小平市　ＩＣＴ業務継続計画

管理文書番号 ： P01

初版作成日 平成27年3月31日

最終更新日 令和5年3月３１日

文　書　版 ： 1.2

目次

本文中に「*」が付されている語句は、巻末に用語説明が掲載されています。

第１章　本計画の位置づけ

1　業務継続の必要性

大規模な震災が発生した際、市は、災害応急対策活動及び災害からの復旧・復興活動の主体として重要な役割を担うことに加え、災害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有している。これらの災害対応業務や市民生活等に必要な通常業務が的確に行われない場合、震災による被害が拡大するとともに、市民生活等に支障が生じるリスクが高まる。

また、過去の震災では、業務継続に支障を及ぼす庁舎の被災や停電等の事例も見受けられるところであり、首都直下地震等の発生時には市自身も被災し、職員、物資、ライフライン等に制約を受ける可能性が高い。

このように業務遂行能力が低下した状況下においても、市として、必要な業務資源を確保し、災害応急・復旧業務を実施しつつ、発災時においても中断することのできない通常業務については、一定水準を確保する必要がある。

また、現在、市の業務遂行においては、その多くをＩＣＴ*に依存している。このため、震災等の大規模災害のみならず、非災害時（セキュリティインシデント*を含む）においても、ＩＣＴの維持に必要な資源の準備や復旧時の対応について、対策を整備することは重要かつ喫緊の課題であると言える。

2　計画策定の目的及びＩＣＴ業務継続方針

前述の必要性を踏まえ、本市における「ＩＣＴ業務継続計画（以下、「本計画」という。）は、災害時はもとより非災害時においても、本市の業務継続に必要なＩＣＴを速やかに復旧させることを目的として　①震災等の大規模発生時に優先的に取り組むべき重要な業務（非常時優先業務）を実施するにあたり必要となる優先システムを事前に定めること　②優先システムの継続に必要な資源（職員、庁舎、電力等のインフラ、システムを構成するハードウェア、ソフトウェア、データ及び通信等）の準備や欠落した際の対応方針・手段を定めるものとする。さらに、本計画は組織改正や情報システムの更改など、都度発生する変化に柔軟な対応が必要となるため、業務継続能力の持続的な向上を図るマネジメントの仕組みの構築も合わせて整備するものである。

3　対象範囲

(1)　対象となる情報システム

本市が管理する情報システムの中から、災害時、非災害時において優先的に実施すべき業

務である「優先業務」に必要不可欠な情報システムを「優先システム」として定義し、本計画の管理対象とする。

(2)　対象となる拠点

優先システムを利用する主管課の拠点すべてを対象とする。主管課と利用する優先システム及び拠点の関係は、「優先システム一覧（C02）」を参照のこと。なお拠点とは各主管課が災害対応業務にあたる場所及び優先システム設置場所を表す。

4　本計画と他の計画との関係

本計画は、災害時、非災害時を想定しているが、本市ではこれらに対して「地域防災計画」「業務継続計画（震災編、新型インフルエンザ等編）」「情報セキュリティポリシー*」等を策定して、全庁的な方針や対応手段を示している。本計画は、「ＩＣＴ」を継続するために特化された計画として、これらの計画との整合性を図り、相互に運用を行うことでそれぞれを補完し合い、効果を最大化する。以下に本計画と関連する計画を示す。

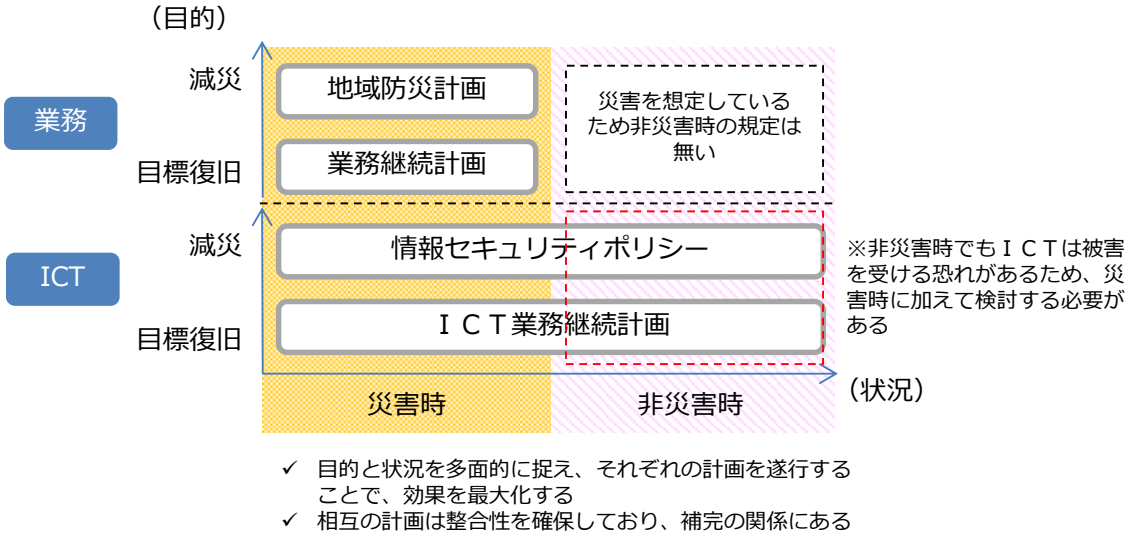

図 1　本計画と他計画の関係

表 1　本市における各計画の所掌範囲

	地域防災計画	業務継続計画（震災編、新型インフルエンザ等編）	情報セキュリティポリシー	ＩＣＴ業務継続計画
計画の目的	地方公共団体が発災時または事前に実施すべき災害対策に係る実施事項や役割分	発災時の限られた必要資源により、非常時優先業務を目標とする時間までに実施可	市が保有する情報資産を漏えい、事故、災害その他の脅威から組織的かつ継続的に	災害時等に実施すべき優先業務を行うために必要となるＩＣＴを喪失しないよう

	担等を規定するための計画である。	能にするための計画である。	保護するための対策について基本的な考え方を定義した計画である。	にする、あるいは喪失したＩＣＴを目標とする時間までに復旧可能とするための計画である。
想定する状況	災害時	災害時	災害時、非災害時	災害時、非災害時
KPI*	死傷者数、ライフラインの復旧率など	業務の目標復旧時間	セキュリティ事故件数	ＩＣＴの目標復旧時間

5　各計画との整合性確保に関する留意事項

本計画は、各計画との整合性を確保するため、関係する他計画にあわせて見直しを行う。また上記表のとおり、本計画はＩＣＴの目標復旧に関係する範囲を扱い、それ以外の領域については、各計画で対応を行う。

6　計画の文書体系

ＩＣＴは情報システムの更新をはじめとして、法制度改正や新規導入など、様々な要因によって構成の変更などが起こりうる。そのため、実効性を確保したＩＣＴ業務継続計画とするためには、経年の更新・管理体制の確立及び発動が非常に重要となり、管理が容易となるような計画の体系とすることが求められる。

本市では、各計画に関係する文書体系を本計画の PDCA サイクル*に基づき体系化することとし、以下に示す文書で構成される。

① ＩＣＴ業務継続に係る基本的な考え方となる「ＩＣＴ業務継続計画（本書）」【PLAN】

本市における業務継続の考え方、被害想定等の前提条件、対象となる優先システム等を定義する。また計画運用にあたっての年間スケジュールや教育訓練及び本計画を継続的に維持・管理するための手順、管理手法等を定義する。

② 職員の BCP 発動時における基本行動を定義した「行動計画書」【DO】

脅威が発生した段階からの行動手順「誰が、何を、いつ、どこで、なぜ、どのように」を明確に示し、システム復旧に向けた具体的な行動手順を定義する。

③ 規定した計画の運用、改善、見直しを定義した「運用手順書」【CHECK, ACT】

本計画の見直しに関する基本方針と作業手順を定義する。分析作業、対策案の立案から対策実施案策定等の手順を規定する。

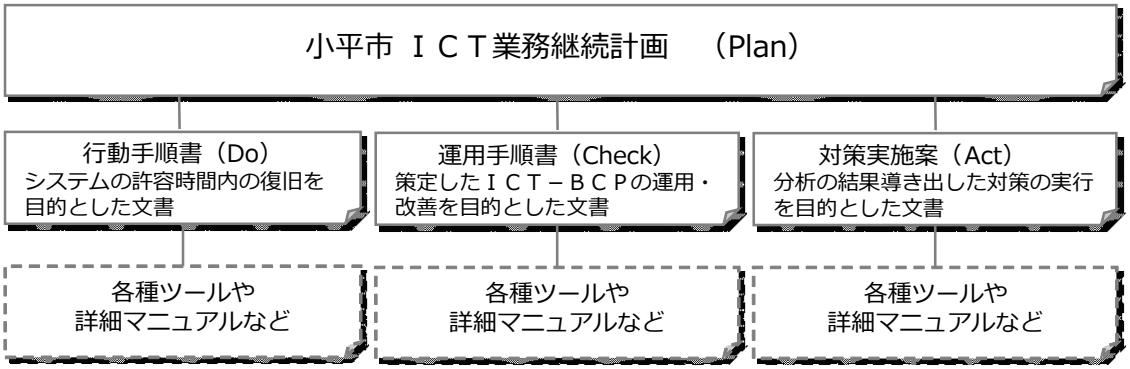

図 2　文書体系一覧

表 2　ICT 業務継続計画管理文書一覧

管理番号		文書名
分類	連番	
P	【Plan】 ICT に係る業務継続計画全体の考え方・方針を規定した文書	
P	01	小平市 ICT 業務継続計画
P	02	想定脅威シナリオ（災害時編）
P	02	想定脅威シナリオ（非災害時編_システム障害）
P	02	想定脅威シナリオ（非災害時編_サイバー攻撃）
P	02	想定脅威シナリオ（非災害時編_停電）
P	03	ICT 業務継続計画管理文書一覧
D	【Do】 実際に脅威が発生した際の行動手順を規定した文書	
D	01	行動手順書（災害時編）
D	02	行動手順書（非災害時編_システム障害）
D	03	行動手順書（非災害時編_サイバー攻撃）
D	04	行動手順書（非災害時編_停電）
C	【Check】ICT 業務継続計画の運用・改善活動の具体的な手順を規定した文書	
C	01	小平市 ICT 業務継続計画運用手順書
C	02	優先システム一覧
C	03	システム一覧及び関連機器等

管理番号		文書名
分類	連番	
C	04	システム現状想定復旧時間調査票
C	05	フィット＆ギャップ分析シート
C	06	リソース毎の対策案一覧（災害時）
C	07	リソース毎の対策案一覧（非災害時）
C	08	対策実施案
C	09	内部及び外部環境分析シート
C	10	マネジメントレビューシート

第２章　想定脅威

1　災害時における想定脅威の考え方

(1)　災害時における脅威の種類

本計画で想定脅威とする災害の種類については、内閣府中央防災会議策定の防災基本計画の考え方に基づくものとする。災害は、「自然災害」と「事故災害」の２種類とし、「自然災害」は震災・津波・風水害・火山災害・雪害、「事故災害」は海上災害・航空災害・鉄道災害・道路災害・原子力災害・危険物等災害・大規模火事災害・林野火災を対象と定義した。

表 3　災害時における脅威の種類

分類	脅威の種類
自然災害	震災・津波・風水害・火山災害・雪害
事故災害	海上災害・航空災害・鉄道災害・道路災害・原子力災害・危険物等災害・大規模火事災害・林野火災

出典：内閣府中央防災会議　防災基本計画

(2)　本計画における災害時の想定脅威

本計画と関連する「地域防災計画」及び「業務継続計画（震災編）」では、多摩東部直下地震・立川断層帯地震を想定脅威としていることから、本計画における災害時の想定脅威は「震災」を想定脅威とする。

なお、新型コロナウイルス感染症を含む感染症が発生、拡大している際は、市民の感染症対応及び職員自身の感染により、要員のリソースが十分に確保できない事態も想定される。

2　非災害時における想定脅威の考え方

(1)　非災害における脅威の種類

本書における“非災害時”とは、「市民は通常の生活を営んでいる状態」であり、ある脅威が発生することにより、市が管理するＩＣＴに何らかの不具合が発生し、業務の継続が困難になるという状況を想定する。このような状況に陥れる脅威は、「外的要因」「内的要因」の２つに大きく分類され、システム障害やセキュリティ事故等が該当する。日々の業務の実施にあたり、大部分をＩＣＴに依存している中で、これらの脅威は業務継続に大きな影響を与えるばかりか、自然災害以上に発生確率の高い脅威である。本計画では情報システムにおける最大の脅威である「セキュリティインシデント」に重点をおきながら非災害時の想定脅威を

定義する。

「セキュリティインシデント」とは、一般的に「情報セキュリティに関する事故・事象」のことであり、広義には文書の紛失、情報漏洩及び電子メール送信ミス等のシステムに直接的な被害が発生しない事象も含まれる。本計画では、システムが停止した際の対応を目的としているため、本計画におけるセキュリティインシデントは、「システムやデータ等、ＩＣＴを構成する要素に直接的な被害を与える事象」と定義し、非災害時における脅威の対象とする。

表 4　非災害時における脅威（セキュリティインシデント）の種類

分類	脅威の種類
内的要因	オペレーションミス、システムバグ、システム関連機器の経年劣化
外的要因	システム管理機器の物理的破壊、システム関連機器の物理的盗難、停電、コンピュータウィルス、システムクラック（不正アクセス）

(2)　本計画における非災害時の想定脅威

非災害時の想定脅威の抽出は、ＩＣＴを構成する資源への被害有無や各セキュリティインシデントの特性、復旧手順の違い等を踏まえて検討した。表 4 に示す脅威についてＩＣＴを構成する資源への被害範囲等を整理すると、以下のようになる。

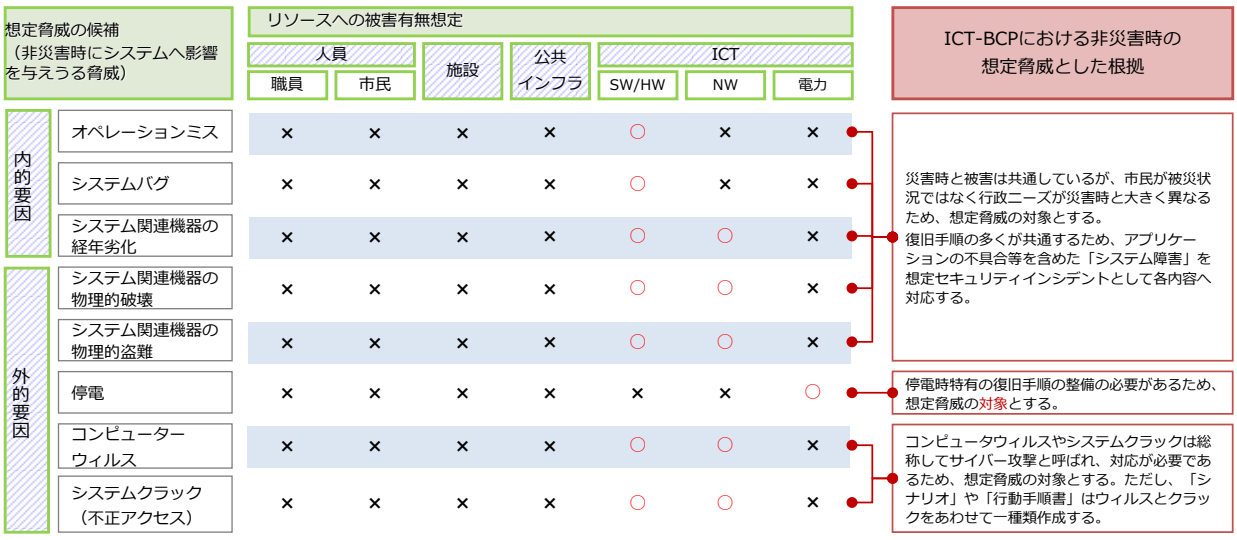

図 3　ICT に影響を与えうる脅威の一覧

上記のとおり、それぞれの脅威はＩＣＴを構成する各リソースに対する影響度合いによっ

て、３つに類型化することができる。よって、次に示すセキュリティインシデントを想定脅威とし、本計画の対象とする。

①　システム障害

「オペレーションミス」、「システムバグ」、「システム関連機器の経年劣化」、「システム関連機器の物理的破壊」、「システム関連機器の物理的盗難」については、被害の範囲が概ね共通しており、システムを復旧する際の手順も概ね共通することから、これらをまとめて「システム障害」として脅威設定する。

②　停電

「停電」は、他のセキュリティインシデントと異なり、ソフトウェアやハードウェアではなく、電力に直接的な被害が発生する。また、電力の復旧や計画停電等を想定したシステムの安全な停止手順等を整備する必要があることから、「停電」として脅威設定する。

③　コンピュータウィルス等によるサイバー攻撃

「コンピュータウィルス」、「システムクラック（不正アクセス）」は、「システム障害」と被害の範囲は共通するものの、“被害が拡大する”特性を持つものであり、被害の拡大を防止するための特有の復旧手順を整備する必要がある。このため、「システム障害」とは別に「サイバー攻撃」を想定脅威とする。

３　各脅威の想定被害

(1)　震災

震災の想定被害は「小平市業務継続計画（震災編）」（令和４年７月修正）に基づき設定する。

＜被害想定＞

①　多摩東部直下地震　震度６強

②　立川断層帯地震　震度６強

いずれも冬季平日 18 時発生、風速８m/秒（想定被害が最大となる設定）

表 5　設定した被害想定の詳細

【人的被害、建物被害等想定（冬の１８時発生、風速８mの場合)】

		多摩東部直下地震	立川断層帯地震
建物全・半壊		3,917 棟	3,767 棟
焼失建物		1,855 棟	1,288 棟
死者		84 人	70 人
負傷者		1,169 人	1,011 人
避難者数		29,054 人	23,301 人
	避難所避難者数（4～1 週間後）	19,369 人	15,534 人
帰宅困難者数		21,347 人	21,347 人
エレベーター閉じ込め		36 台	32 台
要配慮者死者数		55 人	46 人
自力脱出困難者		341 人	314 人
震災廃棄物		31 万 t	28 万 t

【ライフライン被害想定】

		多摩東部直下地震	立川断層帯地震	復旧日数（想定）
電力	停電率	8.0%	7.4%	2 日後～1 週間以内 ※延焼による停電除く。
通信	固定電話不通率	4.1%	3.0%	2 日後～1 週間以内
ガス	低圧ガス供給停止率	59.2%	26.9%	約 6 週間以内
上水道	断水率	16.6%	14.1%	4 日後～1 か月以内
下水道	管きょ被害率	3.6%	2.9%	1 週間後～1 か月以内

＜被害の特徴＞

○ 火気器具利用が最も多いと考えられる時間帯で、これらを原因とする出火数が最も多くなるケースである。

○ オフィスや駅では、帰宅等のため人が滞留する。

○ ビル、ブロック塀の倒壊や落下物等により被災する危険性が高い。

○ 鉄道、道路もほぼラッシュ時に近い状況で人的被害や交通機能支障による影響拡大の危険性が高い。

○ 一部職員は既に退庁しており、要員の十分なリソースが確保出来ない状態が想定される。

(2)　非災害時

① システム障害の被害想定

情報システムの正常な動作や内容を脅かす事象（平日業務時間帯に、業務アプリケーションの不具合によりシステムの挙動が不安定またはデータの破損）が発生する。

システム障害は、市が構築しているシステムの他、クラウドサービス事業者側の障害により、被害を受けることも想定される。

② 停電の被害想定

情報システム等の正常な動作や内容を脅かす事象（平日業務時間帯に、東京電力からの電力供給停止や市役所内部の電気設備の故障）が発生する。

③ サイバー攻撃の被害想定

情報システム等の正常な動作や内容を脅かす事象（平日業務時間帯に、インターネット環境からセキュリティホール*を攻撃）が発生する。

サイバー攻撃は、更新プログラムが最新でなく脆弱性を狙われること、Ｗｅｂ会議利用時に機密性の高い情報が盗聴されて攻撃に利用されること、ホームページの DDoS 攻撃等により、被害を受けることも想定される。

第３章　脅威発生時の対応

1　脅威発生時の体制図

本計画は、企画政策部情報政策課が中心となり掌握し、管理を実行する。常時の体制を定義し、このうち、脅威発生時はそれぞれ災害時と非災害時の体制を定義する。（本計画の維持・管理等運用に関する体制については、第８章　運用管理規定を参照のこと。）

	企画政策部系				その他部署			
	常時(脅威発生時も含む)	脅威発生			常時(脅威発生時も含む)	脅威発生		
		CSIRT体制	非災害時	災害時		CSIRT体制	非災害時	災害時
市長	-	-	-	-	-	-	-	災害対策本部長（市長）
副市長	-	-	-	-	最高情報セキュリティ責任者（CISO）	-	-	災害対策副本部長（副市長、教育長）
部長	統括情報セキュリティ責任者	CSIRT責任者	CSIRT責任者	災対企画政策部長	情報セキュリティ責任者	CSIRT副責任者	CSIRT副責任者	ICT業務継続計画責任者
				統括ICT業務継続計画責任者				
課長	統括情報セキュリティ管理者	CSIRT管理者	CSIRT管理者	災対企画政策部情報システム班長	情報セキュリティ管理者	インシデント対応管理者	インシデント対応管理者	ICT業務継続計画管理者
				統括ICT業務継続計画管理者	情報システム管理者			
係長	情報政策課職員	インシデントハンドラー	インシデントハンドラー	-	情報システム担当者	インシデントハンドラー	インシデントハンドラー	-
主事・主任	情報政策課職員	インシデント対応要員	インシデント対応要員	-	情報システム担当者	インシデント対応要員	インシデント対応要員	-

※赤枠部分がこの後に定義する災害時及び非災害時に定義する体制の要員名

図 ４　常時(脅威発生時も含む)体制

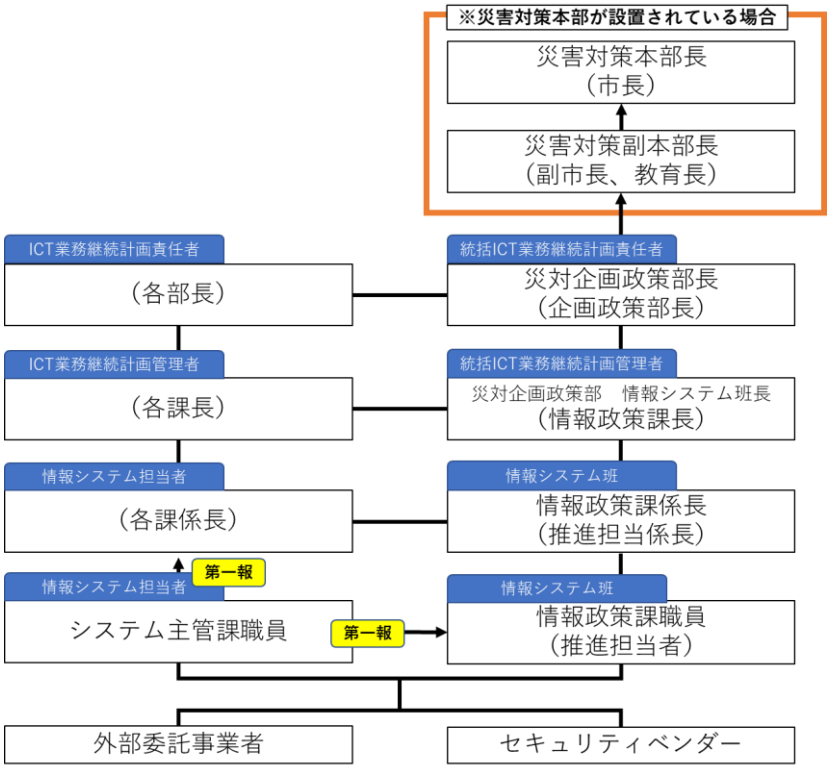

図 5　脅威発生時（本計画発動時）の体制（災害時）

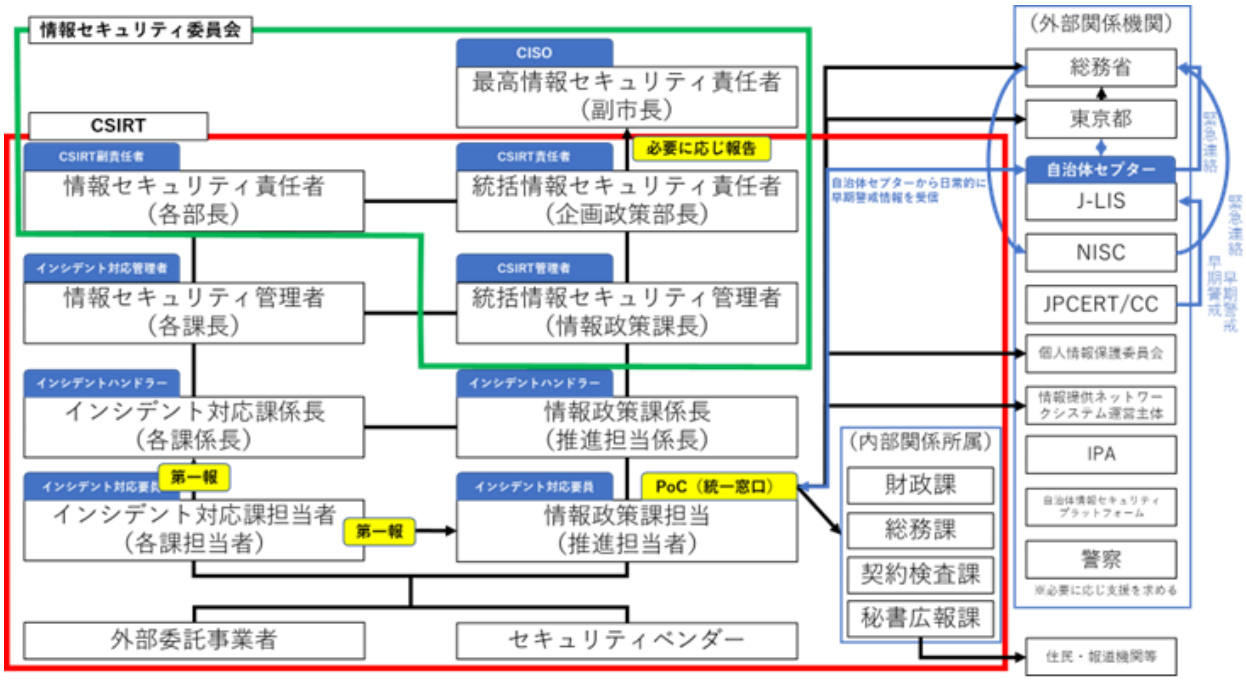

図 6　脅威発生時（本計画発動時）の体制（非災害時）

2　各要員の役割

体制図で示した各要員の役割を以下に示す。

表 6　災害時における各要員の役割

災害時における役割	
要員（＝役職）	役割
・災害対策本部長 （＝市長）	（災害対策本部が設置されている場合のみ） 本部の事務を総括し、本部の職員を指揮監督する。本計画における情報システムの状況を報告した上で、復旧に関する対応の最終判断を行う。
・災害対策副本部長 （＝副市長、教育長）	（災害対策本部が設置されている場合のみ） 災害対策本部長が何らかの要員により不在の場合、代理で本部の職員を指揮監督するとともに、情報システムの復旧に関する対応の最終判断を行う。
・災対企画政策部長 ・統括 ICT 業務継続計画責任者 （＝企画政策部長）	災害時において優先システムに重大な被害が発生した際の対応事項を審議・決定する。
・災対企画政策部　情報システム班長 ・統括 ICT 業務継続計画管理者 （＝情報政策課長）	電子計算組織の保守及び復旧に関すること、各種情報の処理に関することを掌握するとともに、災害発生時における本計画の統括・遂行責任者であり、ＩＣＴ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を行う。 ・ＩＣＴ復旧に係る対応や方法の意思決定 ・災害対策本部への状況報告と全部門への伝達 ・他主管課との調整の総括、支援依頼等
・情報政策課職員	ＩＣＴ被害状況の確認、報告及び復旧にむけた調整及び復旧作業等、ＩＣＴ復旧活動全般の主体となり作業を行う。
・ICT 業務継続計画責任者 （＝各部の部長相当職）	自身の部が管轄する優先システムの状況を適宜把握し、情報システム班と連携しながらＩＣＴの業務継続に関わる活動を承認する。
・ICT 業務継続計画管理者 （＝各課の課長相当職）	自身の課が管轄する優先システムの状況を適宜把握し、ICT 業務継続計画責任者、情報システム班と連携しながらＩＣＴの業務継続に関わる作業を管理する。
・情報システム担当者 （＝システム主管課職員）	情報システム班（情報政策課職員）と連携し、委託事業者との連絡・調整、システム復旧に必要な資源の調達の支援、復旧後のシステムの動作確認等を行う。
・委託事業者	情報政策課職員及び情報システム担当者の指示に基づきＩＣＴ復旧にむけた作業等を行う。

表 7　非災害時における各要員の役割

非災害時における役割	
要員（＝役職）	役割
・CSIRT 責任者 （＝企画政策部長）	インシデント対応の責任者。インシデント対応の作業を監督し評価する責任を負う。 セキュリティインシデント発生時において優先システムに重大な被害が発生した際の対応事項を審議・決定する。 また、CISO やほかの組織などとの調整役となり、危機を打開し、チームに必要な要員・リソース・技能を確保する。
・CSIRT 管理者 （＝情報政策課長）	電子計算組織の保守及び復旧に関すること、各種情報の処理に関することを掌握するとともに、セキュリティインシデント発生時における本計画の統括・遂行責任者であり、ＩＣＴ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を行う。 ・　ＩＣＴ復旧に係る対応や方法の整理及び意思決定 ・　CSIRT 責任者への状況報告と全部門への伝達 ・　必要な要員・技能等の確保 ・　PoC、CSIRT チーム、他主管課、及び他の組織等との調整の総括、支援依頼等
・PoC（Point of Contact、ポック） （＝情報政策課職員）	インシデントについて庁内外の者からの連絡受付の役割を担う、情報セキュリティに関する統一的な窓口 ＩＣＴ障害状況の確認、報告及び復旧にむけた調整及び復旧作業等、ＩＣＴ復旧活動全般の主体となり作業を行う。
・CSIRT 副責任者 （＝各部の部長相当職）	優先システムでインシデントが発生した時に所管する部長が対応する。 自身の部が管轄する優先システムの状況を適宜把握し、情報政策課と連携しながらＩＣＴの業務継続に関わる活動を承認する。
・インシデント対応管理者 ・情報システム管理者 ・情報セキュリティ管理者 （＝各課の課長相当職） ※各課所管インシデント時のみ設置	チームのリーダー。インシデントハンドラーの作業を調整し、インシデントハンドラーからの情報を収集し、インシデントに関する最新情報を必要な関係者に提供する。また、高い技術的な技能とインシデント対応経験を持ち、インシデント対応チーム全体の技術的な作業品質を監督して、その品質に最終的な責任を持つ。 自身の課が管轄する優先システムの状況を適宜把握し、CRSIT 副責任者、情報政策課と連携しながらＩＣＴの業務継続に関わる作業を管理する。

非災害時における役割		
要員（＝役職）		役割
・情報システム担当者（＝システム主管課職員）	・インシデントハンドラー（＝インシデント対象課の担当係長）	インシデント発生時の、インシデント分析及び対処法の検討、情報政策課職員等と連携し、各課で整備した関係者の連絡先を基に委託事業者との連絡・調整システム復旧に必要な資源の調達の支援、復旧後のシステムの動作確認等を行う等、インシデントに対応する CSIRT を、実務的な観点から中核として支え、対応方針を検討し、インシデントハンドリング全体に係るプロジェクトマネジメント等を行う。
	・インシデント対応要員（＝システム主管課職員）	インシデントハンドラーを補助し、ともにインシデントハンドリングに当たる。
・委託事業者		情報政策課職員及び情報システム担当者の指示に基づきＩＣＴ復旧にむけた検査・分析、証拠の取得・保全・確保・記録、インシデントの封じ込めと根絶、復旧措置、再発防止策の検討等に係る一部作業等を行う。

※セキュリティインシデント以外の非災害時の対応も、これに準じた体制とする。

第４章　優先業務

1　優先業務の定義

優先業務とは、業務を行う上で必要となる資源（職員などの要員、施設や設備、ＩＣＴなど）が何らかの要因で欠落または不足した状況においても、地方公共団体の責務において実施すべき業務と定義する。

2　非常時優先業務

(1)　非常時優先業務の定義

上記のうち、災害時における優先業務を「非常時優先業務」と定義する。非常時優先業務とは、応急対策業務、復旧復興業務（優先度が高いもののみ）といった地域防災計画で定義される業務と、行政機能そのものを回復させるための応急復旧・復興業務や災害時に優先度の高い通常業務を包括したものである。これらは単に重要な業務か否かではなく、市民の生命、生活等に及ぼす影響の大きさを評価基準として、災害発生後の限られた資源の中にあっても、他の業務に優先して継続、早期復旧を図る必要のある緊急性の高い業務のことをいう。非常時優先業務の詳細を以下に示す。

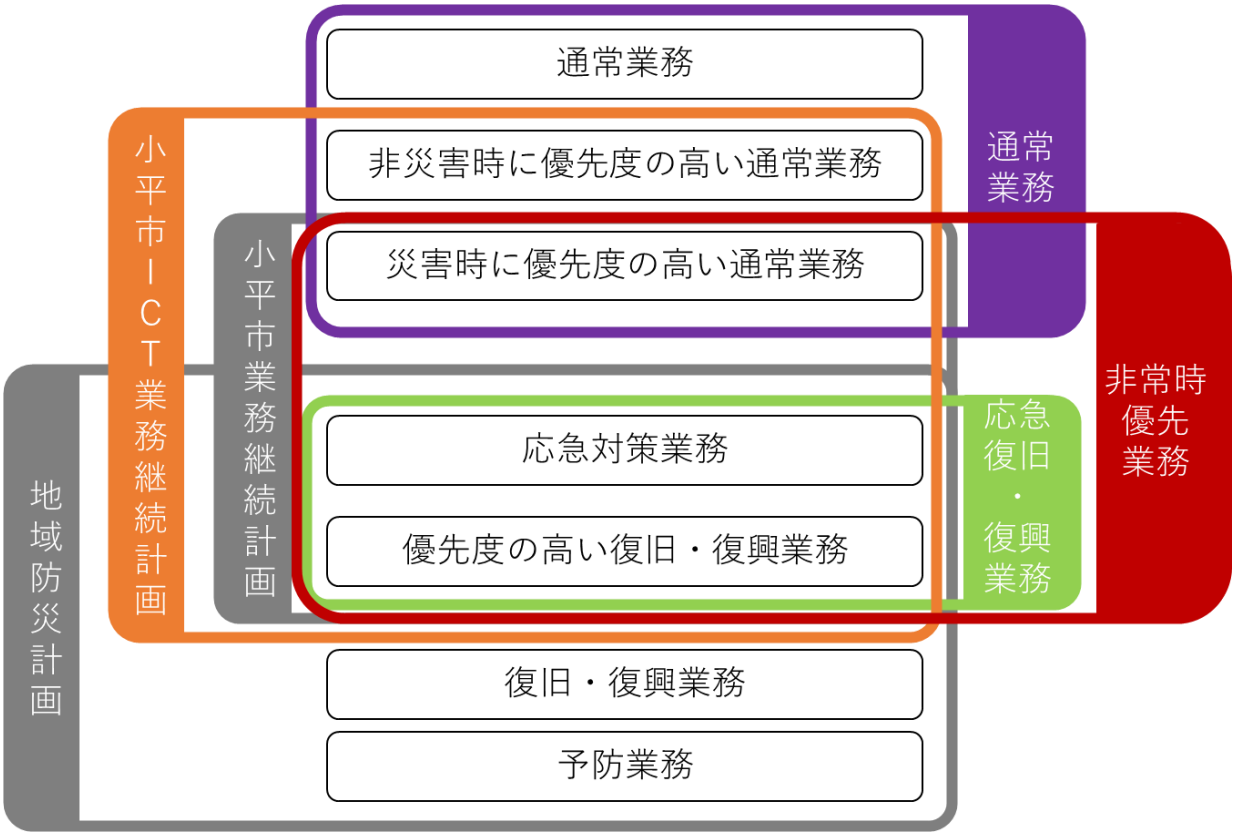

図 7　非常時優先業務の考え方

(2)　非常時優先業務の選定

本市における業務継続計画（震災編）の見直しと合わせ、令和４年度までの組織改正を加味した上で、主に業務継続計画（震災編）に規定された応急復旧・復興及び通常業務に基づき非常時優先業務を選定した。非常時優先業務となる条件は、以下のとおりである。

○　「地域防災計画」に規定された「応急復旧・復興業務」のうち、発災後、業務開始目標時間が１週間以内の業務
○　「小平市業務継続計画（震災編）」に規定された「災害時に優先度の高い通常業務」のうち、発災後、業務開始目標時間が１週間以内の業務
○　その他特筆すべき業務

東日本大震災の事例を見ても、発災後１週間の初動が市民の生命、生活等に直接的な影響を及ぼす可能性が非常に大きいことから、発災後１週間以内に実施すべき業務を非常時優先業務として選定した。

3　非災害時優先業務

(1)　非災害時優先業務の定義

非災害時の優先業務とは、非常時優先業務における「災害時に優先度の高い通常業務[1]」に加え、市民の生命、財産及び信義則に従い、一時的にでも停止することが困難な業務を包括したものである。非災害時においては、「システム障害」や「停電」等のセキュリティインシデントの発生により市の業務が継続できない状況を想定するが、市民は通常の生活を営んでおり、市民への被害は発生していないことに留意した。

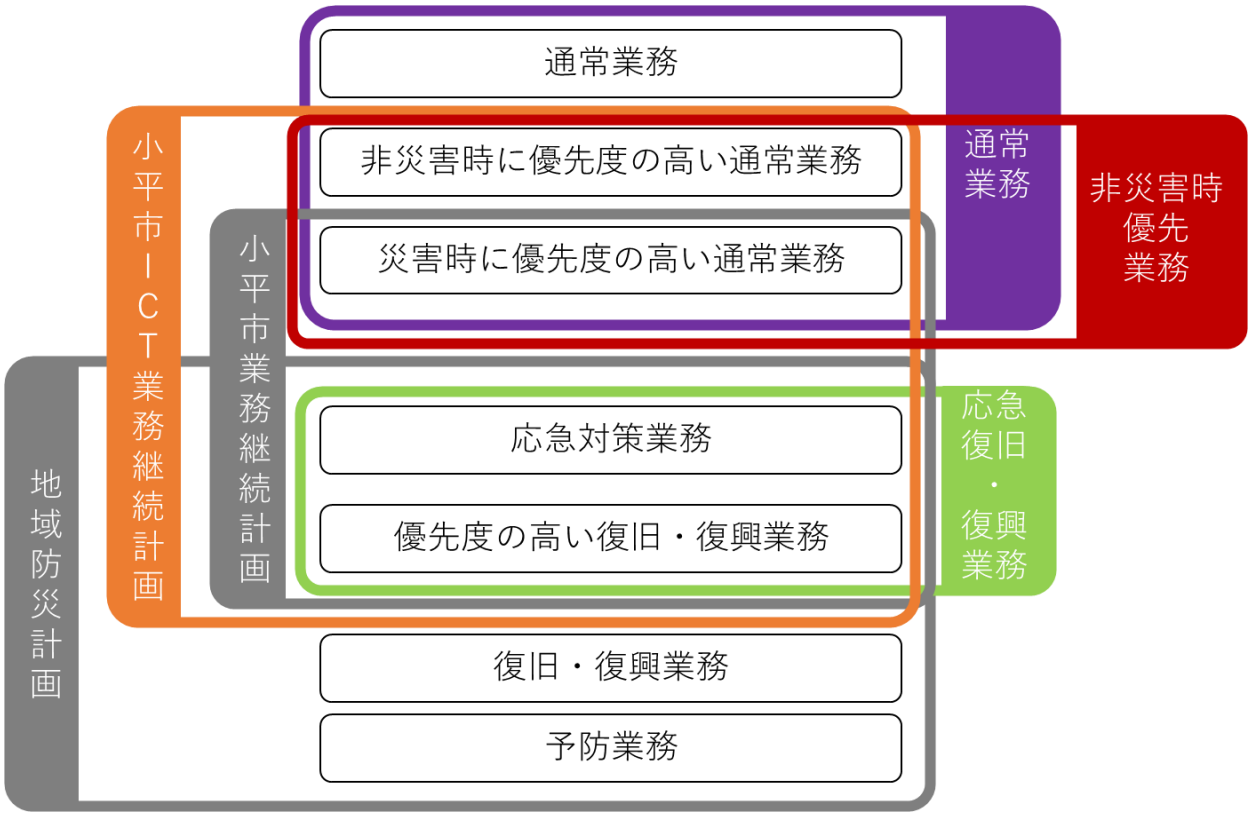

図 8　非災害時優先業務の考え方

(2)　非災害時優先業務の選定

業務を実施するために必要となる資源に何らかの不具合が発生したケースを想定して、そのような状況下でも継続すべき業務について整理を行った。非災害時優先業務となる条件は、以下のとおりである。

---

[1] 災害時に実施すべき通常業務は、当然非災害時においても優先度の高い業務となる。

○　「小平市業務継続計画（震災編）」に規定された「災害時に優先度の高い通常業務」のうち、発災後、業務開始目標時間が 24 時間以内の業務

○　「非災害時に優先度の高い通常業務」と判断した業務のうち、発災後、業務開始目標時間が 24 時間以内の業務

○　その他特筆すべき業務

非災害時は職員であれば代替職員、ＩＣＴであれば運用保守事業者の復旧対応が可能である。また「社会（市民生活、市民の生命、市民の財産）への影響有無」、「法令・条例や契約義務への違反有無」の観点から精査を実施し 24 時間以内に復旧すべき業務を非災害時優先業務として選定した。

第５章　優先システム

1　優先システムの定義

優先システムとは、非常時優先業務及び非災害時優先業務を実施するにあたり必要不可欠となるＩＣＴ資源のことである。優先システムには庁内ＬＡＮ*やＷＡＮ*を構成するネットワーク、業務用端末機等も含まれる。

優先システムの選定に当たっては、「小平市業務継続計画（震災編）」に規定された非常時優先業務の遂行に必要なシステムや、必要に応じて、特筆すべきシステムを考慮の上、選定を行った。

2　優先システムの選定

(1)　非常時優先システム

非常時優先業務を実施するにあたり必要となるＩＣＴを非常時優先システムとして選定を行った。また、優先システムについて、「小平市業務継続計画（震災編）」に規定された業務開始目標時間をシステムの目標復旧時間とした。

以下に非常時優先システムの一覧を示す。

表 8　非常時優先システム一覧

No.	優先システム名		システム管理担当
1	住民情報システム	住民記録	市民課
2		印鑑登録・カード管理	市民課
3		学齢簿	学務課
4		就学援助	学務課
5		個人住民税	税務課
6		法人住民税	税務課
7		軽自動車税	税務課
8		固定資産税	税務課
9		収納管理	収納課
10		滞納管理	収納課
11		国保資格	保険年金課
12		国保賦課	保険年金課

No.	優先システム名		システム管理担当
13		国保給付	保険年金課
14		国民年金	保険年金課
15		宛名管理	関係各課
16		プリントサーバー	情報政策課
17		バックアップ	情報政策課
18	後期高齢者医療		保険年金課
19	DC 向け回線		情報政策課
20	下水道台帳管理システム		下水道課
21	文書管理		総務課
22	グループウェア（メールサービス含む）		情報政策課
23	AD サーバー（プライマリ、セカンダリ）		情報政策課
24	全庁ファイルサーバー（情報系、業務系、管理職）		情報政策課
25	プリント WSUS サーバー		情報政策課
26	庁内 LAN		情報政策課
27	出先機関 1 WAN（重要拠点）、出先機関 2 WAN		情報政策課
28	LGWAN		情報政策課
29	インターネット（FW、アクセス回線含む）		情報政策課
30	防災行政無線		防災危機管理課
31	仮想ブラウザシステム		情報政策課
32	メール無害化システム		情報政策課
33	市ホームページ（※）		秘書広報課
34	J-ALERT（※）		防災危機管理課
35	EM-NET（※）		防災危機管理課
36	保育園・学童クラブ保護者連絡メール配信（※）		子育て支援課・保育課
37	東京都災害情報システム（※）		防災危機管理課
38	東京都被災者生活再建支援システム（※）		防災危機管理課
39	Logo チャット（※）		情報政策課

（優先度毎の並び順は、住民情報システムの記載統合等の後、【C02】優先システム一覧に準じて列記している。）

※のシステムは SaaS 利用であり、本市が主体的に復旧作業を行うことが困難であるため留意が必要である。

(2)　非災害時優先システム

非災害時優先業務を実施するにあたり必要となるＩＣＴを非災害時優先システムとして選定を行った。非災害時優先システムも非常時優先システムと同様に「小平市業務継続計画（震災編）」に規定された業務開始目標時間をシステムの目標復旧時間とした。

以下に非災害時優先システムの一覧を示す。

表 9　非災害時優先システム一覧

No.	優先システム名		システム管理担当
1	住民基本台帳ネットワークシステム		市民課
2	処理装置 X		情報政策課
3	住民情報システム	住民記録	市民課
4		印鑑登録・カード管理	市民課
5		学齢簿	学務課
6		就学援助	学務課
7		個人住民税	税務課
8		法人住民税	税務課
9		軽自動車税	税務課
10		固定資産税	税務課
11		収納管理	収納課
12		滞納管理	収納課
13		国保資格	保険年金課
14		国保賦課	保険年金課
15		国保給付	保険年金課
16		国民年金	保険年金課
17		宛名管理	関係各課
18		バックアップ	情報政策課
19		プリントサーバー	情報政策課
20	選挙人名簿登録		選挙管理委員会
21	証明書コンビニ交付システム		市民課
22	投票管理		選挙管理委員会
23	戸籍情報管理		市民課

No.	優先システム名	システム管理担当
24	DC 向け回線	情報政策課
25	用水路管理システム	水と緑と公園課
26	下水道台帳管理システム	下水道課
27	下水道資産管理システム	下水道課
28	校務用グループウェア	学務課
29	財務会計	会計課・財政課・契約検査課
30	文書管理	総務課
31	グループウェア（メールサービス含む）	情報政策課
32	AD サーバー（プライマリ、セカンダリ）	情報政策課
33	全庁ファイルサーバー（情報系、業務系、管理職）	情報政策課
34	プリント WSUS サーバー	情報政策課
35	庁内 LAN	情報政策課
36	IDC 向け WAN	情報政策課
37	住民基本台帳ネット WAN	情報政策課
38	出先機関 1 WAN（重要拠点）、出先機関 2 WAN	情報政策課
39	LGWAN	情報政策課
40	インターネット（FW、アクセス回線含む）	情報政策課
41	公園台帳管理システム	水と緑と公園課
42	防災行政無線	防災危機管理課
43	仮想ブラウザシステム	情報政策課
44	メール無害化システム	情報政策課
45	市ホームページ（※）	秘書広報課
46	J-ALERT（※）	防災危機管理課
47	EM-NET（※）	防災危機管理課
48	保育園・学童クラブ保護者連絡メール配信（※）	子育て支援課・保育課
49	学習系ネットワーク（※）	学務課
50	東京都災害情報システム（※）	防災危機管理課
51	東京都被災者生活再建支援システム（※）	防災危機管理課
52	Logo チャット（※）	情報政策課

（優先度毎の並び順は、住民情報システムの記載統合等の後、【C02】優先システム一覧に準じて列記している。）

※のシステムは SaaS 利用であり、本市が主体的に復旧作業を行うことが困難であるため留意が必要である。

第６章　ＩＣＴ業務継続体制の確立及び発動

１　ＩＣＴ業務継続体制確立及び発動までの流れ

本計画における脅威発生時の行動手順は、①「初動対応手順」と②「ＩＣＴ業務継続対応手順」の二段階の流れとなる。

各手順の詳細については、別途「行動手順書（D01～04）」を脅威毎に定める。なお、「行動手順書」は、様々な脅威を事前に想定して、即時に対応できるよう手順を定めるものであるが、脅威によるリスクは常に変化するため、行動手順書に基づき対応すると同時に、その都度の状況判断に応じた行動を取るものとする。

(1)　初動対応手順

脅威発生直後は、「初動対応手順」に定められた行動を実行する。初動対応手順は、「緊急体制の確立及び発動」「被害状況の基礎調査」「ＩＣＴ業務継続体制確立及び発動の判定」を行うものである。これらの結果に基づいて、優先システムの継続が脅威により脅かされる可能性があると判定される場合は、ＩＣＴ業務継続対応手順に基づき対応を行う。優先システムの継続の危険がないと判断した場合には、通常のシステム障害として対応を行う。

(2)　ＩＣＴ業務継続対応手順

優先システムの継続が脅威により脅かされる可能性があると判断された場合、「初動対応手順」から「ＩＣＴ業務継続対応手順」へと移行する。「ＩＣＴ業務継続対応手順」では、「ＩＣＴ業務継続体制の確立及び発動」「被害状況の詳細調査」「復旧活動」を行い、システムの目標復旧時間内での復旧を目指す。

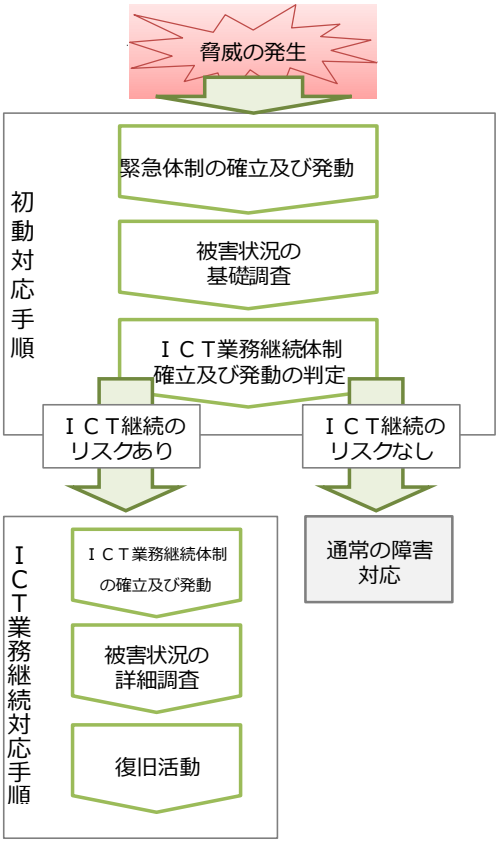

図９　ＩＣＴ業務継続計画体制確立及び発動の流れ

(3)　体制確立の基準

初動対応手順における「緊急体制の確立及び発動」と、ＩＣＴ業務継続対応手順における「ＩＣＴ業務継続体制」の確立及び発動の基準を図 10 に示す。このうち、非災害時（セキュリティインシデント等）は、新たに体制を確立するものではなく、既に設置されている CSIRT 体制が発動し、対応する。なお、想定脅威毎の「ICT 業務継続体制」の確立及び発動基準は、「行動手順書」に定める。

	想定脅威	
	災害時（震災）	**非災害時（セキュリティインシデント等）**
【初動対応手順 】 緊急体制の確立及び発動基準	● 本部管理部長（危機管理担当部長）より、災害対策本部設置の通知を受けた場合。 ● 夜間、休日等の勤務時間外において震度 5 弱以上の地震が発生した場合。 ● 上記基準に満たない地震発生時において、担当者からの連絡を受け、統括 ICT 業務継続計画管理者が優先システムの正常運用への影響を確認した場合。	● 下記を契機に、担当者からの報告を受け、統括 ICT 業務継続計画管理者がセキュリティインシデント等の発生を確認した場合。 ・システム利用課からの障害連絡時 ・運用者（常駐 SE 等）からの障害連絡時（メール、電話、対面） ・緊急連絡網による連絡発生時 ※非災害時（セキュリティインシデント等）は、新たに体制を確立するものではなく、既に設置されている CSIRT 体制が発動し、対応する。
【ＩＣＴ業務 継続対応 手順】 ＩＣＴ 業務継続体制の確立及び発動基準	● 被害状況の調査結果や人員の参集状況を考慮し、統括 ICT 業務継続計画責任者が優先システム運用継続の危機があると判断した場合。	

図 10　体制確立及び発動基準

第７章　運用管理規定

1　運用体制

(1)　体制図

本計画の運用・改善活動は、情報政策課が中心となって推進・実行するものとする。以下に、計画の運用・改善に係る体制図を示す。

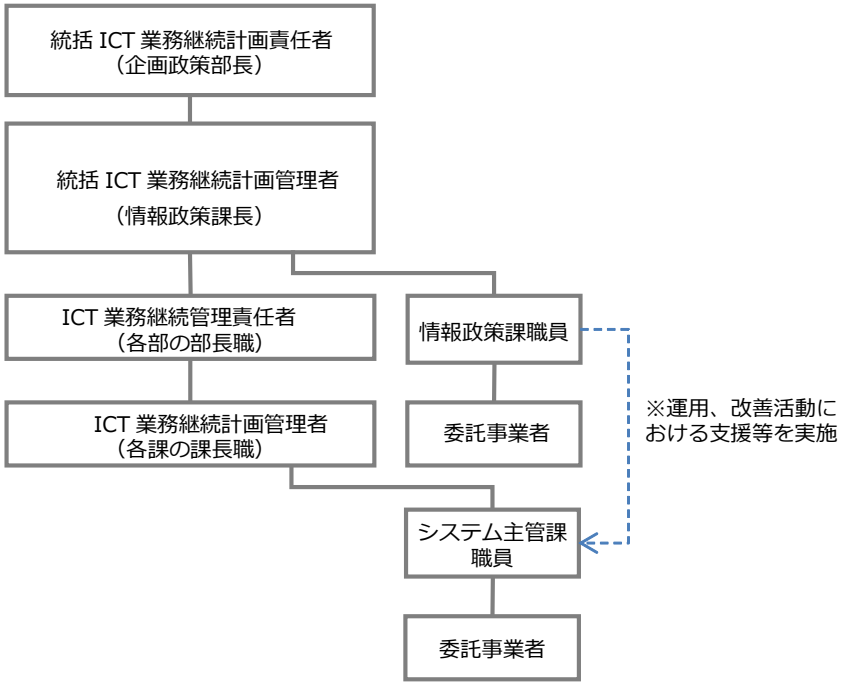

図 11　計画の運用・改善に係る体制図

(2)　各要員の役割

各要員の役割を以下に示す。

表 10　各要員の役割

要員（＝役職）	役割
・統括 ICT 業務継続計画責任者（＝企画政策部長）	本計画の運用、改善活動全体に関する承認を行う。
・統括 ICT 業務継続計画管理者（＝情報政策課長）	本計画で定めた運用の手続に基づき、本計画に関する日常の運用・進捗確認に係る管理を行う。
・情報政策課職員	本計画で定められた各種対策の実施や日常の運用、計画の見直し等を行う。

要員（＝役職）	役割
・ICT 業務継続計画責任者 （＝各部の部長相当職）	自身の部が管轄する優先システムに係るリスクを適宜把握し、リスク回避等に向けた対策の承認等を行う。
・ICT 業務継続計画管理者 （＝各課の課長相当職）	自身の部が管轄する優先システムに係るリスクを適宜把握し、ICT 業務継続計画責任者、情報政策課と連携しながら具体的な対策案の立案など、ＩＣＴの業務継続に関わる作業を管理する。
・情報システム担当者 （＝システム主管課職員）	情報政策課職員等と連携し、リスク回避に向けた具体的な対策案の立案、システム更改時におけるリスク分析等、本計画の運用・改善活動に必要な作業の支援を行う。
・委託事業者	情報システムの詳細情報に係る部分について、本計画の運用・改善活動に必要な助言や作業の支援を行う。

(3)　運用管理に係る年間の基本活動計画

年間の基本活動計画を以下に示す。本計画は当年度の状況などに応じて活動回数の増減、取り組み期間の変更等を行い計画の弾力性を維持する。

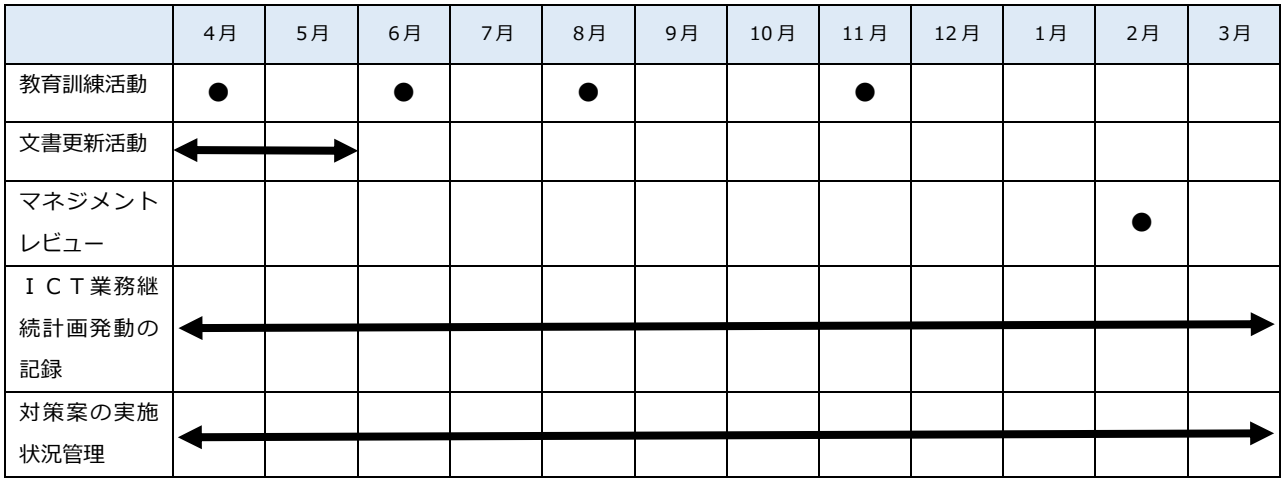

図 12　年間の基本活動計画

(4)　各活動の内容

①　教育訓練活動

ＩＣＴ業務継続計画に関する理解度の向上、ＢＣＰ発動時の対応に係るシミュレーション及びＢＣＰ運用に係る技能の習得のため、以下に示す教育訓練を実施する。教育訓練の結果は、「マネジメンレビューシート」の「別紙 教育訓練結果記録（一覧）」に記録する。

表 11　教育・訓練内容

実施項目	教育・訓練内容
ＩＣＴ業務継続計画研修（概要説明）	情報政策課に新たに配属となった職員と人事異動に合わせて新たに採用した職員等に対して、必要な研修を実施する。主にＩＣＴ業務継続計画に関する概要説明を行う。
ＩＣＴ業務継続計画研修（情報政策課職員内）	情報政策課職員に対して、ＩＣＴ業務継続計画の概観と、文書更新活動によって更新された部分の共有を行う。
ＩＣＴ業務継続計画研修（全職員向け）	業務継続に係るトピックスや他自治体の事例等を中心に紹介を行うとともに、その重要性について共有する。
ＩＣＴ業務継続計画研修（演習）	演習として、各課が自らの障害発生時等の対応フローを作成する。
障害訓練	障害発生時の訓練として、バックアップデータからの帳票出力等の手順を確認する。

② 文書更新活動

本計画の維持とその継続的な改善のため、各文書の更新を実施する。実施時期は、４月から５月までとする。更新活動は、前年度のＩＣＴ業務継続活動の結果、システム等ＩＣＴ更新の状況及び本市の組織改正等の変更事項を踏まえ、分析作業（フィット＆ギャップ分析）や次年度実施の対策案一覧の確定、その他必要な文書の更新を行う。なお、分析作業や対策案の検討、各種文書更新作業に係る具体的な作業手順については、「運用手順書（C01）」に示す。

③ マネジメントレビュー

統括 ICT 業務継続計画管理者は、マネジメントレビューとして、本計画の運用状況確認、分析作業や対策案の検討、各種文書更新作業等の妥当性評価及び前年度更新箇所の承認を行うこととし、原則年１回、２月に実施する。

マネジメントレビューで確認すべき項目は、「マネジメントレビューシート（C10）」を例とする。

④　ＩＣＴ業務継続計画発動の記録（通年活動）

本計画の維持とその継続的な改善を目的として、本計画発動の行動実績を記録することとし、ＩＣＴ業務継続体制が確立及び発動された場合の対応内容を各課にて記録する。本記録は、次年度以降の文書更新活動において計画の改善に利用する。

⑤　対策案の実施状況管理（通年活動）

優先システムに係るリスクを適切に管理するため、対策案の実施状況を確認する。確認は、年間を通して実施する。「リソース毎の対策案一覧（C06、C07）」、「対策実施案（C09）」により、実施状況を把握するとともに、必要に応じて、実施結果の記録を行い、次年度以降の文書更新等に反映させる。

(5)　文書管理

①　管理対象文書

管理対象となる文書は、「ICT 業務継続計画管理文書一覧（Ｐ03）」に記載する全ての文書とする。管理対象文書は、庁内ファイルサーバー上の電子ファイルを正本とし、紙媒体の文書は副本とする。なお、文書の正本を更新した場合は、紙媒体の副本も最新版となるよう管理する。

②　文書の保管

最新の紙媒体の副本については、緊急時に利用することを想定し、優先システムを有する課において、各課の執務室に１部以上保管する。

③　文書更新の手続き

新規作成又は更新した文書については、統括 ICT 業務継続計画管理者が承認を行う。文書の新規作成や更新の際には、「ICT 業務継続計画管理文書一覧（Ｐ03）」の「初版作成日」、「最終更新日」及び「版数」を更新する。

④　文書の命名規則

文書の電子ファイル名は、『【管理番号】＋資料名_日付(yyyymmdd).拡張子』の方式で命名する。管理番号については、「文書分類＋連番」の方式で採番する。「文書分類」は以下のとおりとし、日付は、文書の「初版作成日」又は「最終更新日」とする。

（例）【Ｐ01】小平市 ICT 業務継続計画_20130331.doc

表 12　文書分類

文書分類	対象の文書
P	ＩＣＴ業務継続計画及びＩＣＴ業務継続計画に紐付くツールや詳細資料
D	行動手順書及び行動手順書に紐付くツールや詳細資料
C	運用手順書及び運用手順書に紐付くツールや詳細資料
A	対策案一覧及び対策実施案に紐づくツールや詳細資料

⑤　文書のバージョン管理ルール

版数は 1.0 から開始し、マネジメントレビューによる承認完了前の更新は、小数点以下をカウントアップする。マネジメントレビューによる承認が完了した場合は、小数点以下を 0 とした上で整数部分をカウントアップする。なお、版数の管理は「ICT 業務継続計画管理文書一覧（P03)」により行う。

用　語　集（五十音・アルファベット順）

セキュリティインシデント

情報漏えい、不正アクセス、ウィルス感染など、情報セキュリティに関する事故や攻撃を総称してセキュリティインシデントと呼ぶ。

セキュリティホール

コンピュータやコンピュータネットワークの安全性を脅かす欠陥部分を指す。特に外部からの不正アクセスに対する弱点を言う。

情報セキュリティポリシー

組織のセキュリティ対策を効率よく、効果的に行うための指針。また恒久的にセキュリティを維持するための仕組み。セキュリティを維持するために必要な対策を対象、目的、方法、レベルを示したもので情報システムを運用、利用する際に指針となる。

ICT

ICT は「情報通信技術(Information and Communication Technology)」の略で、IT「情報技術（Information Technology）」とほぼ同義。コンピュータ関連の技術を「IT」、コンピュータ技術の活用に着目する場合を「ICT」と、区別して用いる場合もある。

KPI

KPI は「重要業績評価指標（Key Performance Indicator）」の略。企業などの組織において、個人や部門の業績評価を定量的に評価するための指標。達成すべき目標に対し、どれだけの進捗がみられたかを明確にできる指標を選択し、これをもとに日々の進捗把握や業務の改善などが行われる。

LAN

LAN は「構内通信網（Local Area Network）」の略。ケーブルや無線などを使って、同じ建物の中にあるコンピュータや通信機器、プリンタなどを接続し、データをやり取りするネットワーク。より対線や同軸ケーブル、光ファイバーなどで配線するものを「有線 LAN」、電波を用いるものを「無線 LAN」という。

PDCA サイクル

品質改善や経費削減、環境マネジメント、情報セキュリティなど、多くの分野で用いられる管理手法の一つ。計画(plan)→実行(do)→評価(check)→改善(act)という 4 段階の活動を繰り返し行うことで、継続的に業務プロセスを改善していく手法。

WAN

WAN は「広域通信網（Wide Area Network）」の略。遠隔地の LAN を連携させたコンピュータネットワー

ク。LAN 等に比べ、より広範囲に及ぶネットワークを意味することもある。LAN 同士の接続には一般の電話回線や専用線、インターネットなどを利用する。

小平市　ＩＣＴ業務継続計画

平成 27 年３月発行
平成 27 年７月改定
令和５年３月改定

編集・発行　小平市企画政策部情報政策課
〒187-8701
東京都小平市小川町二丁目 1333 番地
電話番号（０４２）３４６－９５０９