2.6.1 情報システムを支える構成要素の明確化
5.4.2.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	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

目次

1. 本計画の目的と基本方針

1.1. 本計画の策定趣旨

[政府機関等] は、国民の経済・社会活動の維持発展と安全を支える自らの業務を、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等の危機的事象の発生時においても継続することにより、自らの責務を果たすために、*[2008 年 4 月]* に *[政府機関等]* 業務継続計画（以下「業務継続計画」という。）を策定した。業務継続計画では、[政府機関等] が非常時優先業務[1]を定めるとともに、それら業務の継続・早期再開のための方法を記している。

このような業務継続計画等に定めた非常時優先業務を継続するためには、業務を支える情報システムの継続が前提であり、予め情報システムに対する十分な備えとしての、業務継続計画等と整合性が確保された情報システム運用継続計画の策定が必要となる。また、この策定に際しては、近年の大型台風による広域大規模停電や新型コロナウイルス感染症等の広域感染症を想定することも重要である。

このような背景のもと、本計画は *[政府機関等]* において情報システム継続性を強化し、適切に維持管理していくための具体的な事項（適用範囲、危機的事象発生時対応計画、事前対策計画、教育訓練計画、維持改善計画）を定め *[政府機関等]* における情報システムの継続性強化・維持管理を図るために計画を策定するものである。

ガイドラインの参照先：「2.1 基本方針の決定」

[1] 本書における「非常時優先業務」とは、危機的事象の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。

1.2. 基本方針

情報システム運用継続計画の基本方針は以下のとおりである。また、基本方針は *[政府機関等]* を取り巻く環境の変化に応じ、定期的に見直しを行うものとする。

情報システム運用継続計画

危機的事象発生時において、情報システムの継続及び復旧を図るため、情報システム運用継続計画の策定と運用に取り組む。

基本方針

（1） 情報システムの継続及び復旧を脅かすリスクを評価し、適切な対策を実施する。
（2） 危機的事象発生時における情報共有手段の継続及び復旧を図るため、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及びこれらにアクセスするための認証基盤等に対する対策を優先的に実施する。
（3） 危機的事象発生時に備え、情報システムの継続及び復旧のための計画と手段を事前に整備する。
（4） 情報システム運用継続計画と業務継続計画の整合性を確保する。

ガイドラインの参照先：「2.1 基本方針の決定」

1.3. 本計画の適用範囲

本計画の適用範囲は、*[政府機関等 A 情報システム部局 A]*、*[政府機関等 A 情報システム部局 B]* が運用管理する以下の情報システムとする。

表 1.3-1 情報システム及び運用管理主体

項	情報システム名	運用管理主体
1	メールシステム	部局 A
2	A システム	部局 A
3	B システム	部局 B
4	C システム	部局 B

上記以外の情報システムは本計画の対象範囲には含まないが、*[情報システムの運用を継続する最高責任者]* 及び *[情報システムの運用を継続する責任者]* は、今後、危機的事象発生時における優先度を考慮し、定期的に対象範囲の見直しを行う。

ガイドラインの参照先：「2.1 基本方針の決定」

1.4. 情報システム運用継続計画の策定・運用推進体制

*［政府機関等］*における情報システム運用継続計画は、*［情報システムの運用を継続する最高責任者］*のもと策定し、対象システムを踏まえて情報システム運用継続計画推進体制を構築し、実施する。

*［政府機関等］*における情報システム運用継続計画推進体制、担当部署及び担当者、推進上の役割を以下に記す。

表 1.4-1 *［政府機関等］*における情報システム運用継続計画推進体制上の担当部署及び担当者、推進上の役割

担当者	所属・氏名	役割の概要
［情報システムの運用を継続する最高責任者］	*［担当者所属］・［氏名］*	・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］	*［担当者所属］・［氏名］*	・所管する情報システムの、情報システム運用継続計画の策定・運用を統括する。
［情報システムの運用を継続する担当者］	*［担当者所属］・［氏名］*	・所管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。

表 1.4-2 関連部局及び委託先等における情報システム運用継続計画推進体制上の担当部署及び担当者、推進上の役割

区分	部署・氏名	役割の概要
［X 部局］	*［担当者所属］・［氏名］*	・庁舎の耐震状況・自家発電装置の設置状況に関する情報提供・対策調整
［B 株式会社］	*［担当者所属］・［氏名］*	・運用保守及び緊急時の状況に関する情報提供・対策調整
・・・	・・・	・・・

本体制は、本計画の情報システムの対象範囲を踏まえた体制であり、対象範囲が変更された場合は、適宜見直しを行う。

ガイドラインの参照先：「2.2 策定・運用体制の構築」

2. 危機的事象発生時の対応計画

2.1. 危機的事象発生時の基本方針

2.1.1. 対象事象

本書における危機的事象発生時の対応計画は、以下の事象を対象とする。

（1）大規模災害（地震、風水害等）
（2）情報セキュリティインシデント（不正プログラム感染、サイバー攻撃等）
（3）感染症（新型インフルエンザ、新型コロナウイルス等）

2.1.2. 参集要員

危機的事象発生時の情報システムの運用継続に係る参集要員を以下のとおり定める。

表 2.1-1 *［政府機関等］*における危機的事象発生時の情報システム運用継続体制

担当者	所属・氏名	役割の概要
［情報システムの運用を継続する最高責任者］	*［担当者所属］・［氏名］*	• 政府機関等の対策本部への参画及び報告を行う。 • 情報システム運用継続計画の発動に係る意思決定を行う。
［情報システムの運用を継続する責任者］	*［担当者所属］・［氏名］*	• 政府機関等の対策本部への参画及び報告を行う。 • 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］	*［担当者所属］・［氏名］*	• 報告管理、監視、分析の対応を行う。 • 被害の最小化、原因解析、再発防止策の対応を行う。 • 各組織との情報共有を行う。
［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］	*［担当者所属］・［氏名］*	• 情報システム運用継続方針を検討する。 • 情報システム復旧完了を利用者に通知する。 • CSIRT と連携する。
［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）］	*［担当者所属］・［氏名］*	• 被害状況又は情報システム復旧状況を取りまとめ関係者へ情報伝達する。 • 情報システムの運用を継続する責任者を支援する。 ・・・

担当者	所属・氏名	役割の概要
［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］	*［担当者所属］・［氏名］*	• 被災拠点における情報システムの被害状況確認と、事務局への報告を行う。 • 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を行う。 ・・・
［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］	*［担当者所属］・［氏名］*	• 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を行う。 ・・・
［委託先］	*［担当者所属］・［氏名］*	• 担当者の指示又はSLAに基づいた作業 • 担当者の支援、報告

2.1.3. 参集基準

初動対応を実施するための参集基準を以下のとおり定める。なお、本書における参集は、参集場所への現地参集及びオンライン（電話会議、Web会議等）への参集の両方の意味を含む。

（1）大規模災害

- *［東京都等対象地域］*において*［震度6弱以上］*の地震や*［超大型］*の台風等が観測された場合、参集要員は自動参集し、初動対応を開始するものとする。
- *［震度6弱未満、中型・大型の台風］*であっても、*［情報システムの運用を継続する最高責任者］*が発動を判断した場合、*［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*［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］*の指示のもとに参集し（後述）、初動対応を開始するものとする。

（2）情報セキュリティインシデント

- 情報システムによる検知や通報・発見等で、*［情報システムの運用を継続する責任者］*又は関係者に情報システムの停止等が認知され、*［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を発動した場合、*［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］*の指示のもと、*［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］*が参集し、初動対応を開始するものとする。

（3）感染症

- 感染症の流行が発生した場合、緊急の参集は行われない場合も想定されるが、*［情報システムの運用を継続する最高責任者］*は*［政府機関等］*が定めた業務継続計画と連動して適時に情報システムの運用継続計画の発動を判断し、*［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］*の指示のもと、*［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］*は対応を開始するものとする。

2.1.4. 参集場所

参集場所を以下のとおり定める。*［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］*から別に指示がある場合は、その指示に従う。

表 2.1-1 参集要員及び参集場所

参集要員	参集場所
［システム A の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］ *［システム A の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］*	第 1 順位：〇〇庁舎〇〇会議室 第 2 順位：〇〇庁舎〇〇会議室
［システム A の運用を継続する被災拠点の復旧担当者］	第 1 順位：システム設置拠点〇〇 第 2 順位：〇〇庁舎〇〇会議室
［システム A の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］	代替拠点〇〇
・・・	

参集場所は現地での参集、オンラインのいずれか適切な方法を選択する。上記参集場所が人命の安全や本部機能の遂行の上で不適切と判断される場合、情報システムの継続と関連組織との情報共有のしやすさを踏まえ、*［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］*が適切な場所を判断し参集を指示するものとする。大規模感染症の感染予防対策として、勤務官署への出勤が抑制されるような状況下では、テレワーク等の対応も検討する。

*［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、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、財布や定期入れ等の中に入れておくことやスマートフォンに保存しておく等、常に携行しておくこと。携行カードの例は「別表 2. 災害用携行カード」に記載する。

※2.1.1 については、その他、地域・業務等の特性に応じ、対応計画の事象を決定する。

ガイドラインの参照先：「2.8.2 危機的事象発生時における対応計画」

2.2. 危機的事象発生時の対応体制

2.2.1. 対応体制・指揮命令系統図

情報システムの継続及び復旧を目的とした危機的事象発生時の体制を以下のとおり定める。危機的事象発生時は通常の連絡手段が不通となる場合も考慮し、メールやWeb、SNS等の手段を想定する。

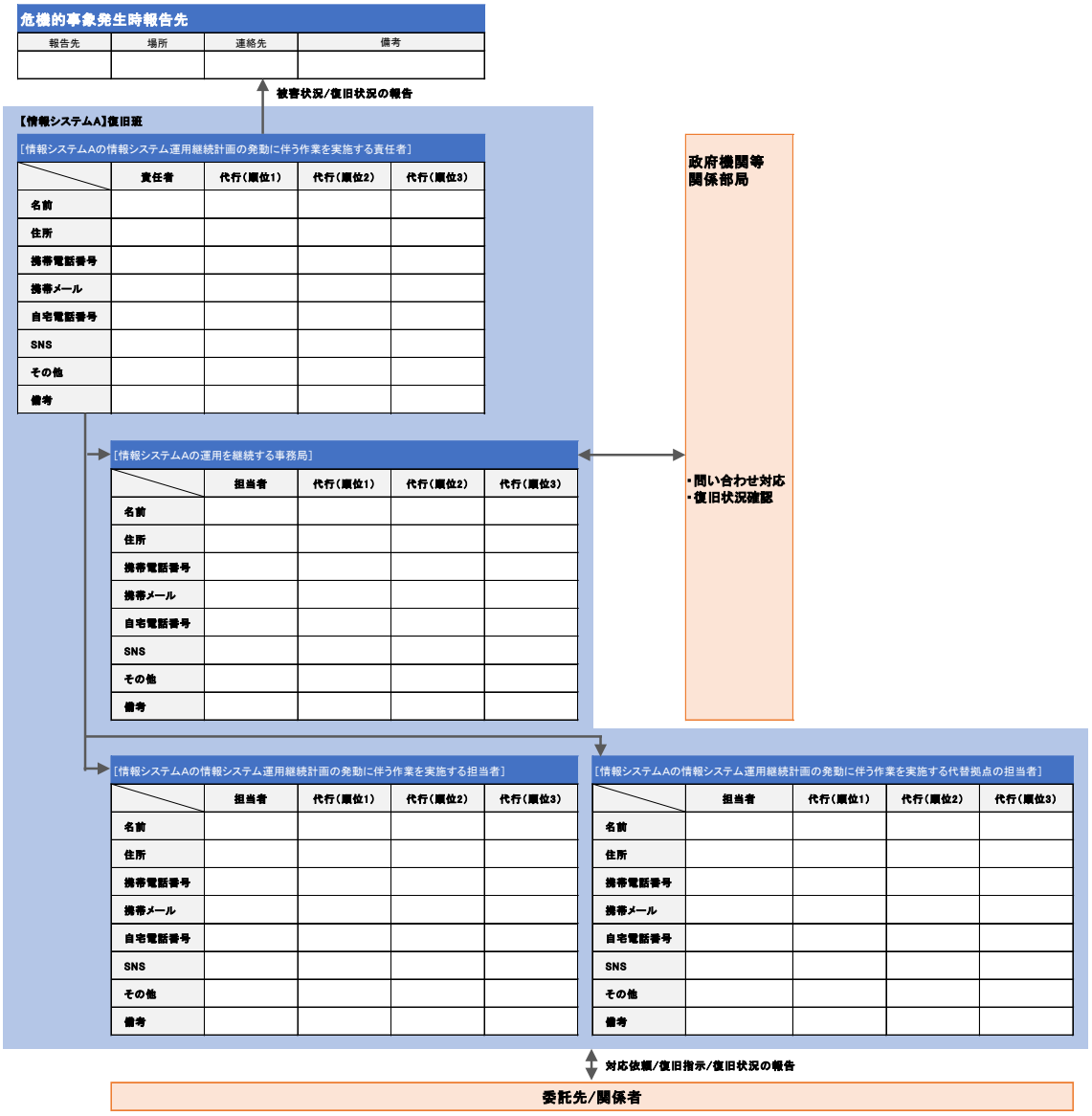


図 2.2-1 危機的事象発生時の体制

2.2.2. 関係部局・関係企業連絡先一覧

関係部署・関係企業の連絡先を以下に示す。

表 2.2-1 関係部局における連絡先

部局名	責任者・担当者	役割	電話	代替拠点の電話	携帯電話	メール
○○	○○					
○○	○○					
○○	○○					
○○	○○					
○○	○○					

表 2.2-2 関係企業（委託先等）における連絡先

会社名	担当者	役割	電話	代替拠点の電話	携帯電話	メール
○○	○○					
○○	○○					
○○	○○					
○○	○○					
○○	○○					

ガイドラインの参照先：「2.8.1 危機的事象発生時の体制構築」

2.3. 危機的事象発生時における対応手順

2.3.1. 全体フロー

危機的事象発生時の情報システムの継続及び復旧に係る対応の流れについて、全体フローを以下に示す。

（1）大規模災害発生時の全体フロー

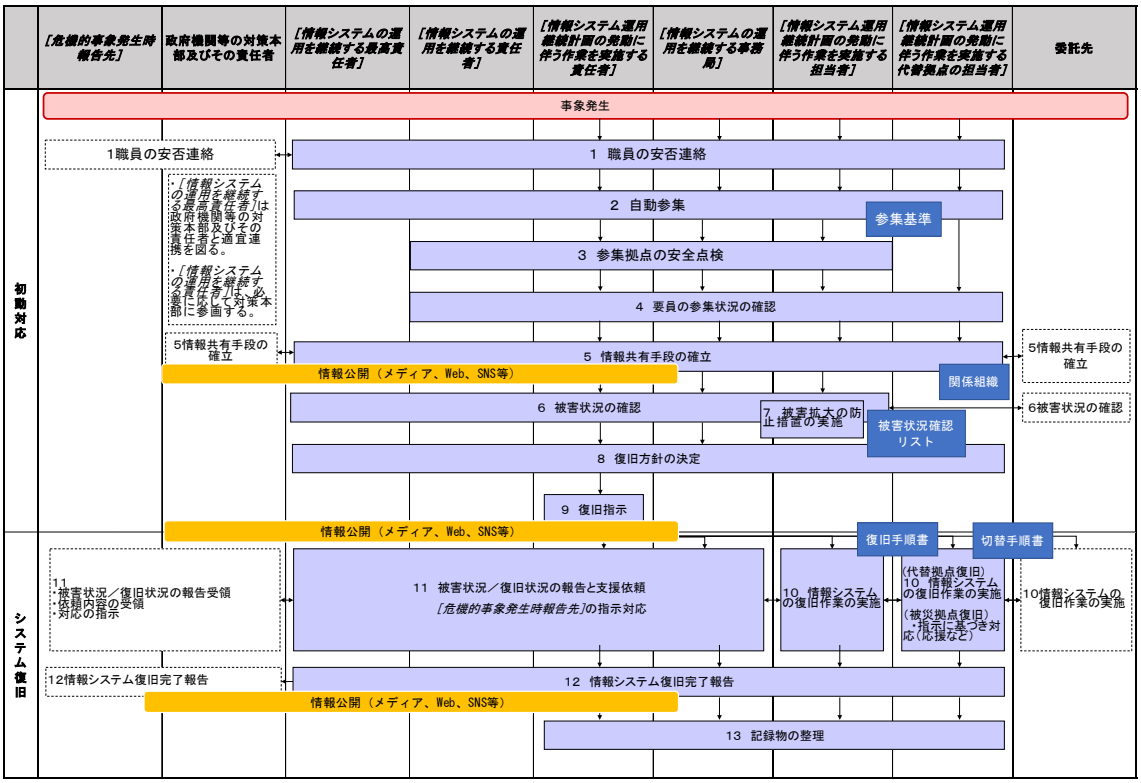


図 2.3-1 大規模災害発生時の全体の対応の流れ

※上記は例示であり、政府機関等で定めた業務継続計画に基づき、情報セキュリティインシデント発生時、感染症発生時等の危機的事象発生時ごとに全体フローを作成する。

※政府機関等の対策本部自体の活動については関連する業務継続計画を参照する。また、危機的事象によっては対策本部が設置されない可能性がある。

※情報セキュリティインシデント発生時の全体フローでは「1．職員の安否連絡」「2．参集拠点の安全点検」は不要であるため削除する。また、危機的事象発生時の連絡先として CSIRT を追加する。

※感染症発生時の全体フローでは、必要に応じて関連する業務継続計画のフローを参照する。

2.3.2. 対応手順

危機的事象発生時の全体フローの各項目について、具体的な対応手順を以下に示す。

（1）大規模災害発生時の対応手順

表 2.3-1 夜間・休日に大規模災害が発生した場合の対応手順

項番	大規模災害発生（夜間・休日）時の対応内容	参照文書類
1	**職員の安否連絡** • 全ての担当者は、自らと家族の安全を確保した後、速やかに安否確認基準に則り安否及び出勤できる時間の目処を連絡する。	○○
2	**自動参集** • 全ての担当者は、テレビやインターネット等のメディア、メールやWeb、SNS等の情報から震度を確認し、指定された場所に自動参集する。 • 参集にあたっては、水、食糧を持参するように努める。 • 参集時は、長そで・長ズボン・ヘルメットの着用や軍手・マスクの準備等、怪我をしないように服装に留意する。	2.1 参集場所 ○○
3	**拠点の安全点検** • 参集した*［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、政府機関等の業務継続計画に基づき、建物の管理担当者と連携して、建物の亀裂や天井の崩落等、参集拠点の安全性を確認する。 • *［情報システムの運用を継続する責任者］*は、政府機関等の業務継続計画の担当者と連携して、情報システム担当部局が所管しない建物の安全、電力供給、水道管破裂等による水損発生の被害状況について確認する。 • 安全が確保できない場合、*［情報システムの運用を継続する最高責任者］*と連絡をとり、代替拠点への移動を指示する。	○○ ○○ ○○
4	**要員の参集状況の確認** • *［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、参集場所における*［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］*の参集状況を確認し、*［情報システムの運用を継続する責任者］*及び*［情報システムの運用を継続する事務局］*に報告する。 • *［情報システムの運用を継続する責任者］*及び*［情報システムの運用を継続する事務局］*は、参集場所における*［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］*の参集状況を確認する。	○○
5	**情報共有手段の確立** • *［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、委託先等の関連組織に、連絡先や早急に依頼すべき事項を連絡する。 • *［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*［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、パソコンや貼り紙等を準備し、*［危機的事象発生時報告先］*や、*［情報システムの運用を継続する事務局］*との情報共有手段を確立する。	○○

項番	大規模災害発生（夜間・休日）時の対応内容	参照文書類
6	**被害状況の確認** • *［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、調査箇所の優先順位を決定し、情報システムの被害状況の確認を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に指示する。*［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］*は確認結果を*［情報システムの運用を継続する最高責任者］*及び*［情報システムの運用を継続する事務局］*に報告する。 • *［情報システムの運用を継続する事務局］*は、随時被害状況の確認結果を記録する。	○○ ○○ ○○
7	**被害拡大の防止措置の実施** • *［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、台帳類やバックアップ媒体等が損傷するおそれがある場合は、安全な場所に搬出する。	○○
8	**復旧方針の決定** • *［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、確認した被害状況をもとに、国民の生命、身体、財産の保護を最優先に考慮した優先順位を定め、今後の情報システムの復旧場所や復旧水準、復旧方式等の対応方針を検討する。また、*［危機的事象発生時報告先］*や各部局に対する依頼事項を取りまとめる。 • *［情報システムの運用を継続する最高責任者］*は、*［政府機関等の対策本部及びその責任者］*との協議の上で復旧方針を決定する。	○○
9	**復旧指示** • （代替拠点で復旧する場合） *［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、被災拠点で目標とする復旧時間内での情報システム復旧が困難と判断した場合、*［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］*に情報システムの切り替えを指示する。 • （被災拠点で復旧する場合） *［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を継続する被災拠点の担当者］*に情報システムの復旧を指示する。また、必要性を鑑み、*［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］*に、自宅待機又は応援要員としての駆けつけを指示する。	○○
10	**情報システムの復旧作業の実施（代替拠点が存在する場合、切り替え作業も含む）** • *［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、復旧指示や復旧方針に基づき、情報システムの復旧作業を行う。必要に応じ委託先に対応を依頼する。また、*［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、適宜復旧状況を*［情報システムの運用を継続する責任者］*及び*［情報システムの運用を継続する事務局］*に報告するとともに、必要な支援を依頼する。	○○ ○○

項番	大規模災害発生（夜間・休日）時の対応内容	参照 文書類
	• *［情報システムの運用を継続する事務局］*は、随時復旧状況を記録するとともに、*［情報システムの運用を継続する責任者］*に必要な支援を行う。また、各部局からの問合せや、*［危機的事象発生時報告先］*からの指示に対して対応する。	
11	**被害状況・復旧状況の報告と支援依頼、*［危機的事象発生時報告先］*の指示対応（以下、継続的に実施）** • *［情報システムの運用を継続する責任者］*は、被害状況と復旧方針、復旧の見込み及び関係部局への依頼事項を、*［危機的事象発生時報告先］*に報告する。また、情報システムの復旧優先度と目標復旧時間を考慮し、*［危機的事象発生時報告先］*に必要な支援を要請する。 • *［情報システムの運用を継続する事務局］*は、*［危機的事象発生時報告先や掲示板等］*をとおし、情報システムの復旧見込みや依頼事項を関係部局に周知する。*［情報システムの運用を継続する最高責任者］*は、*［政府機関等の対策本部及びその責任者］*と必要に応じて協議する。	○○
12	**情報システム復旧完了報告** • *［情報システムの運用を継続する最高責任者］*は、情報システムが復旧した場合、復旧の完了を*［危機的事象発生時報告先］及び［政府機関等の対策本部及びその責任者］*に報告する。 • *［情報システムの運用を継続する事務局］*は、*［危機的事象発生時報告先や掲示板等］*をとおし、情報システムの復旧と依頼事項を関係部局に周知する。	○○
13	**記録物の整理** 全ての担当者は、復旧作業で記載した記録物が紛失しないよう情報を整理する。被災時に記録した内容については、今後の計画の見直しにおける重要な参考資料となることから、特に対応に苦慮した点等があれば、確実に記録に残しておく。	○○

※上記は例示であり、平日昼間に被災した場合の対応手順も作成する。

ガイドラインの参照先：「2.8.2 危機的事象発生時における対応計画」

3. 事前対策計画

3.1. 情報システムを支える構成要素ごとの現状対策レベルとリスク

情報システムの現状対策レベルとリスクの評価結果について、以下に記す。

表 3.1-1 メールシステムにおける現状対策レベルとリスクの評価結果

管理部局		復旧優先度	RLO（目標復旧レベル）
部局 A		A（数時間～数日）	平時の 50%まで復旧
大規模災害におけるリスク			
情報システムを支える構成要素		現状対策レベル[1]	目標対策レベル[2]	情報システムを支える構成要素ごとのリスク
情報システム	ハードウェア	0	3	• 現状、免震又は耐震措置が取られておらず、サーバが損壊する可能性が高い。サーバが損壊した場合、同等機の再調達に長期間（約○週間）を要する。
	システム領域	0	3	• バックアップ媒体が、危機的事象発生時に損壊する可能性のある場所に保管されている。
	データ領域	0	3	• バックアップが未取得であり、被災時に必要なデータが消失する可能性がある。
	・・・	・・・	・・・	• ・・・
外部組織	委託先	0	3	• 担当者の個人連絡先のみ登録されているため、担当者と連絡が取れない場合、委託先の連絡先がわからない可能性がある。
	・・・	・・・	・・・	• ・・・

※政府機関等の業務継続計画において代替拠点を活用する場合は、情報システム運用継続計画にハードウェアやソフトウェア等の追加的措置が必要な場合があるため、必ず確認を行う。

ガイドラインの参照先：「2.7.1 現状の対策の確認及びリスクの評価」

[1]本計画「5.4.2. 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」で定義する対策レベルに沿って、現状の情報システムの運用環境を評価し、現状対策レベルを記載する。
[2]それぞれの対策レベルの内容は、本計画「5.4.2. 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」にて定めている。なお、大規模災害においては、一部復旧でも可とするケースもあることを考慮しても良い。

3.2. 事前対策の実施計画

（1）情報システムの継続性強化方針

情報システムの中長期の事前対策実施方針について、以下に記す。

表 3.2-1 メールシステムにおける中長期の事前対策実施方針

<table>
<tr><th>管理部局</th><th>RTO（目標復旧時間）</th><th>RLO（目標復旧レベル）</th></tr>
<tr><td>部局 A</td><td>数時間～数日</td><td>平時の 50%まで復旧</td></tr>
<tr><td colspan="3">事前対策実施方針</td></tr>
<tr><td colspan="3">ステップ 1（実施予定年度：〇〇年度～〇〇年度）
<table><tr><td>実施内容</td><td>（1）大規模災害に備えた現状のシステムの堅牢化
• サーバの免震又は耐震措置の推進
• バックアップの実施と同時被災しない拠点への外部保管
• 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
（2）情報セキュリティインシデントに備えたルール・手順書の整備
• 不正プログラム感染によりシステムが停止した場合の対処方法の手順化
・・・</td></tr><tr><td>期待効果</td><td>• サーバの免震又は耐震措置により、大規模災害発生時もシステムが停止する可能性が低減される。
• バックアップの確実な実施によりデータの消失を防ぎ、危機的事象発生時に少なくとも復旧可能な状態となる。
・・・</td></tr><tr><td>残存リスク</td><td>• 想定以上の被害に見舞われた場合は、情報システム機器の再調達が必要になり、システムの復旧まで 1～3 ヵ月強の時間を要し、いずれの情報システムも RTO 及び RLO の想定復旧レベルを達成できない可能性がある。
・・・</td></tr></table></td></tr>
<tr><td colspan="3">ステップ 2（実施予定年度：〇〇年度～〇〇年度）
<table><tr><td>実施内容</td><td>（1）外部サービス（データセンター、クラウドサービス等）へのバックアップ（又は移行）
• 委託先のメールやグループウェア等の提供サービスの活用
・・・</td></tr><tr><td>期待効果</td><td>・・・</td></tr><tr><td>残存リスク</td><td>・・・（外部サービス特有の契約上の残存リスクも考慮する）</td></tr></table></td></tr>
<tr><td colspan="3">・・・</td></tr>
</table>

（2）対策ステップ詳細

事前対策実施方針に基づき、各ステップで実施する内容について、以下に記す。

表 3.2-2 メールシステムにおける各ステップで実施する内容

ステップ１	実施予定年度：〇〇年度～〇〇年度 （1） 大規模災害に備えた現状の情報システムの堅牢化 （2） 情報セキュリティインシデントに備えたルール・手順書の整備

ステップ 1-(1)「大規模災害に備えた現状のシステムの堅牢化」対策の詳細一覧

情報システムを支える構成要素		現状レベル	ステップ１到達レベル	対策実施内容	必要予算（千円）	実施主体
情報システム	ハードウェア	0	1	・免震ラックの導入 ・・・		部局Ａ ○担当
	システム領域	0	1	・バックアップ頻度の検討 ・バックアップ方式検討 ・・・		部局Ａ ○担当
	データ領域	1	1	・バックアップ頻度の検討 ・バックアップ方式検討 ・・・		部局Ａ ○担当
	・・・	・・・	・・・	・・・		
外部組織	委託先	0	1	・委託先の緊急時連絡先一覧の作成 ・・・		部局Ａ ○担当
	・・・	・・・	・・・	・・・		

ステップ 1-(2)「情報セキュリティインシデントに備えたルール・手順書の整備」対策の詳細一覧

情報システムを支える構成要素		現状レベル	ステップ１到達レベル	対策実施内容	必要予算（千円）	実施主体
人的資源	情報システム運用体制	0	1	・情報セキュリティインシデントに備えた連絡体制の構築及び対応手順の作成		部局Ａ ○担当

情報システムを支える構成要素		現状レベル	ステップ1到達レベル	対策実施内容	必要予算（千円）	実施主体
外部組織	委託先	0	1	・委託先の緊急時連絡先一覧の作成（上記ステップ1-(1)と共通） ・・・		部局A ○担当

※事前対策実施方針の残存リスクについては、対策が必要であるものの優先順位等の関係で未実施の事項を明記する。

ガイドラインの参照先：「2.7.2 事前対策計画の策定とその実施」

4. 教育訓練計画・維持改善計画

4.1. 教育訓練計画

（1）教育訓練の目的

情報システム運用継続計画の実効性を維持改善していくため、定期的に教育訓練を実施するものとする。

（2）教育訓練の内容

*［情報システムの運用を継続する最高責任者］*及び*［情報システムの運用を継続する責任者］*は、*［4 月］*に年間の教育訓練計画を作成し、計画に沿った訓練が適切に実施されるよう監督するものとする。

（3）教育訓練の評価

*［情報システムの運用を継続する最高責任者］*及び*［情報システムの運用を継続する責任者］*は、教育訓練の目標を定め、その結果を評価し「4.2.維持改善計画」の参考情報として活用する。

年間の教育訓練計画を次頁に示す。

ガイドラインの参照先：「2.9.1 教育訓練の計画とその実施」

令和 XX 年度教育訓練計画 ※可能な限り委託先等関係者の参加を依頼する。

No	教育訓練内容	教育訓練方法	受講対象	教育訓練実施時期												企画者	備考
				上期						下期							
				4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月		
				情報システム運用継続計画見直し ▼					地震防災訓練 ▼								
1	手順書確認訓練	省内訓練	危機的事象発生時の対応体制に定められる者		○												部局A・部局Bにて合同実施
2		省内訓練	一般職員														情報システムの運用継続に関する要件の確認、情報システム停止時の代替業務手順の確認等を実施
3	シナリオ非提示型訓練	省内訓練（外部講師）	危機的事象発生時の対応体制に定められる者										○				
4		省内訓練（外部講師）	一般職員										○				
5	システムリカバリ訓練	省内訓練	危機的事象発生時の対応体制に定められる者						○								委託先A参加

No	教育訓練内容	教育訓練方法	受講対象	教育訓練実施時期												企画者	備考
				上期						下期							
				4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月		
				情報システム運用継続計画見直し ▼					地震防災訓練 ▼								
6	システム切り替え訓練	省内訓練	危機的事象発生時の対応体制に定められる者						○								
7	新規配属者教育	社内研修 外部研修	一般職員	○			○										配属時に随時実施

4.2. 維持改善計画

4.2.1. 計画の実施に伴う維持改善

*［情報システムの運用を継続する最高責任者］*及び*［情報システムの運用を継続する責任者］*は、以下の契機にて、情報システム運用継続計画の見直しを行う。

表 4.2-1 運用継続計画の見直し契機

No	契機	実施内容
1	主要な 事前対策の 完了後	・事前対策に係る現状対策レベルを更新する。 ・必要に応じて危機的事象発生時の対応計画の改訂を行う。
2	訓練実施後	・訓練結果により、事前対策や危機的事象発生時の対応計画等に解決すべき課題が発生した場合、随時課題の解決を図る。 ・短期間での解決が困難な場合は、事前対策の実施計画の見直しを行い、適切に対応する。
3	新規システムの構築時	・新規システムの構築時に、情報システム運用継続計画作成の有無を検討する。作成する場合、ガイドラインに基づき当該システムの情報システム運用継続計画を作成し、必要な対策を調達時の仕様書に盛りこむ。

4.2.2. 危機的事象の発生に伴う維持改善

*［情報システムの運用を継続する最高責任者］*及び*［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で対象とする事象、又はそれに近い事象が発生した際は、事態の収束後、以下の事項についての報告を整理し、情報システム運用継続計画を改訂する。

① 発生事象の分析
　1）発生事象の性質について
　2）発生原因について
② 危機的事象発生時対応の評価
　1）あらかじめ役割を割り当てられた担当者の対応の適切さ
　2）職員の対応の適切さ
③ RTO（目標復旧時間）及びRLO（目標復旧レベル）の達成度合い
　1）実際の復旧時間・復旧レベルについて
　2）対応の実効性について
④ 情報システム運用継続計画の改善点
　1）RTO 及びRLO と実対応ギャップの原因について
　2）その他、情報システム運用継続計画の有効性向上につながる改善点について

4.2.3. 定期的な見直しによる維持改善

*［情報システムの運用を継続する最高責任者］*及び*［情報システムの運用を継続する責任者］*は、毎年*［4月～5月］*頃定期的に以下の内容について確認し、記録（見直し実施日や実施担当者等）を残すものとする。見直しの結果、改善の必要がある場合は適切な措置を講ずる。

表 4.2-2 見直し事項

見直し事項	見直し内容
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。
	• 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。
	• 訓練の結果を踏まえて計画の見直しを行ったか。
	• 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。
危機的事象発生時対応計画	• 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。
	• 教育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。
	• 訓練の結果を踏まえて計画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る、情報システム運用継続計画の見直しの必要性がないか検討したか。
	• 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、危機的事象発生時の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。

ガイドラインの参照先：「2.9.2 維持改善の計画とその実施」

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

（1）対象とする危機的事象

本書で対象とする危機的事象は、ガイドラインの推奨事項に基づき、以下を対象とする。

・大規模災害
・情報セキュリティインシデント
・感染症

（2）危機的事象の発生時の条件

それぞれの危機的事象の発生時の条件については、[政府機関等] の業務継続計画の想定を踏まえるとともに、情報システム運用継続の条件が最も厳しくなるケースを想定し、以下のとおり特定する。

大規模災害（例）
- 都心南部を震源とするM7.3 の地震(東京湾北部地震)が、冬の夕方6 時に風速15m／s の強風の状況下で発生。
- 日曜日の夕方6時発生。
・・・

情報セキュリティインシデント（例）
- 日曜日の午前0時に○○システムが停止。
・・・

感染症（例）
- 東アジアを中心に新型のウイルスによる感染症が流行。
- 月曜日に国内で初めて発症者を確認。
・・・

付録の参照先：「2.1.危機的事象発生時の基本方針」

ガイドラインの参照先：「2.3 危機的事象の特定」

5.2. 想定する被害状況

対象とした危機的事象が発生した際の被害を以下のとおり想定するものとする。

（1）大規模災害発生時の被害想定
大規模災害発生時の被害状況の想定結果について、下表に示す。

表 5.2-1 大規模災害発生時の被害状況の想定結果

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	職員や委託先、協力者が被災し、業務に対応できない可能性がある。
建物・設備	情報システムの設置場所	建物自体は高い耐震・防災性能が確保されており、損傷はなく利用可能。最悪の事象では建物が被災する可能性がある。
	交通インフラ	震度 5 強以上の区域は地震発生後 3 日間途絶。3 日目以降は徐々に回復。30 日で全路線が運行できる程度まで回復。遠地に居住しているため、復旧要員の〇%は〇日間参集できない可能性がある。
	電力	発災直後は断線等により電力供給が中断する可能性が高い。 〇日間は停止する可能性がある。 庁舎内の自家発電装置により発災直後から〇時間は稼働できる。自家発電装置の燃料は補給できない可能性がある。
	水道	断水により〇日間は、庁舎に水道供給されない可能性がある。
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・中断により利用できない可能性がある。 外部と接続する情報通信ネットワークは、断線等が発生し地震の発生後〇日間程度は、事業者による復旧も行われないため使用できない可能性がある。 基幹 LAN についても、同様に通信回線の断線等が発生し、〇日間程度使用できない可能性がある。
	情報システム機器	免震・耐震措置を実施していないシステム機器については、大きく機器が損壊し復旧には機器の再調達が必要とみられる。 免震・耐震措置を実施しているシステム機器については、被害は少ないと思われるが、ディスクが破損し復旧にディスクの交換が必要な可能性がある。
	データ	損壊したシステムのデータは、バックアップを取得していない場合、消失する可能性が高い。

上記の被害を想定するにあたり、情報システム設置場所、交通機関、電力、水道及び電話については、業務継続計画等と同様の被害を想定した。また、情報通信ネットワーク、情報システム機器及びデータについては、情報システム設置場所の被害を考慮の上想定した。

（2）情報セキュリティインシデント発生時の被害想定

情報セキュリティインシデント発生時の被害状況の想定結果について、下表に示す。

表 5.2-2 情報セキュリティインシデント発生時の被害状況の想定の結果

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	被害はないが、職員や委託先、協力者が業務に対応できない時間帯の可能性がある。
建物・設備	情報システムの設置場所	被害はなく平常どおり利用可能。
	交通インフラ	被害はなく平常どおり利用可能。
	電力	被害はなく平常どおり利用可能。
	水道	被害はなく平常どおり利用可能。
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）のサービスは被害がなく、平常どおり利用可能。 物理的被害はないが、外部から大量の処理要求が殺到することで、LAN やインターネット回線を介するシステムが利用できない。
	情報システム機器	物理的被害はないが、想定をはるかに上回る急激な処理要求の増大が予想され、極端な処理の遅延や停止の発生が考えられる。
	データ	○○システムで提供している○○が改ざん、消去される可能性がある。

情報システムが利用できなくなることを除き、ライフライン等に対する影響は生じないと想定されるため、上記のとおり被害を想定した。

（3）感染症発生時の被害想定

感染症発生時の被害状況の想定結果について、下表に示す。

表 5.2-3 感染症発生時の被害状況の想定の結果

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	職員や委託先担当者、協力者が罹患し、罹患者及び濃厚接触者が一定期間隔離され、業務に対応できない可能性がある。
建物・設備	情報システムの設置場所	物理的被害はないが、情報システムの設置場所の管理者が罹患した場合、消毒作業等の対応が必要となり一時的に立ち入れない可能性がある。
	交通インフラ	感染症の拡大により公共交通機関はダイヤを変更する可能性がある。
	電力	被害はなく平常どおり利用可能。
	水道	被害はなく平常どおり利用可能。
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）のサービスは被害がなく、平常どおり利用可能。 物理的被害はないが、テレワークが推奨された場合はアクセスの集中により通信回線帯域が不足する可能性がある。また、テレワーク用ソフトウェアのライセンスが不足する可能性がある。
	情報システム機器	物理的被害はないが、新たな調達機器の納入や既存機器が故障した場合の交換に時間を要する可能性がある。
	データ	被害はなく平常どおり利用可能。

※上記の想定の例によらず、各政府機関によって想定される被害想定を検討の上で記載することに注意すること。例えば、電話局火災、更新後のソフトウェアの不備、テレワークの増加による回線のひっ迫、といった事象によって情報ネットワークが停止する場合もあることに留意する。

付録の参照先：「2.3.2 対応手順」

ガイドラインの参照先：「2.4 被害想定」

5.3. 情報システムの復旧優先度の設定

ガイドラインに記載される方法に基づき情報システムに対し、目標復旧時間（以下「RTO」という。）及び目標復旧レベル（以下「RLO」という。）を設定した。検討結果を以下に示す。

（1）業務の RTO と情報システム停止時の代替手段の検討

*［情報システムの運用を継続する責任者及び担当者］*は、既存の業務継続計画を確認し業務の RTO を「別表 1. 業務システム関連表」に記載する。下表を利用し、以下の検討結果を記載する。

1. 業務継続計画に定められた非常時優先業務と情報システムの関連性
2. 業務継続計画に定められた非常時優先業務の RTO 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

表 5.3-1 業務の RTO と情報システム停止時の代替手段分析結果

非常時優先業務	業務の RTO	業務を支える情報システム	情報システム停止時の代替手段の有無	代替手段で継続可能な時間	RTO（目標復旧時間）	RLO（目標復旧レベル）
○○業務	3 時間	メールシステム	初期段階では電話による業務遂行が主なため、メールは必須ではない。	12 時間	15 時間	完全復旧
・・・						

それぞれの情報システムと優先業務の関連性の一覧は、「別表 1. 業務システム関連表」に記す。

（2）RTO 及び RLO 検討結果

「（1）業務の RTO と情報システム停止時の代替手段の検討」での検討結果に基づき、情報システムの RTO 及び RLO を設定した。また、RTO 及び RLO の設定結果に基づき、情報システムの復旧優先度を 6 段階（S、A、B、C、D、E）に整理した。整理結果を以下に示す。

表 5.3-2 情報システムの RTO 及び RLO の検討結果

情報システム名	システム概要	RTO（目標復旧時間）	RLO（目標復旧レベル）	復旧優先度	情報システム管理部局
メールシステム	電子メール送受信用のシステム	15 時間	完全復旧	A	部局 A
システム A	・・・	1 日	平時の 70%まで復旧	A	・・・
システム B	・・・	・・・	・・・	・・・	・・・
・・・					

なお、上記表の情報システムの復旧優先度は、以下を基準とする。

表 5.3-3 情報システムの復旧優先度

情報システムに求められる RTO（目標復旧時間）	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

※（1）について、大規模災害においては、一部復旧でも可とするケースもあることを考慮しても良い。

※表 5.3-3 は RTO に基づく復旧優先度を例示しているが、政府機関等にて検討した方法で、RTO 及び RLO を総合的に判断して復旧優先度を定める。

付録の参照先：「3.1.情報システムを支える構成要素ごとの現状対策レベルとリスク」

ガイドラインの参照先：「2.5 情報システムの復旧優先度の設定」

5.4. 情報システムを支える構成要素の関連整理

5.4.1. 情報システムを支える構成要素の整理

危機的事象の発生に備え、情報システムを支える構成要素について整理する。ガイドラインの例、*[政府機関等]* の業務継続計画内で作成している危機的事象発生時の対応手順、既に作成している情報システム運用継続の対応手順等を参考にしながら、危機的事象が発生した際の対応をイメージし、必要な要素に漏れがないように洗い出す。

（1）大規模災害に備えた情報システムを支える構成要素の整理
大規模災害に備えた情報システムを支える構成要素の整理について、下表に示す。

表 5.4-1 大規模災害に備えた情報システムを支える構成要素の整理

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体制と役割分担、手順書の整備及び連絡手段の確保
建物・設備	施設	情報システム機器の設置環境（庁舎、代替拠点、データセンターの場所・堅牢性・自家発電装置の有無・バックアップセンターの有無、電力系統の冗長性、上下水道等）
情報システム	ハードウェア	サーバ等のハードウェア機器の台数及び所在（代替機がある場合はそれも含む）（代替拠点においても同様に確認する）
	システム領域	アプリケーションやシステム設定情報等の情報システム復旧に必要なデータの所在及び管理状況（バックアップ媒体の外部保管等）（代替拠点においても同様に確認する）
	データ領域	重要なデータの所在及び管理状況（バックアップ媒体の外部保管等）（代替拠点においても同様に確認する）
	情報通信ネットワーク	情報システムを利用するために必要な情報通信ネットワーク（庁舎内及び拠点間等の外部接続）の敷設状況（利用キャリア・種類・ルート分散状況等）（代替拠点においても同様に確認する）
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把握、SLA の締結等（代替拠点においても同様に確認する）

※上記は例示であり、政府機関等で定めた業務継続計画に基づき、情報セキュリティインシデント発生時、感染症発生時等の危機的事象発生時ごとに構成要素を整理する。

付録の参照先：「3.1.情報システムを支える構成要素ごとの現状対策レベルとリスク」

ガイドラインの参照先：「2.6.1 情報システムを支える構成要素の明確化」

5.4.2. 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

情報システムの復旧優先度に対応する対策目標（目標対策レベル）を、目標復旧時間を踏まえ情報システムを支える構成要素ごとに整理した。設定結果を以下に示す。

（1）大規模災害に対する情報システムの復旧優先度に対応する対策目標

表 5.4-2 ハードウェアにおける復旧優先度別の対策目標

情報システムの復旧優先度	対策目標	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、バックアップ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		
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、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、被災時に情報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 5.4-3 システム領域における復旧優先度別の対策目標

情報システムの復旧優先度	対策目標	対策レベル
S	**ホットスタンバイ方式** ・本番機のシステムメンテナンス時に、本番機のシステム領域のバックアップデータを代替拠点の代替機上に転送している。 ・代替機についてもシステムメンテナンスを行い、切替可能な環境を保っている。	4
A B	**ウォームスタンバイ方式** ・本番機のシステムメンテナンス時に、本番機のシステム領域のバックアップデータを代替拠点の代替機上に転送している。	3
C D	**コールドスタンバイ方式** ・システムメンテナンス時にシステム領域をバックアップし、予備機の準備してある代替拠点に転送（配送）、保管している。 ・災害発生時は、バックアップからリストアし、予備機に反映する。	2
E	**外部サービス（データセンター、クラウドサービス等）への移行** ・システムメンテナンス時にバックアップ媒体（テープ等）にシステム領域をバックアップし、本番機と同時被災しない遠隔地又は堅牢な金庫に保管している。災害発生時は、バックアップを取り寄せる。又は堅牢なデータセンターや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外部サービスを利用する。	1

表 5.4-4 データ領域における復旧優先度別の対策目標

情報システムの復旧優先度	対策目標	対策レベル
S	・代替拠点で、データ同期を利用し本番環境における災害発生直前のデータを保全している。	4
A B	・代替拠点で、オンラインバックアップ[1]を利用し本番環境における災害発生時数時間前のデータを保全している。	3
C D	・代替拠点で、オンラインバックアップを利用し本番環境における災害発生時１日前のデータを保全している。	2
E	・本番機と同時被災しない遠隔地又は堅牢な金庫に、災害発生時１週間前のデータを保全している。災害発生時は、バックアップを取り寄せる。又は堅牢なデータセンターや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外部サービスを利用する。	1

[1] オンラインバックアップ：情報通信ネットワークを介してバックアップデータを転送する方式のこと。本番環境の性能に影響を与えるため、本番環境が利用されない夜間等の時間帯を利用する必要がある。

表 5.4-5 委託先の事業継続能力における復旧優先度別の対策目標

情報システムの復旧優先度	対策目標	対策レベル
S A B	**契約の締結** （対策レベル 2 に加え） ・委託先との SLA、災害時協定に関する条項を、契約書や仕様書の中に含めている。	3
C D	**事業継続能力の把握** （対策レベル 1 に加え） ・事業継続への取り組みについて委託先に質問するアンケートを配布する等して、情報システムの復旧対応において必要不可欠な委託先の事業継続能力を把握している。	2
E	**連絡先の明確化** ・情報システムの復旧対応において必要不可欠な委託先（ハードウェア・ソフトウェアの調達先、システム構築業務の委託先等）が明確になっている。 ・同委託先の緊急時連絡先（窓口及び代替拠点先）が代理者も含め明確になっている。	1

※（1）は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した目標対策レベルを例として記載している。政府機関等の検討結果に応じて、適切な対策レベルを設定する。

付録の参照先：「3.1.情報システムを支える構成要素ごとの現状対策レベルとリスク」

ガイドラインの参照先：「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」

別表 1.業務システム関連表

No.	情報システム名	部局	部局A								情報システム目標復旧時間（最小値）*1	リスク・課題	リスク・課題に対する対策
		業務名	優先業務1	優先業務2	優先業務3								
		環境	外部委託先 省庁内	省庁内	関係各所								
		業務目標復旧時間	3時間	1日	3日								
1	メール管理システム		●	●	●						3時間	外部委託先との対応連携	SLA見直し
2	システムA			●							1日	システム冗長化	バックアップ拠点の見直し
3	システムB				●						3日	担当者・職員が登庁できない	対応計画の見直し
4													
5													
6													
7													
8													
9													

*1同一システム上で行われている各優先業務の中で業務目標復旧時間が最も短い時間を記載する。

別表 2.災害用携行カード

本カードは、定期入れや財布に納め、
常に携帯するようにしてください。

[災害用]携行カード

本人情報

氏名	
住所	
携帯電話番号	
自宅電話番号	
保険証番号	
終業時の避難場所	
自宅付近の避難場所	

自由記入欄	

1.初動対応

屋内	屋外
1. 落ちついて行動 2. 棚や窓から離れるなどして身を守る 3. 揺れが収まったら落ち着いて火元を確認 4. 戸を開けて、出入り口の確保 5. 靴を履き、非常時持ち出し品を準備 6. 消火活動・救助活動に協力	1. 落ちついて行動 2. 鞄などで頭を保護し、できるだけ建物から離れる（ビルの外壁、看板、窓ガラスなどに注意） 3. 切れた電線には近寄らない 4. 避難の際は車を利用しない 5. 消火活動・救助活動に協力

2.参集基準と参集場所

・東京都において、震度6弱以上の地震が観測された場合
・責任者が指示した場合

参集場所
第1順位： 第2順位：

参集場所について別途指示がある場合は、それに従う。

3-1.家族への連絡先

氏名	連絡先

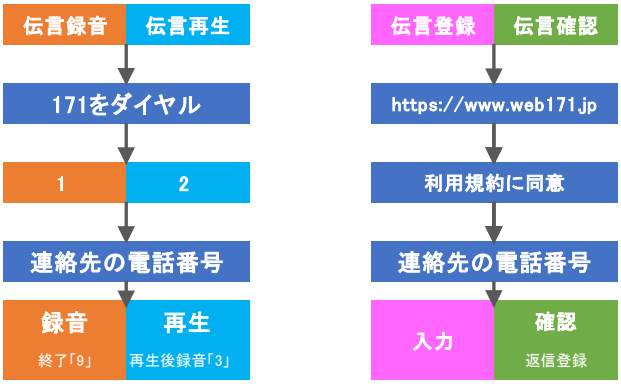
緊急時の集合場所	

3-2.職場への連絡先

	所属/氏名等	連絡先		
		携帯電話番号	携帯メール	自宅電話
安否報告先				

連絡内容 （安否/連絡手段等）	

4-1.災害用伝言ダイヤル「171」／災害用伝言版「web171」



4-2.携帯電話　災害用伝言板サービス

	URL	スマートフォン/携帯電話	
		アプリ	アクセス方法
DoCoMo	http://dengon.docomo.ne.jp/	・ドコモケータイ（iモード） 「iMenu」→「災害用安否確認」→「災害用伝言版」 「dメニュー」→「災害用安否確認」→「災害用伝言板」 ・スマートフォン 「災害用キット」アプリを選択 ・ドコモケータイ（spモード） メニューの「あんしん」を選択	
au	http://dengon.ezweb.ne.jp/	・au災害対策アプリ https://www.au.com/mobile/service/saigai-taisaku/	・ケータイ（4G LTE） メニュー画面 ＞ アプリ ＞ au災害対策 ＞ 災害用伝言板 ・auケータイ（3G）から EZボタン ＞ トップメニュー ＞ 災害用伝言板
SoftBank	http://dengon.softbank.ne.jp/	・iPhone、iPad https://apps.apple.com/jp/app/id425650996#softbank ・スマートフォン、タブレット https://play.google.com/store/apps/details?id=jp.softbank.mb.dmb&hl=ja	・4Gケータイ メインメニューから「サービス」または「安心機能」を選択し、「災害用伝言板」を選択 ・3Gケータイ Yahoo!ケータイのトップから「災害用伝言板」を選択