別　紙　3

案

葛飾区ICT部門業務継続計画
(ICT-BCP)

＜地震編＞

平成２X年X月

葛　飾　区

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
初　版	平成　　年　　月　　日	

【本計画の保管について】

（１）本計画書（原本）及びその写し（１部）を情報システム課内の書庫にて保管する。

（２）本計画書の写しを、情報システム課長及びその代行者（情報システム課係長職の者）が自宅に保管する。

（３）情報システム課長及びその代行者に異動があった場合、自宅に所持する計画書は速やかに後任者に引き継ぐ。

目次

1　計画の目的・基本方針

(1) 計画の目的

大地震が発生した場合に、区の災害時優先業務を実施・継続させるためには、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。しかし、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早期復旧が困難であるという特性を持つ。そこで、「葛飾区業務継続計画（ＢＣＰ）〈地震編〉」（以下「全庁ＢＣＰ〈地震編〉」という。）の個別計画として、「葛飾区ＩＣＴ部門業務継続計画（ＩＣＴ－ＢＣＰ）〈地震編〉」（以下「本計画」という。）を策定し、震災が発生した際に災害時優先業務の実施･継続を行うための基盤を整えることを目的とする。

(2) 計画の基本方針

本計画を策定するに当たり、次の事項を基本方針とする。

基本方針	
ＩＣＴ部門の責務遂行	災害時において、区民の生命の安全確保や区民生活、地域経済活動に必要な区の重要業務システムを早期復旧する。
来訪者、職員、関係者の安全	災害時において、執務室等への来訪者、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。
本計画の有効性の維持･改善	本計画は、毎年、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う。そして、それらの結果を踏まえて是正措置を講ずるとともに、少なくとも年に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う。
外部事業者等との連携	外部事業者（公的団体を含む。以下同じ。）や保守事業者と連携し、葛飾区の情報システムの業務継続を図り、代替対応の可能な業務継続計画を立案する。

(3) 計画策定の前提

ア　計画の対象範囲

本計画の対象範囲は、情報システム課が管理するシステム（庁内基盤、ネットワーク、インターネットサービス、電算センター内のサーバ、住民情報系端末、ＩＴパソコン、情報システム課が契約しているＩＤＣ）と、全庁ＢＣＰ〈地震編〉における「災害時優先業務」の遂行に不可欠な情報システムのうち電算センターを利用する情報システムとする。

各課が独自に管理運営する情報システムについては、今後、本計画を参考に各主管課で作成している「情報セキュリティ対策実施手順」に盛り込むこととする。

イ　対象リスク

本計画の対象リスクは、「全庁ＢＣＰ〈地震編〉」と同様、大規模地震とする。

なお、被害想定についても、「全庁ＢＣＰ〈地震編〉」の被害想定と同様とする。

また、大規模地震に類似した災害及び新型インフルエンザに類似した感染症に対しても、当面本計画を準用して対応するものとする。

ウ　計画の発動

本計画の発動は、「全庁ＢＣＰ〈地震編〉」の発動と同時とする。

エ　計画の構成

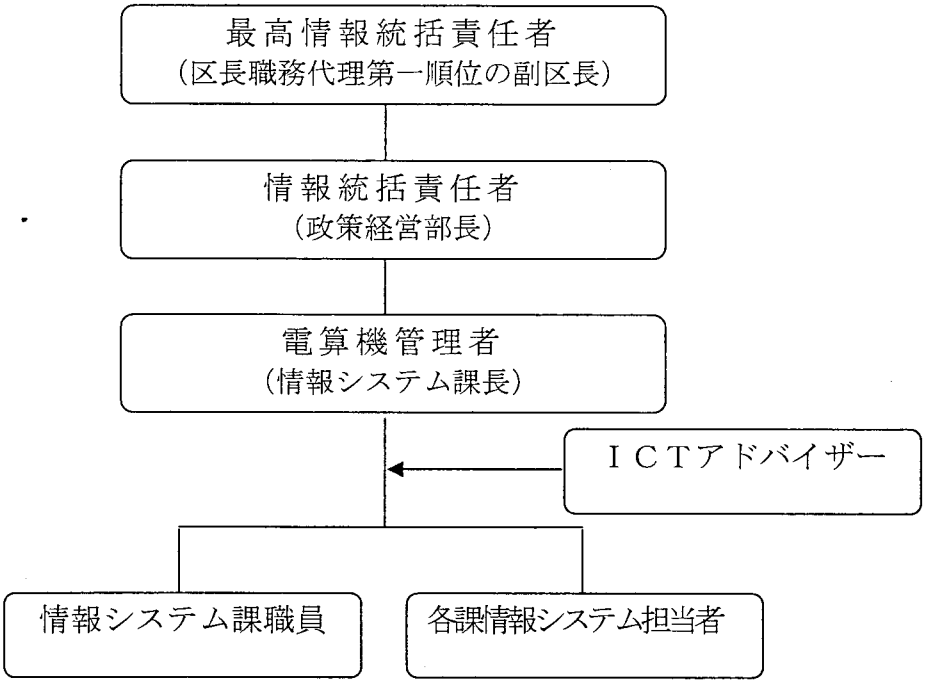
本計画の構成は、「地方公共団体におけるＩＣＴ部門の業務継続計画（ＢＣＰ）策定に関するガイドライン」（平成20年8月総務省）の第３章全体を踏まえたものである。

2　計画の運用体制と役割

本計画の管理運用に当たり、葛飾区電子計算組織の管理運営に関する規則（平成17年葛飾区規則第46号）で定める最高情報統括責任者を中心に本計画の運用体制を整備する。

発災時は災害対策本部と連携し、復旧体制は5（1）緊急時対応体制のもと、業務の復旧を実施する。

＜本計画の運用体制＞



組織	役割の概要	災害対策本部との関係
最高情報統括責任者（区長職務代理第一順位の副区長）	・本計画の全般を統括し、制定・改訂の承認を行う。	副本部長
情報統括責任者（政策経営部長）	・最高情報統括責任者を補佐し、本計画の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
電算機管理者（情報システム課長）	・本計画に関する課題及び対策遂行、検証などを行う。 ・災害時の本計画の運用責任者	
情報システム課職員	・本計画の策定、改訂を行う。 ・本計画で定められた各種施策を執行する。	
各課情報システム担当者	・各課の情報システムの業務継続計画を策定する。 ・本計画で定められた各種施策を執行する。	

3　被害想定

災害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

災害の名称	東京湾北部地震

ア　想定する災害の度合い

①　地震発生時期　　就業時間内及び就業時間外、休日

②　庁舎周辺震度　　震度６強（マグニチュード７．３）

イ　起こりうる二次災害

・庁舎内の局所的な火災

・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

ウ　想定される被害

項　目		想　定　被　害　状　況
庁舎	本館	耐震工事済み、使用可能
	新館	使用可能
電算センター	サーバ	庁舎内の電算センターに設置しているサーバは、耐震固定により転倒しない。
庁舎内	パソコン	各庁舎に設置している窓口用デスクトップパソコンは、地震対策として落下、転倒防止の固定措置を施しているため、被害は少ない。
要員		災害発生後１時間以内25.0%、24時間以内80.1%、１週間以内85.6%が参集する。
ライフライン・インフラ	電力	停電率44.9%
	水道	上水道　断水率73.7% 下水道　管きょ被害率32.7%
	電話	不通率38.4% 職員や外部事業者等との連絡に影響が生じる。
	道路	自動車は３日間通行禁止の後、再開 主要幹線道路の橋梁については通行可能 職員や外部事業者等の登庁、交換部品の配送等に影響が生じる。
	鉄道	３日間運行停止の後、再開 職員や外部事業者等の登庁、交換部品の配送等に影響が生じる。

4　重要システム

全庁ＢＣＰ〈地震編〉の策定に当たって、全庁の災害時優先業務の調査結果を基に、本計画で対応する重要システムの目標復旧時間を以下の手順で決定する。

(1) 対象業務が、業務遂行上情報システムにどの程度依存しているかを下記基準Ａ、Ｂ、Ｃにて整理する。

(2) 目標復旧レベルへの到達が遅れることによる影響の重大性がⅣになる場合の経過時間を業務の目標復旧時間とする。

(3) 対象業務の情報システム依存度がＡの場合は、業務の目標復旧時間＝情報システムの目標復旧時間として設定する。

(4) 対象業務の情報システム依存度がＢの場合は、手作業である程度代替が可能な状況であるため、業務の目標復旧時間よりは緩やかな目標レベルのシステム復旧時間を設定する。

業務分析ワークシート
Ａ：情報システムなしでは不可能
Ｂ：手作業で一部代替可
Ｃ：手作業で対応可

No.	主管業務部門	業務名	情報システム依存度	システム名	目標復旧レベルの到達が遅れることによる影響の重大性					業務目標復旧時間	業務機能停止の影響	目標レベルシステム目標復旧時間	重点対象
					Ⅰ軽微	Ⅱ小さい	Ⅲ中程度	Ⅳ大きい	Ⅴ甚大				

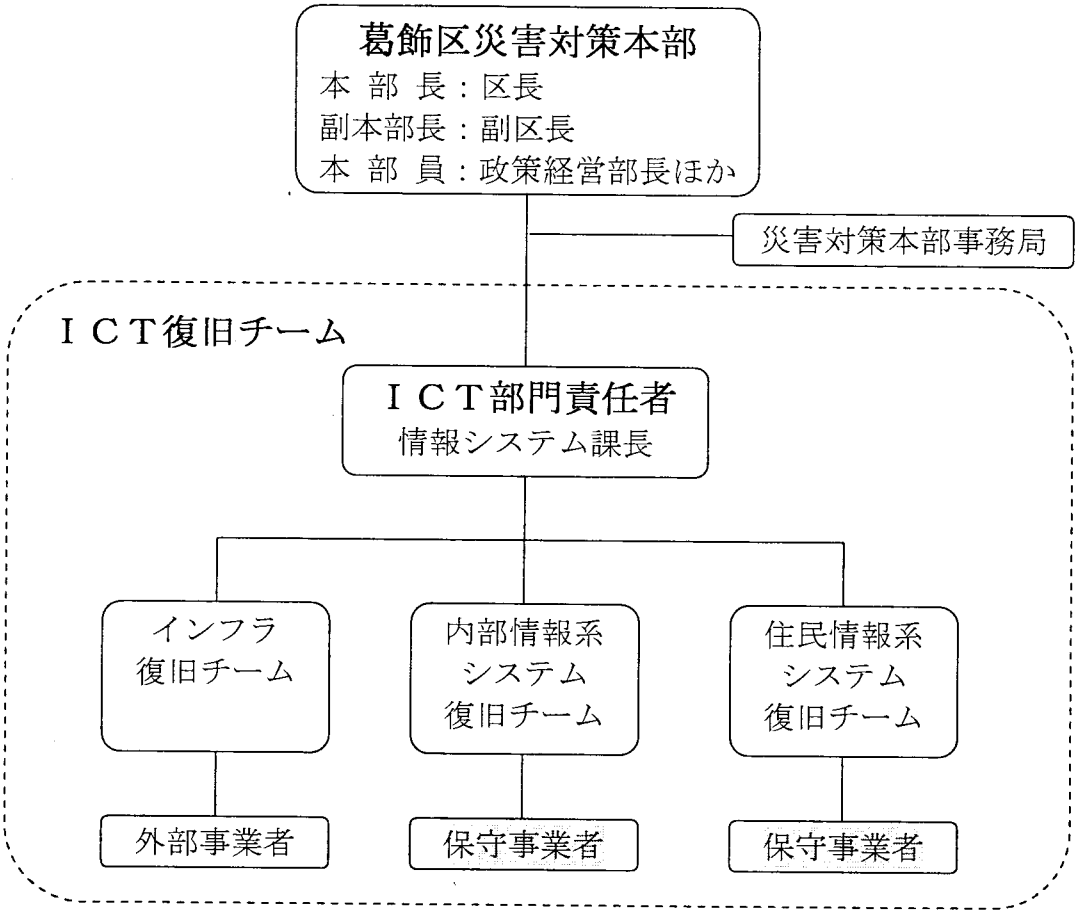
重要システム	目標レベル	目標復旧時間	システム停止時の代替手段

※当リストは、情報セキュリティ確保のため、非公開情報とする。

5　緊急時対応・復旧計画

(1) 緊急時対応体制

大規模な災害が発生した場合に、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　ＩＣＴ復旧チームの役割

チーム・メンバー	役　　割
ＩＣＴ部門責任者 (情報システム課長)	・ＩＣＴ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 ・本計画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
インフラ復旧チーム	以下の被害状況の確認、報告、復旧等 ・電算センター内の電源、空調機等の機器 ・庁内ネットワーク（ＬＡＮ及びＷＡＮ） ・回線事業者のネットワーク確認 ・外部事業者への復旧依頼
内部情報系システム 復旧チーム	以下の被害状況の確認、報告、復旧等 Ａ　情報システム課 ・内部情報系システム、インターネット、ファイルサーバ等 ・保守事業者への復旧依頼 Ｂ　各課 ・ＩＴパソコン、情報システム課から貸付されたパソコン ・ＩＴパソコン用プリンタ
住民情報系システム 復旧チーム	以下の被害状況の確認、報告、復旧等 Ａ　情報システム課 ・住民情報系システムのサーバ ・電算センター内の端末機及びプリンタ ・後方処理室の機器 ・保守事業者への復旧依頼 ・業務系システム復旧後の支援（データ追加の方法等） Ｂ　業務システム主管課 ・業務系システムの端末機 ・業務系システムのプリンタ及び周辺機器 ・業務系システム復旧までの代替手段遂行

※ＩＣＴ部門責任者が不在の場合は、代行者１がその役割を担当する。責任者、代行者１が共に不在の場合は代行者２がその役割を担当する。

ＩＣＴ部門責任者	情報システム課長
代行者１	情報システム課システム調整係長
代行者２	情報システム課係長職の者
各復旧チームリーダー	ＩＣＴ部門責任者が指名する情報システム課職員

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) 就業時間外（夜間・早朝・休日）に震度５強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、停電が区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、情報システム課システム調整係長とする。
・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、参集ができない場合等については、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。
・詳細は、安否確認マニュアルによるものとする。

注）参集ルールの詳細に関しては、緊急時参集ルール（防災課作成）を参照のこと。

（イ）その他

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、ＩＣＴ部門責任者の指示により行う。

ウ　外部事業者及び保守事業者への復旧依頼

大規模な災害が発生した場合は、必要に応じて、外部事業者又は保守事業者に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

ＩＣＴ部門の職員は、(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）

（ケース１：就業時間内の場合）

＃	復　旧　手　順	ＣＫ	補足
1	来訪者･職員等の負傷者対応、誘導： ・執務室内及び周辺の来訪者、職員（契約先職員等を含む。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、次項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、留まるよう指示する。		
2	庁舎からの避難： ◇避難指示があった場合又は庁舎に留まっていると危険と判断される場合には、来訪者、職員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： ◇執務室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、火災の発生を庁舎管理部門に至急連絡するとともに、可能な範囲で初期消火を行う。 ◇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。 ・防火扉を閉鎖し、煙の侵入や延焼を防止する。鎮火後に、復旧等の対応活動を開始する。 ・緊急用システムを除くサーバ類を一旦停止する。		
4	職員、関係する要員の安否確認： ◇避難の必要がなく、負傷者対応、二次被害の防止への対応以外に手が空く要因が確保でき次第、ＩＣＴ部門責任者又はその指名する者が、点呼により職員の安否情報を確認する。執務室への来訪者についても、職員に誰が来訪していたか報告させ、漏れなく安否を確認すること。 ◇外出者や休暇中の職員がいる場合は、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。 ◇外出者や休暇中の職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		緊急連絡先リスト

	門番号（****）で登録された情報が無いかを確認する（なお、平常時より、１７１は災害時に活用するよう職員に周知しておくこと。）。 ◇ＩＣＴ部門責任者は、災害対策本部へＩＣＴ部門の安否確認結果を報告する。報告時間に定めがない場合は、途中経過でよいので、本部立上げを見計らって第一報をする。		
5	重要書類・データ類の保護： ◇執務室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措置を行う。		
6	外部事業者、保守事業者との連絡確保： ◇至急対応を要請すべき外部事業者や保守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。 ◇業務継続に必須の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。		事業者連絡先一覧
7	被害状況の調査： ◇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。 ◇被害状況は時間経過で変わるため、継続的に監視を行う。		被害チェックシート
8	業務継続・代替復旧活動の開始判断： ◇ＩＣＴ部門責任者は、被害情報の報告結果及び要員の参集状況を考慮して、どのような業務継続の対応活動を開始するかを判断する（一部の業務継続の活動の開始の判断は、例えば情報が十分に揃うまで、後刻に先送りすることも考えられる。）。 ◇全庁の災害応急・復旧活動の整合を取りつつ、開始を決定した対応活動に必要な要員を指名し、情報システムの業務継続の体制を確立する。		

各項目を実施後、チェック欄にチェックを入れる。補足欄には、必要に応じて復旧手順の補足事項を記載する。

（ケース2：就業時間外、夜間･休日の場合）

＃	復　旧　手　順	ＣＫ	補足
1	自己及び家族の安全の確認： ◇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。		
2	自動参集対応： ◇震度５強以上の地震の場合、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。 ◇既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、全庁ＢＣＰ〈地震編〉に定める基準に準ずる。 ◇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、全庁ＢＣＰ〈地震編〉に準ずる。		
3	職員その他関係する要員の参集状況及び安否の確認： ◇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。 ・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。 ◇安否が確認できない職員がいる場合、災害時伝言ダイヤル（１７１）を活用し、部門番号（****）で登録された情報が無いかを確認する（なお、平常時より１７１は災害時に活用するよう、あらかじめ職員に周知すること）。 ◇ＩＣＴ部門責任者は、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は、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。		緊急連絡先リスト

4	重要書類・データ類の保護： ◇執務室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	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。		
6	外部事業者、保守事業者との連絡確保： ◇至急対応を要請すべき外部事業者、保守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。 ◇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。		事業者連絡先一覧
7	被害状況の調査： ◇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	業務継続・代替復旧活動の開始判断： ◇ＩＣＴ部門責任者は、被害情報の報告結果及び要員の参集状況を考慮して、どのような業務継続の対応活動を開始するかを判断する（一部の業務継続の活動の開始の判断は、例えば情報が十分に揃うまで、後刻に先送りすることも考えられる。）。 ◇全庁の災害応急・復旧活動の整合を取りつつ、開始を決定した対応活動に必要な要員を指名し、情報システムの業務継続の体制を確立する。		

(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、各復旧チームが主体となり実施する。

＃	復　旧　手　順	ＣＫ	補足
9	予想復旧時間の見積もり： ◇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	災害対策本部との連絡： ◇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	復旧方針の検討： ◇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	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。 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。		
13	システム復旧準備： ◇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	システム復旧作業計画： ◇新庁舎が利用できない場合 ＩＣＴ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。 ◇ＩＣＴ部門責任者は代替機器の調達を指示する。 各チームリーダーは、損壊し調達又は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。		
15	<u>システム復旧：</u> ◇ＩＣＴ部門責任者は、システム復旧の作業計画に基づきシステムの復旧を各チームリーダーに指示する。各チーム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 各チームリーダーは、作業の進捗状況を必要に応じ随時にＩＣＴ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 各チームリーダーは、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、ＩＣＴ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（ex.パスワードなど）を明確にして報告する。		
16	<u>復旧システムの運用開始：</u> ◇復旧システム開始判断 ＩＣＴ部門責任者及び各チーム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、再開について防災課に確認する。 ◇復旧システムの利用開始 ＩＣＴ部門責任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、ＩＣＴ部門責任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。		
17	通常システムへの復帰： ◇通常システムへの復帰判断 ＩＣＴ部門責任者は、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う。 ◇通常システムへの復帰 ＩＣＴ部門責任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。 ＜復帰する場合＞ 復帰するための作業計画を各チームリーダー、外部事業者又は保守事業者と策定し、業務部門との調整を経て、防災課の承認を得る。		
18	ＩＣＴ部門の業務継続計画書の見直し： ◇ＩＣＴ部門責任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。		

(4) 参照文書リスト

No.	文書名	管理者	保管場所
1	情報セキュリティ対策基準	最高情報統括責任者	情報システム課
2	情報セキュリティ実施手順	課情報セキュリティ管理者	各システム主管課
3	緊急時参集ルール	防災課長	防災課
4	緊急連絡先リスト	ＩＣＴ部門責任者	情報システム課
5	事業者連絡先一覧	ＩＣＴ部門責任者	情報システム課

※当リストは、情報セキュリティ確保のため、非公開情報とする（３を除く。）。

(5) 緊急連絡先リスト

ＩＣＴ部門責任者は、ＩＣＴ復旧チームの緊急連絡リストを作成する。

氏名	所属	業務継続における役割	居住地			電話番号			メールアドレス	
			住所	庁舎までの距離	参集手段	職場	自宅	携帯電話	職場	携帯電話

※当リストは、個人情報保護及び情報セキュリティ確保のため、非公開情報とする。

(6) 事業者連絡先一覧

ＩＣＴ部門責任者は、事業者連絡先一覧を作成する。

No.	システム又は機器名称	事業者	責任者（平常時）	所在地	電話番号（平常時）	メールアドレス（平常時）
		担当部署	責任者（緊急時）		電話番号（緊急時）	メールアドレス（緊急時）

※当リストは、個人情報保護及び情報セキュリティ確保のため、非公開情報とする。

(7) 被害チェックリスト

確認者：　　確認日時：　　月　　日　　時　　分

○項目１：全体チェックシート

分　類	項　　目	被　　害	確　認　方　法
要員安否	死者	名	◇就業時間内は点呼で、時間外は電話等で確認する。 ◇就業時間内は来客、外部要員、帰宅・休暇要員の安否を確認する。 ◇死者、行方不明者、負傷者に該当者がいる場合は、氏名も記録する。
	行方不明者	名	
	負傷者	名	
	ＩＣＴ部門の参集者（在勤者）	名	◇参集者の氏名も参考として記入する。
	参集可能との連絡があった者	名	
ライフライン（庁舎への供給）	電気	あり／なし	◇庁舎管理部門が把握している情報を確認する（自ら確認しても良い。）。
	ガス	あり／なし	
	水道	あり／なし	
庁舎	新庁舎（入館可能か否か）	あり／なし	◇庁舎管理部門が把握している情報を確認する。
	本庁舎（入館可能か否か）	あり／なし	
	電算センター	あり／なし	
	電源設備	あり／なし	
	空調設備	あり／なし	
	通信設備	あり／なし	
コンピュータ機器、媒体	サーバ設備等の物理損害	あり／なし	◇目視で外観上の破損、異常ランプの点灯、出火、漏水、異臭などがないかを確認する。被害がある庁舎内に入る場合はできる限り複数名で行動する。
	ネットワークの損害	あり／なし	
	磁気媒体（電算センター内）	あり／なし	
	磁気媒体（各主管課書庫等）	あり／なし	

システム稼働状況	電算センター内に格納しているシステム及び機器	あり／なし	◇システム又は機器単位に損害状況を調査する。 ・電源がＯＮとなっているか。 ・異常ランプが点灯していないか。 ・コンソールに異常メッセージが出力されていないか。 ・端末から接続可能か。 ・出火、異臭がないか。 ・外観からわかる破損がないか。

○項目２：稼働環境の確認

分類		調査項目	状況	確認方法	行動補足
電源装置	1	停電していないか。	あり／なし	ＩＣＴ部門の担当が、目視で確認する。	庁舎管理部門から情報収集する。
	2	配電盤、ブレーカーの稼働状態に問題はないか。	あり／なし		故障があった場合、庁舎管理部門へ復旧作業を依頼する。対応可能な期日を確認すること。
	3	ＵＰＳ装置の損害・故障はないか。	あり／なし		被害がある場合は、事業者へ連絡する。
空調装置	1	水冷式の場合、冷却水の温度、圧力に異常はないか。	あり／なし	ＩＣＴ部門の担当が、目視で確認する。	故障があった場合、事業者へ復旧作業を依頼する。通気など可能な限りの対策を実施し、必要とあれば優先度の低いサーバの稼働を一時停止する。
	2	空調システムの明確な物理的損害はないか。	あり／なし		
	3	漏水していないか。	あり／なし		

○項目３：ネットワーク個別確認リスト

項　　目	ホスト名	確認ＩＰアドレス	確認結果 (問題があるか)
庁舎内接続			あり／なし
出先機関の接続			あり／なし

※当リストは、情報セキュリティ確保のため、非公開情報とする。

○項目４：情報通信機器個別確認リスト

機器別に以下の確認優先順位に沿って状況を確認する。被害がある場合は、わかる範囲で復旧の見込み時間を記入する。

①機器が転倒又はフリーアクセスフロアの陥没により落下していないか。
②機器が大きく位置ずれていないか。
③外観からわかる破損がないか（異常ランプの点灯の有無も調べる）。
④水没や消火時の放水等による水損又は出火の際の発煙、塵等による汚染、異臭がないか。
⑤空調機器から漏水していないか。
⑥電源ケーブル、ネットワークケーブルが離脱していないか。
⑦電源が入っているか否か。

電算センター内ラック名	システム又は機器名	①	②	③	④	⑤	⑥	⑦	復旧見込み時間

※当リストは、情報セキュリティ確保のため、非公開情報とする。

6　リソースの現状（脆弱性）と代替の有無

各種資源の状況評価

２０１０年１０月現在の葛飾区の情報システムその他のリソースの現状とバックアップ等についての有無は以下のとおりである。

○庁舎（建物）の状況

	新庁舎	本庁舎
庁舎の建築時期	１９７８年	１９６２年
新耐震基準	未	未
耐震補強の有無	無	有
耐震診断の結果	○	○
洪水ハザードマップによる危険の有無（浸水予想区域内か否か）	予想区域内	
周辺からの延焼の可能性	火災危険度ランク３	

○電算センター内のシステム

No.	システム情報			サーバの状況		ソフトウェア対策			データ対策			運用体制			
	システム名	ネットワークの種類	ソフト保守事業者	ラック名	冗長化の有無	バックアップの有無	バックアップ保管場所	外部保管の有無	バックアップの有無	バックアップ保管場所	外部保管の有無	バックアップの頻度	運用担当職員数	非常用連絡手段として、運用担当職員の連絡先を一元管理しているか。	システムの運用業務を業者に委託しているか。

・バックアップデータが無事でもサーバが使用不能の場合は、システム処理ができず、業務を継続することができない。データセンターの活用などを検討する必要がある。

※当リストは、情報セキュリティ確保のため、非公開情報とする。

○システム機器設置場所の状況

	電算センター	新庁舎	本庁舎
主な設置機器	サーバ、デスクトップパソコン	デスクトップパソコン	デスクトップパソコン
建物の耐震性	IS値0.77以上	IS値0.77	IS値0.72
システム機器の耐震対策の実施状況（固定しているかなど）	サーバはアンカーボルトによる固定	固定なし	固定なし
フロアの防火対策	ハロゲン化消火装置	消火器による初期消火 屋内消火栓による消火	消火器による初期消火 屋内消火栓による消火
フロアの水防対策	浸水予想区域外（問題なし）	浸水予想区域外（２階以上問題なし）	浸水予想区域外（２階以上問題なし）

・本計画の対象機器の設置場所の耐震、防火及び水防対策は概ね良好である。

○ネットワークの状況

集積ハブなど主要ネットワーク機器は新庁舎に設置されている。耐震対策済み。ただし、一部のネットワーク機器の二重化はされていないため、ネットワークが断線した場合は電算室以外の端末からシステムにログインできない可能性がある。庁舎間のネットワークケーブルが断線した場合、当該庁舎でのシステム利用ができなくなる。

○ＩＣＴ部門の参集可能性の評価

夜間・休日に被災した場合、遠隔地に居住の職員は参集できる可能性が低いほか、被災の状況によっては参集できない要員がいるため参集可能性はさらに低下する。代替・復旧活動の遂行において、要員は必須であり、今後全庁ＢＣＰの庁内応援体制の構築の中で検討する必要がある。

○ 外部事業者との関係

A．契約事項について	災害時を含むサービス稼働率に関する取決め事項があるか。	なし
	一定の被害が起きた場合に、担当者の参集時間に関する取決め事項があるか。	なし
	災害によるサービス提供停止や被害が免責事項となっているか。	免責
	一定以上の被害が起きた場合に、代替機器を提供するなどのサービス継続に関る取決め事項があるか。	なし
B．同時に被害を受ける可能性	地震等の広域災害において、事業者の事務所が同時被災する地域内にあるか。	一部あり
	事務所が同時被災する地域内にあっても、より遠隔に別の支援の拠点あるか。	一部あり
C．契約以外の協力関係	一定以上の被害が起きた場合に、担当者が自動的に参集する決めがあるか。	一部あり
	災害時用に保守事業者の要員の連絡先を把握しているか。	あり
	保守事業者の要員に直接連絡できるような取決めをしているか。	一部あり

・外部事業者に運用委託している情報システムが多いので、非常時における事業者からのサポートの有無が、情報システムの運用継続や復旧に大きく影響する。
・委託先担当者との連絡体制については、確立しているシステムが多い。
・契約において明確に非常時のサポートを規定しているシステムは少ないので、今後、契約内容を見直すことが望まれる。
・事業者との協議事項として、契約以外の協力関係について話し合っておく。

○電力供給、通信手段に関するリスク

A．電力供給について

	結果
非常用電源が情報通信機器の作動に必要な容量まで準備されているか。	□ あり ■ なし
数時間稼働できるだけの燃料の準備があるか。	□ あり ■ なし
燃料に関する供給契約があるか。	□ あり ■ なし

B．通信手段について

	結果
災害時優先電話が準備されているか。	■ あり □ なし
非常用連絡手段として、ＩＣＴ部門の職員の携帯メールアドレスを一元管理しているか。	■ している □ していない
非常用連絡手段として、保守事業者の要員の携帯メールアドレスを一元管理しているか。	■ している □ していない

7　被害を受ける可能性と事前対策計画

(1) 現状の脆弱性と改善に向けての対策・実施時期

電算センター内のシステムの調査結果を踏まえ、改善に向けての対策・実施時期は、以下のとおりである。

○電算センター内のシステム

システム名	対象項目	現状レベル（脆弱性）	対策・実施時期	備　考

※当リストは、情報セキュリティ確保のため、非公開情報とする。

(2) 対策が未決定の問題点一覧

問題点の内容	現状レベル	当面の対策と効果	検討スケジュール	備　考
代替手段	中	内部事務は、システム化以前の事務処理をすることを全庁で取り決めをする。住民サービスは、情報システムが復旧するまでの処理内容を検討し、できるだけ業務を継続する措置を施す。	全庁ＢＣＰ〈地震編〉と合わせ、順次行う。	
災害時における事業者の支援体制	中	災害時の復旧支援について、保守事業者や外部事業者との支援体制を確立させる。	新規契約や契約更改の時期に合わせ、順次行う。	
情報システムの冗長化	低	クラウドコンピューティングに代表される最新の技術やサービスを取り入れ、順次セキュリティが強固なデータセンターの活用を検討する。	システムのリプレイス時期	

(3) 必要最小資源

必要資源			発生後必要数量 1日	3日	7日	予想被害	既存の代替手段 代替	代替方法
庁舎	新庁舎		1	1	1	・被害なし（想定以上の場合は損壊の可能性あり）	―	―
要員	職員（インフラ担当）		2	2	2	・全庁ＢＣＰ〈地震編〉に準ずる。	有	・登庁した職員は、交代要員が来るまで退庁しない。 ・２交代制の復旧体制を取る。
	職員（住民情報系システム担当）		2	8	8			
	職員（内部情報系システム担当）		1	3	3			
	職員（各課住民情報系システム担当）		22	22	22			
	職員（各課内部情報系システム担当）		63	63	63			
	外部事業者		2	3	3	・交通機関が停止している場合は、全員は当日参集できない。	有	・災害時の取り決めを協議しておく。
	保守事業者		1	1	1			
	運用事業者		2	7	7			
機器・設備・備品	電算センター（57システム）	インターネット運用	1	1	1	・被害なし（想定以上の場合は損壊の可能性あり）	有	・データは外部保管データから復旧させる。 ・データセンターの利用を検討する。
		NW運用監視	1	1	1			
		バッチスケジュール管理	1	1	1			
		業務システム	19	19	19			
	ネットワーク機器		1	1	1	・被害なし（想定以上の場合は損壊の可能性あり）	無	・代替機の検討をする。

	パソコン（予備機） 内部情報系40台 住民情報系10台	50	50	50	・各所属のパソコンが損壊し、代替機が必要になる。	有	・代替機を提供する。
データ・文書	ＩＣＴ部門業務継続計画書	1	1	1	・被害なし（想定以上の場合は損壊の可能性あり）	有	・紙文書と電子データの両方保管する。
	サーバ運用マニュアル	1	1	1			
	システム運用マニュアル	1	1	1			
	ネットワーク設定情報文書	1	1	1			
	ネットワーク運用マニュアル	1	1	1			
インフラ	ＬＡＮケーブル	1	1	1	場所によっては事務室内のＬＡＮケーブルが断線する。	有	・交換用ケーブルを用意している。
	インターネット回線	1	1	1	・被害なし（想定以上の場合は接続不可の可能性あり）	無	・回線の二重化を検討する。
	広域イーサネット回線	1	1	1			
	電子メール	1	1	1	・被害なし（想定以上の場合はサーバ被災の可能性あり）	有	・データは別途復旧
	認証システム	1	1	1			
	ファイアウォール	1	1	1			
	ウィルス対策システム	1	1	1			

8　計画の運用体制

(1) 運用及び検討体制

ア　体制

本計画における基本的な役割を以下のとおり定める。全庁での体制と関連して運用維持作業を遂行する場合は、報告ルートを確認の上、運用維持作業を進める。

区 分	役 割	備 考
ＩＣＴ部門責任者	・本計画の運用の責任 ・ＩＣＴ部門の教育、訓練の実施統括 ・ＩＣＴ部門の対策の実施と対応状況の確認	
ＩＣＴ部門メンバー	・平常時の本計画の維持管理 ・本計画の定期点検（毎月）、年次見直し ・個別対策の状況の把握・改善・確認 ・訓練の実施	

イ　計画の見直しについて

本計画は、以下のとおり定期的に見直しを行う。

・定期的に最新性、正確性をチェックする。
・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、次に掲げる事項の状態になった場合に計画の見直しを行う。

・組織体制に大きな変更があった場合
・保守事業者に大きな変更があった場合
・主要な情報システムに大幅な変更があった場合
・国又は都の制度変更により改訂の必要がある場合

ウ　承認ルール

本計画を改訂した場合及び定期見直しを実施した場合（更新内容が無い場合も含む。）は、ＩＣＴ部門責任者に承認をもらい、「計画の新規発行／改訂記録」に記述する。

エ　見直し項目

チェック	点　検　項　目	補　　足
□	人事異動、組織の変更による業務継続要員の変更がないかを確認する。	
□	各要員やベンダ等の電話番号やメールアドレスの変更がないかを確認する。	
□	計画を変更した場合、計画に関連する文書がすべて最新版に更新されているかを確認する。	

□	復旧用の媒体、復旧手順書が予定どおりに準備されているか（破損等がないか）を確認する。	
□	ＵＰＳ（無停電電源装置）、非常用通信手段が問題なく使用できるか点検する。	
□	取引関係の変更などにより、協力関係を構築すべき外部事業者に変更がないかを確認する。	
□	机上訓練、連絡・安否確認訓練などの訓練が計画どおりに実施されているかを確認する。	
□	訓練実施により判明した要改善点の反映が確実に行われているかを確認する。	
□	新たなシステムの導入による計画の変更の必要性はないか確認する。	
□	検討された課題への対策案が確実に実施されているか。責任部門や対応スケジュールが未定のものは予算編成時に予算化するとともに、上位者、組織との相談が必要な案件については上位者と対応を相談する。	
□	重要な外部事業者の業務継続（協力体制の構築）への取組みの進捗を確認する。	
□	既に検討した前提とは異なる事象（災害・事故）を想定した計画検討の必要性を確認する。	
□	現時点で対象範囲外とした情報システムがある場合、対象を広げる必要性を検討する。必要があれば、検討スケジュールを立案し、策定状況を継続的に管理する。	
□	外部環境の変化や情報システムの変更などにより選定した重要システム・インフラに変更がないか分析結果の見直しを行う。	

注）組織の変更、人事異動の状況を見て、見直しのタイミングは適宜決定する。

新たなシステムの導入による計画の変更については、基本的に新たなシステムの導入時に見直しを行い、年次の見直しはその確認、補完とする。

(2) 訓練計画

訓練名称	訓練の概要	実施者	時　期	備　考
机上訓練	各要員は、本計画を読み、緊急時にすべき行動を確認する。	情報システム課職員、各課システム担当者、保守事業者等	毎年1回	各課
緊急連絡、安否確認訓練	緊急連絡先リストにより、ＩＣＴ復旧チームとの連絡を付ける。	情報システム課職員、各課システム担当者、保守事業者等	全庁ＢＣＰ〈地震編〉の訓練時	情報システム課
システム復旧訓練	バックアップデータからリカバリできるか、どの程度の時間を要するか検証する。	情報システム課職員、各課個別システム担当者、保守事業者等	適宜	情報システム課、個別システム主管課

9　計画の実効性を高めるために検討すべき事項

(1) 各情報システムの対策マニュアルの作成

本計画では、本区の情報システムの現状を踏まえて対策の方向性を示したに過ぎない。実際に大地震が発生したときには、担当職員が（あるいは担当外の職員が）何から手を付ければ良いのか、具体的な作業手順が書かれているマニュアルが必要である。

(2) ＩＣＴ復旧チームの要員の確保

災害時優先業務を実施・継続させるためには、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前提となる。そのためには、ＩＣＴ復旧チームの要員の確保が必要であり、今後全庁ＢＣＰの庁内応援体制の構築の中で優先的に検討する。

(3) 短期・中期的な対策の検討

通常の保守契約において大地震等の天災事変は、不可抗力の免責事項に該当するため、災害時の保守内容について取り決めをしていないことがある。保守事業者に業務継続計画（ＢＣＰ）の整備を依頼し、大地震が発生した際の復旧手順を確立する。

(4) 長期的な対策の検討

情報システム課の主要なシステムを収容している電算センターは、想定を超えた巨大地震により大きな被害を受けることもあり得る。その場合、現状ではセンターの代替施設はないので、バックアップデータを活用することができず、情報サービスが長期間にわたり停止することになる。

このことを踏まえてクラウドコンピューティングの活用やデータセンターの利用など長期的な対策を検討する必要がある。