情報システム部門における業務継続計画

海　津　市

平成２３年８月

目　　次

1.　業務継続計画の趣旨・基本方針

（1）趣旨

「情報システム部門における業務継続計画」（以下「業務継続計画」という。）とは、大規模な災害、事故、事件等（以下、「災害・事故」という。）で海津市（以下、「市」という。）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。

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、市民生活や地域経済活動に大きな支障が生じる。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。

今日において、このような市の業務の実施・継続には、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ていては稼働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っている。そこで、総務省の「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（平成２０年８月）」に基づき、情報システム部門の業務継続のための基礎的な対策計画として、海津市の「情報システム部門における業務継続計画」を策定し、災害・事故による情報システム障害発生時の重要業務の実施・継続を行うための基盤を整えることとする。

（2）基本方針

①情報システム部門の責務遂行

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業務を最優先で復旧するため、情報システム部門として業務に必要な情報システムの稼働維持又は早期復旧に努める。

②来訪者、職員、関係者の安全確保

災害・事故時の業務に必要な情報システムの稼働維持又は早期復旧に当たっては、事務室等への来訪者、職員、契約先職員その他関係者の安全確保を第一とする。

③計画の有効性の維持・改善

情報システム部門は本業務継続計画を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い、それらの結果を踏まえて是正措置を講ずる。少なくとも年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い、必要に応じて改定する。

④関係機関との連携

他の地方公共団体や外部事業者と連携し、市の情報システム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。

２．用語の定義

本業務継続計画において使用する用語の意義は、次の各号に定めるところによる。

①情報システム部門

総務部総務課情報政策係をいう。

②ネットワーク

データ通信を行うための情報通信網で、情報機器、通信機器及び通信回線で構成されるものをいう。

③情報システム

サーバ等を使用して業務処理を行うためのハードウェア、ソフトウェア及びネットワークの総称をいう。

④職員等

当市の職員、並びに当市が雇用する非常勤嘱託員及び日日雇用職員等の臨時職員をいう。

⑤外部事業者

当市との契約により、当市が保有する情報を取扱う業務、又は当市の情報システムに係る開発、導入、保守等の業務に携わる者をいう。

⑥初期対応要員

総務課情報政策係の職員等及び情報システム部門責任者があらかじめ任命した職員をいう。

⑦対応要員

初期対応要員、情報推進委員及び業務所管部署の所属長があらかじめ指名する情報システム運用に携わる職員等をいう。

⑧情報推進委員

情報システムを所管する部署の情報推進委員をいう。

⑨部署

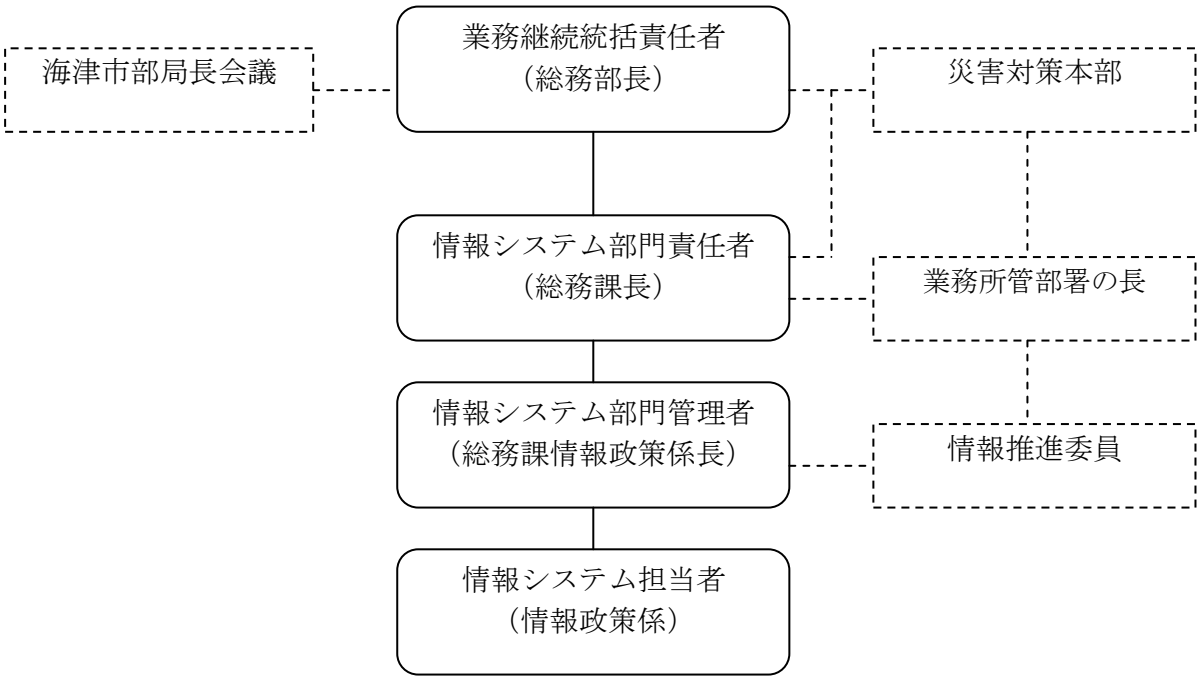
課に相当する組織をいう。

３．運用体制と役割

（１）運用体制

情報システム部門の業務継続計画の運用管理は、業務継続運用管理体制により実施する。

業務継続運用管理体制（図１参照）においては、各業務部門の参画支援を得て業務継続計画を運用する。また、災害発生時には、災害対策本部の指揮に従い、復旧体制は６．（１）緊急時対応体制により、業務の復旧を実施する。



＜図１：業務継続運用管理体制＞

業務継続運用管理体制に係わる緊急時の対応要員は、あらかじめ「緊急時対応要員連絡表」に登録し、緊急事態発生時に連絡が取れるようにする。

また、緊急事態発生時の連絡に備え「緊急連絡網」を整備し、連絡ルートを明確にする。

（２）役割

①業務継続統括責任者

業務継続統括責任者は、総務部長とする。

情報システム部門の業務継続計画運用の全般を統括する。

業務継続計画の制定、改定の承認を行う。

業務継続に関わる全庁的調整を行う。

情報システム部門の業務継続計画に関する重要な意思決定が必要な場合は、部局長会議に諮る役割を担う。

②情報システム部門責任者

情報システム部門責任者は、総務課長とする。

業務継続統括責任者を補佐し、情報システム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。

情報システムに関係する業務所管部署との調整を行う。

③情報システム部門管理者

情報システム部門管理者は、総務課情報政策係長とする。

情報システム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。

情報システム部門の業務継続計画における業務推進を行う。

業務プロセスの分析、情報システム復旧要件について業務部門に対し支援依頼をする。

④情報システム担当者

情報システム担当者は、総務課情報政策係の職員等とする。

情報システムに関する業務継続計画運用を担当する。

４．被害の想定

（１）対象とする事象

情報システムに関わる被害は、発生する事象及びその規模によって異なるため、次の事象について発生時の被害を想定する。

①地震（建物等に被害が及ぶ地震）

②風水害（台風）（建物等に被害が及ぶ風水害）

③火災（庁舎における火災）

④サイバーテロ（情報システム障害に結びつくサイバーテロ）

⑤その他事故（情報システム障害につながる事故）

（２）想定される被害

想定される被害は、次のものに対して検討する。

①庁舎の被害

②庁舎の周辺被害

③庁舎内の機器（空調装置、サーバ、パソコン等）の被害

④通信回線の被害

⑤要員の被害

⑥ライフライン（電力、水道、電話、道路、鉄道等）の被害

５．重要情報システム

（１）重要情報システムの洗出し

情報システム部門は、重要業務に関わる情報システムについて、次の事項を調査し、当該業務の特性を把握し、速やかに復旧対応ができるよう「重要情報システム一覧表」を作成する。

調査項目は、次の通りとする。

①情報システム名
②業務名
③業務所管部署
④担当者
⑤業務停止影響度
⑥ＩＴ依存度
⑦目標復旧レベル
⑧業務目標復旧時間
⑨情報システム目標復旧時間
⑩復旧遅延影響度
⑪優先度
⑫関係外部事業者

（２）情報システム稼働環境の洗出し

重要情報システム毎に、当該システム稼働環境を明確にすることにより、緊急事態発生時の稼働可能性等を把握できるようにする。

「情報システム別稼働環境一覧表」を作成し、重要情報システム毎に稼働に必要な環境、当該情報システムを利用するために必要な環境等をまとめ、復旧箇所の優先度等の判断資料とする。

「情報システム別稼働環境一覧表」の作成に当たって、次の事項を留意する。

①情報システムは、「情報系システム」、「庁内システム」、「基幹系システム」、「独立システム」に分けて列挙する。
②稼働環境は、「建物」、「サーバ」、「ネットワーク」、「端末等」、「庁内電源」、「空調」、「外部事業者」等別に具体化する。

６．緊急時対応

（１）緊急時対応体制の確立

災害・事故が発生した場合に、職員等が適切に対応し、正確に情報が伝達されるように、業務継続運用管理体制により、活動する。

①情報システム部門責任者
　情報システム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
　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
　災害対策本部への状況報告と災害対策本部決定事項の部門内への伝達
　他の業務部門との調整の総括、支援依頼
②情報システム部門管理者
　業務継続に関わる活動の指揮
　被害状況、対応状況等のまとめ

データセンターとの連絡、調整
情報システム部門責任者への報告

③情報システム担当者

以下の被害状況の確認と復旧

・ＬＡＮ
・無線ＬＡＮ
・情報システム
・各システムの利用端末

以下の外部事業者（メーカ、保守ベンダー等）への支援依頼など窓口業務

・ネットワークに関係する事業者
・情報システムに関係する事業者

情報システム復旧遅延時の代替手段遂行の支援・調整（本番システムへの後からの情報追加方法等）

④安否確認担当者

災害・事故の発生時における対応要員の安否確認が必要な場合に備え、情報システム部門管理者はあらかじめ安否確認担当者を指名し、その任にあたらせる。

（２）対応要員と参集ルール

①大規模災害・事故が発生した場合

原則、対応要員は参集することとする。

大規模災害・事故とは、次の場合をいう。

・市内で震度５弱以上の地震が発生した場合
・大型台風等により市内の広範囲に大規模な被害が発生した場合
・復旧見込みの立ってないネットワーク障害、停電が市役所周辺で発生したことが報道された場合

安否確認は、以下の通り行う。

・安否確認担当者による安否確認の作業は、就業時間内は事務室で行う。夜間・休日の場合は、事務室に出勤して行うことを原則とするが、庁舎には入れない場合、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。
なお、安否確認担当者が事故又は家族の災害対応に追われ安否確認活動ができない場合は、速やかに情報システム部門管理者に報告する。報告を受けた情報システム部門管理者は代替要員を指名し、安否確認を行う。
・対応要員は、自動参集を原則とするが、安否確認担当者に自己の安否の連絡をする。
・連絡のない対応要員に対しては、安否確認担当者から連絡を継続的に試みる。

②中規模災害・事故が発生した場合

原則、初期対応要員は参集することとする。

中規模災害・事故とは、次の場合をいう。

・震度４の地震が発生した場合
・重要業務の情報システム障害が発生した場合

あらかじめ任命された初期対応要員は、情報通信機器等の被害状況を情報システム部門管理者に報告する。

その後の対応は、情報システム部門管理者の指示に従う。

③その他の場合

上記①、②以外の災害・事故が発生した場合の参集及び実施すべき対応については、情報

システム部門管理者の指示により行う。

（３）外部事業者への対応

大規模災害・事故発生時には、データセンター及び外部事業者に連絡がつくかを確認する。

契約外の支援の要請に関わ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。

年次の計画見直しにおいて、協力関係の維持を各社に確認すること。

情報システム更新などにより協力関係を結ぶ外部事業者に変更があった場合は、同様の協力関係を構築するように努める。

７．緊急時における行動計画

（１）就業時間内の初期対応

①来訪者・職員等の負傷者対応、誘導

・情報システム部門内及び周辺の来訪者、職員等（契約先社員等を含む。以下同じ。）で負傷している者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、事項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、とどまるように要請する。

②庁舎からの避難

・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、職員等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

・情報システム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、火災の発生を総務課長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。

・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、以下の措置を講ずる。

1)　防火扉を閉鎖し、煙の侵入や延焼を防止する。

2)　緊急用システムを除くサーバ類を一旦停止する。

3)　鎮火後に、復旧等の対応活動を開始する。

④対応要員の安否確認

・避難の必要がなく、負傷者対応、二次災害の防止への対応を優先し、情報システム部門管理者又は安否確認担当者が、点呼により対応要員の安否を確認する。

・安否確認担当者は、「緊急時対応要員連絡表」に基づいて、対応要員の安否を優先的に確認する。

・情報システム部門への来訪者についても、職員に誰が来訪したか報告させ、もれなく安否を確認する。

・外出者や休暇中の対応要員がいる場合は、固定電話、携帯電話又は携帯メールにより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。

・外出者や休暇中の対応要員の安否が確認できない場合は、災害時伝言ダイヤル（１７１）を活用し、部門の電話番号で登録された情報がないかを確認する。なお、平常時より１７１は災害時に活用するよう対応要員に周知しておく。

・安否確認の結果は「緊急時対応要員安否確認表」にまとめ報告資料とする。

・「緊急時対応要員安否確認表」は、状況の変化に応じて適宜作成する。

・情報システム部門責任者は、災害対策本部へ情報システム部門の安否確認結果を報告す

る。報告時間に定めがない場合、途中経過でよいので、災害対策本部の立ち上げを見計らって第一報する。

（２）就業時間外（夜間・休日）の初期対応

①自己及び家族の安全の確認

・災害・事故発生時には、対応要員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めどを伝える。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。

②自動参集対応

・震度５弱以上の地震の場合、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、食料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、参集するかの判断は、別に定める基準に従う。

・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、災害発生時の「職員初動マニュアル」に従う。

③対応要員の参集状況及び安否の確認

・安否確認担当者は、「緊急時対応要員連絡表」に基づいて、対応要員の参集状況及び未参集者の安否を確認する。

1)　安否確認担当者も出勤して安否確認を受ける。

2)　連絡がない対応要員には安否確認担当者が連絡を行う。

3)　緊急連絡網に記載されている外部事業者の責任者へも同様に連絡を行う。

・安否が確認できない対応要員がいる場合、災害時伝言ダイヤル（１７１）を活用し、部門の電話番号で登録された情報がないかを確認する。なお、平常時より１７１は災害時に活用するよう、あらかじめ対応要員に周知する。

・安否確認の結果は「緊急時対応要員安否確認表」にまとめ報告資料とする。

・「緊急時対応要員安否確認表」は、状況の変化に応じて適宜更新する。

・情報システム部門責任者は、災害対策本部へ情報システム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、災害対策本部立ち上げを見計らって第一報をする。

（３）情報システムに関わる初期対応

①重要書類・データ類の保護

・情報システム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。

・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。

②二次被害防止策の実施

・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。

③外部事業者（データセンター、保守ベンダー等）との連絡確保

・至急対応を要請すべき外部事業者（データセンター、保守ベンダー等）との連絡手段は固定電話、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り確保する。そのほか、職員・外部事業者従業員による直接往来（状況によっては自転車など利用）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、「緊急時対応要員連絡表」を参照して、連絡手段を必ず確保する。

④被害状況の調査

・施設別「被害状況確認表」を使用して情報システム、稼働環境（インフラ）に関する被害を確認し、その結果を「情報システム稼働環境被害状況確認表」にまとめ、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、入館可能かどうか当該庁舎の所管部署に確認する。

・被害状況は時間経過で変わるため、継続的に監視を行う。

⑤業務継続・代替復旧活動の開始判断

・情報システム部門責任者は、被害情報の報告結果及び対応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とりつつ、最低限必要な対応要員を確保して、情報システムの復旧体制を確立する。

・対応要員は状況によって、全庁的支援要請があった場合でも当該要請を断り、情報システムの復旧を優先させる。

（４）代替・復旧への対応

①予想復旧時間の見積もり

・情報システムの予想復旧時間、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。

②災害対策本部との連絡

・災害・事故状況に関しては、速やかに「情報システム関連緊急事態報告書」を作成し、災害対策本部に報告する。
また、時間経過とともに変化する状況についても適宜報告書を提出する。

・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情報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。

③復旧方針の検討

・情報システム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。

・復旧方針、暫定対応方法等は「サーバ別情報システム一覧表」及び「情報機器一覧表」を参考に検討する。

④応急措置の実施

・必要に応じて、以下の応急措置を実施する。

1)　庁舎間及びデータセンター間のネットワークが遮断している場合は、予備回線での応急措置を実施する。

2)　使用できない庁舎がある場合は、使用できる庁舎の会議室に応急スペースとしてパソコン等を数台設置する。

・庁舎の使用状況等は、「設備等現状確認表」を参考に使用可能性を検討する。

⑤情報システム復旧準備

・③で決定した優先度の順位に応じてソフトウェアとデータの復旧順序を確認する。

・情報システム復旧に必要な設備、対応要員、稼働環境（空調など）がそろ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。

⑥情報システム復旧作業計画

・庁舎が使用できない場合、情報システム部門責任者は、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情報システム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。

・情報システム部門管理者は代替機器の調達を指示する。情報システム担当者は情報推進委員の協力を得て、調達品リストに基づき、損壊し調達、修理が必要な情報システム、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、情報システム復旧の作業計画を立案する。

⑦情報システム復旧

・情報システム部門管理者は、情報システム復旧の作業計画に基づき情報システムの復旧を情報システム担当者に指示する。情報システム担当者は作業計画に基づき、対応要員と作業計画を確認し、作業を開始する。

・情報システム、通信機器の起動テストを行う。

・情報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情報システムで使用するデータ（情報システムに登録されていたデータ等）の復旧を行う。

・情報システム担当者は、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、運用に制約事項が派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。

・情報システム担当者は、テストを実施した情報システムの動作確認を行う。テスト終了後、情報システム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（例えばパスワードなど）を明確にして報告する。

⑧復旧情報システムの運用開始

・情報システム部門管理者及び情報システム担当者は情報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、再開について情報システム部門責任者及び全庁の防災責任者に確認する。

・情報システム部門責任者は、業務所管部署に対し、運用開始の連絡を行う。連絡に当たっては、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。

・各利用部門もしくは情報システム部門は、情報システム停止期間に損失したデータの復旧を図る。情報システム部門でデータを登録した場合は、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。

・各利用部門からの問い合わせ窓口を情報システム部門に設置し、利用に関する問い合わせ対応がスムーズにできるよう体制を整える。
・利用中に不具合が発生した場合には、情報システム部門管理者が業務所管部署と協議し、対応策を決定し、復旧に当たる。

⑨通常情報システムへの復帰

・情報システム部門管理者は、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、情報システム部門責任者及び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。
・情報システム部門管理者は、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＞

情報システム部門管理者は、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。

＜復帰する場合＞

情報システム部門管理者は、復帰するための作業計画を情報システム担当者、外部事業者と策定し、業務部門との調整を経て、情報システム部門責任者及び全庁の防災責任者に承認を得る。

⑩情報システム部門の業務継続計画の見直し

・情報システム部門管理者は、情報システム担当者と災害・事故時に想定していなかった事項など、業務継続計画の改善点をまとめ、修正を行う。

８．業務継続計画の運用

（１）運用及び検討

①役割

情報システム部門の業務継続計画における基本的な役割は、以下の通りとする。

情報システム部門責任者

1)　情報システム部門の業務継続計画の運用の責任
2)　情報システム部門の教育、訓練の実施統括
3)　情報システム部門の対策の実施と対応状況の確認

情報システム部門の職員

1)　平常時の計画の維持管理
2)　業務継続計画の年次見直し
3)　個別対策の状況の把握・改善・確認
4)　訓練の実施

②計画の見直し

業務継続計画は、毎年予算要求の時期に合わせて、内容の全面的な確認及び見直しを行う。

上記以外に、次の状況の場合に必要に応じて見直しを行う。

1)　組織体制に大きな変更があった場合
2)　外部事業者に大きな変更があった場合
3)　主な情報システムに大幅な変更があった場合
4)　国、県の制度変更により改定の必要がある場合
5)　首長等から改定するよう指示があった場合

業務の繁忙時期や人事異動の状況に応じて、見直しのタイミングは適宜決定する。

③承認ルール

業務継続計画を新規作成した場合、改定した場合及び定期見直しを実施した場合（内容に変更がない場合も含む）、は業務継続統括責任者に承認を得る。

（２）訓練計画

可能な限り下記の訓練を実施する。

①机上訓練

情報システム部門責任者、情報システム部門管理者、情報システム担当者、情報推進委員、外部事業者のリーダ及び特定技術者が参画し、業務継続計画を読み合わせ、各要員の緊急時に実施すべき行動を確認する。

②緊急連絡、安否確認訓練

「緊急連絡網」に基づき、確実に連絡が取れることを検証する。可能ならば、電話（固定電話、携帯電話）の通話機能を使用せずに、対応要員との連絡が取れることを検証する。

③情報システム復旧訓練

バックアップデータからリカバリーできるか、リカバリーにどの程度の時間を要するかを検証する。

④初動訓練

災害・事故発生時の初動事項を確認する。