さいたま市
ICT-BCP 基本計画書

第 2.2 版

令和 6 年 1 月 24 日

改版履歴

版数	年月日	修正又は改定の内容
初版（作成）	平成25年3月14日	－
1.1版（修正）	平成31年4月1日	・本書を補完するものとして、「ICT-BCP サイバー攻撃編」を策定したことに伴う所要の修正
2.0版（改定）	令和4年3月29日	・感染症の流行が直接的な影響を及ぼす人的資源に関する内容を拡充 ・感染症の流行の影響が局面を変えながら長期化する場合を想定した内容を拡充 ・文書構成等の整理
2.1版（修正）	令和5年11月6日	・令和５年３月に「さいたま市事業継続計画【地震対策編】」がさいたま市業務継続計画【自然災害対策編】に改定されたことに伴う所要の修正
2.2版（修正）	令和6年1月24日	・ICT 復旧対策本部管理チームを担当する部名を最新化するための修正

目次

資料①：「ICT-BCP 実行計画書（ひな形）」　（3. 本書の文書構成）
資料②：「リスクシナリオ一覧表」　（4.1.5. さいたま市のリスクシナリオ）
資料③：「目標対策レベル一覧」　（4.2.2. 目標対策レベルの設定）
資料④：「全体フロー」　（5.2. 危機的事象発生時における ICT 復旧フロー、5.3. 危機的事象発生時における初動対応手順）
資料⑤：「個別手順書（ICT 復旧対策本部）」　（5.3. 危機的事象発生時における初動対応手順）
資料⑥：「個別手順書（各原課）」　（5.3. 危機的事象発生時における初動対応手順）
資料⑦：「記入シート様式集」　（5.3. 危機的事象発生時における初動対応手順）

※ ホームページ掲載に当たっての追記事項
以上の資料については、情報セキュリティ確保のため非公開とする。

1. ICT-BCP の概要と目的

1.1. 計画の趣旨

地震等による大規模災害が発生した際、地方公共団体は、災害応急対策や災害からの復旧・復興対策の主体として重要な役割を担うことになる一方、災害発生時であっても継続して行わなければならない通常業務を抱えている。しかしながら、過去の災害では、地方公共団体自身が被災し、庁舎や電気・通信機器の使用不能等により災害発生時の対応に支障を来たした事例が多数見受けられるところであり、このような非常時であっても優先的に実施すべき業務を的確に行えるよう、業務継続計画の策定等により、業務継続性を確保しておくことが極めて重要である。

そのため、さいたま市では、「さいたま市地域防災計画」のもとに「さいたま市事業継続計画【自然災害対策編】」において、業務を継続させる計画（BCP : Business continuity planning）を策定している。

また、地方公共団体の重要業務の多くは情報システムやネットワーク等の ICT 環境に依存しており、災害発生時に ICT 環境が稼動していることが極めて重要である。

このことから、さいたま市の「ICT-BCP 基本計画書（本書。以下「ICT-BCP」という。）」は、ICT 環境に関する業務継続視点からの責務を果たすための戦略的計画として、災害発生時における業務の継続性確保に必要となる ICT 環境の迅速な復旧対応計画を明確化することを目的に策定するものである。

加えて、近年、新型インフルエンザ（H1N1）や高病原性鳥インフルエンザ（H5N1）、重症急性呼吸器症候群（SARS）等の大規模な感染症が発生しており、これらは世界規模の流行に発展する可能性もあることから、警戒が必要な状況となっている。そのため、さいたま市では、新型インフルエンザ等の発生時における通常業務継続の観点から、「さいたま市新型インフルエンザ等対策業務継続計画」（本書においては、「さいたま市事業継続計画【自然災害対策編】」と併せて「全庁 BCP」という。）を策定している。

感染症により、直接的にシステムの停止や破壊が引き起こされることは想定しないが、ICT 環境を維持・継続するためには人的資源が必要となるため、感染症流行時における「人的資源の確保」という視点から対応する必要がある。

そのため、「ICT-BCP」においては、上位計画との整合性を保ちながら、「感染症」についても想定脅威とする。なお、令和 2 年より世界的な大流行（パンデミック）を引き起こしている新型コロナウイルス感染症（COVID-19）についても、令和 4 年 3 月時点で全庁 BCP に記述は無いが、本書においては想定脅威として念頭に置いて記述する。

なお、さいたま市の情報システムには様々な管理・運用形態があり、各々の情報システムごとの継続性への責任範囲は、運用管理の主体や稼働環境等によっても異なる。しかしながら、各業務の情報システムの継続性確保は、それぞれの業務を所管する原課が責任部署となり、事前対策を含めた ICT 復旧体制の構築や、災害発生時及び感染症流行時（以下「危機的事象発生時」という。）の業務の継続・復旧対応を担うことになる。

また、危機的事象発生時において、それらを総合的に管理し、横断的な見地から支援・指揮する本部機能は、後述する「ICT 復旧対策本部」が担い、平時においては、事前対策としての体制整備、ドキュメント例の提示等の継続マネジメントに関する事項を、都市戦略本部デジタル改革推進部が支援する。

本計画の策定に当たっては、さいたま市の現状に即した具体性、実行性のある計画とする必要があり、更には ICT-BCP を管理・運用する「業務継続管理体制（ICT-BCM 体制）」も整えていくこととする。

1.2. 基本方針

本計画における基本方針は、次のとおりとする。

ア　情報システムを管理・運用する責任を負う課の責務遂行

危機的事象発生時の業務の継続・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、デジタル改革推進部においても業務に必要な情報システムを早期復旧する。

イ　来訪者、職員、関係者の安全確保

危機的事象発生時の業務の継続・早期復旧に当たっては、庁舎への来訪者、職員、委託契約業者その他の関係者の生命の安全確保を第一とする。

ウ　計画の有効性の維持・改善

本計画は、毎年度関係者に周知するとともに、可能な範囲で訓練を行うこととし、最新の状況を反映した計画となるよう点検を行う。さらに、それらの結果を踏まえて、可能な範囲で是正措置を講ずるとともに、定期的に又は必要に応じて、その都度計画全般を検証の上、全庁 BCP との整合性を図りながら見直しを行う。

エ　計画の実施（ICT-BCP の発動）

危機的事象発生時の緊急事態等において、ICT の継続・早期復旧を本計画に従い実施するタイミングは、それぞれのシステム保有課において判断することとなる。危機的事象発生時に立ち上がる対策本部の指示待ちにならず、策定した実行計画を参考にし、臨機応変な対応を実施する。

ただし、全庁的な立場で対策本部からの指示があれば、その指示に従う。

1.3. 本書の位置づけ

さいたま市における ICT-BCP の位置づけは、次のとおりとする。

ア　さいたま市危機管理指針との関係

ICT-BCP 関連文書は、さいたま市危機管理指針の下に作成される細部計画の一つである。

イ　全庁 BCP との関係

ICT-BCP と全庁 BCP 又はその代替となる計画との関係を、図１－１「ICT-BCP と全庁 BCP の関係」に示す。

全庁 BCP における非常時優先業務及び業務開始目標時期と、ICT-BCP におけるシステム重要度及び情報システムとして達成すべき目標復旧時間（RTO：Recovery Time Objective。以下「目標復旧時間」という。）については、整合性を図り、危機的事象発生時において情報システムに要求されるサービスレベルを満たす必要がある。

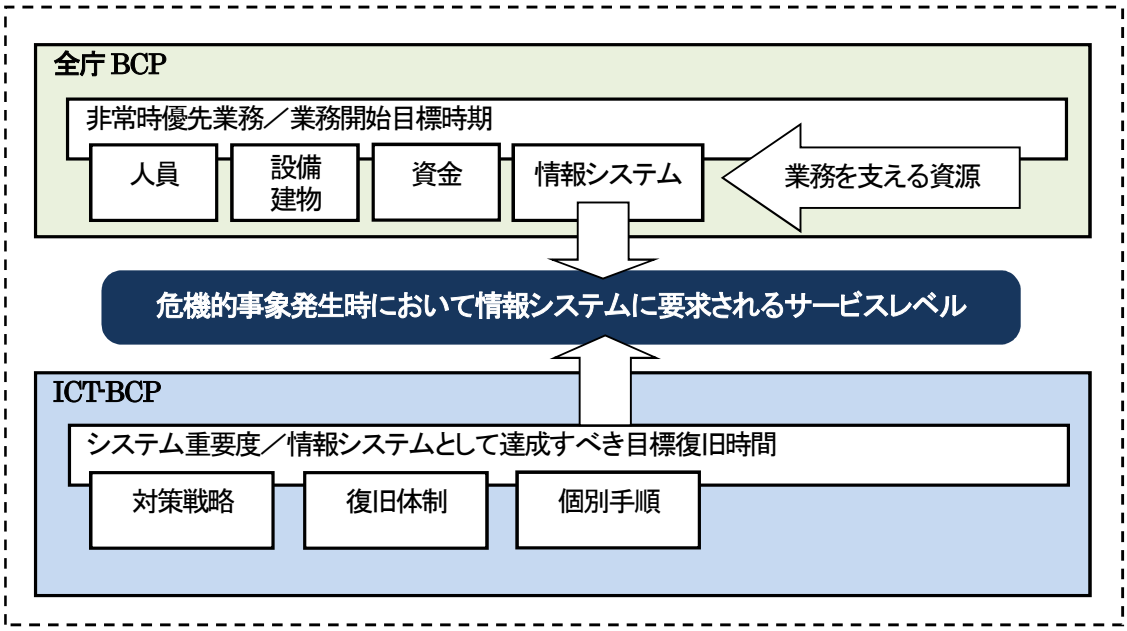

図１－１「ICT-BCP と全庁 BCP の関係」

ただし、ICT-BCP において情報システムの継続性強化策、復旧対策をどれだけ綿密に計画しても、危機的事象発生時に発生する「想定外の事象」により情報システムは停止し、目標復旧時間内に復旧できないこともあり得ることを想定した全庁 BCP の対策戦略が必要である。

ウ　総務省が公表したガイドラインとの関係

さいたま市の ICT-BCP は、平成 20 年 8 月 21 日に総務省が公表した「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」の内容に準拠したものとし、かつ、実効性及びメンテナンス性を考慮した構成とする。

なお、同ガイドラインのステップ構成に対する構成は、適用文書の項に記す。

1.4. 本書の適用範囲

本書は、さいたま市のすべての情報システムに関する継続計画の基本的な枠組みを定めるものであるため、情報部門はもとより、さいたま市の業務を担うすべての情報システムを管理・運用する局、区役所等に適用する。

さいたま市の情報システムには下図のとおり様々な管理・運用形態があり、各々の情報システムごとの継続性への責任範囲は、運用管理の主体や稼働環境等によっても異なる。しかしながら、各業務の情報システムの継続性確保は、それぞれの業務を所管する原課が責任部署となり、事前対策を含めたICT復旧体制の構築や、危機的事象発生時の業務・復旧対応を担うことになる。

そのため、後述するように、情報システムを管理・運用する課ごとに、「ICT-BCP 実行計画書」を策定するものとする。

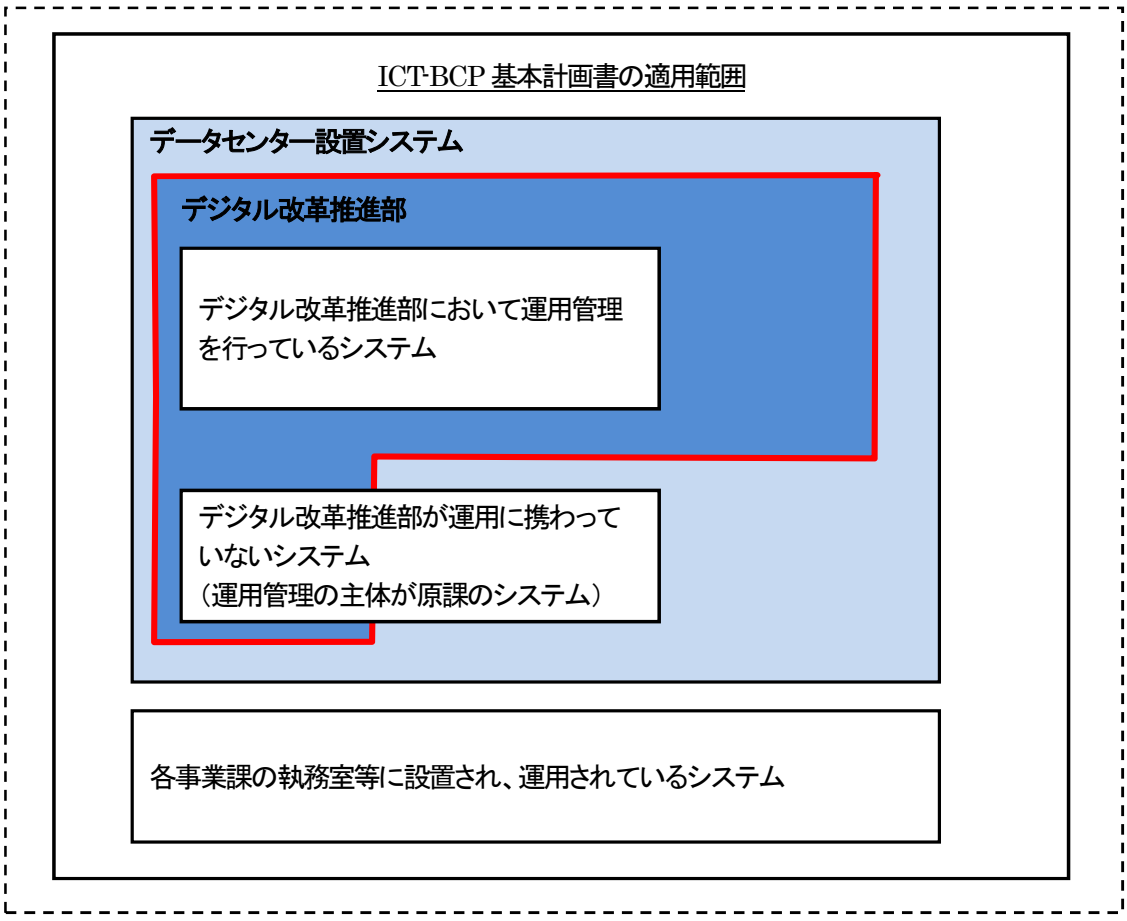

図１－２「基本計画書の適用範囲」

2. 関係文書

本書に関係する文書等とその関係を以下に示す。

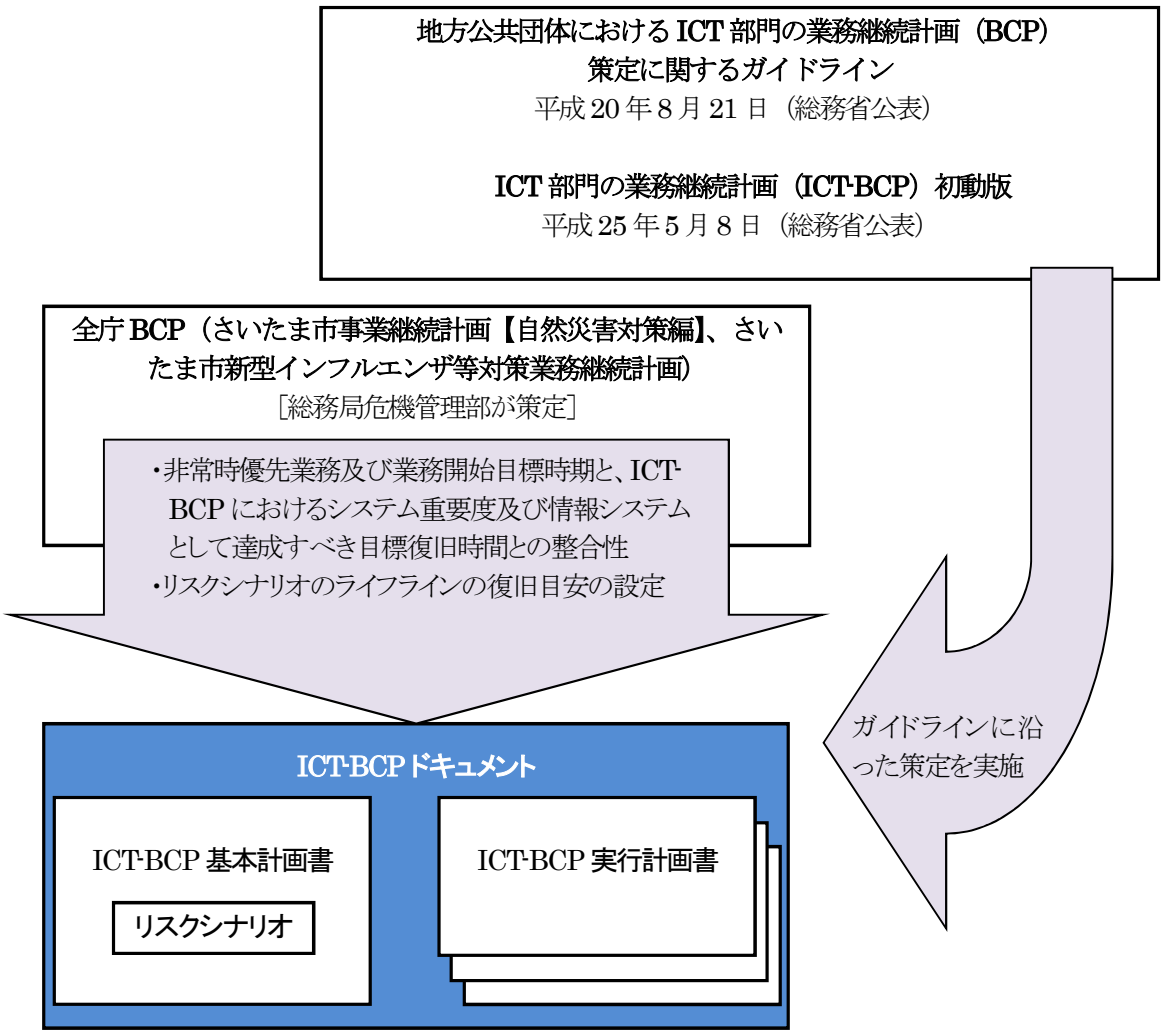

図２－１「本書と適用文書の関係」

（1）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

本計画は、平成 20 年 8 月 21 日に総務省が公表したガイドラインのステップ構成における、調査・分析、BCP 策定工程の項目（図２－２「総務省ガイドラインのステップ構成」の点線枠内）を対象とし、定着化の工程については、後述する「ICT-BCM 推進計画書」の中で具体的な実施方針等を定める。

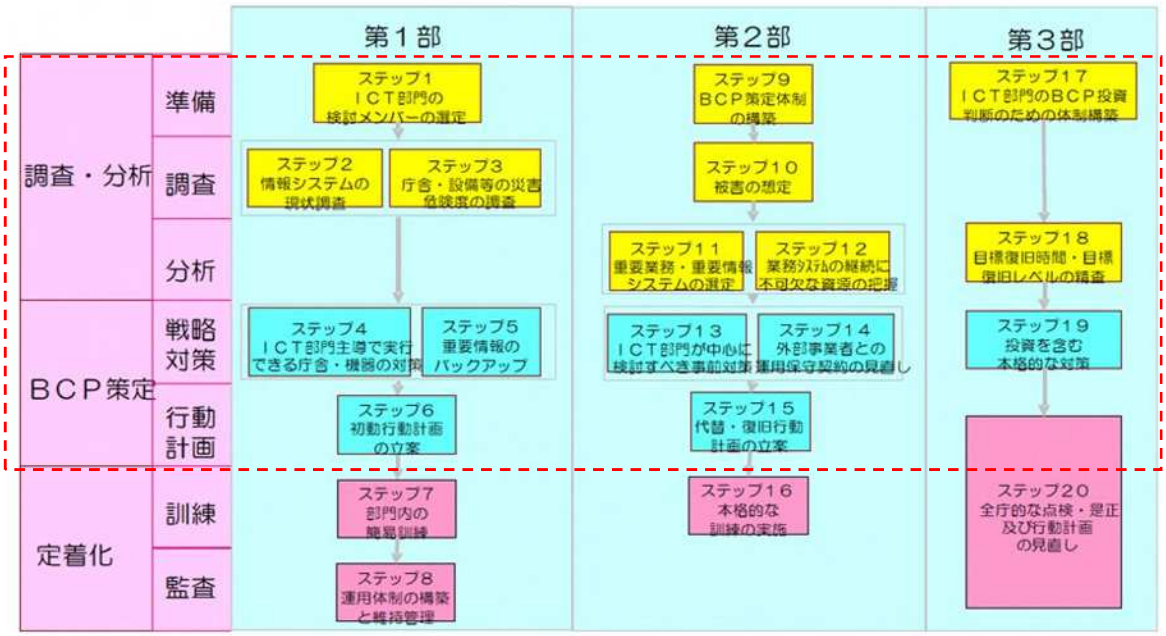

図２－２「総務省ガイドラインのステップ構成」[1]

（2）全庁 BCP（さいたま市事業継続計画【自然災害対策編】、さいたま市新型インフルエンザ等対策業務継続計画）

全庁業務の継続計画としての全庁 BCP とは密接な関係を保つ必要がある。

全庁 BCP における非常時優先業務及び業務開始時期と、ICT-BCP における重要システムに要求されるサービスレベル及び情報システムとして達成すべき目標復旧時間との整合性を図り、また、ICT 復旧対策本部の役割や予算・人員計画についても整合性をとることは、重要な課題である。また、本書「６．ICT 継続マネジメント」に沿って継続して実施する教育及び訓練並びにこれに伴うマニュアルの見直し、承認手続きなどについても連携していく必要がある。

[1] 総務省「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　15 ページより抜粋

3. 本書の文書構成

（1）ICT-BCP 基本計画書の文書構成

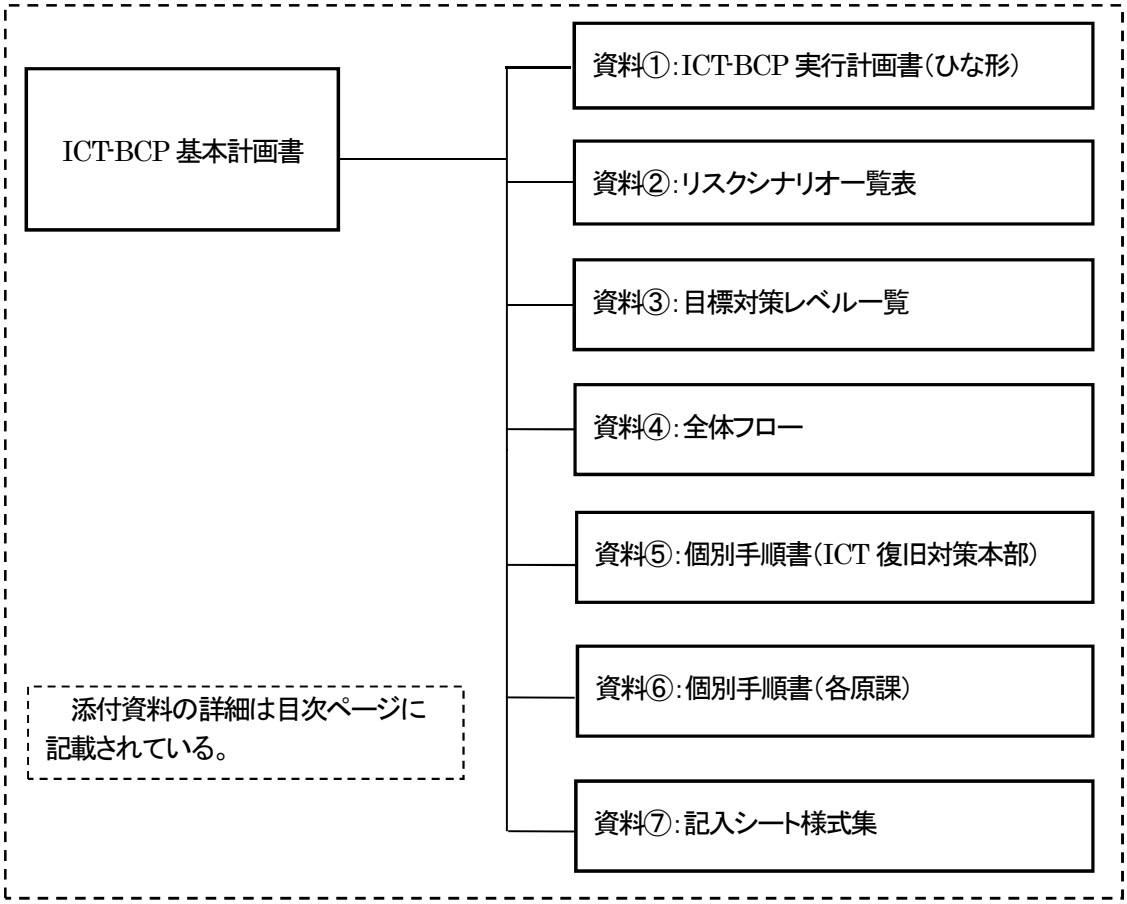

図３－１「ICT-BCP 基本計画書の文書構成」

（2）ICT-BCP 文書の種類と位置づけ

さいたま市が定める ICT-BCP の文書は、表３－１「ICT-BCP の文書の種類」のとおりである。本書は、そのうちの「ICT-BCP 基本計画書」である。

文書名	概要
ICT-BCP 基本計画書 ※本書	危機的事象発生時を想定し、さいたま市の情報システムに関する継続性強化等のため、危機的事象発生時の対策、情報システム復旧に関する体制や役割、手順等に係る基本的な事項を定めるもの。
ICT-BCP 実行計画書	情報システムの所管課ごとに、管理・運用する情報システムについて、ICT 復旧に関する基本的な要件（システム重要度と目標復旧時間、脆弱性に対する対策）や危機的事象発生時の ICT 復旧体制、初動対応手順、システム復旧手順といった、個別具体的な事項を定めるもの。
（参考） ICT-BCM 推進計画書	ICT 部門における業務継続マネジメント（ICT-BCM）を効率的かつ効果的に運用するため、各年度において実施する内容について、実施スケジュールや実施手順等を定めるもの。

表３－１「ICT-BCP の文書の種類」

なお、サイバー攻撃によるシステム障害等の情報セキュリティインシデント発生時の対応については、「ICT-BCP 基本計画書」を補完するものとして、別途「ICT-BCP サイバー攻撃編」を策定している（なお、情報セキュリティインシデント発生時については、災害発生時や感染症流行時における全庁 BCP は無い。）。

（3）「ICT-BCP 実行計画書」に記載すべき要件（「ICT-BCP 実行計画書」作成のガイドライン）

「ICT-BCP 実行計画書」は、情報システムを管理・運用する課単位で、ICT-BCP 実行計画書の目的・位置づけなどの基本事項と、当該課が管理・運用するすべての情報システムを対象として、システムの重要度や目標復旧時間、現状対策レベルと脆弱性、その脆弱性に対する対策を記述する。また、実際に危機的事象発生時のマニュアルとして活用するための要件として、危機的事象発生時の復旧体制と役割、初動対応手順、システム復旧対応手順を記述する。

資料①「ICT-BCP 実行計画書（ひな形）」に、参考とする資料を付し、以下にその記載すべき要件を明示する。

ア　基本項目（はじめに）

「ICT-BCP 実行計画書」の目的、位置づけ、適用範囲、改定要件などを記載する。

イ　当該課所管システムの現状

（ア）システム重要度と目標復旧時間

システム重要度と目標復旧時間の設定基準、当該情報システムの重要度と目標復旧時間を明示する。

（イ）現状対策レベルと脆弱性

さいたま市の ICT 環境に関する目標対策レベル（「ICT-BCP 基本計画書」記載要件）に対する当該情報システムの現状の対策レベルを評価軸ごとに明確にし、目標対策レベルとの乖離を当該情報システムの脆弱性として明示する。

※評価軸は、ICT-BCP 基本計画書において定める目標対策レベルの項目のうち、当該課が管理責任を持つ項目を対象とし、ファシリティや共通のネットワークなどは除外する。

（ウ）脆弱性に対する対策

前項で示した脆弱性に対して当該課が実施する対策を記載する。また、その取組状況を確実に把握、管理していくために、情報システムごとに実施状況が一覧できる管理表形式で記載する。

ウ　危機的事象発生時のマニュアルとして活用する要件

（ア）危機的事象発生時の ICT 復旧体制と役割

当該課の ICT 復旧体制と役割について記載する。

枠組みは「ICT-BCP 基本計画書」に準ずることを明記し、役割ごとの担当者名を明記した「担当者リスト」を作成して記載する。

また、当該情報システムごとの保守・運営を担う外部委託先について「ベンダ連絡先リスト」を作成記載する。

（イ）危機的事象発生時の初動対応手順

危機的事象発生時における当該課の ICT 復旧に関する初動対応手順を記載する。

当該課の初動対応手順は、「ICT-BCP 基本計画書」で定めた全体フロー（「ICT-BCP 実行計画書」の別紙資料）に準ずることを明記し、各役割の初動対応手順は、当該課の個別手順書に記載する。個別手順書は所定の書式を使用し、「ICT-BCP 実行計画書」の別紙資料とする。

また、その個別手順書にて使用する各種資料（様式）は、当該課の環境に応じたものを用い、「危機的事象発生時に使用する様式一覧」に記載して、「ICT-BCP 実行計画書」の別紙資料とする。

（ウ）危機的事象発生時のシステム復旧手順

危機的事象発生時における情報システムごとの復旧手順書名を「復旧手順書一覧」に記載し、併せてその作成、改廃情報を管理する。

情報システムごとの復旧手順書は「ICT-BCP 実行計画書」の別紙資料とする。

なお、復旧手順書には、復旧後に当該情報システム、及び当該データが確実に復旧されたことを検証（証明）する手段を記載するよう努める。また、データの連携など関連する情報システムがある場合、その影響と不整合の検査、検証方法も記載する。

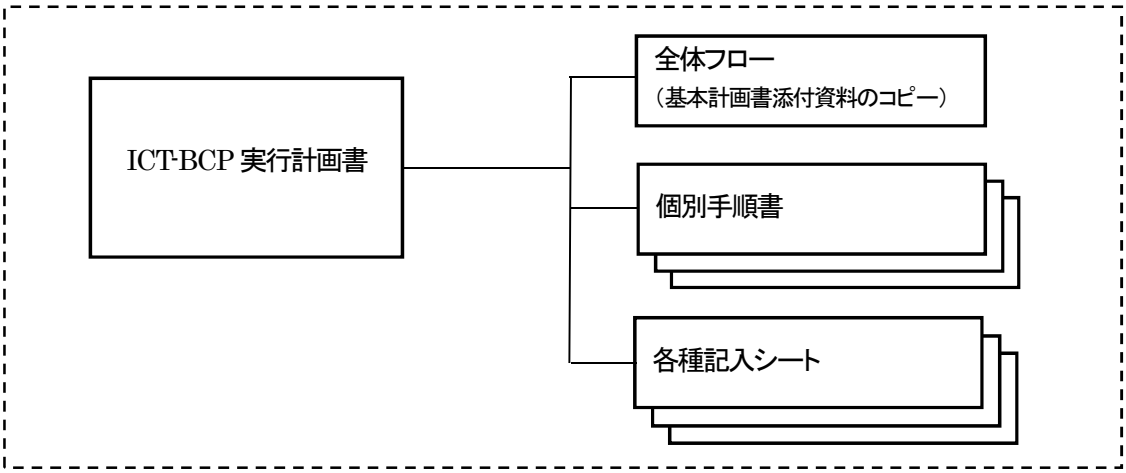

図３－２「ICT-BCP 実行計画書の文書構成」

4. ICT の現状と対策戦略

4.1. 被害の想定

4.1.1. 大規模地震による被害の想定

本計画の前提条件となる、想定地震とそれに基づく被害想定については、「さいたま市事業継続計画【自然災害対策編】」における被害想定に準じて、下記のとおりとした。

なお、不測の事態発生により庁舎自体が利用できなくなるような「想定外の事象」についても検討する必要がある（「4.3.4 想定外の事象への対応（初動対応）について検討すべき対策」に後述）。

種別	被害項目	被害単位	さいたま市 直下地震
地盤	急傾斜地崩壊	危険性が高い急傾斜地［箇所］	16
建物	揺れ	全壊棟数[棟]	17,300
		半壊棟数[棟]	48,400
	液状化	全壊棟数[棟]	203
		半壊棟数[棟]	6,040
	急傾斜地崩壊	全壊棟数[棟]	2
		半壊棟数[棟]	4
火災（冬 18 時）	出火	炎上出火件数[件]	101
	延焼	焼失棟数[棟]	44,900
人	死者	[人]	2,040
	負傷者	[人]	8,150
	重傷者	[人]	1,400
ライフライン	上水道	断水人口（1 日後）	265,000
	下水道	機能支障人口（1 日後）	57,300
	電力	停電件数（1 日後）	107,000
	通信	不通回線数（1 日後）	95,500
	都市ガス	供給停止件数（直後）	257,000
交通	道路	緊急輸送道路被害箇所数	46
		橋梁被害箇所数	2
	鉄道	被害箇所数	227
生活支障等	避難者	避難者　直後・1 日後［人］ （内、避難所生活者）	204,000 (123,000)
		避難者　1 か月後［人］ （内、避難所生活者）	204,000 (61,300)
	帰宅困難者	人（平日　12 時）	116,000～141,000
	災害廃棄物	発生量［万㎥］	679
	経済被害	直接経済被害額［兆円］	3.88

表４－１「さいたま市直下地震の被害想定」[2]

[2] さいたま市「さいたま市事業継続計画【自然災害対策編】」令和５年３月　７ページより抜粋

4.1.2. 新型インフルエンザ等の感染症による被害の想定

大規模地震による被害の想定と同様に、新型インフルエンザ等の感染症流行時における被害想定については、「さいたま市新型インフルエンザ等対策行動計画」における被害想定に準じて、下記のとおりとした。

患者種別		最大値	最小値
受診患者数（人）	全国	約　25,000,000	約　13,000,000
	埼玉県	約　1,400,000	約　750,000
	さいたま市	約　243,700	約　130,600
全人口の 25%が罹患（りかん）すると想定した場合の医療機関を受診する患者数の推計			

表４－２「新型インフルエンザ等発生時におけるさいたま市患者数」[3]

感染症の流行により、直接的にシステムの停止や破壊が引き起こされることは想定しないが、ICT を維持・継続するためには人的資源が必要となるため、感染症流行時における「人的資源の確保」という視点から対応する必要がある。

特に、新型コロナウイルス感染症（COVID-19）の流行時においては、令和元年 12 月に「原因不明のウイルス性肺炎」として確認されて以降世界的に感染が拡大し、日本国内においても、全国的かつ急速な蔓延により国民生活及び国民経済に甚大な影響を及ぼすおそれがある事態が発生し、令和 2 年 4 月には、新型インフルエンザ等対策特別措置法第 32 条第 1 項に基づく「緊急事態宣言」も発令された。この際、国から各関係団体に対し「出勤者 7 割削減」の要請がされ、地方公共団体に対しても、「緊急事態宣言時に事業の継続が求められる事業者に該当するものであるが、感染症の蔓延防止の緊要性に鑑みれば、自らも出勤者の削減に最大限取り組むこと」が求められ、さいたま市においても、職員の接触機会低減の取組強化（テレワークの推進等）に取り組んだところである。なお、新型コロナウイルス感染症については、その後幾度かの波を繰り返しながら、令和 4 年 3 月現在も流行が継続している状況である。

感染症流行時は、脅威発生により急に業務が停止するのではなく、業務遂行に必要な人員が徐々に減少していくという特徴がある。災害発生時のように、「いかに『早い時間に復旧』するか。」という観点ではなく、「いかに『市民生活の維持等に必要な業務を継続』するか。」という観点が重要となってくる。加えて、新型コロナウイルス感染症のように、感染症の影響が局面を変えながら長期化する場合、外出抑制やテレワーク等の働き方の変化に伴い、システムで利用する機能や利用環境が変化するが、これら変化への適応が円滑に行われない、又はこれらの変化により新たに問題が発生する可能性を踏まえた視点での対応も検討しなければならない。

4.1.3. サイバー攻撃による被害の想定

サイバー攻撃における被害想定は、「ICT-BCP サイバー攻撃編」に記載する。

[3] さいたま市「さいたま市新型インフルエンザ等対策行動計画」平成 26 年 12 月　9 ページより抜粋

4.1.4. リスクシナリオの設定

被害の想定（以下「リスクシナリオ」という。）は、さいたま市のICT環境の脆弱性評価を実施する上での前提となるものである。

リスクシナリオ作成にあたっては、図４－１「被害想定の方法」のように、“どこで”、“どのような脅威が原因で”、その結果“システムにどのような被害が生じるか”という観点で検討を行う。

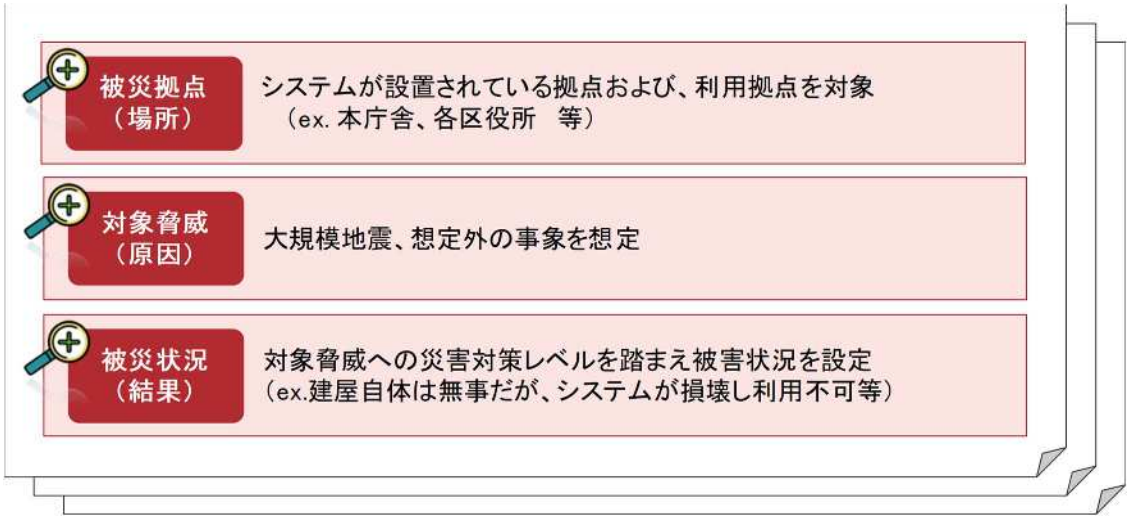

図４－１「被害想定の方法」

（1）リスクシナリオ設定の考え方

リスクシナリオは、論理的には被災拠点（場所）、対象脅威（原因）、被災状況（結果）の組み合わせの数だけ存在するが、脅威の発生確率及び被害の大きさの両面から、重点的に検討すべきリスクシナリオを選定する。

（2）リスクシナリオの考え方

リスク要因（地震や火災、風水害等の被害発生の原因となる事象）と自庁リソースが抱える脆弱性（対策が不十分な状況）を評価し、リスク要因が発生した場合に生じる被害状況の想定をリスクシナリオとして整理する。

4.1.5. さいたま市のリスクシナリオ

さいたま市で設定するリスクシナリオは、表４－３「さいたま市のリスクシナリオ」のとおりである。

対象脅威（原因）	被災拠点（場所）	No	被災状況（結果）
大規模地震	システム設置拠点	1	✓ <u>建屋は無事だが、サーバが一部損壊するシナリオ</u> ・ 大規模地震等により、システムが設置されている建屋は無事だが、建屋内に設置してある一部サーバ機器などの筐体（きょうたい）が損壊し、重要なシステムの一部が利用できない状況
		2	✓ <u>建屋が全壊するシナリオ</u> ・ 大規模地震等により、システムが設置されている建屋が全壊し、すべてのシステムが損壊・利用できない状況
	システム利用拠点	3	✓ <u>建屋への立ち入りが不可能となり、その拠点からのシステム利用が一定期間不可能となるシナリオ</u> ・ 大規模地震等により、建屋が倒壊又は修復不能なダメージを受け、建屋が使用できず一定期間システムが利用できない状況
		4	✓ <u>建屋が無事だが、社内外のネットワークが被災することにより一定期間システム利用が不可能となるシナリオ</u> ・ 大規模地震等により、建屋は無事だが、外部ネットワーク及び拠点内 LAN が被災することにより、一定期間システムが利用できない状況
新型インフルエンザ等の感染症	―	5	✓ <u>建屋、機器、システム等は無事だが、利用、運用、保守等する人がいなくなるシナリオ</u> ・ 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、消毒作業等の対応が必要となり一時的に立ち入れない状況 ・ 物理的被害はないが、テレワーク（在宅勤務）が推奨されたことで、アクセスの集中によって通信回線帯域が不足する状況。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状況 ・ 職員又は委託先担当者が罹患し、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状況
サイバー攻撃	―	―	（「ICT-BCP サイバー攻撃編」に記載する。）
想定外の事象	―	6	✓ <u>想定外の事象の発生により、一部のシステム利用が不可能となるシナリオ</u> ・ 想定外の事象が発生することにより、一定期間システムが利用できない状況

表４－３「さいたま市のリスクシナリオ」

なお、各リスクシナリオにおける ICT リソースごとの被害状況については、資料②「リスクシナリオ一覧表」を参照のこと。

4.1.6. ライフラインの被害想定（さいたま市独自の設定根拠）

地震災害の発生時における前項各リスクシナリオのライフラインの復旧目安については、全庁 BCP（「さいたま市事業継続計画【自然災害対策編】」）表２．１．２災害シナリオ（さいたま市直下地震）で想定している情報から抜粋した。

項目	～12 時間後	～3 日	～7 日	～14 日
電力	直後は、震度６強以上の地域全域にあたる約345,000軒が停電となる（停電率62.9%）。	電柱折損（約890本）や火災による家屋焼失により、約107,000軒が停電の影響を受ける（停電率19.4%）。病院等の重要施設では非常用発電装置で対応し、設備を有さない施設には電源車を配備して対応。ただし、燃料の供給に支障。	すべての地域で応急復旧がほぼ完了する。	
通信	直後は、約267,000人が通信の影響を受ける（不通率59.2%）他、さいたま市全域で輻輳（ふくそう）のため通話はほとんどできなくなる。メールもかなりの遅延を生じる。災害用伝言ダイヤルの運用開始。	電柱折損（約350本）や火災による家屋焼失により、約95,000人（不通率21.2%）が通信の影響を受ける。通話の輻輳（ふくそう）は続くが、つながり始める。メールはほぼ正常化。一方で、停電エリアの基地局等で非常用電源の燃料補充が間に合わず停波するところも生じる。避難所等では、衛星携帯電話や携帯各社の移動中継局が配備され始める。	すべての地域でほぼ応急復旧が完了する。	
上水道	約450件の配水管被害が発生し、発災直後は約476,000人（断水率39.0%）が断水の影響を受けると想定される。配管被害により、道路で漏水する箇所も発生。	引き続き断水状態継続。１日後においても約265,000人（断水率21.7%）が断水の影響を受ける。給水車等による応急給水対応。	応急復旧作業が開始され、市内の断水世帯数が減少。配水幹線付近で仮設給水栓設置。	市内の多くで断水は解消。

表４－４「ライフラインの被害想定、設定根拠」[4]

[4] さいたま市「さいたま市事業継続計画【自然災害対策編】」令和５年３月　10 ページから抜粋

4.2. システム重要度と目標復旧時間

4.2.1. システム重要度の設定

（1）災害発生時におけるシステム重要度の設定

災害発生時には、それぞれのシステムに関連する業務の復旧に応じ、システムの目標復旧時間を定める必要がある。

本計画においては、システムに関連する業務の「業務開始目標時期」と業務遂行にあたっての「システム依存度」の両面を考慮し、「システム重要度」を定め、併せて目標復旧時間を以下に設定した。

システム重要度	目標復旧時間
S	3 時間以内
A	24 時間以内
B	3 日以内
C	7 日以内
D	30 日以内

表４－５「システム重要度と目標復旧時間」

（2）感染症流行時におけるシステム重要度の設定

感染症流行時におけるシステム重要度については、「さいたま市新型インフルエンザ等対策業務継続計画」における、「新型インフルエンザ等対応業務（業務継続方針S)」及び「通常業務」の「業務継続方針A（通常)」・「同B（縮小・変更)」・「同C（休止)」・「同D（積極的休止)」にそれぞれ合わせて適用することとする。

具体的には、「新型インフルエンザ等対応業務（業務継続方針 S)」と「通常業務の業務継続方針A（通常)」を「優先業務」とし、優先業務を実施するにあたってシステムが必要不可欠な場合は、当該システムを、システム重要度がS又はAとなる「優先システム」とする。以下、「通常業務の業務継続方針B（縮小・変更)」・「同C（休止)」・「同D（積極的休止)」において使用するシステムは、それぞれシステム重要度B・C・Dとする。

新型インフルエンザ等対策業務継続計画における業務継続方針		対応するシステム	システム重要度	システムの継続維持内容
S	新型インフルエンザ等発生時に優先的に対応する。	業務継続方針Sの業務が依存するシステム	S	最優先
A	第三段階（市内感染期）の時、できるだけ通常通り継続する。	業務継続方針Aの業務が依存するシステム	A	優先
B	第三段階（市内感染期）の時、縮小したり、取扱い方法を変更したりして継続する。	業務継続方針Bの業務が依存するシステム	B	縮小・変更
C	第三段階（市内感染期、市内発生早期）の時、中断・休止する。	業務継続方針Cの業務が依存するシステム	C	中断・休止
D	前段階～第二段階（国内発生早期まで）のうちから中断・休止する。	業務継続方針Dの業務が依存するシステム	D	早期に中断・休止

表４－６　「感染症流行時のシステム重要度と継続維持内容」

感染症流行時、業務が中断・休止となった場合は、当該業務が依存するシステムを休止することは構わないが、業務が継続中に、当該業務が依存するシステムが休止することは避けなければならない。

4.2.2. 目標対策レベルの設定

継続的にICT運用の継続性を強化・維持していくためには、ICT運用継続に必要な評価軸ごとに、どのような対策が必要かを管理するためのフレームワークを構築する必要がある。

そのため、情報システムの稼動に必要となる構成要素ごとに、システム重要度に応じた対策の目標（以下「目標対策レベル」という。）を設定し、「何に対してどの程度対策を図っていく必要があるのか」を明らかにする必要がある。なお、目標対策レベルは、現状の脆弱性把握や今後の対策を検討する際の基準となるものである。

さいたま市では、多くのシステムのサーバ等の機器を、より災害に強い、堅牢なデータセンターに設置しており、それを前提として、システム重要度に応じて災害対策の観点からシステムが目指すべき目標対策レベルを図４－２「目標対策レベルの設定（概要）」のとおり５段階にて設定した。

なお、ファシリティなど全システムに共通する評価軸に関する対策レベルについては、システム重要度に応じた個別設定とせず、システム重要度が最も高いシステムにあわせて設定することとした。

			市庁舎利用拠点 利用拠点のファシリティ（利用拠点の堅牢性）	市庁舎利用拠点 ネットワーク設計・機器	データセンター ファシリティ
重要度	復旧目標	対策レベル	利用拠点のファシリティ設備について	利用拠点のネットワーク機器について	データセンター設置サーバの建屋について
S	3時間	5	（対策レベル2に加え） ・商用電力は複数の異なる電力会社から経路も別にして受電している。（一つの電力供給の途絶の場合も重要システムの運用を継続できる） ・停電（商用電力の受電停止）時もサーバールームの空調設備、ネットワーク機器、重要システムの端末等が稼動できるよう、１日以上電力供給できる自家発電装置等の非常用電源を装備している。	同下	1. 立地 ・PL値の結果、液状化危険度が「かなり低い」となっている。或いは、液状化危険度が「かなり低い」より高い結果の場合、杭打ち等により液状化対策を講じている。 2. 建物 ・新耐震基準（1981年6月改正）を満たしている。（耐震） ・施設・設備に対し、次に挙げるいづれかの免震・制震対策を講じている。 ①建物の免震・制震構造 ②フロア（床）の免震構造 ③サーバラックの免震対策 3. 電気設備 ・商用電力は複数の異なる電力会社から経路も別にして受電している。（一つの電力供給の途絶の場合も重要システムの運用を継続できる） ・建物内の電源経路が複数経路で冗長化されている。 ・自家発電設備及び無停電電源設備を有している。 ・燃料の確保、オイル供給会社との優先供給契約により、商用電源喪失時でも1週間の電源供給が可能である。 4. 空調設備 ・空調設備の冗長化が図られている。 ・空調設備への電源経路が複数経路で冗長化されている。 ・自家発電設備からの電源供給が可能である。 5. 通信設備 ・複数キャリアかつ複数経路により冗長化されている。 ・建物内のネットワークについては、複数経路で冗長化されている。 ・経路上のネットワーク機器については、冗長化されている。 ・自家発電設備からの電源供給が可能である。 6. その他設備 ・バックアップテープを安全に保管するための設備を有している。 7. 設備運用 ・8時間／日以上の常駐管理体制となっている。 ・災害発生時に早期に復旧するための体制として、緊急対応マニュアルや防災マニュアル、BCP等を策定している。
A	24時間	4	同下	（対策レベル3に加え） ・ネットワーク機器に非常用電源からの電力供給がされるよう構成されている。 ・非常用電源が不要なネットワーク構成を作っている。	
B	3日	3	同下	（対策レベル2に加え） ・主回線と副回線が同時に被災しないよう回線の経路を考慮している。 ・主回線と副回線それぞれについて引込口を分ける等の対策を実施している。 ・拠点内のLANの冗長化を行っている。	
C	7日	2	（対策レベル1に加え） ・電源設備が水没しないよう地下に設置していない。もしくは、地下にあっても水が入らないようなつくりになっている。	（対策レベル1に加え） ・ネットワークの設定情報等のバックアップを行い、同時被災しない場所に保管している。	
D	30日	1	・庁舎は新耐震基準を満たしている。 （1981年以降に設計された庁舎） ・新耐震基準と同等以上の耐震性能を証明できる。	・販売終了や保守契約切れのネットワーク機器の更改を行うことにより、災害発生時に少なくとも同等機器の再調達を可能にしている。 ・併せて、海外ネットワーク機器全てが安易に再調達可能 ・ネットワーク機器の設定情報等のバックアップを取っている。	

図４－２「目標対策レベルの設定（概要）」

※さいたま市の具体的な目標対策レベルについては、資料③「目標対策レベル一覧」を参照のこと。

4.3. さいたま市としてのICT災害対策戦略

さいたま市のICT災害対策方針は、以下のとおりとする。

（1）ICT継続戦略は「復旧戦略」と「代替戦略」の観点で検討する。

（2）ICT継続戦略に基づく事前対策を、リスクシナリオに合わせてシステム設置拠点、システム利用拠点ごとに実施する手順を定め、継続的な改善を図る。

（3）ICT継続戦略に基づく事前対策を施しても、災害発生時には想定外の事象が必ず発生する。想定外の事象に遭遇した場合にも有効なツールや機能、資材など、特に発災直後の初動をできる限り効率的かつ有効的に遂行できるように準備する。

4.3.1. ICT継続戦略

業務継続戦略としては、一般的に「復旧戦略」と「代替戦略」が挙げられ、ICT継続戦略も同様である。

「復旧戦略」と「代替戦略」の両方の戦略を検討しておく必要があり、危機的事象発生時には通常、「復旧戦略」をとるが、目標復旧時間内に復旧できない場合に「代替戦略」をとることになる。

さいたま市においては、情報システムの多くを外部の堅牢なデータセンターに移設しているため、当該情報システムは災害発生時にも障害となる可能性は低く、システム設置拠点に対するICT継続戦略の必要性は著しく低くなった。ただし、市庁舎等にサーバを設置して各事業課にて運用している情報システムに対しては、災害が発生した場合を想定した戦略が必要である。

また、システム利用拠点とシステム設置拠点とを結ぶネットワークについては、設備の冗長化や各区役所間の協業体制などを含めた、ICT継続戦略を講じる必要があり、これらはシステム設置拠点が外部の堅牢なデータセンターに移管された後も継続的に改善を図っていかなければならない。

戦略の種類	内容	対策例
復旧戦略	平常時に利用している資源（拠点・設備・要員・情報システム等）を修理・再調達等により復旧し、業務を再開する。目標復旧時間が比較的長い場合に採用されることが多い戦略。	復旧を早めるための耐震対策、情報システムの重要データのバックアップ等。
代替戦略	平常時とは異なる場所や手段を使い、代替の方法で業務を再開する。目標復旧時間が短く早急な再開が必要な場合に採用されることが多い戦略。	代替拠点の設置、複数拠点への重要な設備機器の設置、他拠点へのバックアップシステムの設置、職員の多能化等。

表４－７「戦略の種類と対策例」

4.3.2. ICT継続戦略実現のための対策

ICT継続戦略を実現するためには、危機的事象発生時に甚大な被害が発生する原因となる重大な脆弱性課題に対する事前対策や、危機的事象発生時に迅速かつ効率的に対応するための対策を実施し、さいたま市のICT継続能力をステップごとに向上していく必要がある。

（1）事前対策の検討（対策ステップによる段階的な対策の実施計画）

ICT 環境の現状の脆弱性概要で明らかになった脆弱性に対し、システムの重要度に応じた対策を３つのステップに分けて段階的に実施（以下「対策ステップ」という。）することで、ICT 環境の脆弱性を解消していく。

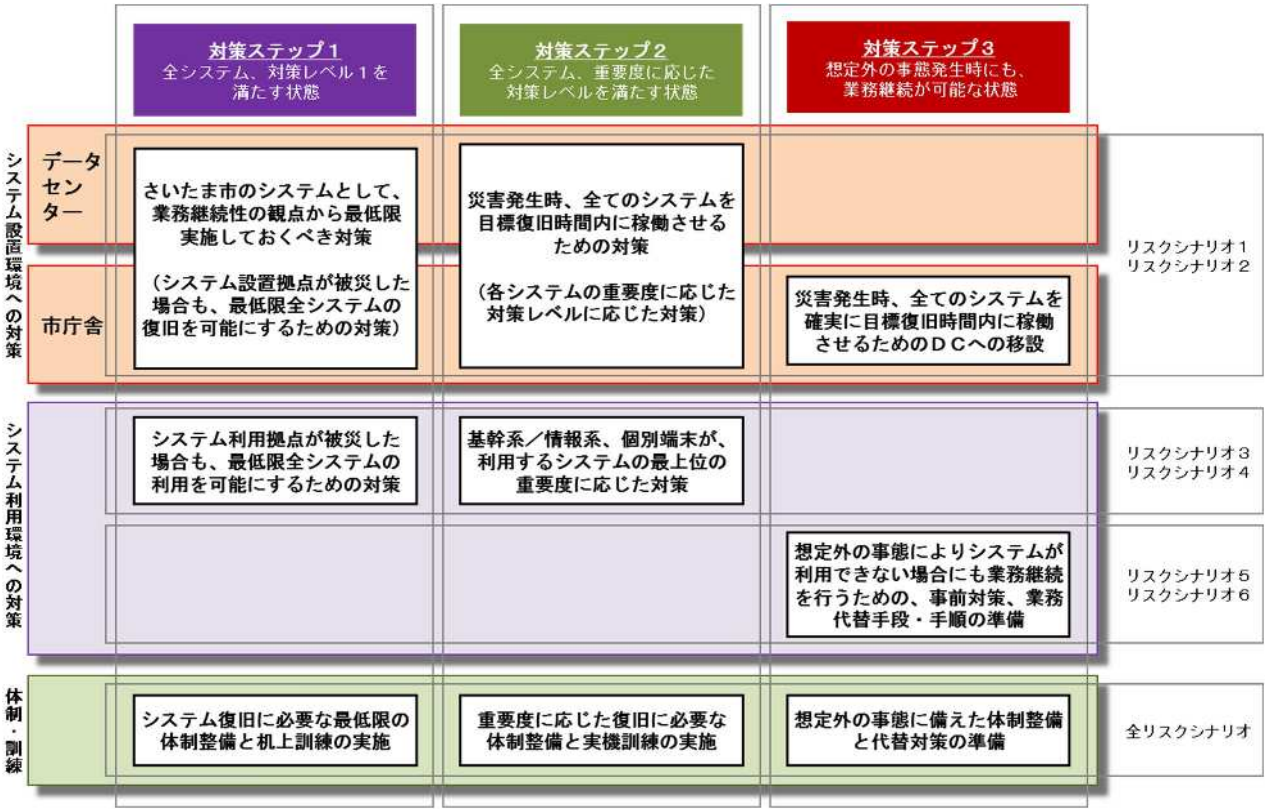

図４－３「対策ステップとリスクシナリオ」

（2）対策ステップごとの対策項目と内容

リスクシナリオに対する対策として実施すべき対策一覧及び内容は、以下のとおりとする。

対策ステップ	番号	対象先	対策内容
対策ステップ１	1	設置拠点	サーバ機器の外、システムを構成するハードウェアは、再調達が可能なものある。
	2	設置拠点	サーバのシステム領域／データ領域のバックアップを取得し、適切な場所に保管している。
	3	利用拠点	ネットワーク機器は再調達が可能なもので、その設定情報のバックアップも取得し、適切な場所に保管している。
	4	利用拠点	ハードウェアやソフトウェアは、再調達が可能なものである。
	5	体制・訓練	危機的事象発生時における連絡体制（休日・夜間を含む。）を整備し、最新の情報に更新している。
	6	体制・訓練	システムの復旧又は運用の継続に必要となる要員を確保できる体制を検討している。
	7	体制・訓練	システムの復旧又は運用の継続を実施するための手順書を整備している。
対策ステップ２	8	設置拠点	サーバ機器の外、システムを構成する機器は、非常用電源が供給されるよう設定している。
	9	設置拠点	市庁舎にサーバが設置されている場合、当該庁舎損壊に備えた代替環境（バックアップサイト）を確保している。
	10	利用拠点	ネットワークの冗長化、ネットワーク機器への非常用電源供給の設定が完了している。
	11	体制・訓練	システムの復旧に関係する事業者と災害発生時における対応のSLAの締結や覚書等の協定を結んでいる。
	12	体制・訓練	災害発生から暫定運用、復旧までのフローが明確化され、職員が熟知している。
	13	体制・訓練	システム単位の復旧手順書に基づく机上訓練及び改善を定期的（1回／年以上）に実施している。
対策ステップ３	14	設置拠点	サーバ機器等が外部の堅牢なデータセンターで運用されている、又はホットスタンバイ用のバックアップサイトがある。
	15	利用拠点	端末・周辺機器に対して、非常用電源を供給できるようにしている。予備機は、即代替できるようセットアップをしている。
	16	利用拠点	システム／データのバックアップを同時被災しない外部に保管している。
	17	利用拠点	システムが利用できない場合に備え、システムの代替手段を準備している。
	18	体制・訓練	システム運用担当者は、24時間365日の運用監視体制としている。
	19	体制・訓練	現場における作業実施が困難な場合に、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等を構築している。
	20	体制・訓練	システム単位の復旧手順書に基づく実機訓練及び改善を定期的（1回／年以上）に実施している。

表４－８「対策ステップごとの対策項目」

4.3.3. 脆弱性及び対策状況の把握

（1）大規模地震に係る脆弱性及び対策状況の把握

情報システム環境の現状を、さいたま市が設定した目標対策レベルの構成要素ごとに調査することで、システム重要度に応じて、目標とする情報システム運用環境と現状の情報システム運用環境の差異を把握する。これにより、災害発生時において復旧のボトルネックとなる脆弱性を洗い出す。

なお、脆弱性及び対策状況については、システム環境の変化や、個別のシステム再構築、改修等により変化することから、適宜内容の見直しを実施していく。

ア．現状の脆弱性把握

（ア）脆弱性評価の考え方

さいたま市が設定した目標対策レベルの構成要素を評価軸とし、各システム環境の現状の対策状況（以下「現状対策レベル」という。）を調査した上で、システム重要度ごとの「目標対策レベル」との差異（どこまで対策が進んでいるのか）を明らかにすることにより脆弱性を把握する。

（イ）脆弱性評価の単位

現状の脆弱性を評価するにあたっては、システムを利用する際に必要となる目標対策レベルの構成要素（評価軸）を評価単位で評価を行う。

（ウ）現状調査（現状対策状況の調査）

現状の脆弱性を把握するため、前述の脆弱性評価の単位ごとに現状の対策状況調査を行う。

イ．脆弱性評価結果

全体的な各システムの脆弱性及び対策状況の進捗等を把握するために、ICT-BCP 継続マネジメント（ICT-BCM）の一環として、「システム対策マトリクス」にてまとめて管理する。また、各システムに共通するシステム環境に関する脆弱性の評価結果については、ICT-BCP 運用マネジメントにおいて管理する。

4.3.4. 想定外の事象への対応（初動対応）について検討すべき対策

東日本大震災では、地方公共団体の庁舎や関連施設が津波の被害を受け、住民データをはじめとした重要な情報資産を消失してしまったほか、災害対策の拠点、コミュニケーション手段までも喪失するなど、地震による直接被害だけではなく、津波や、更にそこから派生した原発被害など想定外の事象の連鎖により甚大な被害をもたらした。

想定外の事象が発生した際にも、住民の生命・生活・財産を守るために、迅速な対応が必要となる初動対応は、極めて重要性が高い。その活動において最も重要な資源は職員であるが、その行動を支える重要な資源である拠点、情報資産及びコミュニケーション手段の確保が望まれる。

以下に想定外の事象への初動対応について検討すべき対策を、既に対策を実施している内容も含めて記載する。なお、以下の対策の一部はセキュリティ面の課題など、直ちに導入等を行うことが困難な対策も含まれるため、今後も継続して対応を検討していく必要がある。

（1）代替拠点の検討

さいたま市の情報システムの設置拠点となっているデータセンターや区役所、消防局、水道局、市立病院等が利用できなくなった場合、ICT 復旧対策本部の要員を含む ICT 部門の職員、各課の ICT 復旧要員の参集場所及び復旧活動の拠点が失われることになる。こうした事態に備え、各拠点が利用できなくなった場合の「代替拠点」を検討しておくことが望ましい。たとえば、ファシリティ面の脆弱性が低く、立地面でも安全性の高い区役所等の市庁舎や耐震性の優れた近隣の外部データセンターのレンタルオフィスなどを代替拠点として設定しておくことが有効な手段のひとつとして考えられる。

具体的には、ICT 復旧対策本部の設置場所や各課の ICT 復旧要員の参集場所を代替拠点も含めて明確にしておくことが望まれ、それらはファシリティの変更（市庁舎等の増改築等）や組織変更に伴う組織・人員の配置変更などの環境変更に適応するため、次項「5. ICT 復旧体制と役割、個別手順」にて制定する各組織の個別手順に明記する。

（2）システム利用拠点の住民データの保全

初動対応において、住民情報は住民の安否確認等に利用されるため、極めて重要な情報資産である。想定外の事象に備えて、事前対策として各区役所等において、定期的に住民情報を PC などの調達の容易な機器で利用できる状態で保全しておくことが望まれる。

ただし、対象とする情報は必要最小限の内容とし、外国人の情報や外字対応など特殊な要因が含まれている点を考慮し、かつ、万全のセキュリティ対策が必要である。また、同データの利用に際して、内容が限定されていることを明確にし、職員に周知しておく必要がある。

（3）SNS 等による情報発信

東日本大震災以降、多くの自治体で Facebook、Twitter 等の SNS（ソーシャルネットワーキングサービス）などによる情報発信を行うようになった。これは、災害発生時等に公式なホームページが復旧するまでの期間の情報提供には有効であることが実証されたためである。災害発生時に住民等への被害状況などの情報提供は、市のホームページ以外にも SNS などを活用して継続していくことが望ましい。

また、平時から SNS などを用いた各種情報提供を行い、その有用性を住民に周知しておくことで、災害発生時にも有効な情報提供手段となることから、継続した情報発信と広報活動が必要である。

（4）モバイル PC、コピー機、各種消耗品（OA 用紙、トナー等）の準備

初動対応を迅速に、効率的に進めていくためには、PC やコピー機、またその消耗品（OA 用紙、トナー等）についても重要なリソースである。特に、モバイル PC は可搬性に富み、先の住民情報の保全データと併せて、避難所などの施設で住民の安否確認等に利用できるように区役所等に配備

しておくことが望ましい。

ただし、災害発生時にすぐに使えるようにするためには、常に充電がされている状態に保ち、かつ、定期的な動作確認が必要となるため、その管理・運用を含めた検討が必要である。また、各種消耗品についても災害発生直後の混乱期には入手が困難になるおそれがあるため、事前に適正量の備蓄をしておくことが望ましい。

（5）復旧の優先順位

複数のシステムを保有する課等は、災害発生時にすべてのシステムが機能しなくなるのか、また、いずれかのシステムが機能しなくなるかは分からない（後述する感染症流行時も同様）。このような想定できない事態に対して、システムの復旧要員が限られている場合には、システムの重要度が同じであっても、システムの復旧優先順位をつけておき、優先順位の高いシステムから復旧させていくことが望ましい。

（6）システム運用担当者の負担軽減

災害発生時においてシステム運用担当者の確保が困難になる可能性がある。そのためにICT運用管理の導入・システム運用のクロス担当化なども必要である（後述する感染症流行時も同様）。

また、システム運用についても、地方公共団体の情報システムの標準化の流れを踏まえ、利便性等の観点から個別に機能のカスタマイズ等を行っているシステムについては、当該機能の必要性の有無等について再検討することも必要である。

（7）建屋が避難場所となることも想定したセキュリティ対策

災害発生時には、混乱に乗じて情報システム機器等が設置された建屋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必要がある。

なお、災害発生時には、建物内に関係者以外の人々の一時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格なセキュリティ管理を実施することは現実的ではない。そこで、最低限必要な措置として、あらかじ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必要がある。

4.3.5. 感染症流行時において特に検討すべき対策

新型インフルエンザ等の感染症流行時においては、「4.3.2 ICT 継続戦略実現のための対策」の「体制・訓練」を適用することになるが、特に、新型コロナウイルス感染症（COVID-19）のように、新型インフルエンザ等対策特別措置法第 32 条第 1 項に基づく「緊急事態宣言」が発令され、「人的資源の確保」が長期間に渡って困難となる事態が生じるおそれがある。

こうした感染症流行時において検討すべき対策について、既に対策を実施している内容も含めて記載する。なお、以下の対策の一部は、セキュリティ面の課題など、直ちに導入等をすることが困難な対策も含まれるため、今後も継続して対応を検討していく必要がある。

（1）職員の感染やテレワーク（在宅勤務）の実施に伴う対応

職員の感染症の罹患やその疑いによる出勤抑制又はテレワーク（在宅勤務）の実施等により、後述する ICT 復旧体制に携わる職員が、勤務公署等に出勤しないという状況が想定される。

そのため、こうした場合であってもシステム運用を継続できるよう、連絡体制の構築、連絡手段の確保、テレワーク（在宅勤務）に係る環境面及び制度面の整備、ICT 復旧体制に携わる職員の代替の確保等について、検討しておく必要がある。

なお、テレワーク（在宅勤務）に係る環境面の整備に当たっては、テレワークの増加によりアクセスが集中し、回線の帯域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も想定する必要がある。

（2）委託先（ベンダ等）の担当者の感染やテレワーク（在宅勤務）の実施に伴う対応

情報システムの保守・運営を担当するベンダ等においても、（1）と同様に、担当者の感染症の罹患やその疑いによる出勤抑制又はテレワーク（在宅勤務）の実施等により、作業場所等に出勤しないという状況が想定される。

そのため、こうした場合であってもシステム運用を継続できるよう、（1）と同様に、連絡体制の構築、連絡手段の確保、テレワーク（在宅勤務）に係る環境面及び制度面の整備、システムの運用継続に携わる要員を確保するための体制等について、検討しておく必要がある。

特に、ベンダにおいては、システムの運用継続に必要となる要員を確保するための体制の検討に当たって、必要な人員及び経験・資格等を所持したバックアップ要員を確保する、交代勤務を考慮したチームを編成する等により、運用継続能力が低下することがないよう留意する必要がある。

なお、（1）と同様に、テレワーク（在宅勤務）に係る環境面の整備に当たっては、テレワークの増加によりアクセスが集中し、回線の帯域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も想定する必要がある。

（3）リモートアクセス環境（遠隔）からの作業実施

感染症の流行等により、作業環境の三密（密閉、密集、密接）や、作業者が共同で利用する機器の汚染による感染リスクが発生することから、現場における作業実施が困難となることが想定される。

そのため、リモートアクセス環境（遠隔）から作業が実施できるよう、テレワークの仕組み等を構築するとともに、現地で手動による対応を実施している作業については、可能な限り当該作業を自動化することも検討が必要である。

なお、（1）・（2）と同様に、テレワークの仕組み等を構築するに当たっては、テレワークの増加によりアクセスが集中し、回線の帯域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も想定する必要がある。

（4）調達が一時的に困難になることを想定した調達計画

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

なることが想定される。

このため、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した調達計画を立てる必要がある。

また、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ことも重要である。（ホストコンピューターやオフィスコンピューター、特殊な仕様で発注した特注品等）

上記（1）～（4）も踏まえ、「さいたま市新型インフルエンザ等対策業務継続計画」の発生段階ごとに対応する、感染症流行時における ICT－BCP 対策例を以下に示す。

新型インフルエンザ等対応業務継続計画		感染症流行時における ICT-BCP 対策例
発生段階	発生段階ごとの対策	
【前段階】 （未発生期）	各課は、業務の取扱いの見直しや、業務継続体制の充実を図り、新型インフルエンザ等流行時に新型インフルエンザ等対策業務継続計画が十分に活用できるよう準備を行う。	・　業務継続方針 S 及び A の業務が依存するシステム（以下「S・A のシステム」という。）を選定する。 ・　S・A のシステムが単独で稼働するもの（他のシステムを必要としないもの）であるか、リモートアクセス環境から作業が実施できるか等を確認する。 ・　S・A のシステムの運用継続に必要となる要員を確保するための体制を検討する。（必要な人員及び経験・資格等を所持したバックアップ要員を確保する、交代勤務を考慮したチームを編成する等）
【第一段階】 （海外発生期）	新型インフルエンザ等の国内発生に備えて、新型インフルエンザ等対策業務継続計画を再度確認し、速やかに業務継続体制へ移行できるよう必要な準備を行う。	・　S・A のシステムについて、運用継続に向けた対策を確認する。 ・　業務継続方針 B、C 及び D の業務が依存するシステム（以下「B・C・D のシステム」という。）を選定する。 ・　すべてのシステムについて、海外製の機器等が無いか等について確認する。
【第二段階】 （国内発生早期（市内未発生期））	新型インフルエンザ等対策業務継続計画が発動された場合には、新型インフルエンザ等対策業務継続計画に基づいて業務体制及び人員体制を移行する。	・　すべてのシステムについて、共同で利用する機器等の消毒、作業実施場所の配置等の見直し、委託元（市）と委託先（ベンダ等）との間の連絡体制（休日・夜間を含む。）の確認・強化を行う。 ・　S・A のシステムについて、リモートアクセス環境から作業するための準備を開始する。
【第三段階】 （市内発生早期（市内感染期））	各課内の職員が最大限協力して業務を実施するとともに、市民生活の維持に最低限必要な業務を継続する。	・　S・A のシステムについて、リモートアクセス環境からの作業を開始する。 ・　感染の状況により、S・A のシステムの構成を変更する。 ・　感染の状況により、B・C・D のシステムを縮減又は休止する。
【第四段階】 （小康期）	流行の終息状況に応じ、次の流行に備えるため、本計画の内容を見直す。	・　感染の状況により、縮減又は休止していた B・C・D のシステムを再開する。 ・　実施した対策の検証及び見直しを行う。

表４－９　「発生段階別のICT-BCP対策等」

5. ICT 復旧体制と役割、個別手順

危機的事象発生時には、正確かつ遅滞なく情報が収集・伝達され、的確な対応の指示がなされる体制が必要である。

意思決定者を中心とし、情報の収集・分析を担う担当者、調査や対策など具体的に行動する担当者などがあらかじめ決められた体制の中で、必要に応じた臨機応変な対応で役割を全うしなければならない。

さいたま市では、危機的事象発生時の ICT 復旧に関する体制とその個々の役割を明確にし、併せてその基本的な行動の基本となる手順書を定めてこれに当たることとする。

実際の危機的事象発生時の対応では、様々な想定外の事象が発生し、あらかじめ定めた体制が整わず、手順書に沿った行動もできない場合が間違いなく発生する。しかし、このような状況においても、あらかじめ定めた体制や行動手順の目的を理解して臨機応変な対応をすることが望まれるため、本項では、危機的事象発生時の対応体制と役割・責任を明確にし、その体制が効率的に機能するための ICT 復旧フロー（全体フロー）と、危機的事象発生時には最も重要な、発災直後の初動を中心とした体制ごとの個別手順を定める。

5.1. 危機的事象発生時の対応体制と役割

危機的事象発生時の ICT 復旧に関する対応体制は、以下のとおりとする。

（1）さいたま市全体及び各セクション単位の ICT 復旧体制

さいたま市の危機的事象発生時における、ICT 復旧対策本部及び各原課の復旧体制は、図５－１「さいたま市 ICT 復旧対策体制（全体図）」のとおりである。

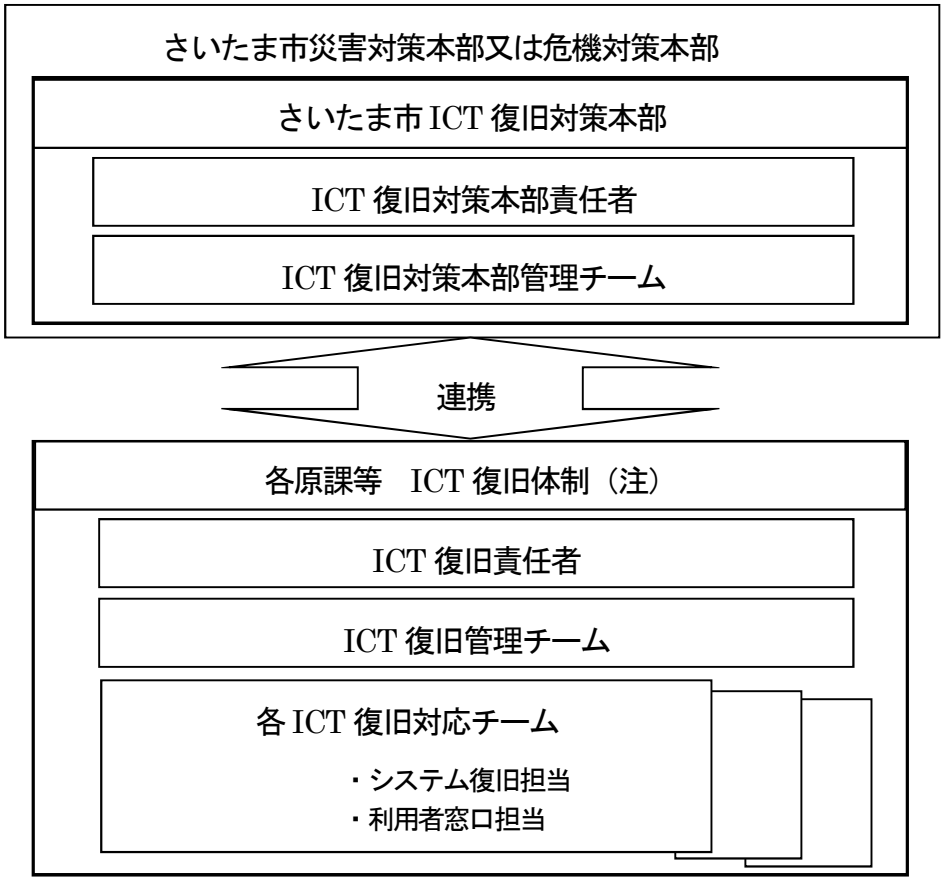

図５－１「さいたま市 ICT 復旧対策体制（全体図）」

（注）各課のICT復旧対応チームは、サーバ等の設置場所やシステムの運用形態により、必要となるタスクが異なる。各課のシステムの運用状況に合わせて必要な復旧担当を割り当てる。例えば、すべてのシステム運用をデジタル改革推進部で実施している場合には、サーバ室、ネットワーク、サーバの復旧は不要となる。
　また、デジタル改革推進部においては、システムごとに担う復旧担当範囲が異なるため、これを正確に把握して必要な対応の実施と各課への情報提供に合わせた復旧作業の継承を行わなければならない。
　デジタル改革推進部は、データセンターに設置されているシステムについてはサーバ及びネットワークの復旧作業をしなければならないが、システム、クライアント等その他の復旧については各システムの運用状況に合わせて必要な作業を担う。

（2）各体制の担当ごとの役割（概要）

担　当		役　割
ICT復旧対策本部	ICT復旧対策本部責任者／代行権限者	・危機的事象発生時における、さいたま市全体のICT継続の総括責任者
	ICT復旧対策本部管理チーム	・各ICT復旧体制の対応状況のとりまとめと横断的な復旧調整を行うチーム
各原課等ICT復旧体制	ICT復旧責任者	・危機的事象発生時における各原課等のICT継続の総括責任者
	ICT復旧管理チーム	・各チーム対応状況のとりまとめと横断的な復旧調整を行うチーム
	ICT復旧対応チーム	・システム重要度に応じた、サーバ／ネットワーク／アプリケーション復旧に向けた対応を行うチーム ・各復旧活動用ＰＣ及び利用者用ＰＣの復旧・調達に向けた対応を行うチーム ・災害発生時におけるシステム利用者からの問い合わせ対応を行うチーム

表５－１「各体制の担当ごとの役割」

なお、各チームの役割と責任の詳細については、各個別手順を参照すること。

5.2. 危機的事象発生時における ICT 復旧フロー

危機的事象発生時における具体的な ICT 復旧フローは、資料④「全体フロー」を参照のこと。

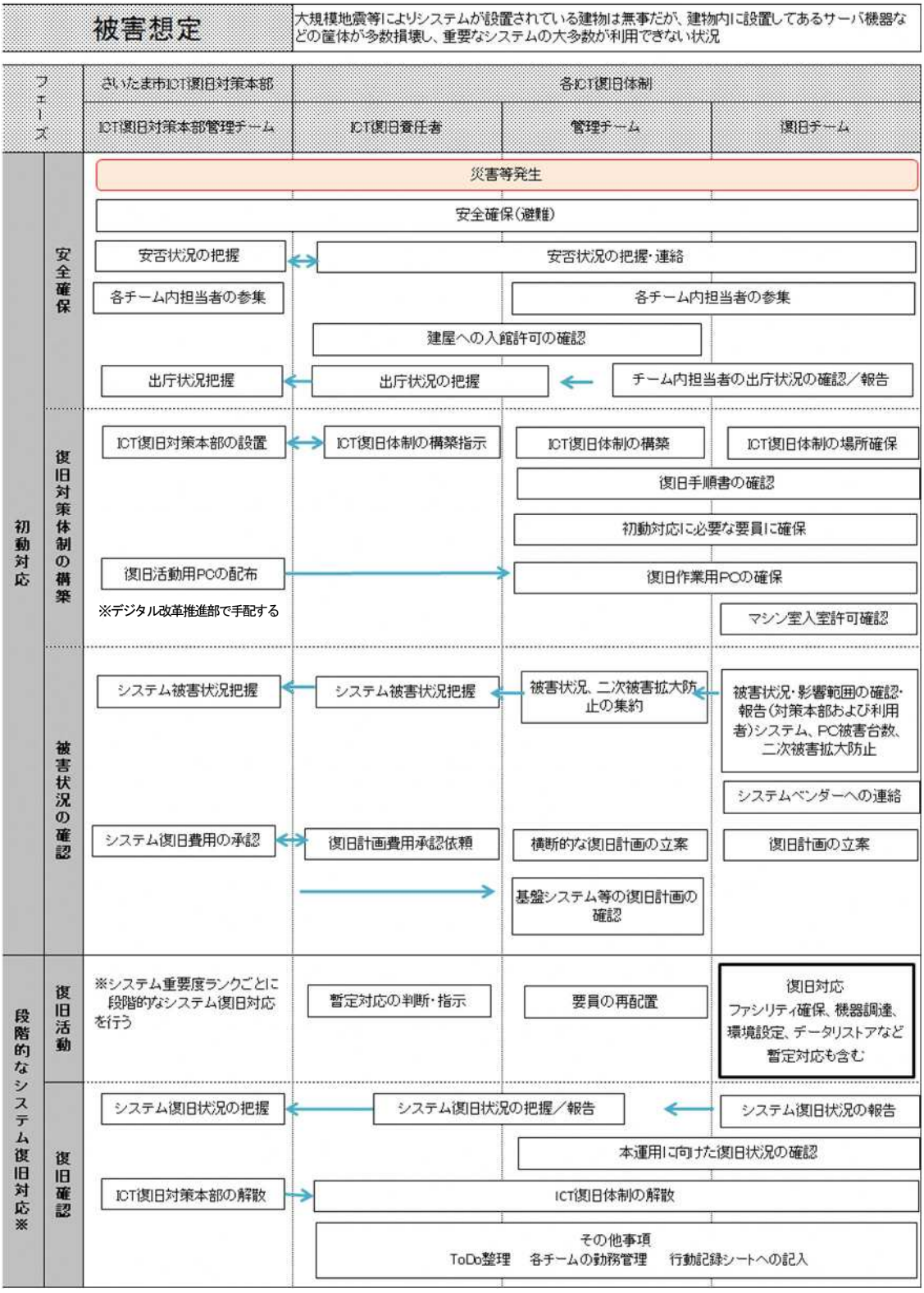

図５－２「緊急事態フロー」

5.3. 危機的事象発生時における初動対応手順

危機的事象発生時における初動対応の具体的な行動計画については、以下の文書で構成されており、その文書に基づき行動する。

（1）全体フロー

前項「危機的事象発生時における ICT 復旧フロー」に記載したフローは、さいたま市全体の ICT 復旧を担う ICT 復旧対策本部と、実際の復旧作業を担う各原課について、復旧体制ごとに設定されるタスクごとの復旧チーム単位で、発災から初動、段階的なシステム復旧対応時における、作業や指揮命令の流れを記載している。

※危機的事象発生時の ICT 復旧の具体的な内容については、資料④「全体フロー」を参照のこと。

（2）個別手順

個別手順は、各チームが危機的事象発生時に行動する際に利用するものである。チームごとに、作業の実施手順、作業の内容、作業を実施する際に参照するドキュメント名、留意事項等が記載されている。

※各体制、チームごとの個別手順については、資料⑤「個別手順書（ICT 復旧対策本部）」及び資料⑥「個別手順書（各原課）」を参照のこと。

（3）様式（各種リスト、記入シート）

個別手順に記載された作業を実施する際に利用する文書であり、その種類は表５－２「様式一覧」のとおりである。

※各種リスト、記入シートの様式については、資料⑦「記入シート様式集」を参照のこと。

※システムの管理形態により、各原課において使用しない様式も存在する。各原課は、必要な様式を選択して作成する。

No.	別紙「記入シート」様式名	作成単位
①	担当者リスト	課で１枚を作成する。
②	ベンダ連絡先リスト	必要に応じて課で１枚を作成する。
③	ネットワーク被害／復旧確認シート	ネットワークの管理及び被害／復旧確認を担う部署が、課で１枚を作成する。
④	サーバ室被害拡大防止策一覧	サーバ室の管理及び被害拡大防止策を担う部署が、課で１枚を作成する。
⑤	サーバ・アプリ被害／復旧確認シート	サーバ・アプリを管理する部署が、課で１枚を作成する。システムごとに作成することも可能。
⑥	クライアントPC被害／復旧確認シート	システム運用に必要な端末を管理する部署が、課で１枚を作成する。
⑦	サーバ室被害／復旧確認シート	サーバ室被害／復旧確認を担う部署が、課で１枚を作成する。
⑧	システム被害状況&復旧進捗一覧表	サーバ・アプリを管理する部署が、課で１枚を作成する。
⑨	ICTの被害・復旧状況レポート	課で１枚、使用できるよう準備する。
⑩	利用者連絡先リスト	課で１枚を作成する。
⑪	問い合わせ・回答管理台帳	課で１枚、使用できるよう準備する。
⑫	行動記録シート	課で１枚、使用できるよう準備する。

表５－２「様式一覧」

6. ICT-BCP 継続マネジメント（ICT-BCM）

本計画にて策定したICT-BCPの実効性を担保するためには、ICT-BCP基本計画書に記載された対策を計画的に実施することはもちろんであるが、常にICT-BCPドキュメントを最新化し、また職員のICT-BCPへの習熟度を高めておくことが非常に重要である。

これをICT-BCP継続マネジメント（ICT-BCM）として位置づけ、PDCAサイクルを回し情報システムにおける業務継続性の向上を高めていくマネジメントを実行していく。

具体的な実施手順等は、年度ごとに「ICT-BCM推進計画書」に定めるものとする。

6.1. 実施方針

6.1.1. ドキュメント管理

ICT-BCP基本計画書及びICT-BCP実行計画書（ひな形）を始めとする各資料の最新化や、訓練等のフィードバックに基づく見直しを実施する。また、各システム所管課で作成するICT-BCP実行計画書について、新規システム導入時又は既存システム更改時において策定又は改定を実施する。

6.1.2. 教育・訓練の実施

ICT-BCPへの習熟度を高め、より高い業務継続性を担保するための教育・訓練を適宜実施する。

実施については、図６－１「習熟度に応じたICTの訓練手法」のとおり、段階的に訓練を高度化し実施することを目指す。

それぞれの訓練手法の説明は表６－１「ICTの訓練手法と特徴」を参照のこと。

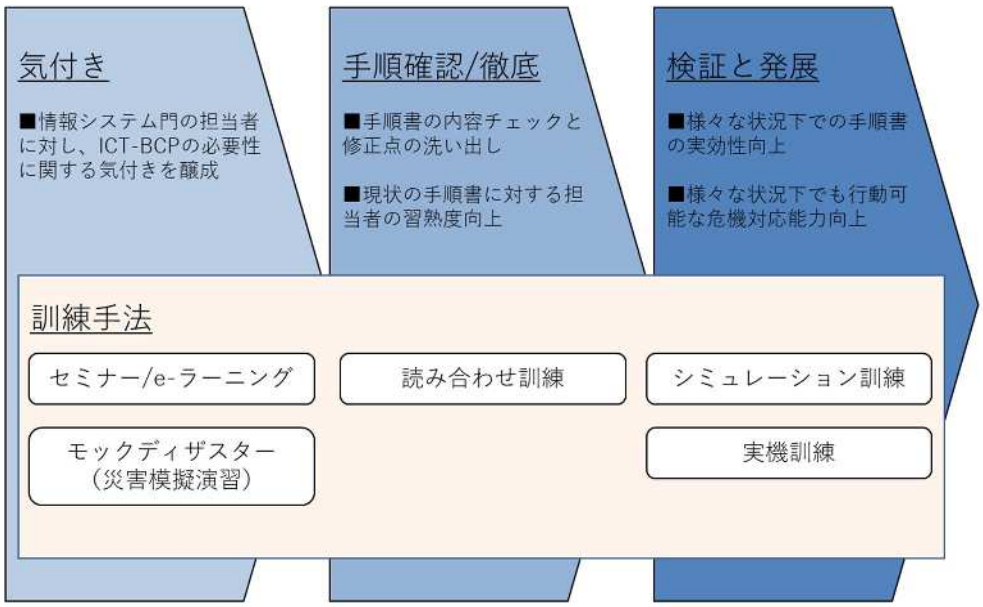

図６－１「習熟度に応じたICTの訓練手法」

訓練手法	訓練の特徴	対象範囲	
		部門全体	個別ｼｽﾃﾑ
セミナー／ ｅラーニング	・一定の人数に対し、精度の高い情報を伝えることができる。 ・一度作成した教材の流用が容易である。	○	
モックディザスター （災害模擬演習）	・効率的にICT-BCPや災害発生に対する備えの必要性に関する気づきを与えることができる。	○	
読み合わせ訓練	・担当者が被災状況を想定し読み合わせを行うことで、手順書の課題や、事前に必要な対策の抽出を行うことができる。 ・担当者それぞれが手順書について習熟することができる。	○	○
シミュレーション訓練	・サーバの被害状況や要員参集状況などの状況を与え、ワークシートなどを活用しながら実働することで、様々な状況に応じた手順書の課題や、事前に必要な対策を抽出することができる。 ・様々な状況の下でも対応できる担当者の危機対応能力を育成することができる。	○	
実機訓練	・実機を用いた具体的な手順を確認することができ、手順書の有効性を確認することができる。 ・事前対策の不備や、あらかじめ定めた目標復旧時間を満たしているのか確認することができる		○

表６－１「ICTの訓練手法と特徴」

さいたま市

ICT-BCP 基本計画書