三鷹市ＩＣＴ事業継続計画書

管理文書番号　：　P-A01
策　　定　　日　：　平成 23 年３月 31 日
最 終 改 正 日　：　平成 23 年 7 月　６日
文　　書　　版　：　1.1

目次

1　基本的事項

(1)　目的

現在では、地方自治体における業務や事業の継続にあたっては、情報システムの稼動が必須となっている。そのため、大規模な災害の発生や非災害時におけるシステム障害が発生した場合は、行政機能が停止し、その復旧に多大な時間を要する可能性がある。

ICT 事業継続計画書（以下、「本計画書」という。）は、災害時や非災害時における脅威発生時においても本市の事業が継続され、かつ、システムが停止した場合については、許容範囲内にシステムを復旧させることを目的として、その取組みの方針を定めるものである。

本市の行政サービスの継続に影響を与える脅威は様々であることから、本計画書の策定にあたっては、「①災害時のみならず、本市の行政サービスの継続に影響を与える全ての脅威を想定して対応する。」、「②組織や情報システムの変更に柔軟に対応できるマネジメントの仕組みを構築する。」ことを策定目標とする。

網羅的な脅威の想定とマネジメントの仕組みを確立することで、不測の事態に備えた対応と早期の業務再開を果たすだけでなく、継続的な取組みとして災害等に対する行政の対応能力の向上を実現し、行政としての責務と市民サービスの向上を実現するものである。

以下に本市における事業継続計画の体系図と関連計画との関係性を示す。なお、本市地域防災計画と ICT 事業継続計画の考え方については、0 章を参照のこと。

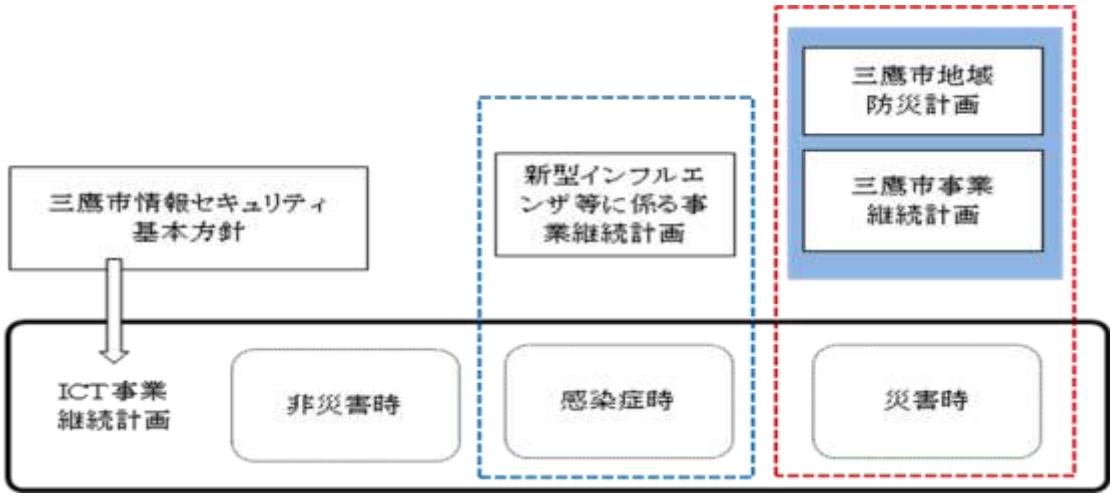

図 1　本市における各事業継続計画の体系と関連計画との関係性

(2)　対象範囲

ア　対象となる情報システム

企画部情報推進課にて管理する情報システムの中から、災害時及び非災害時の障害発生時を想定した本市の優先業務に必要不可欠となる情報システム（優先システム）を本計画書の管理対象とする。優先システムの選定方法と選定結果は、7 章に記載する。なお、優先システム以外も含めた情報推進課が管理するシステムは「管理範囲システム一覧(P-B01)」に記載している。

イ　対象となる主管課

ICT 事業継続計画の実行主体は、企画部情報推進課とする。

優先システムを利用している全主管課が対象であり、当該課において、優先システムの RTO の調整やシステム停止中における業務の代替手段の検討、システム復旧時において復旧作業に係る要員が不足した場合の支援作業等を行うこととする。主管課と利用システムの関係については、「主管課と利用システムの関係（P-B02）」のとおりである。

2　定義

(1)　用語の定義

本計画書における用語の定義は、以下のとおりとする。

表 1　ICT 事業継続計画における用語の定義

用語	意味
ICT	情報通信技術のこと。（Information and Communication Technology）
BCP	事業継続計画のこと。（Business Continuity Plan）
ICT-BCP	事業継続（Business Continuity）の ICT を対象とした計画（Plan）。 自然災害等の脅威に遭遇した場合において、事業資産の損害を最小限にとどめつつ、中核となる事業の継続あるいは早期復旧を可能とするために、非災害時に行うべき活動や緊急時における事業継続のための方法、手段などを取り決めておく計画のこと。ICT が付属すると、事業継続に必要となる ICT（システムやネットワークインフラ）を継続するための計画となる。
脅威	地震や風水害等の自然災害、セキュリティ事故等の人為的災害といった市職員や行政サービス等に対して重大な被害や影響を及ぼす可能性のある事態のこと。
RTO	目標復旧時間（Recovery Time Objective） 優先業務を復旧させなければならない時間のこと。本計画書では ICT を復旧させなければならない時間のことを表している。
RPO	目標復旧時点（Recovery Point Objective） 優先業務を復旧させなければならない時点のこと。本計画書ではデータを復旧させなければならないバックアップ時点のことを表している。
RLO	目標復旧レベル（Recovery Level Objective） 優先業務を復旧させなければならないレベル（状態）のこと。本計画書では ICT を復旧させなければならないレベル（機能）のことを表している。 本計画書では各システムの機能は全復旧を前提としている。

3　文書管理

(1)　一般

ICT 事業継続計画の構築及び維持とその継続的な改善のための手順及び関連する事項を

文書により明確化するとともに、関連文書の所在を明らかにするために必要となる事項を以下に定める。

(2)　文書体系図

ICT 事業継続計画の文書体系は、以下のとおりとする。

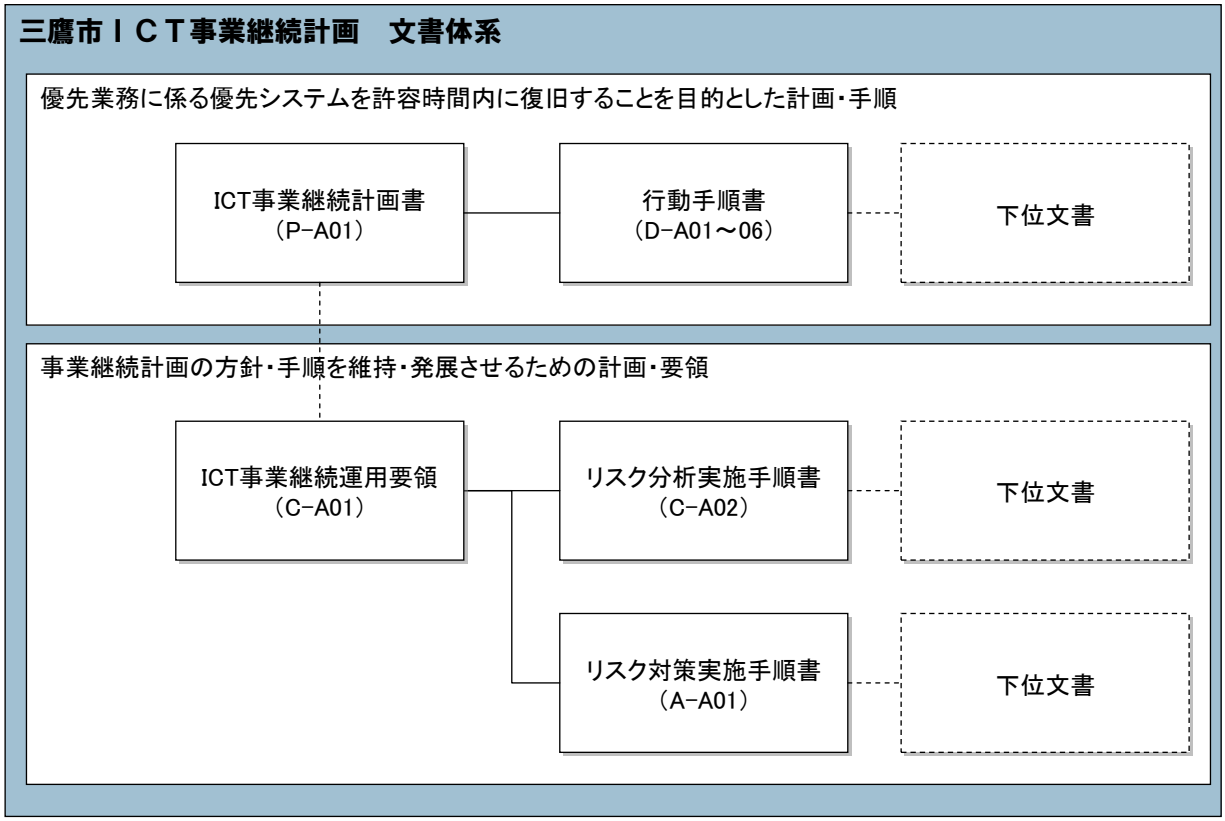

図 2　三鷹市 ICT 事業継続計画　文書体系

(3)　各文書の概要

ア　上位文書

(ｱ)　ICT 事業継続計画書（P-A01）

本市における ICT 事業継続計画策定の考え方、被害想定等の前提条件、対象となる優先システム、運用及び改善方法等を規定する。

(ｲ)　行動手順書（D-A01~06）

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、職員が有するスキルやノウハウに依存せず、復旧に向けた行動を取ることができる手順を規定する。

(ｳ)　ICT 事業継続運用要領（C-A01）

年間の活動スケジュール（見直し、マネジメントレビュー、対策実施に係る予算化、教育訓練活動、ICT 事業継続体制確立結果の記録、対策実施の進捗管理）及び ICT 事業継続計画を継続的に維持・改善させるためのルール並びに管理手法を規定する。

(ｴ)　リスク分析実施手順書（C-A02）

ICT 事業継続運用要領にて規定する見直しに関して、対策実施状況やシステム更改等により生じる構成変更を管理し、変更部分について実施するリスク分析や対策案の抽出等の実施手順を規定する。

(ｵ)　リスク対策実施手順書（A-A01）

ICT 事業継続計画を継続・改善するために必要となる資源のリスクについて、対策実施の計画について規定する。

イ　下位文書

各上位文書に紐付けて、各作業時のワークシートや詳細な情報の参照先として利用する。

4　推進体制

(1)　体制図

ICT 事業継続計画は、企画部情報推進課により推進・実行するものとし、災害時及び非災害時における ICT 事業継続体制確立時の管理体制は、以下のとおりとする。

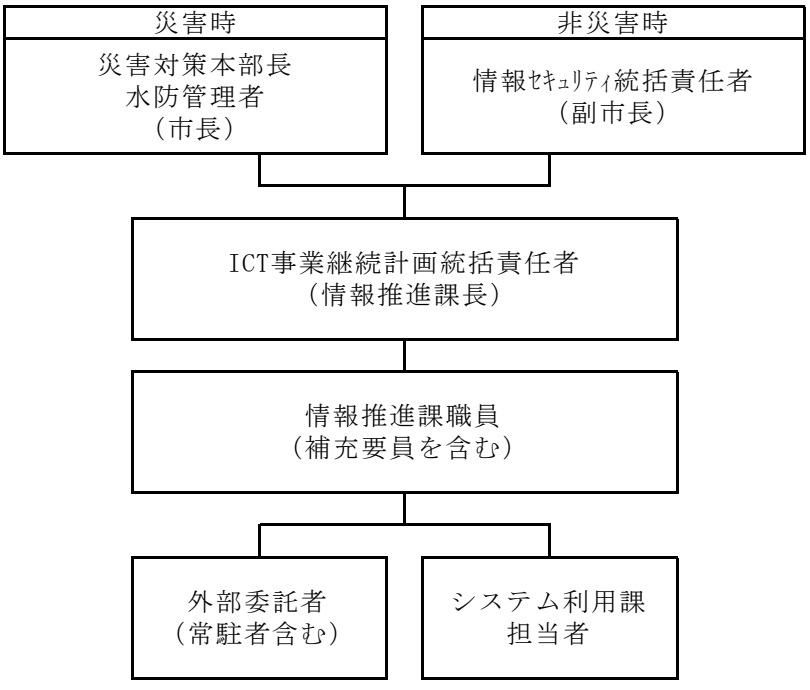

図 3　ICT 事業継続計画管理体制図

(2)　各要員の役割

ア　ICT 事業継続計画体制確立時の管理体制

表 2　ICT 事業継続計画体制確立時管理体制における各要員の役割

要員（組織）	役割
災害対策本部長、水防管理者（市長）	災害時において設置される災害対策本部または水防本部を統括し、災害対策に係る重要事項を審議・決定する。
情報ｾｷｭﾘﾃｨ統括責任者（副市長）	非災害時において重大なセキュリティインシデントが発生した際の対応事項を審議・決定する。
ICT 事業継続計画統括責任者	災害発生時及び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意思決定 ・災害対策本部、水防本部への状況報告と本部決定の部門内への伝達 ・他主管課との調整の総括、支援依頼等
情報推進課職員（補充要員を含む）	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支援等を行う。
外部委託者（常駐者含む）	情報推進課職員の指示に基づき ICT 復旧にむけた作業等を行う。
システム利用課担者	ICT 事業継続計画の実行にあたり、情報システムの復旧作業に係るシステム動作確認作業等を行う。

5　三鷹市地域防災計画及び三鷹市事業継続計画（震災編）との関係

三鷹市地域防災計画（平成 20 年 3 月改正。以下、「防災計画」という。）では、「第 2 部災害予防計画　第 6 章事業継続計画 BCP の策定」で「災害発生時においても、市の行政サービスの一定レベルを確保するとともに、全ての業務が最短で再度提供できる」ことを目的として事業継続計画を策定することとしている。市の行政サービスの多くは、情報システムに依存してサービス提供をしている状況であることから、震災等の災害時における通常業務の前提となる情報システムの継続利用及びシステム復旧は、最優先課題であり、三鷹市事業継続計画（震災編）における広報情報班（情報推進課）の応急対策業務に係る優先業務として位置付ける。また、災害時における優先システム以外の情報システムの復旧は、情報推進課における通常業務とする。

防災計画は、人命の安全確保や物的被害の軽減等に焦点が当てられているが、ICT 事業継続計画とは無関係ではない。災害時においては、防災計画と ICT 事業継続計画は相互に補完しあう役割を担っているため、整合性を確保した実効性のある ICT 事業継続計画を策定する必要がある。

ICT 事業継続計画では、防災計画で定義された人命の安全確保や物的被害の軽減に加え、優

先業務（復興支援に直結する業務）の継続及び早期復旧の視点をより大きくして計画を策定する。最終的には、復旧時間や復旧レベルを定量的に算出しつつ、どのシステムを、いつまでに、どの程度まで、復旧させるかという視点から必要事項を取りまとめるものとする。

6　被害想定

(1)　脅威の選定理由

ア　災害

(ｱ)　災害の定義

ICT 事業継続計画で想定する「災害」を定義する際には、上位計画との整合性を保つ必要性がある。上位計画である防災計画、また、防災計画の上位計画である内閣府中央防災会議策定の防災基本計画により、災害の定義を行う。

表 3　内閣府中央防災会議策定　防災基本計画における災害の定義

分類	災害の種類
自然災害	震災・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

(ｲ)　想定脅威の抽出

本計画書における想定脅威は、6(1)ア(ｱ)の災害の定義のうち、本市の地勢、人口、交通、施設・設備及び過去の災害発生状況等を考慮して、本市における発生可能性が高いものとし、地域特性等を踏まえた結果、本市において発生可能性が考えられる震災・風水害を災害時における想定脅威として選定し、他の脅威については、本市の ICT 事業継続に影響を与えるような甚大な被害は発生しないものと考えられる。

表 4　自然災害・事故災害における想定脅威の抽出とその評価

災害の種類		ICT 継続への影響	本市における発生可能性	ICT 事業継続計画での想定脅威
自然災害	震災	高い	高い	○
	風水害	高い	高い	○
	火山災害	高い	低い	×
	雪害	低い	低い	×
事故災害	海上災害	無し	無し	×
	航空災害	低い	低い	×
	鉄道災害	無し	低い	×
	道路災害	無し	低い	×
	原子力災害	無し	低い	×

災害の種類		ICT 継続への影響	本市における発生可能性	ICT 事業継続計画での想定脅威
	危険物災害	無し	低い	×
	大規模火事災害	高い	低い	×
	林野災害	無し	低い	×

イ　セキュリティインシデント

(ｱ)　セキュリティインシデントの定義

自然災害等に拠らずとも、システム障害やセキュリティ事故を原因とするシステムの停止は、事業継続に大きな影響を与えることとなり、自然災害以上に発生する確立の高いものである。本市では、より実効性の高い ICT 事業継続計画とすべく、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ついても想定脅威として設定し、事業継続に向けた対策を行うこととする。

なお、セキュリティインシデントは、「望まないまたは予期しない情報セキュリティ事象」であると定義される。本市の ICT 事業継続計画におけるセキュリティインシデントの定義も本内容を踏まえた上で、「システムまたはデータに直接的な被害を与える事象であり、事業継続に直接的に影響を及ぼす事象」として定義する。

表 5　セキュリティインシデントの定義

項目	内容
情報セキュリティ事象	システム、サービス又はネットワークにおける特定の状態の発生。特定の状態とは、情報セキュリティ基本方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関連するかもしれない未知の状況を示しているもの。
情報セキュリティインシデント	望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。
本市 ICT 事業継続計画におけるセキュリティインシデントの定義	上記 2 点を踏まえ、システムまたはデータに直接的な被害を与える事象であり、ICT 事業継続に直接的に影響を及ぼす事象

(ｲ)　想定脅威の抽出

情報セキュリティに関する評価の際の指標は、一般的に「機密性」・「完全性」・「可用性」が用いられていることから、セキュリティインシデントの抽出にあたっては、「機密性」・「完全性」・「可用性」と脅威の発生要因（意図的・偶発的）に分類し整理を行った。

このうち「機密性」に整理されたセキュリティインシデントは、脅威ではあるものの