# 松山市ICT部門業務継続計画
# （松山市ICT－BCP）

４．３版

令和８年 10 月

システム管理課

■計画の新規発行／改定記録

| 発行／改定年月日 | 版数 | 文書の新規発行／改定内容 | 備考 |
|---|---|---|---|
| 平成 24 年 5 月 | 1.0 | 新規発行 | 高度情報化推進委員会で承認 |
| 改定<br>平成 26 年 4 月 | 1.1 | ・計画の運用体制や緊急時対応体制等を最新化<br>・非公開情報を別紙に移行 | |
| 改定<br>平成 26 年 8 月 | 1.2 | ・松山市電子計算組織の管理運営に関する規則の全部改定に伴う文言修正 | |
| 改定<br>平成 28 年 3 月 | 2.0 | ・CISO、CSIRT の設置に伴う運用体制、行動計画等の修正<br>・地域防災計画の見直しに伴う被害想定の修正 | 高度情報化推進委員会で承認 |
| 改定<br>平成 30 年 3 月 | 3.0 | ・ICT-BCP＜初動版＞作成<br>・ICT-BCP＜初動版＞作成に伴う資料等の修正 | 高度情報化推進委員会で承認 |
| 改定<br>平成 31 年 4 月 | 3.1 | ・職員異動、課名変更に伴う資料等の修正 | |
| 改定<br>令和 2 年 4 月 | 3.2 | ・職員異動等に伴う資料等の修正 | |
| 改定<br>令和 3 年 4 月 | 3.3 | ・職員異動等に伴う資料等の修正 | |
| 改定<br>令和 4 年 4 月 | 3.4 | ・職員異動、課名変更に伴う資料等の修正 | |
| 改定<br>令和 5 年 4 月 | 3.5 | ・職員異動に伴う資料等の修正 | |
| 改定<br>令和 5 年 10 月 | 3.6 | ・職員異動に伴う資料等の修正 | |
| 改定<br>令和 6 年 4 月 | 3.7 | ・職員異動に伴う資料等の修正<br>・高度情報化推進委員会の名称変更 | |
| 改定<br>令和 6 年 7 月 | 3.8 | ・情報セキュリティポリシーの改定に伴う資料等の修正 | |

| | | | |
|---|---|---|---|
| 改定<br>令和 6 年 10 月 | 3.9 | ・職員異動に伴う資料等の修正 | |
| 改定<br>令和 7 年 4 月 | 4.0 | ・職員異動等に伴う資料等の修正 | |
| 改定<br>令和 7 年 10 月 | 4.1 | ・職員異動に伴う資料等の修正 | |
| 改定<br>令和 8 年 4 月 | 4.2 | ・職員異動に伴う資料等の修正 | |
| 改定<br>令和 8 年 10 月 | 4.3 | ・職員異動に伴う資料等の修正 | |

# 目　　次

１．ＩＣＴ部門の業務継続計画の趣旨・基本方針 ---------- １
（１）業務継続計画の趣旨 …… １
（２）基本方針 …… １
（３）計画策定の前提 …… ２
２．被害想定---------- ３
３．重要システム---------- ５
４．リソースの現状（脆弱性）と代替の有無 ---------- ６
５．被害を受ける可能性と事前対策計画 ---------- ７
６．緊急時対応・復旧計画---------- ７
（１）緊急時対応体制 …… ７
（２）緊急時における行動計画 …… １０
（３）代替・復旧の行動計画 …… １５
７．本計画の維持管理---------- １８

## １．ＩＣＴ部門の業務継続計画の趣旨・基本方針

### （１）業務継続計画の趣旨

「業務継続計画」とは、大規模な災害、事故、事件等（以下、「災害･事故」という。）で松山市の庁舎、職員等に相当の被害を受けても、重要業務をなるべく中断させず、中断してもできるだけ早急に（あるいは、許容される時間内に）復旧させるために策定するものである。

松山市が平常時に提供している行政サービスが長期間停止した場合、市民生活や経済活動に大きな支障を生じる。また、災害・事故の発生時は、たとえ庁舎、職員等に相当な被害が発生しても、市民の救助･救援の責任ある担い手として、災害応急対応、災害復旧の業務を実施しなければならない。このため、災害・事故時においても市の重要業務を実施・継続できるような周到な備えが不可欠である。

特に、市の業務の実施・継続には、今日において、その業務を支える情報システムやネットワーク等の稼働が必要不可欠である。また、情報システムやネットワーク等は、あらかじめ対策を講じておかないと、災害・事故の発生後から対策を始めるのでは、稼動できないことはもとより、早期復旧も困難であるという特性を持つ。そこで、「ＩＣＴ部門の業務継続計画」を策定し、災害･事故時の重要業務の実施･継続を行う基盤を整えることとする。

### （２）基本方針

本計画を策定するにあたり、次の事項を基本方針とする。

| 基本方針 | |
|---|---|
| ＩＣＴ部門の責務遂行 | 災害・事故時の業務の継続･早期復旧に当たっては、市民の生命の安全確保、市民生活や地域経済活動の早期復旧のために必要となる市の重要システムを最優先で復旧する。 |
| 来訪者、職員、関係者の安全 | 災害・事故時の業務の継続・早期復旧に当たっては、執務室等への来訪者、職員、契約先職員その他の関係者の安全確保を第一とする。 |
| 計画書の有効性の維持･改善 | 本計画は、適切に関係者に周知し、訓練を行い、また常に最新の状況を反映した計画となるよう点検を行う。そして、それらの結果を踏まえて是正措置を講ずるとともに、少なくとも年に1度定期的に（前提条件に大きな変更があればその都度）、計画の全般にわたる見直しを行う。 |
| 関係機関との連携 | 外部事業者等と連携し、松山市のＩＣＴ部門の業務継続を図り、代替対応の可能な業務継続計画を立案する。 |

## （３）計画策定の前提

ア　計画の対象範囲

本計画の対象範囲は、システム管理課が管理するシステム（電子計算室内サーバ、庁内ＬＡＮ等）とする。

各課が独自に管理運営する情報システムについては、今後、本計画を参考に各主管課が業務継続計画を策定することとする。

イ　対象リスク

本計画の対象リスクは、震度６弱を想定する。なお、被害想定については、「松山市地域防災計画（地震災害対策編）」の被害想定と同様とする。

また、大規模地震に類似した災害、新型インフルエンザ及びそれに類似した感染症に対しても、当計画を準用して対応するものとする。

ウ　計画の発動

本計画の発動は、災害対策本部（大規模地震等の場合）、それに類似した本部が設置されたとき、総合政策部長が発動を決定する。

エ　計画の構成

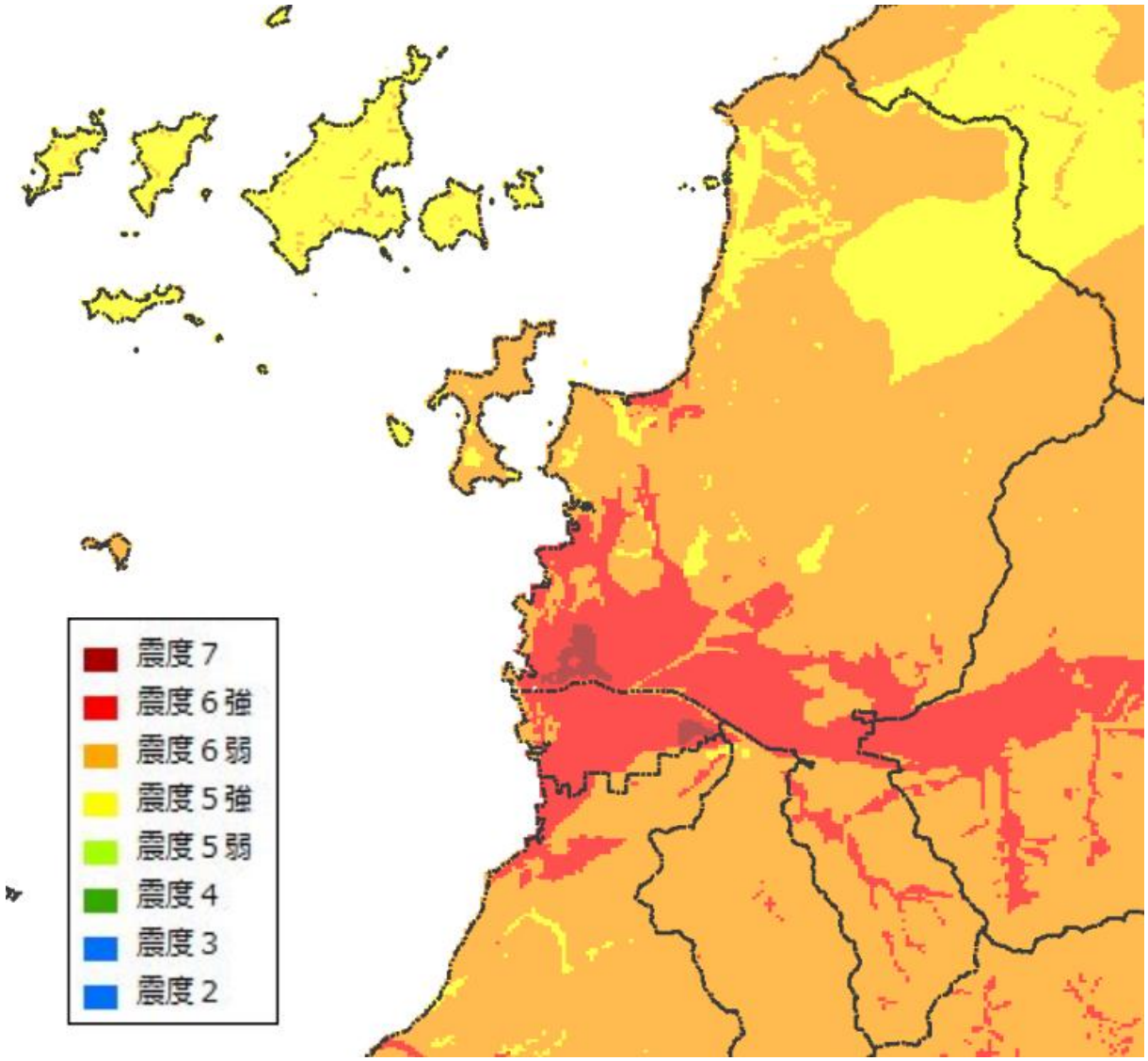
本計画の構成は、「地方公共団体におけるＩＣＴ部門の業務継続計画（ＢＣＰ）策定に関するガイドライン」の第３章全体を踏まえたものである。

## ２．被害想定

松山市では、発生時の影響度及び発生する可能性を考慮して、以下の事象が発生したことを想定して検討する。

災害による被害の想定

| | |
|---|---|
| **災害の想定** | **震度６弱の地震** |




推定震度分布図（想定地震：南海トラフ巨大地震（陸側ケース）　Ｍ９．０）

※出典：松山市地域防災計画（地震災害対策編）

Ａ．想定する災害・事故の度合い

① 地震発生時期　　就業時間内及び就業時間外、休日

② 震　　度　　６弱

Ｂ．想定される被害

| 項目 | | 想定被害状況 |
|---|---|---|
| 庁舎 | 本館 | 耐震工事済みのため、倒壊せず庁舎利用可能。<br>庁舎内の固定していない什器・備品は転倒している。 |
| | 別館 | 耐震工事済みのため、倒壊せず庁舎利用可能。<br>庁舎内の固定していない什器・備品は転倒している。 |
| | 第3別館 | 耐震工事済みのため、倒壊せず庁舎利用可能。<br>庁舎内の固定していない什器・備品は転倒している。 |
| | 第4別館 | 耐震工事済みのため、倒壊せず庁舎利用可能。<br>庁舎内の固定していない什器・備品は転倒している。 |
| 庁舎内の機器 | 空調装置 | 庁舎が耐震工事済みのため、空調設備が影響の可能性は低い。 |
| | サーバ関連 | アンカーボルトによりラックを固定及びラック同士を連結して固定しているため、転倒等の可能性は低いが、ディスク故障等のため、再稼働まで数日を要するサーバがある程度想定される。 |
| | パソコン（マイナンバー利用事務系） | セキュリティワイヤー等により落下はある程度は防げると予想されるが、それでも２０％程度のパソコンが利用できないと想定される。 |
| | パソコン（マイナンバー利用事務系以外） | セキュリティワイヤー等により落下はある程度は防げると予想されるが、それでも２０％程度のパソコンが利用できないと想定される。 |
| 要　員 | | ○就業時間内<br>システム管理課職員の負傷者は軽微と想定される。<br>○就業時間外、休日<br>家屋倒壊によりシステム管理課でも登庁できない職員が出る可能性がある。<br>災害発生後１時間以内で５０％程度、翌朝までには８０％程度の職員が参集できると想定される。 |

| | | |
|---|---|---|
| ライフライン・インフラ | 電力 | 発生直後は断線などにより電力供給が７０％程度*停止すると想定している。 |
| | 水道 | ５９%程度*の断水が想定される。 |
| | 電話 | 固定・携帯電話とも回線が不通になり、職員や業者等との連絡に影響が生じる。 |
| | 道路 | 道路の被害により通行止めや通行規制が発生し、職員や業者等の登庁や交換部品の配送等に影響が生じる。 |
| | 交通機関 | 軌道敷等の被害により鉄道が不通となり、職員や業者等の登庁や交換部品の配送等に影響が生じる。 |

＊　松山市地域防災計画（地震災害対策編）の想定地震Ｉによる

## ３．重要システム

本計画で対応する重要システムの目標復旧時間を別紙１のとおり設定する（別紙１は、情報セキュリティ確保のため、非公開とする。）。

## ４．リソースの現状（脆弱性）と代替の有無

○システム機器設置場所の状況

| 項目 | 電子計算機室・サーバ室 |
|---|---|
| 主な設置機器 | マイナンバー利用事務系システム機器、LGWAN 接続系システム機器 |
| 建物の耐震性 | 震度６強まで耐震性あり |
| システム機器の耐震対策の実施状況 | アンカーボルトによるラックの固定及びラック同士を連結することによる固定を行っている。 |
| 室の耐火対策 | ハロゲン化消火装置を設置 |
| フロアの耐水対策 | 浸水予想区域外 |

※電算室については、ハロゲン化消火装置を設置しているが、上の階等で水による消火を行った場合、雨漏り等の危険性がある。そのため、電算室全体の耐水対策を考える必要がある。

○電力供給、通信手段に関するリスク

A．電力供給について

| | |
|---|---|
| 非常用電源が情報通信機器の作動に必要な容量まで準備されているか。 | ■　あり<br>□　なし |
| 何時間稼働できるだけの燃料の準備があるか。 | ２０時間 |
| 燃料に関する供給契約があるか | □　あり<br>■　なし |

B．通信手段について

| | |
|---|---|
| 災害時優先電話もしくは衛星電話が準備されている。 | □　あり<br>■　なし（危機管理課にはあり） |
| 非常用連絡手段として、ＩＣＴ部門の職員の携帯メールアドレスを一元管理しているか。 | ■　している<br>□　していない |
| 非常用連絡手段として、保守事業者の要員の連絡手段を一元管理しているか。 | ■　している<br>□　していない |

○情報システムのバックアップ状況及び運用体制

別紙２のとおり（別紙２は、情報セキュリティ確保のため、非公開とする。）。

## ５．被害を受ける可能性と事前対策計画

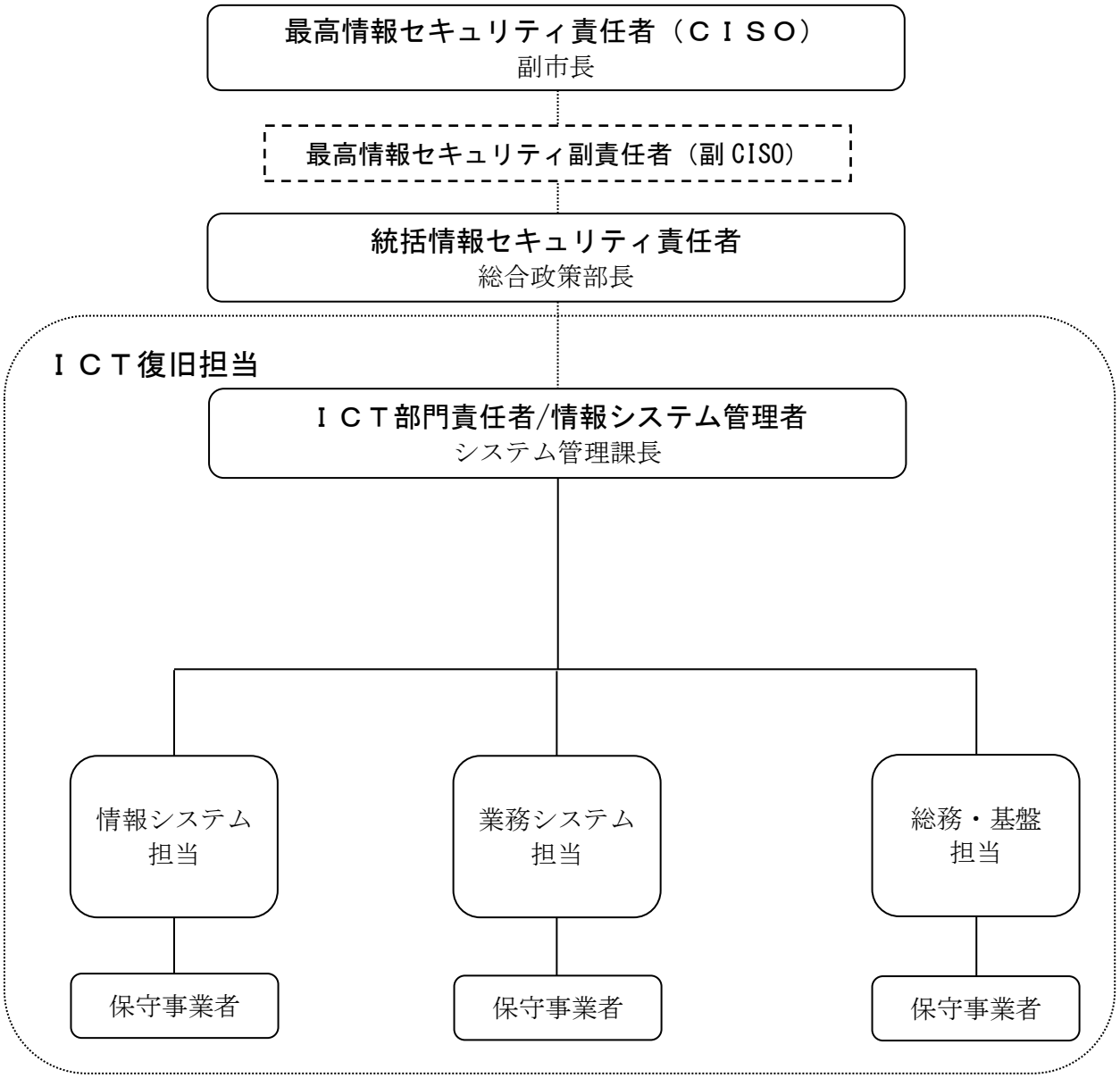
情報通信機器及び情報システムの脆弱性の調査結果、及び調査結果を踏まえての対策等は別紙３のとおり（別紙３は、情報セキュリティ確保のため、非公開とする。）。

## ６．緊急時対応・復旧計画

### （１）緊急時対応体制

緊急時は、下図のとおり最高情報セキュリティ責任者（ＣＩＳＯ）の下で、被害情報の収集及び復旧に当たるものとする。

また、災害対策本部や各システム所管課、保守事業者などの関係者と連携し、対応しなければならない。




※各担当は、手の空いた者から他の担当の応援をする。

ア.各担当の役割

| 担　当 | 役　　割 |
|---|---|
| ＩＣＴ部門責任者 | ・ＩＣＴ部門の業務継続に関わる調査や対応活動の開始と終了の判断及び指示<br>・情報システムの業務継続に関する方針や方法の意思決定<br>・災害対策本部への状況報告及び本部決定の部門内への伝達<br>・他の業務部門との調整の総括、支援依頼 |
| 情報システム管理者 | ・ＩＣＴ部門責任者の補佐<br>・被害状況の確認と復旧、保守事業者等への支援依頼等に関する指揮 |
| 情報システム担当 | ・以下の被害状況の確認と復旧<br>LGWAN接続系システムのサーバ<br>LGWAN接続系システム<br>ネットワーク全般<br>LGWAN接続系端末、タブレット<br>・機器及びソフト導入業者への支援依頼<br>・保守事業者への支援依頼 |
| 業務システム担当 | ・以下の被害状況の確認と復旧<br>マイナンバー利用事務系システムのサーバ<br>マイナンバー利用事務系システム<br>マイナンバー利用事務系ネットワーク<br>マイナンバー利用事務系端末<br>・機器及びソフト導入業者への支援依頼<br>・保守事業者への支援依頼 |
| 総務・基盤担当 | ・地域イントラネットの被害状況の確認と復旧<br>・空調設備、電源設備<br>・保守事業者への支援依頼<br>・災害対策本部の情報処理<br>・他担当の支援 |

※ＩＣＴ部門責任者が不在の場合は、代行者１が役割を担当する。責任者、代行者１がともに不在の場合は代行者２が、代行者２も不在の場合は代行者３が役割を担当する。

| 役　割 | 職　　名 |
|---|---|
| ＩＣＴ部門責任者 | システム管理課長 |
| 代行者１ | 総務・基盤担当執行リーダー |
| 代行者２ | 情報システム担当執行リーダー |
| 代行者３ | 業務システム担当執行リーダー |

イ. 対応要員と参集ルール

（ア）初期対応要員による自動参集

震度４の地震が発生した場合は、ＩＣＴ部門責任者、情報システム管理者及び各執行リーダーが自動参集し、その他の初期対応要員についても、必要に応じてＩＣＴ部門責任者の指示により自動参集する。

震度５弱の地震が発生した場合は、ＩＣＴ部門責任者、情報システム管理者及びすべての初期対応要員が自動参集する。

| 役割 | 所属 | 震度４ | 震度５弱 |
|---|---|---|---|
| ＩＣＴ部門責任者 | システム管理課長 | ○ | ○ |
| 情報ｼｽﾃﾑ管理者 | システム管理課長 | ○ | ○ |
| 初期対応要員 | 情報システム担当執行リーダー | ○ | ○ |
| | 情報システム担当執行グループ職員 | ※ | ○ |
| | 業務システム担当執行リーダー | ○ | ○ |
| | 業務システム担当執行グループ職員 | ※ | ○ |
| | 総務・基盤担当執行リーダー | ○ | ○ |
| | 総務・基盤担当グループ職員 | ※ | ※ |

※ＩＣＴ部門責任者の指示により参集する。

（イ）全員参集

システム管理課職員は、次の場合には、全員自動参集とし、全員が対応要員となる。

(a) 松山市内で震度５強以上の地震が発生した場合

(b) 復旧見込みの立っていない大規模ネットワーク障害、停電が本庁舎周辺で発生したことが報道された場合

（ウ）その他

上記以外の災害・事故が発生した場合の参集及び行うべき対応については、ＩＣＴ部門責任者の指示により行う。

（エ）安否確認及び参集確認

・安否確認及び参集確認は、震度５弱以上の地震が発生した場合に行う。
・安否確認担当者は、総務・基盤担当執行リーダーとし、その代理は情報システム担当執行リーダーが行う。
・安否確認の作業は、就業時間内は執務室で行う。終業時間外の場合は執務室に出勤して行うのを原則とするが、庁舎に入れない場合、参集ができない場合等については、ＩＣＴ部門責任者の指定する場所で行う。
・職員は、自動参集に該当する災害・事故の発生時には、安否確認担当者に安否の連絡を行う。
・連絡のない職員に対しては、安否確認担当者から連絡を継続的に試みる。
・連絡方法は下記のとおりとする。

職員は、総務・基盤担当執行リーダー及び情報システム担当執行リーダーの携帯メールまたは、ＬｏＧｏチャットで参集の可否及び参集時間を連絡する。この手段で連絡ができない場合は、システム管理課又は総務・基盤担当執行リーダーに電話する。

ウ. 保守事業者への支援依頼

大規模な災害が発生した場合は、必要に応じて、保守事業者に支援を要請する。

## （２）緊急時における行動計画

ア. 参集要領

システム管理課の職員は、（１）のイにより参集し、システムの被害状況確認、対応活動を開始するものとする。

イ. 実施項目（初期対応項目）

※各項目を実施後、チェック欄にチェックを入れる。補足欄には、必要に応じて復旧手順の補足事項を記載する。なお、補足欄中の別紙については、個人情報保護及び情報セキュリティ確保のため、非公開とする。

（ケース１：就業時間内の場合）

| No. | 復旧手順 | チェック | 補足 |
|---|---|---|---|
| 1 | **来訪者･職員等の負傷者対応、誘導**<br>□ＩＣＴ部門内及び周辺の来訪者、職員（契約先職員等を含む。以下同じ。）で負傷しているものへの応急措置を行う。また、重傷者以外の来訪者については、次項２の避難の必要性がない場合には、適切な場所へ誘導して集め、そこに当分の間、とどまるよう要請する。 | | |
| 2 | **庁舎からの避難**<br>□避難指示があった場合又は庁舎にとどまっていると危険と判断される場合には、来訪者、職員を庁舎の外の安全な場所に退避させる。来訪者については、適切に誘導する。 | | |
| 3 | **初期消火、延焼防止措置等の二次被害防止策**<br>□ＩＣＴ部門及びその周辺で火災が発生し、初期消火が有効であると判断される場合には、火災の発生を庁舎管理部門に至急連絡するとともに、可能な範囲内で初期消火を行う。<br>□庁舎内で小規模な火災が発生し、緊急避難が必要でない場合には、以下の措置を講じる。<br>・防火扉を閉鎖し、煙の侵入や延焼を防止する。鎮火後に、復旧等の対応活動を開始する。<br>・緊急用システムを除くシステムを一旦停止する。 | | |
| 4 | **職員その他関係者の安否確認**<br>□避難の必要がなく、負傷者対応、二次災害の防止への対応以外に手が空く要員が確保でき次第、ＩＣＴ部門責任者又はその指名する者が、点呼により職員の安否状況を確認する。ＩＣＴ部門への来訪者についても、職員に誰が来訪していたか報告させ、漏れなく安否を確認すること。<br>□外出者や休暇中の職員がいる場合は、固定電話、携帯電話、又は携帯メールで連絡がつく範囲で安否確認を行う。ただし、至急連絡を取る必要がなければ、ある程度落ち着いてからでもよい。 | | 緊急連絡先リスト（別紙４） |
| 5 | **重要書類・データ類の保護**<br>□ＩＣＴ部門のフロアから退去が必要な場合、庁舎の損傷で漏水等が懸念されるなど、重要書類、バックアップ媒体等が損傷するおそれのある場合は、それらを庁舎内の安全な場所に移動させるか、庁舎外へ持ち出す（ただし、危険が迫り至急避難する場合を除く。）。<br>□重要書類やデータが損傷した場合、あらかじめ保管してあるバッ | | |

| No. | 復旧手順 | チェック | 補足 |
|---|---|---|---|
| | クアップ媒体を活用して、業務継続に必要な情報の復元処置を行う。<br>□情報セキュリティインシデントを認知した場合は、直ちにＩＣＴ部門責任者のほか関係各所に報告するとともに、ＣＳＩＲＴとして情報を集約する。 | | |
| 6 | **外部事業者（保守事業者等）との連絡確保**<br>□保守事業者等の至急対応を要請すべき外部事業者との連絡手段を確保する。固定電話、メール、携帯電話、携帯メールなどによる。そのほか、職員・外部事業者従業員による直接の往来（状況によっては自転車などを利用）などあらゆる手段を使用する。<br>□業務継続に必須の外部事業者の要員については、事業者連絡先リストを参照して、連絡手段を必ず確保する。 | | 事業者連絡先リスト（別紙５） |
| 7 | **被害状況の調査**<br>□倒壊の危険がある庁舎、二次災害が発生している庁舎の場合、ＩＣＴ部門としては、入館可能かどうか庁舎管理部門に確認する。<br>□被害チェックシートを使用して情報システム、インフラに関する被害を確認し、必要な報告を行う。<br>□被害状況は時間の経過により変化するため、継続的に監視を行う。 | | 被害チェックシート（別紙６） |
| 8 | **業務継続・代替復旧活動の開始判断**<br>□ＩＣＴ部門責任者は、被害情報の報告結果及び要員の参集状況を考慮して、どのような業務継続の対応活動を開始するかを判断する（一部の業務継続の活動の開始の判断は、例えば情報が十分にそろうまで、後刻に先送りすることも考えられる）。<br>□全庁の災害応急、復旧活動と整合を取りつつ、開始を決定した対応活動に必要な要員を指名し、情報システムの業務継続の体制を確立する。 | | |

（ケース２：就業時間外の場合）

| No. | 復旧手順 | チェック | 補足 |
|---|---|---|---|
| 1 | **自己及び家族の安全の確認**<br>□災害・事故発生時においては、自己及び家族の安全の確認後、自宅の火災発生などの二次災害の防止を講じた上、次項２の自動参集対応に入る。<br>□速やかに安否確認担当者に安否の連絡を行い、可能であれば出勤できる時間のメドも伝える。すぐにつながらない場合には、一定時間ごとに連絡を試みる。<br>□自己又は家族に負傷者等が出た場合、自宅が大きく損傷した場合などは、参集できない旨を連絡する。 | | |
| 2 | **自動参集対応**<br>□震度４以上の地震でＩＣＴ部門責任者、情報システム管理者及び各執行リーダーが、震度５弱以上の地震でＩＣＴ部門責任者、情報システム管理者及びすべての初期対応要員が、震度５強以上の地震で職員全員が自動参集する。震度はラジオ等で確認するが、確認できない場合、まずは参集を開始する。<br>□参集に当たっては、通勤途上の安全に配慮し、靴、服装などに留意する。また、水、食糧を持参するよう努める。<br>□規定の集合場所に自動参集する。公共交通機関が途絶している場合、徒歩・自転車・バイク等を使用し、道路状況に注意しながら、できるだけ速やかに参集する。参集困難な場合は、安否確認と同様の方法で、参集困難であることを連絡する。<br>□自宅周辺及び参集途上において、救助の必要がある被害者がいる場合、参集すべきか救助に当たるべきかの判断は、各自が実施し、その旨を安否確認と同様の方法で連絡する。 | | |
| 3 | **職員その他関係する要員の参集状況及び安否の確認**<br>□ＩＣＴ部門の職員の参集状況及び未参集者の安否確認を行う。<br>・安否確認担当者も出勤して安否確認を受ける。<br>・連絡がない職員には安否確認担当者が連絡を行う。<br>・必要に応じて、事業者連絡先リストに記述されている保守事業者へも同様に連絡を行う。 | | 緊急連絡先リスト（別紙４）<br><br>事業者連絡先リスト（別紙５） |
| 4 | **重要書類・データ類の保護**<br>□ＩＣＴ部門のフロアから退去が必要な場合、庁舎の損傷で漏水等が懸念されるなど、重要書類、バックアップ媒体などが損傷するおそれのある場合は、それらを庁舎内の安全な場所に移動させるか、庁舎外へ持ち出す（ただし、危険が迫り至急避難する場合を | | |

| No. | 復旧手順 | チェック | 補足 |
|---|---|---|---|
| | 除く）。<br>□重要書類やデータが損傷した場合、あらかじめ保管してあるバックアップ媒体を活用して、業務継続に必要な情報の復元処置を行う。<br>□情報セキュリティインシデントを認知した場合は、直ちにＩＣＴ部門責任者のほか関係各所に報告するとともに、ＣＳＩＲＴとして情報を集約する。 | | |
| 5 | **二次被害防止策の実施**<br>□火災など二次災害が発生している場合は、一時的に緊急用システムを除くサーバ類を一旦停止し、災害での混乱が落ち着いた後、復旧を開始する。 | | |
| 6 | **外部事業者（保守事業者等）との連絡確保**<br>□保守事業者等の至急対応を要請すべき外部事業者との連絡手段を確保する。固定電話、メール、携帯電話、携帯メールなどによる。そのほか、職員・外部事業者の従業員による直接の往来（状況によっては自転車などを利用）などあらゆる手段を使用する。<br>□業務継続に必須の外部事業者の要員については、事業者連絡先リストを参照して、連絡手段を必ず確保する。 | | 事業者連絡先リスト（別紙５） |
| 7 | **被害状況の調査**<br>□倒壊の危険がある庁舎、二次災害が発生している庁舎の場合、入館可能かどうか庁舎管理部門に確認する。<br>□被害チェックシートを使用して情報システム、インフラに関する被害を確認し、必要な報告を行う。<br>□被害状況は時間の経過により変化するため、継続的に監視を行う。 | | 被害チェックシート（別紙６） |
| 8 | **業務継続・代替復旧活動の開始判断**<br>□ＩＣＴ部門責任者は、被害情報の報告結果及び職員や保守事業者要員の参集状況を考慮して、継続・復旧活動を開始するかを判断する。<br>□全庁の活動への参加と整合を取りつつ、最低限必要な要員を確保して、情報システム・インフラの復旧体制を確立する緊急時対応に引き続き、代替・復旧に向けた活動を、各復旧担当が主体となり実施する。 | | |

## （３）代替・復旧の行動計画

緊急時対応に引き続き、代替・復旧に向けた活動を各復旧担当が主体となり実施する。

| No. | 復旧手順 | チェック | 補足 |
|---|---|---|---|
| ９ | **予想復旧時間の見積もり**<br>□システム・ネットワークの予想復旧時間、災害対応時のセキュリティ対策を検討する。<br>□不足物資、要員を確認する。 | | |
| １０ | **災害対策本部との連絡**<br>□必要に応じて、災害対策本部に対して予想復旧時間の報告を行うとともに、優先して復旧すべきシステムの変更の有無を確認する。<br>□復旧方針の検討に必要な情報を災害対策本部から入手する。 | | |
| １１ | **復旧方針の検討**<br>□システム・ネットワーク復旧に関する優先順位の確定・変更や暫定対応方法を検討する。<br>□担当編成、役割、担当者、深夜に作業が及ぶ場合の交代方針などを決めておく。 | | |
| １２ | **応急措置の実施**<br>□必要に応じて、以下の応急措置を実施する。<br>庁舎間ネットワークが断線している場合は、予備ケーブルでの応急措置等を実施する。職員でできない場合は業者に依頼する。 | | |
| １３ | **システム復旧準備**<br>□１１で決定した優先度の順にソフトウェアとデータの復旧順を確認する。<br>□システム復旧に必要な資源を確認する。<br>設備、対応要員、稼働環境（空調など）が揃っているかどうかを確認し、当初想定した順序で復旧できるかどうかを確認する。 | | |
| １４ | **システム復旧作業計画**<br>□システムを設置している庁舎が利用できない場合、ＩＣＴ部門責任者は、全庁の防災責任者とＩＣＴ部門が業務遂行するための場所や機器について協議し決定する。<br>□ＩＣＴ部門責任者は代替機器の調達を指示する。各執行リーダーは調達品のリストに基づき、損壊し調達、修理が必要なシステム、通信機器を整理し、調達を開始する。調達の際には、調達品の搬入予定日時を確認する。納期遅延の可能性がある場合は、その調整を行う。<br>□データ保管場所から外部データ保管媒体の搬送を指示する。搬送 | | |

| No. | 復旧手順 | チェック | 補足 |
|---|---|---|---|
| | されたデータを受け取り、利用できる機器（もしくは調達された機器）を考慮し、システム復旧の作業計画を立案する。 | | |
| １５ | **<u>システム復旧</u>**<br>□ＩＣＴ部門責任者は、システム復旧の作業計画に基づきシステムの復旧を各執行リーダーに指示する。各執行リーダーは、作業計画に基づき、要員と作業計画を確認し、作業を開始する。<br>□システム、通信機器の起動テストを行う。<br>□システム復旧を開始する。再インストールを実施する場合は、バックアップ媒体からＯＳ、業務アプリケーションなどの復旧を行う。<br>□あらかじめ保管してあるバックアップ媒体を活用してシステムで使用するデータ（システムに登録されていたデータ等）の復旧を行う。<br>□復旧作業中の報告<br>各執行リーダーは、作業進捗を３時間毎（もしくは報告ポイントや必要に応じ随時）にＩＣＴ部門責任者へ報告を行う。復旧に当たっては、運用に制約事項が発生することが考えられるため、制約事項についても把握された時点で報告する。<br>□復旧作業完了の報告<br>各執行リーダーは、テストを実施しシステムの動作確認を行う。テスト終了後、ＩＣＴ部門責任者に対して完了報告を行う。その際、どの時点までデータが戻っているのか、制約事項は何か、特例事項は何かを明確にして報告する。 | | |
| １６ | **<u>復旧システムの運用開始</u>**<br>□復旧システム開始判断<br>ＩＣＴ部門責任者及び各執行リーダーはシステム間のデータ連携も加味し、サービスを開始してよいかの判断を行い、部分的にでもサービスを開始ができるものについては、サービス内容を確認する。<br>□復旧システムの利用開始<br>ＩＣＴ部門責任者は業務部門に対し、運用再開の連絡を行う。連絡を行うに当たっては、作業場所（端末設置場所）、制約事項、データ復旧状況を伝える。<br>□システム停止期間に損失したデータの復旧<br>システム管理課はデータの復旧を図る。システム管理課でデータを復旧した場合には、必ずデータチェックを利用部門に依頼し、 | | |

| No. | 復旧手順 | チェック | 補足 |
|---|---|---|---|
| | 内容が正常であることを確認後、利用を開始する。<br>□利用中の問合せ対応<br>各利用部門からの問合せ窓口をシステム管理課に設置し、利用に関する問合せ対応がスムーズにできるよう体制を整える。<br>□利用中の不具合対応<br>利用中に不具合が発生した場合には、ＩＣＴ部門責任者が担当執行リーダーと協議し、対応策を決定し復旧にあたる。 | | |
| １７ | **通常システムへの復帰**<br>□通常システムへの復帰判断<br>ＩＣＴ部門責任者は復旧状況や機器の調達状況を加味し、通常運用に移行するかどうかの判断を行う。<br>□通常システムへの復帰<br>ＩＣＴ部門責任者は、判断結果に基づき作業計画を作成する。<br>＜仮運用を続ける場合＞<br>時間経過により影響する事項（例えば通常より少ないディスク容量や処理能力の設備で仮運用していた場合など）を取りまとめ、対応策を検討する。<br>＜復帰する場合＞<br>復帰するための作業計画を各執行リーダー、外部事業者と策定し、業務部門との調整を図る。 | | |
| １８ | **ＩＣＴ部門の業務継続計画書の見直し**<br>□ＩＣＴ部門責任者は各執行リーダーと災害時に想定していなかった事項など、本計画書の改善点をまとめ、修正を行う。 | | |

## ７．本計画の維持管理

ア　周知・教育

本計画は、常に最新のものを所定の場所に保管し、システム管理課内で情報共有を図るほか、人事異動や訓練の都度、説明を行うなどして周知、教育を行っていくものとする。

イ　訓練

定期、随時に必要な範囲で訓練を計画及び実施する。

| 訓練名称 | 訓練の概要 | 参加者 | 時期 | 備考 |
|---|---|---|---|---|
| 机上訓練 | 各要員は本計画を読み、緊急時にすべき行動を確認する。 | システム管理課職員 | 年１回 | |
| 緊急連絡、安否確認訓練 | 電話を使用せずに、携帯メールまたは、ＬｏＧｏチャットで連絡をする。 | システム管理課職員 | 年１回 | |
| サーバ緊急停止訓練 | 本庁舎の停電時に合わせて、サーバの緊急停止の手順を確認するとともに、どの程度の時間を要するか検証する。 | システム管理課職員<br>保守事業者 | 年１回 | |
| システム復旧訓練 | バックアップデータからリカバリできるか、どの程度の時間を要するか検証する。 | システム管理課職員<br>保守事業者 | 適宜 | |

ウ　本計画の見直しについて

本計画は、次に掲げる事項になった場合に見直しを行う。

・人事異動があった場合
・職員又は保守事業者の連絡先に変更があった場合
・組織体制に大きな変更があった場合
・保守事業者に大きな変更があった場合
・情報システムに大幅な変更があった場合
・国、県の制度変更により改定の必要がある場合

エ　承認ルール

本計画を改定する場合は、デジタル戦略推進本部の承認を得るものとする。

ただし、人事異動や保守事業者の変更に伴う連絡先の変更などの別紙様式の修正や本文中の文言修正など、ICT 部門責任者が軽微な変更と認める場合は、ICT 部門責任者の承認で改定するものとする。

なお、デジタル戦略推進本部の承認で改定した場合は整数の版数を、ICT 部門責任者の承認で改定した場合は小数点以下の版数を繰上げ、本文中の「計画の新規発

行／改定記録」に記述する。

【見直し項目】

| チェック | 点　検　項　目 | 補足 |
|---|---|---|
| □ | 人事異動、組織の変更による各要員の変更がないかを確認する。 | |
| □ | 各要員や事業者等の電話番号やメールアドレスの変更がないかを確認する。 | |
| □ | 本計画を変更した場合、関連する文書が全て最新版に更新されているかを確認する。 | |
| □ | 復旧用の媒体、復旧手順書が予定どおりに準備されているか（破損等がないか）を確認する。 | |
| □ | 自家発電機やＣＶＣＦが問題なく使用できるか確認する。 | |
| □ | 取引関係の変更などにより、運用支援事業者等に変更がないか確認する。 | |
| □ | 机上訓練、連絡・安否確認訓練などの訓練が計画どおりに実施されているか確認する。 | |
| □ | 訓練実施により判明した要改善点の反映が確実に行われているかを確認する。 | |
| □ | 新たなシステムの導入による計画の変更の必要性はないか確認する。 | |
| □ | 検討された課題への対策案が確実に実施されているか。責任部門や対応スケジュールが未定のものは予算編成時に予算化するとともに、上位者、組織との相談が必要な案件については、上位者と対応を相談する。 | |
| □ | 重要な外部事業者の業務継続（協力体制の構築）への取り組みの進捗を確認する。 | |
| □ | 既に検討した前提とは異なる事象（災害・事故）を想定した計画検討の必要性を確認する。 | |
| □ | 現時点で、対象範囲外とした情報システムがある場合、対象を広げる必要性を検討する。必要があれば、検討スケジュールを立案し、策定状況を継続的に管理する。 | |
| □ | 外部環境の変化や情報システムの変更などにより、選定した情報システム・インフラに変更がないか分析結果の見直しを行う。 | |

注）組織の変更、人事異動の状況を見て、見直しのタイミングは適宜決定する。新たなシステムの導入があった場合は、基本的に新たなシステム導入時に見直しを行い、年次の見直しはその確認、補完とする。