

新居浜市 I C T 業務継続計画

新 居 浜 市

令和2年3月

■計画の新規制定／改訂一覧

版数	制定／改訂年月日	計画の新規制定／改訂内容	備考
初版	令和2年3月	新規制定	
	改訂：令和 年 月		

目 次

1. 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) 計画の発動.....	1
2. 運用体制と役割.....	2
3. 被害想定.....	3
4. 重要システム.....	5
5. 緊急時対応・復旧計画.....	6
(1) 緊急時対応体制.....	6
(2) 緊急時における行動計画.....	8
(3) 代替・復旧の行動計画.....	10

1. 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、事故等で新居浜市の庁舎、職員等に相当の被害を受けても、重要業務をできる限り中断させず、速やかに復旧させるために策定するものである。

新居浜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。

地方公共団体の重要業務の多くは情報システムに依存しており、災害時に情報システムが稼働していることが極めて重要である。情報システムの利用が前提となっている今日の行政事務において、その実施・継続には、情報システムや情報通信ネットワークの稼働が必要不可欠である。これらの情報基盤は、災害・事故が発生した後に対策を始めるのではなく、あらかじめ講じておかないと、稼働できないことはもとより、復旧に多大な時間を要しかねない。そこで、本市の主要な情報システムにおける「ICT業務継続計画」を策定し、災害・事故等、緊急時の重要業務の継続、早期の復旧を実現する基盤を整えることとする。

(2) 基本方針

基本方針	
ICT部門の責務遂行	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業務を最優先で復旧するため、業務に必要なシステムを早期復旧する。
来訪者、職員、関係者の安全	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	本計画を、適切に関係者に周知するとともに、最新の状況を反映した計画となるよう定期的に点検を行い、必要に応じ計画の見直しを行う。
関係機関との連携	責務遂行のため、関係外部事業者等と連携し、代替対応の可能な業務継続計画を立案する。

(3) 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、企画部長が発動を決定する。

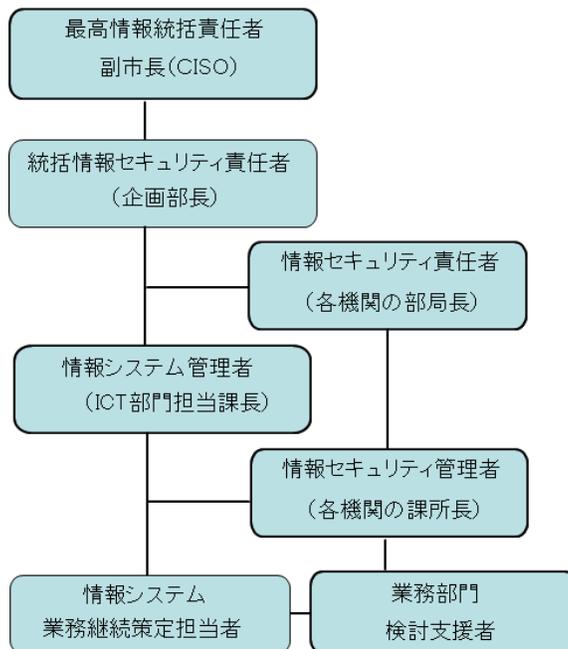
2. 運用体制と役割

本計画の運用管理は、CISOを中心とした新居浜市情報セキュリティ委員会（下図参照）により実施する。

当この推進体制において、各事業担当課の情報提供及び参画支援を得て計画を策定し、リスク軽減や復旧時間短縮に向けた対策の強化及び計画の見直しを進める。

また、発災時は災害対策本部の指揮に従い、復旧体制は 5.(1)緊急対応体制のもと、業務の復旧を実施する。

<新居浜市情報セキュリティ委員会体制>



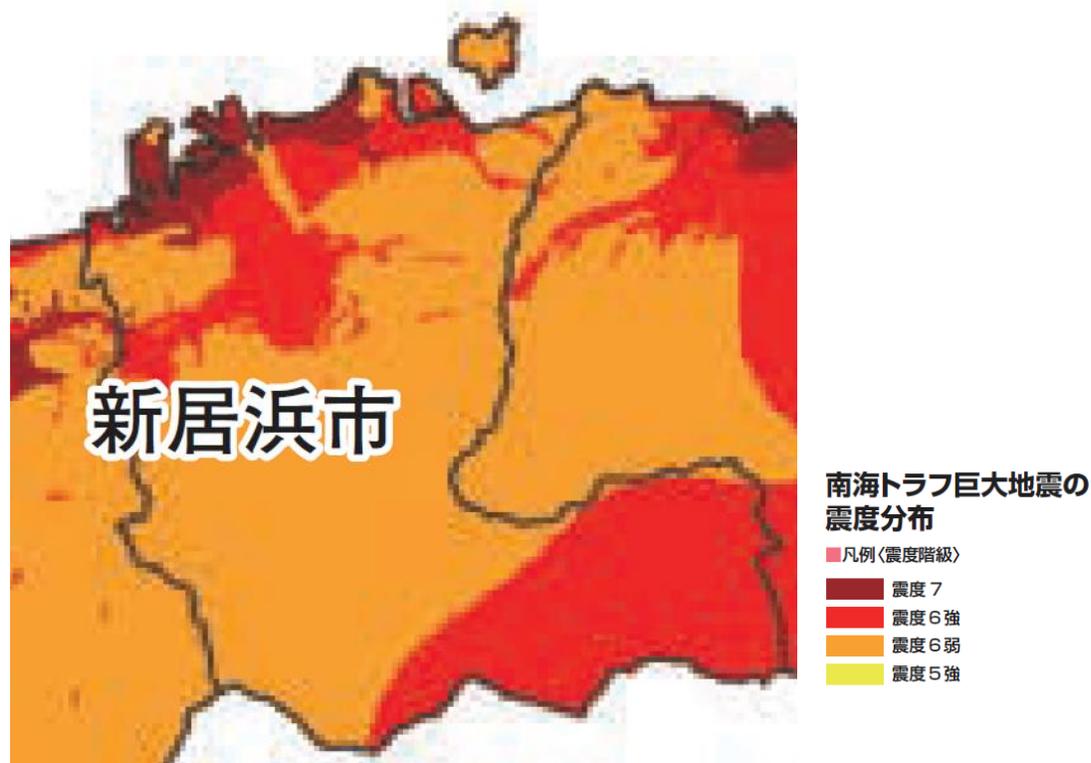
組織名称	役割の概要	災害対策本部との関係
最高情報統括責任者 副市長（CISO）	ICT部門の業務継続計画運用の全般を統括する。 制定、改訂の承認を行う。	副本部長
情報セキュリティ委員会	ICT部門の業務継続計画を含むリスクに関する重要な意思決定を行う。	本部員により構成
統括情報セキュリティ責任者 (企画部長)	最高情報統括責任者を補佐し、ICT部門の業務継続計画運用に関する課題及び対策遂行、検証などを統括する。	本部員
情報システム管理者 (ICT部門担当課長)	統括情報セキュリティ責任者を補佐し、ICT部門の業務継続計画における業務推進の責任を管理する。	情報処理班
情報システム業務継続策定担当者 (ICT部門担当者)	ICT部門の業務継続計画の作成及び計画で定められた各種施策を担当する。	情報処理班
業務部門検討支援者 (各課所業務担当者)	業務プロセスの分析、システム復旧要件についてICT部門に助言する。	

3. 被害想定

新居浜市では、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・事故の名称	南海トラフ巨大地震
----------	-----------



出展：愛媛県 自主防災組織活動マニュアル（Vol.1愛媛で想定される災害）

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、就業時間外
- ② 庁舎周辺震度 7

B. 起こりうる二次災害

- ・電算機室などでの局所的な火災
- ・公共電力供給の途絶
- ・公共通信回線（音声、データのネットワーク）の途絶

C. 想定される被害

通常時システム運用の障害対策と同様に、障害対応マニュアルに従い、一時的なサービスの仮復旧を実施し各設備の修繕などの復旧作業を実施する。

項目		想定被害状況
庁舎	本庁舎	耐震工事済みのため、倒壊せず庁舎利用可能であり、電算機室内のサーバにおいては、非常用電源からの電力供給は確保されている。庁舎内の固定していない什器・備品は転倒している。
	消防防災合同庁舎	十分な耐震・免震構造を備え、非常用電源からの電力供給も確保されていることから、重要システムが即座に停止する可能性は低い。電力供給が確保される拠点においては、点検後に継続利用が可能と考えられる。
庁舎内の機器	空調装置	庁舎が耐震工事済みのため、空調設備の影響の可能性は低い。
	サーバ	アンカーで固定しているため、転倒等の可能性は低いが、ディスク故障等のため、再稼働まで数日は必要なサーバがある程度あると想定される。
	パソコン	消防防災合同庁舎に設置しているパソコンは、利用できる可能性が高い。本庁舎に設置したパソコンは、電源設備及び伝送路への影響により利用できない可能性が高い。
	電算機室電源	非常用電源からの電力供給は確保されている。
	各フロア電源	消防防災合同庁舎の各フロアに設置されている非常用電源は使用可能である。本庁舎の各フロアの電源は利用できない可能性が高い。
要員	<p>○就業時間内 ICT部門担当職員の負傷者は軽微と想定される。</p> <p>○就業時間外、休日 家屋倒壊により ICT部門担当職員でも登庁できない職員が出る可能性がある。</p> <p>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。</p>	

4. 重要システム

重要業務の多くは情報システムに依存しており、災害時に情報システムが稼働していることが極めて重要である。直後の情報収集連絡体制の確立と災害対策本部の立ち上げ当初から72時間の救急・救命、避難対策、生活支援が重視されており、この時間帯における業務継続計画は特に求められる。災害対策本部で使用する情報システム及びネットワークの稼働を最優先として、重要システムからシステムの稼働確認及び復旧作業を実施する。

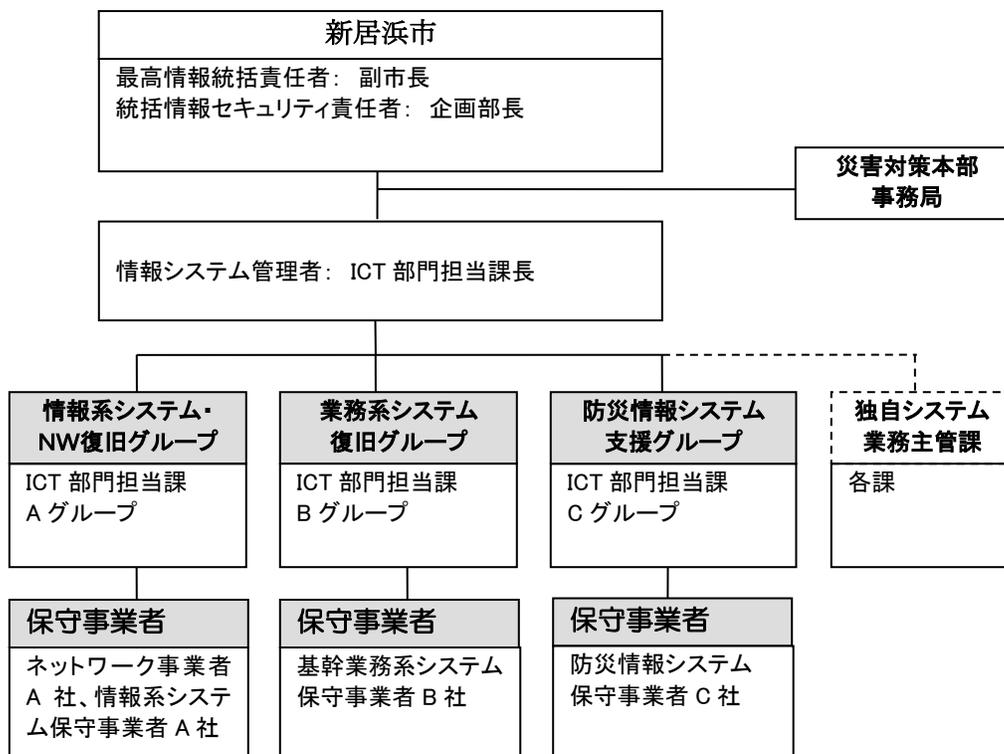
重点対象	重要システム	目標レベル	目標復旧時間	システム停止時の代替手段
●	災害対策本部 外部情報連絡システム (メール・市ホームページ 各種インフラ・ICT 資源確保)	災害対策本部設置時点からの外部との連絡及び情報公開を最重要として稼働させる必要がある。	1 時間	BWA 等のインターネット接続ルータを使用し、スタンドアローン端末から直接インターネットへ接続する。
●	防災情報システム	災害対策本部での被害状況等の情報を登録し共有するために、災害対策本部設置時点からの稼働が求められる。	3 時間	従来(紙ベース)の情報受付(処理)票での対応を一時的に行い、復旧後に蓄積された情報の登録を行う。
●	被災者支援システム	発災時点の住民基本台帳データを取得し、被災者支援システムを立ち上げる。	1 2 時間	Excel 又は紙ベースでの被災者台帳作成、り災証明の発行を行う。 クラウド環境での稼働を検討する。
	基幹業務システム (住民基本台帳・福祉・税)	被災者支援システムのために、最新の住民基本台帳を ICT 部門で出力する。	2 4 時間	外部データセンターのバックアップシステム(前日データ)を使用した、機能を制限し縮小稼働によるシステムの利用が可能である。
	庁内 LAN 運営 (メール・ファイルサーバ)	消防防災合同庁舎間の LAN の被災状況確認し、正常稼働していること。	2 4 時間	庁舎間のケーブル断線している場合、予備のケーブルで庁舎間を直接接続する。

本計画で対応する重要システムの目標復旧時間の詳細を別紙 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。)

5. 緊急時対応・復旧計画

(1) 緊急時対応体制

非常時に職員が適切に対応し、正確に情報が伝達されるように、以下の組織体制で活動する。



ア. 各グループ・メンバーの役割

グループ・メンバー	役割
情報システム管理者	情報システム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 ・ 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 ・ 市の災害対策本部への状況報告と本部決定の部門内への伝達 ・ 他の業務部門との調整の総括、支援依頼
情報系システム・NW(ネットワーク)復旧グループ	・ 以下の被害状況の確認と復旧 ・ ネットワーク(基幹業務系、情報系、LGWAN系) ・ 情報系システム ・ 各システム利用端末
業務系システム復旧グループ	・ 業務系システムの被害状況確認と復旧 ・ 業務系システム復旧遅延時の代替手段遂行の支援・調整
防災情報システム支援グループ	・ 防災情報システムの立ち上げと運用 被災者支援システムの立ち上げと運用

ア. 各グループ・メンバーの役割

<代行者>

情報システム管理者が不在の場合は、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が役割を担当する。

情報システム管理者	ICT 部門担当課長
代行者1	ICT 部門担当副課長
代行者2	情報系システム・NW復旧グループ係長

イ. 対応要員と参集ルール

(ア) 全員参集

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) 新居浜市内で震度4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、停電が市役所周辺で発生したことが報道された場合

安否確認

- 安否確認担当者は、ICT部門担当課長とする。
- 安否確認の作業は、就業時間内は執務室で行う。夜間・休日の場合、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、庁舎の近隣の市の関連施設又は自宅で行う。
- 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。

(イ) その他の自動参集

震度4以上の地震が発生した場合は、以下の初期対応要員が自動参集し、情報通信機器等の被害状況を情報システム管理者に報告する。その後の対応は、情報システム管理者の指示に従う。

(ウ) 指示による参集

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、情報システム管理者の指示により行う。

ウ. 外部事業者

A社・B社・C社においては、新居浜市内で震度6以上の地震が発災した場合は、自動的に自社に参集することとする。外部事業者に実際に連絡がつくか確認する。また、契約外の支援の要請に係る協力関係について事前に合意していた内容を実施するよう要請する。

(2) 緊急時における行動計画

ア. 参集要領

情報政策課の職員は、(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 (初動対応項目)

NO.	復旧手順	チェック	補足
1	<p>自己及び家族の安全の確認：</p> <ul style="list-style-type: none"> □ 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。 □ 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。 □ 自己及び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。 		就業時間外
2	<p>自動参集対応：</p> <ul style="list-style-type: none"> □ 震度4以上の地震の場合、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。 □ 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。 □ 規定の集合場所に自動参集する。集合場所から距離があり、公共交通機関が途絶している場合、参集するか判断は、別に定める基準に従う(別途、参集基準を定めておく)。 □ 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、別に定める基準に従う(別途、参集基準を定めておく)。 		就業時間外
3	<p>職員その他関係する要員の参集状況及び安否の確認：</p> <ul style="list-style-type: none"> □ 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。 <ul style="list-style-type: none"> ・安否確認担当者も出勤して安否確認を受ける。 ・連絡がない職員には安否確認担当者が連絡を行う。 ・緊急連絡網に記述されている保守事業者の責任者へも同様に連絡を行う。 □ 情報システム管理者は、災害対策本部へICT部門の安否確認結果を報告する。報告時間に定めや指示がない場合、途中経過でよいので、本部の立上げを見計らって第一報をする。 		緊急連絡網

NO.	復旧手順	チェック	補足
4	<p>重要書類・データ類の保護：</p> <ul style="list-style-type: none"> □ ICT部門のフロアから退去が必要な場合（ただし、危険が迫り至急避難する場合を除く）、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。 □ 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。 		
5	<p>二次被害防止策の実施：</p> <ul style="list-style-type: none"> □ 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	<p>外部事業者との連絡確保：</p> <ul style="list-style-type: none"> □ 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、災害対策本部の災害時優先電話、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。 □ 業務継続に必須の外部事業者の要員については、連絡先一覧を参照して、連絡手段を必ず確保する。 		連絡先一覧
7	<p>被害状況の調査：</p> <ul style="list-style-type: none"> □ 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。 □ 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。 □ 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
8	<p>業務継続・代替復旧活動の開始判断：</p> <ul style="list-style-type: none"> □ 情報システム管理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。 □ 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（指名する職員は事前に各班で氏名を明確にしておく。状況によっては、全庁的支援要請があった場合でも当該要請を断る必要もある）。 		

(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、各復旧グループメンバーが主体となり実施する。

NO.	復旧手順	チェック	補足
9	<p>予想復旧時間の見積もり：</p> <ul style="list-style-type: none"> □ システム・ネットワークの予想復旧時間、災害時のセキュリティ対策を検討する。 □ 不足物資、要員を確認する。 		
10	<p>災害対策本部との連絡：</p> <ul style="list-style-type: none"> □ 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。 □ 復旧方針の検討に当たって必要な情報を災害対策本部から入手する。 		
11	<p>復旧方針の検討：</p> <ul style="list-style-type: none"> □ 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。 □ チーム編成、役割、担当者、深夜に作業が及ぶ場合の交代方針などを決定する。 		
12	<p>応急措置の実施：</p> <ul style="list-style-type: none"> □ 必要に応じて、以下の応急措置を実施する。 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を実施する。 B庁舎が使用できない場合は、耐震庁舎（A、C庁舎）の会議室に応急作業スペースとしてPC数台を設置する。 		
13	<p>システム復旧準備：</p> <ul style="list-style-type: none"> □ 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序を確認する。 □ システム復旧に必要な資源を確認する。 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	<p>システム復旧作業計画</p> <ul style="list-style-type: none"> □ B庁舎が利用できない場合 情報システム管理者は、あらかじめ準備していた案を踏まえ、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。 □ 情報システム管理者は代替機器の調達を指示する。 各グループ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。納期延期の可能性がある場合は、その調整を行う。 □ 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。 		

NO.	復旧手順	チェック	補足
15	<p>システム復旧</p> <ul style="list-style-type: none"> □ 情報システム管理者は、システム復旧の作業計画に基づきシステムの復旧を各グループリーダーに指示する。 各グループ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。 □ システム、通信機器の起動テストを行う。 □ 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等の復旧を行う。 □ 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。 □ 復旧作業中の報告 各グループリーダーは、作業の進捗状況を3時間毎（もしくは報告ポイントや必要に応じ随時）に情報システム管理者へ報告を行う。 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。 □ 復旧作業完了の報告 各グループリーダーは、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、情報システム管理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（例えばパスワードなど）を明確にして報告する。 		
16	<p>復旧システムの運用開始</p> <ul style="list-style-type: none"> □ 復旧システム開始判断 情報システム管理者及び各グループ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できるものについては、再開について全庁の防災責任者に確認する。 □ 復旧システムの利用開始 情報システム管理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。 □ システム停止期間に損失したデータの復旧 各利用部門（もしくはICT部門）でデータの復旧を図る。 ICT部門でデータを登録した場合には、必ずデータチェックを利用部門に依頼し、利用を開始する。 □ 利用中の問合せ対応 各利用部門からの問合せ窓口をICT部門に設置し、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。 □ 利用中の不具合対応 利用中に不具合が発生した場合には、情報システム管理者がシステム担当リーダーと協議し、対応策を決定し復旧にあたる。 		

NO.	復旧手順	チェック	補足
17	<p>通常システムへの復旧</p> <ul style="list-style-type: none"> □ 通常システムへの復旧判断 情報システム管理者は、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い、全庁の防災責任者と設置場所、投資などについて協議を行い、その判断を求める。 □ 通常システムへの復旧 情報システム管理者は判断結果に基づき、作業計画を作成する。 <仮運用を続ける場合> 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。 <復旧する場合> 復旧するための作業計画を各グループリーダー、外部事業者と策定し、業務部門との調整を経て、全庁の防災責任者に承認を得る。 		
18	<p>ICT部門の業務継続計画書の見直し</p> <p>情報システム管理者は各グループリーダーと災害時に想定していなかった事項など、計画書の改善点をまとめ、修正を行う。</p>		