葛飾区ICT部門業務継続計画
（ICT-BCP）

令和４年９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２３年３月３１日	新規制定
第２版	令和４年９月７日	区の情報システム環境の変更、BCP〈水害編〉の制定及び情報セキュリティ等その他脅威への対応検討の反映に伴う改訂

【本計画の保管について】

（１）本計画を印刷したものを情報システム課内の書庫に保管する。

（２）情報システム課職員は、本計画を業務用スマートフォンに電子データで保存し、いつでも閲覧できる状態にしておく。

目次

１　計画の目的・基本方針

（１）計画の目的と位置付け

東日本大震災のような大地震、近年激甚化している台風や豪雨のような風水害といった災害が発生した場合においても、区は災害時優先業務を実施・継続させることが求められている。そして、今やその業務の前提となっている業務システム、業務端末、プリンタ、ネットワーク等（以下「情報システム」という。）の稼働は必要不可欠である。

また、ICT利用に関して発生しうる事象であるサイバー攻撃（※）や情報システム障害等（以下「情報セキュリティ事象」という。）が発生した場合においても、区は業務を実施・継続することが求められる。

このような可能性がある中で、情報システム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。したがって、あらゆる事態における想定を行い、事前に備えておくことが極めて重要である。

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。）」及び「葛飾区業務継続計画（BCP）〈水害編〉（以下「全庁BCP〈水害編〉」という。）」並びに「葛飾区情報セキュリティポリシー（※）（以下「セキュリティポリシー」という。）」及び「葛飾区デジタル技術を活用した区政の推進及び情報システムの管理運営に関する規則（平成17年規則第46号）」に基づき、ICT部門における対応の基本方針や業務停止を伴うリスク検討などについて定める「葛飾区ICT部門業務継続計画（ICT-BCP（※））（以下「本計画」という。）」を策定するとともに、本計画を基に実際の動きを具体化したマニュアルを別に整備し、有事の際に各種業務の実施・継続を迅速に行うための体制を整えることを目的とする。

なお、本計画は先述の全庁BCP等を前提として策定するものであるが、実際にはこれだけでなく、その他の関連計画等も参照している。このことについて、本計画の位置付けを以下の図に示す。

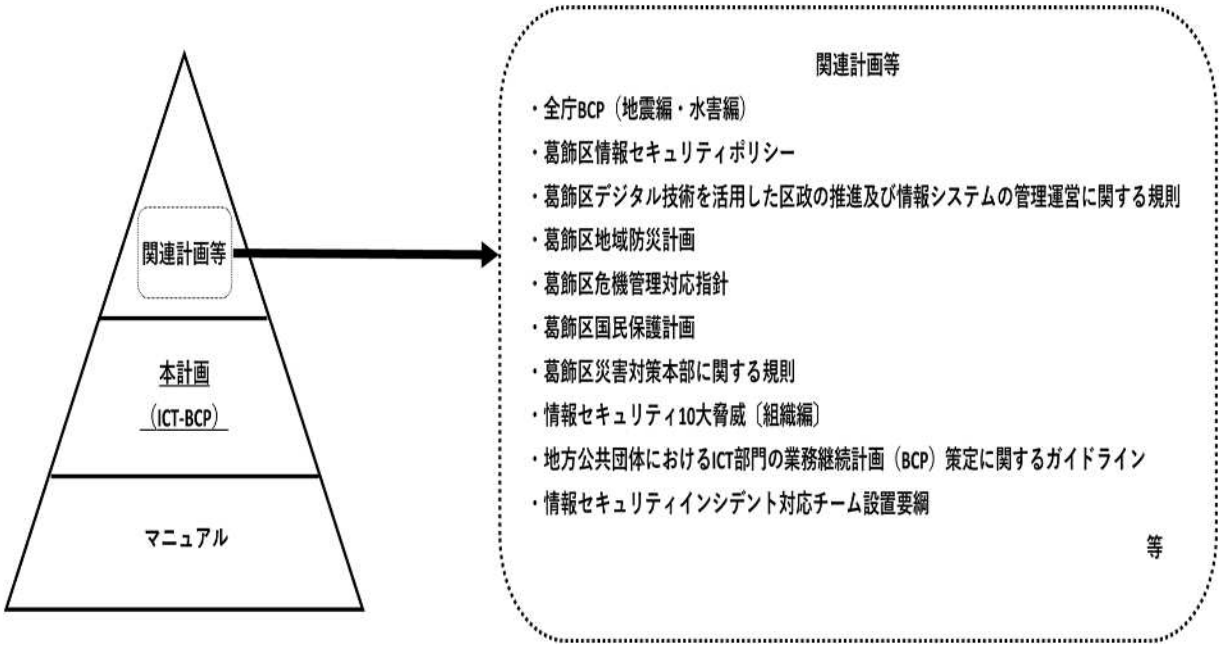


図　本計画の位置付け

（２）見直しの背景

本区では、平成23年３月に本計画の初版を策定したが、その後、情報システムに係るハードウェアの庁舎内電算センター（※）からデータセンターへの移行や業務端末環境の仮想化（※）を行うなど、区を取り巻く情報システム環境は大きく変化している。

これらの対応は、災害時の業務継続を目的の一つとしているとともに、区が直接管理するハードウェアを減少させることにより、復旧業務における役割の分担やリスクの分散を実現することが可能となっている。

また、本区では平成23年３月に策定された全庁BCP〈地震編〉に加え、令和３年３月に全庁BCP〈水害編〉が新たに策定され、水害時における区としての災害時優先業務が掲げられている。

さらに近年、国や他自治体、民間企業などにおいて悪意のある者からのサイバー攻撃等によって情報システムの利用に影響が出るといった情報セキュリティ事象の被害も発生している。その他、甚大な自然災害、大規模事故等、新型インフルエンザ等健康危機などの発生も考えられる。

これらを受けて、改めてリスクの想定や対策を講ずる必要があるため、見直しを行うこととした。

（３）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	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業務で利用する情報システムを早期復旧・継続させる。
来訪者、職員及び関係者の安全	執務室等への来訪者、職員、運用・保守事業者、その他の関係者の安全及び生命の確保を第一に優先する。
本計画の実効性の担保と改善	毎年、関係者が参加する訓練を行い、ICT部門として有事の際に備える。また、本計画は、訓練結果や情報システムの更新状況等を踏まえ、定期的に（「（４）計画策定の前提」に大きな変更があればその都度）見直しを行うとともに、適切に関係者に周知する。
運用・保守事業者（※）等との協力体制の確立	情報システムの早期復旧・継続に当たり、運用・保守事業者等と協力する体制を確立する。

（４）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端末、プリンタ及びネットワーク（機器を含む。）並びにデータセンターで稼働している業務システムとする。ASP（※）や独自ネットワークでシステムを構築しているものなど、各業務所管課が個別に管理をしている業務システムについては、本計画を踏まえ、情報システム課がインシデント（※）対応等について助言をしたうえで、個別に復旧手順や業務継続を定める。

イ　葛飾区における被害想定

災害については、地域防災計画の被害想定と同様とする。地震では、最も被害が見込まれる東京湾北部地震（首都直下地震）を想定する。また、風水害では、河川の氾濫（外水氾濫）や下水処理が追い付かないことによる氾濫（内水氾濫）を想定する。

情報セキュリティ事象については、IPA（※） が公表する「情報セキュリティ10大脅威（※）〔組織編〕」を踏まえることとする。具体的には、ランサムウェアや標的型攻撃、情報システム障害など区の環境において発生する可能性があるものを想定する。

その他、甚大な自然災害、大規模事故等並びに新型インフルエンザ等健康危機については、「葛飾区危機管理対応指針」を踏まえることとする。

ウ　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）を踏まえるとともに、その他の様々な脅威に係る検討も加えたものである。

２　情報システム環境の現状とリスク

（１）情報システムに係るインフラ（※）環境の現状

本区の情報システムに係るインフラ環境は、以前は庁舎内の電算センターにサーバ機器（ハードウェア）などを設置していたが、平成 25 年度から順次、区が調達したサーバ機器などを耐震対策がとられた民間のデータセンターに移設した（第１次インフラ統合基盤の構築）。さらに、令和元年度には、区がサーバ機器などを所有せず、インフラ環境をサービスとして利用する環境に移行した（第２次インフラ統合基盤の構築）。

これによって、従前はサーバ機器などが故障した際、新たに機器を調達してから設定を行わないとシステム利用ができなかったが、インフラ環境をサービスとして利用する環境へ移行したことで、特定のサーバ機器などに依存しないため、その手順を省略化できるようになった。また、区の庁舎が被災した場合でも、立地や建物の災害対策が講じられたデータセンターを利用することで、リスクの低減が図られ、情報システムを停止することなく利用できる可能性を高めることができた。

なお、現在利用しているデータセンターは、震度７（震度階級における最大階級）に耐えられる耐震設計となっている。

（２）情報システムに係る利用環境（端末環境）の現状

本区の情報システムに係る利用環境（端末環境）は、令和元年度から令和２年度にかけて行った端末の更改において、端末環境の仮想化（仮想デスクトップ化）を行った。このことにより、端末に紐づいた環境ではなく、利用者に紐づいた端末環境を実現した。このため、同一利用者であれば、どの端末からでも同じ業務環境にアクセスすることができ、情報システムを利用できるようになったため、災害時に特定個人が使用していた端末が使用できなくなった場合においても、別の端末で業務継続が可能になっている。

また、令和３年度には端末へのテレワーク設定を行い、庁舎外からでも同じ業務環境にアクセスできるようになった。このことにより、庁舎が被災した際も代替施設等から端末を活用することが可能となっている。

なお、本区では情報セキュリティ対策として、国の要請に基づき三層分離を行っており、各環境には認証機能を設けている。内部の業務環境である総合行政ネットワーク（LGWAN）（※）環境とインターネット環境は無害化通信を適用することでリスクを分断し、住民情報を取り扱う環境は他の領域と完全に分離することで、ネットワークを経由した攻撃リスクを極力低減させている。

（3）現状におけるリスク

地震や風水害については全庁 BCP〈地震編〉及び全庁 BCP〈水害編〉、情報セキュリティ事象については IPA が公表する「情報セキュリティ 10 大脅威〔組織編〕」を前提として、事象別のリスクを以下に記述する。

ア　地震の場合

事象（原因）	想定されるリスク
停電の発生	地震により停電が発生すると、情報システム利用の前提となる機器やネットワークが集約されている電算センターへの電力供給ができなくなる。 情報システム機器は稼働に電力が必要であるため、電力供給ができなくなると、情報システムの利用ができない。
断水・管きょ被害（上下水道被害）の発生	地震により断水が発生すると、電算センター内の空調機への給水が断たれ、温度・湿度管理ができなくなってしまう可能性がある。この場合、各種機器の稼働に必要な温度・湿度が保てず、機器が破損し、情報システムの利用に影響が出る。 また、管きょ被害が発生した場合、排水ができず、断水がない場合には電算センター内に漏水する可能性がある。この場合、各種機器が水損してしまうと、情報システムの利用に影響が出る。
通信の断絶	激しい揺れによって通信回線が物理的に切断されることや、庁舎内のネットワーク機器自体が破損してしまうことが考えられる。 被害を受ける場所によって、情報システムの利用ができなくなる範囲が異なる。例えば、本庁舎内一部エリアに設置されているネットワーク機器の破損であれば、一部エリアのみ情報システムの利用ができないだけであるが、電算センターに設置されているネットワーク機器が破損すると、本庁舎内での情報システムの利用ができないという事態になる。 また、庁舎内は問題なくても、通信事業者が管理する回線が被害を受ける可能性があり、このような場合、データセンターとの通信ができないことから、情報システムの利用ができない。 なお、インターネット接続回線が別途用意できる場合は、テレワーク環境から情報システムの利用ができるが、この場合、住民情報を取り扱う環境は使用できないことに留意する必要がある。
庁舎の被災 （立ち入り不可）	激しい揺れによって庁舎自体に立ち入れない場合には、被害箇所を特定できなくなる。このこと

	により、原因の特定が遅れ、復旧に時間を要する。 　また、庁舎への立ち入りができないとなると、庁舎内の端末が使えないため、それらを利用して情報システムを利用することができなくなる。
情報システム課職員及び運用・保守事業者の参集不可	激しい揺れによって公共交通機関が止まったり、職員自身や家族が怪我をしたりすること等で参集することが困難になることが想定される。 　このような場合、災害対策本部からの要請や情報システムの復旧作業に即応できなくなる可能性が高く、場合によっては情報システムの利用に影響を与える。

イ　風水害の場合

事象（原因）	想定される被害と影響
停電の発生	風水害により停電が発生すると、情報システム利用の前提となる機器やネットワークが集約されている電算センターへの電力供給ができなくなる。 　情報システム機器は稼働に電力が必要であるため、電力供給ができなくなると、通信ができず情報システムが利用できない。
断水・管きょ被害（上下水道被害）の発生	風水害により断水が発生すると、電算センター内の空調機への給水が断たれ、温度・湿度管理ができなくなってしまう可能性がある。この場合、各種機器の稼働に必要な温度・湿度が保てず、機器が破損し、情報システムの利用に影響が出る。 　また、管きょ被害が発生した場合、排水ができず、断水がない場合には電算センター内に漏水する可能性がある。この場合、各種機器が水損してしまうと、情報システムの利用に影響が出る。
通信の断絶	暴風によって通信回線が物理的に切断されることや、浸水によって基地局が被災してしまうことが考えられる。 　また、庁舎内は問題なくても、通信事業者が管理する回線が被害を受ける可能性があり、このような場合、データセンターとの通信ができないことから、情報システムの利用ができない。 　なお、インターネット接続回線が別途用意できる場合は、テレワーク環境から情報システムの利用ができるが、この場合、住民情報を取り扱う環境は使用できないことに留意する必要がある。

情報システム課職員及び運用・保守事業者の参集不可	暴風や浸水によって公共交通機関が止まったり、職員自身や家族が怪我をしたりすること等で参集することが困難になることが想定される。 このような場合、災害対策本部からの要請や情報システムの復旧作業に即応できなくなる可能性が高く、場合によっては情報システムの利用に影響を与える。

ウ　情報セキュリティ事象の場合

事象（原因）	想定される被害と影響
サイバー攻撃（ウィルス、ランサムウェア（※）、標的型攻撃（※）、不正アクセス（※）、Dos 攻撃（※）、DDos 攻撃（※）など）	OS（※）・ミドルウェア（※）等のソフトウェアの脆弱性を狙った外部からの攻撃によって不正アクセスを受け、認証情報の窃取や改ざん、保有するデータの破壊・改ざんにより、情報システムが使用できなくなる。添付ファイルメールの開封などによってウィルス感染した場合も同様のことが想定される。 また、Dos／DDos 攻撃により情報システムに過剰な負荷がかかり、情報システムが停止して利用できなくなる。
データセンターとの通信回線障害	データセンターへの通信回線が過剰なネットワーク負荷によってパンクしてしまうことや、メンテナンス作業の不注意などにより、データセンターと庁舎との疎通が断絶し情報システムが使用できない。
情報システム障害	サーバ等の処理能力を超えるような負荷、バッチ（※）処理の異常終了、プログラムの変更適用誤り、誤操作、ソフトウェアや機器の故障や性能劣化などの理由によって、情報システムが使用できなくなる。この場合、影響範囲は特定の情報システムのみの場合もあれば、情報システム全体に影響が出る場合もある。

３　その他の脅威への対応

（１）その他の脅威への対応の重要性

「２　情報システム環境の現状とリスク」において地震や水害、情報セキュリティ事象について検討を行ったが、現実はそれだけに限らず、テロや爆発・危険物事故をはじめ様々な事態が発生する可能性が考えられる。これを踏まえ、あらゆる事態にも対処することができるよう備えておくことが非常に重要である。

したがって、本計画でも想定される脅威と情報システムに係る被害想定の整理を行い、それらへの対処を検討し、実効性を担保していくこととする。

（２）想定される脅威とリスク

想定される脅威は、「葛飾区危機管理対応指針」で掲げる危機事象を前提とし、各事象における情報システムに係るリスクを記載する。

ア　甚大な自然災害（異常気象・火山噴火等）の場合

事象（原因）	想定されるリスク
停電の発生	「２　情報システム環境の現状とリスク（３）現状におけるリスク」に記載の内容に準ずる。
断水・管きょ被害（上下水道被害）の発生	
通信の断絶	
庁舎の被災（立ち入り不可）	
情報システム課職員及び運用・保守事業者の参集不可	

イ　大規模事故（爆発・危険物事故等）、武力攻撃事態、緊急対処事態（テロ等）の場合

事象（原因）	想定されるリスク
停電の発生	「２　情報システム環境の現状とリスク（３）現状におけるリスク」に記載の内容に準ずる。
断水・管きょ被害（上下水道被害）の発生	
通信の断絶	
庁舎の被災（立ち入り不可）	
情報システム課職員及び運用・保守事業者の参集不可	

ウ　新型インフルエンザ等、健康危機（食中毒、感染症等）の場合

事象（原因）	想定されるリスク
庁舎への立ち入り不可	「２　情報システム環境の現状とリスク（３）現状におけるリスク」に記載の内容に準ずる。
情報システム課職員及び運用・保守事業者の参集不可	

（３）対処方針

（２）においてその他の脅威と情報システムに係る被害想定を行ったが、情報システムに係る被害のきっかけとなるのは、機器の故障や通信障害、停電といった情報システムの継続利用が脅かされるような物理的な被害を受ける場合、情報システム課職員や運用・保守事業者が参集できないといった運用の継続体制が脅かされるような人的な被害を受ける場合の２つに大別される。

それぞれの具体的な対応は、また細かく分類することになるが、結果的には、被害規模が大きいとされる地震や水害で発生する事象への対処を組み合わせることで対応が可能と考える。

したがって、各事象に対するマニュアルの整備にあたっては、その組み合わせで対応していくこととする。

４　計画の運用体制と役割

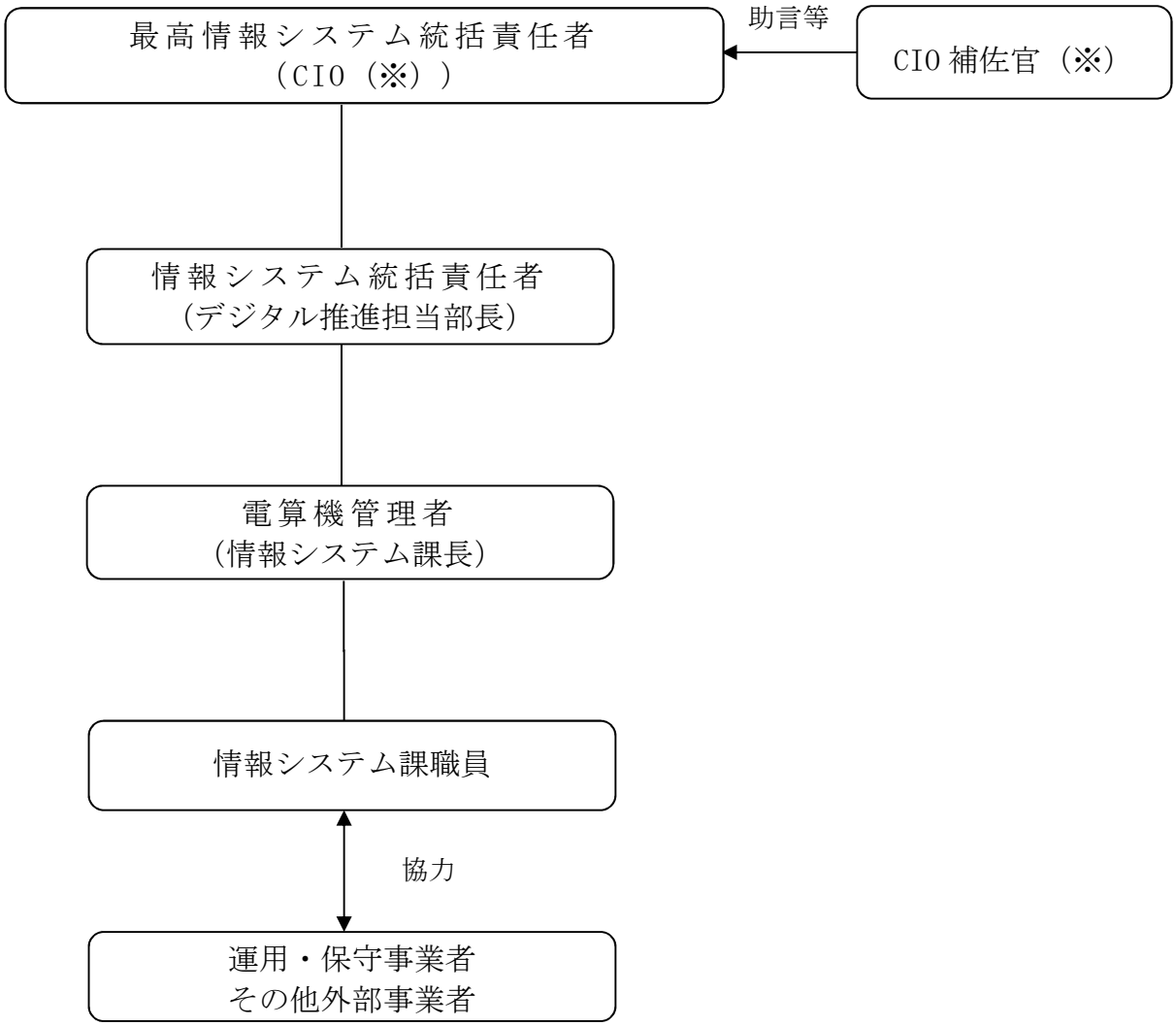
本計画の管理運用に当たり、あらゆる事態が発生した場合においても、迅速な対応が求められることから、平常時や災害時、情報セキュリティ事象発生時それぞれにおいて、必要な体制と役割をあらかじめ整備する。

なお、災害と情報セキュリティ事象が同時に発生した場合は、両体制を並行して構築し対応する。

（１）平常時の体制と役割

平常時における本計画の運用に関する課題整理、対策遂行、検証等を行うため、以下の体制と役割とする。

＜平常時の体制＞



＜平常時の役割＞

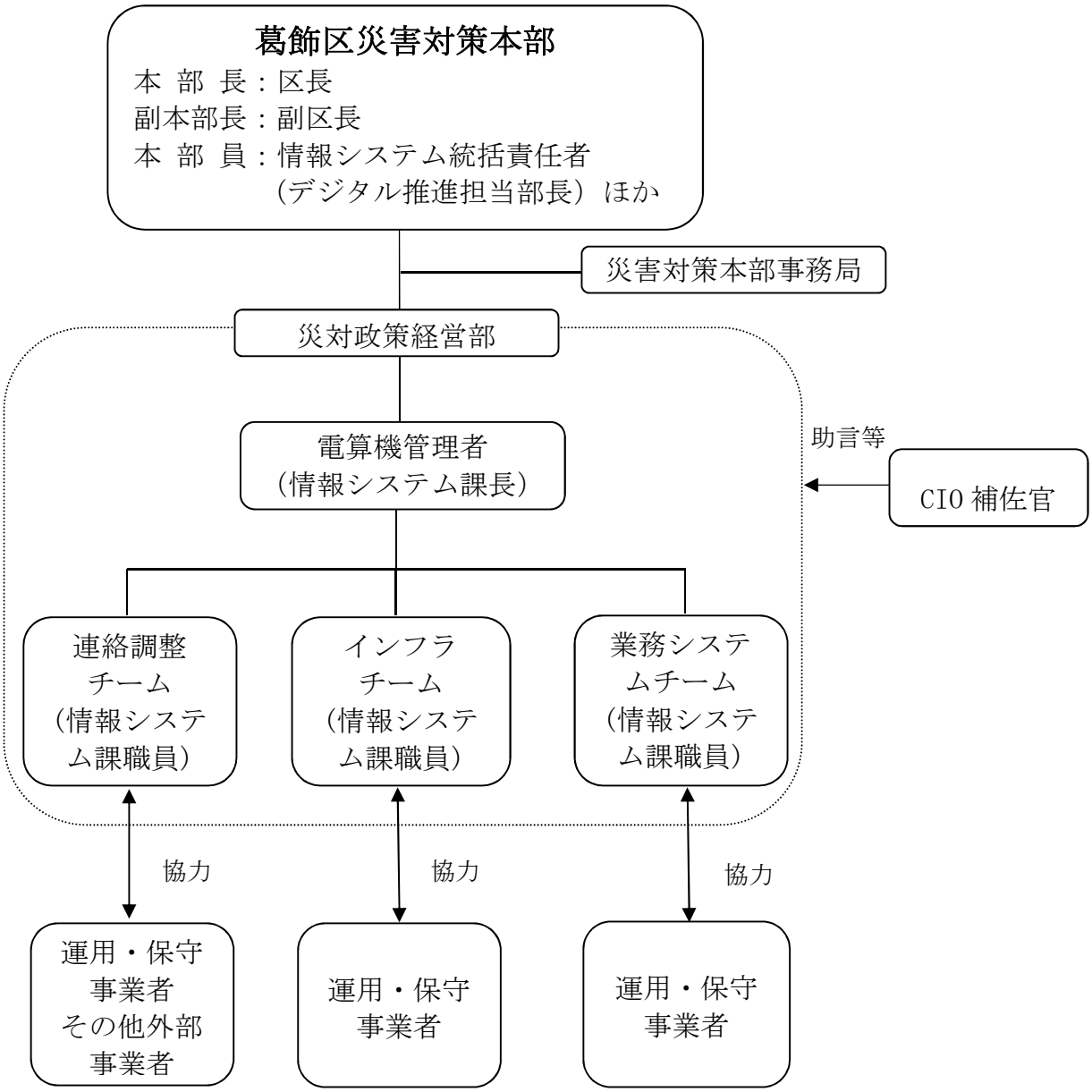
組織	役割の概要	災害対策本部との関係
最高情報システム統括責任者(CIO)（政策経営部を担任する副区長）	葛飾区デジタル技術を活用した区政の推進及び情報システムの管理運営に関する規則に規定される以下を実施する。 ・情報システム統括責任者に対し、情報システムの運用状況について報告を求め、又は必要な措置を講ずること ・本計画の見直しに関すること	副本部長
情報システム統括責任者（デジタル推進担当部長）	葛飾区デジタル技術を活用した区政の推進及び情報システムの管理運営に関する規則に規定される以下を実施する。 ・情報システムの適正な運用の確保に関すること ・本計画の運用に係る課題の把握、対策の実行、検証等の統括に関すること	本部員
電算機管理者（情報システム課長）	葛飾区デジタル技術を活用した区政の推進及び情報システムの管理運営に関する規則に規定される以下を実施する。 ・情報システム課が所管する情報システムの運用及び管理に関すること ・本計画の運用に関する課題整理、対策遂行、検証に関すること	災対政策経営部員
情報システム課職員	・本計画の改訂を行う ・平常時の本計画の維持管理を行う ・本計画の定期点検（年次）を行う ・訓練を実施する	災対政策経営部員

	（年１回以上） ・本計画の下に作成するマニュアルの整備・更新・点検（年次）を行う	
運用・保守事業者 その他外部事業者	・本計画の実行時に区と協力して必要な対応を行う	
CIO 補佐官	葛飾区デジタル技術を活用した区政の推進及び情報システムの管理運営に関する規則に規定される以下を実施する。 ・情報システムに関する事項全般について、情報通信技術の専門的見地から助言を行う ・最高情報システム統括責任者を技術面で補佐する	

（２）災害時（地震・風水害等）の体制と役割

災害が発生し、災害対策本部が設置された場合の対応として、職員が正確に情報を把握し、適切に対応できるようにするため、以下の体制と役割とする。

＜災害時の体制＞



＜災害時の役割＞

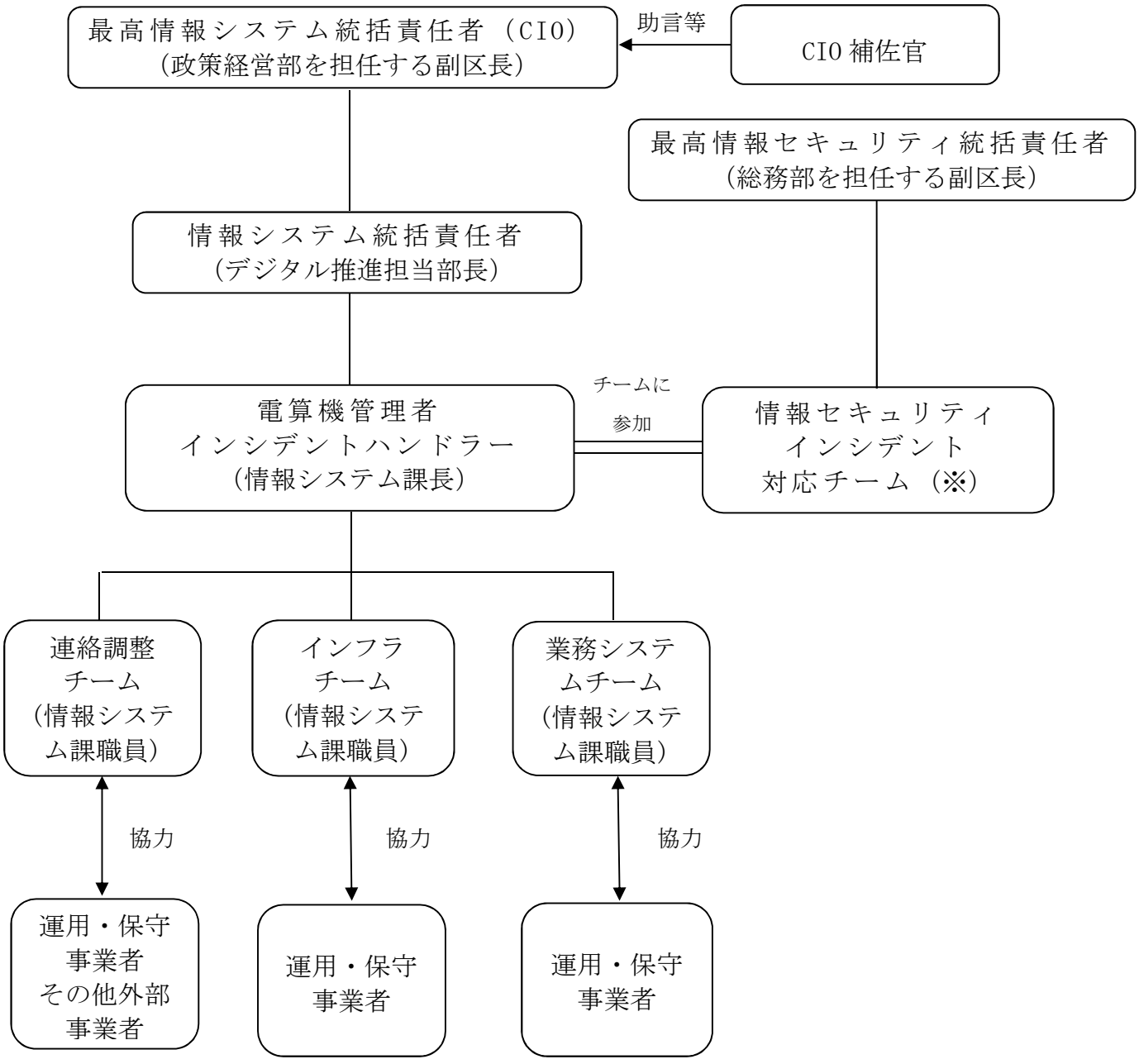
組織	役割の概要
葛飾区災害対策本部	葛飾区災害対策本部に関する規則（平成15年葛飾区規則第54号）に規定される以下を実施する。 ・災害地の被害及び復旧の状況に関する情報を収集すること ・本部及び防災関係機関との連絡及び調整に関すること ・自衛隊法(昭和29年法律第165号)第83条に規定する災害派遣の要請に関し、本部に意見を述べること ・本部長の指示に基づく災害地の災害応急対策の推進に関すること ・前各号に定めるもののほか、緊急を要する災害地の災害応急対策の実施に関すること
災対政策経営部	葛飾区災害対策本部に関する規則及び葛飾区地域防災計画に規定される以下を実施する。 ・災害復旧計画及び復興計画の策定に関すること ・災害対策予算に関すること ・義援金及び義援品の受入れ及び配分に関すること ・電算センター及びデータセンターに設置されている情報システムの保全及び管理に関すること ・葛飾区デジタル技術を活用した区政の推進及び情報システムの管理運営に関する規則第６条第２項第４号に規定する区長が別に定める情報システムの管理に関すること ・被災者生活再建支援システムに関すること
電算機管理者（情報システム課長）	葛飾区デジタル技術を活用した区政の推進及び情報システムの管理運営に関する規則に規定される「情報システム課が所管する情報システムの運用及び管理に関すること」の具体的対応として以下を実施する。 ・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統括、支援依頼
連絡調整チーム（情報システム課職員）	・職員の安否確認 ・災害対策本部事務局からの要請対応や伝達事項の連絡調整 ・庁内や出先施設等からの問い合わせ対応 ・執務室や電算センターの原状復帰等の実施 ・状況に応じた各チームへの人員配置調整

	・被害情報等の把握及び電算機管理者への報告 ・復旧に向けた運用・保守事業者やその他外部事業者との新規契約に向けての連絡調整
インフラチーム（情報システム課職員）	・電算センター内の電源、空調機等の機器設備、庁内ネットワーク（LAN）、通信事業者のネットワーク（回線）、データセンター、インターネット、業務端末やプリンタの状況確認、復旧見込みの報告等 ・被害状況等の連絡調整チームへの報告 ・執務室や電算センターのインフラに係る原状復帰等の実施 ・インフラに係る運用・保守事業者への被害状況の確認及び復旧に向けた協力依頼
業務システムチーム（情報システム課職員）	・各業務システムの被害状況の確認 ・被害状況等の連絡調整チームへの報告 ・執務室や電算センターの業務システムに係る原状復帰等の実施 ・業務システムに係る運用・保守事業者への被害状況の確認及び復旧に向けた協力依頼
運用・保守事業者（外部事業者）	・情報システムに係る被害状況の確認及び復旧に向けて、区と協力し必要な対応を行う
CIO 補佐官	葛飾区デジタル技術を活用した区政の推進及び情報システムの管理運営に関する規則に規定される以下を実施する。 ・情報システムに関する事項全般について、情報通信技術の専門的見地から助言を行う ・最高情報システム統括責任者を技術面で補佐する

（3）情報セキュリティ事象発生時の体制と役割

情報セキュリティ事象発生時においては、葛飾区情報セキュリティに関する規則に基づき策定された「情報セキュリティインシデント対応チーム設置要綱（令和３年４月１日付２総総第 1251 号副区長決裁）」の規定により、初動対応、対策遂行等を行うため、以下の体制と役割とする。

＜情報セキュリティ事象発生時の体制＞



＜情報セキュリティ事象発生時の役割＞

組織	役割の概要
最高情報システム統括責任者（CIO）（政策経営部を担任する副区長）	葛飾区デジタル技術を活用した区政の推進及び情報システムの管理運営に関する規則に規定の以下を実施する。 ・情報システム統括責任者に対し、情報システムの運用状況について報告を求め、又は必要な措置を講ずること
情報システム統括責任者（デジタル推進担当部長）	葛飾区デジタル技術を活用した区政の推進及び情報システムの管理運営に関する規則に規定の以下を実施する。 ・情報システムの適正な運用の確保に関すること
電算機管理者（情報システム課長）	葛飾区デジタル技術を活用した区政の推進及び情報システムの管理運営に関する規則に規定される「情報システム課が所管する情報システムの運用及び管理に関すること」の具体的対応として以下を実施する。 ・情報セキュリティ事象発生時における情報システムの初動対応（情報システムにおける被害状況整理等）、対策遂行などを行う。 ・情報セキュリティインシデント対応チームへの状況報告及び協議を行う。
連絡調整チーム（情報システム課職員）	・情報セキュリティインシデント対応チームへの報告事項のとりまとめなどの調整 ・庁内や出先施設等からの問い合わせ対応 ・被害情報等の把握及び電算機管理者への報告 ・復旧に向けた運用・保守事業者やその他外部事業者との新規契約に向けての連絡調整
インフラチーム（情報システム課職員）	・情報システムに係るインフラ環境の被害状況確認、復旧見込みの報告等 ・被害状況等の連絡調整チームへの報告 ・インフラに係る運用・保守事業者への被害状況の確認及び復旧に向けた協力依頼
業務システムチーム（情報システム課職員）	・各業務システムの被害状況確認、復旧見込みの報告等 ・被害状況等の連絡調整チームへの報告 ・業務システムに係る運用・保守事業者への被害状況の確認及び復旧に向けた協力依頼
運用・保守事業者 その他外部事業者	・状況セキュリティ事象発生時に区と協力して必要な対応を行う。
CIO 補佐官	葛飾区デジタル技術を活用した区政の推進及び情報システムの管理運営に関する規則に規定の以下を実施する。

	・情報システムに関する事項全般について、情報通信技術の専門的見地から助言を行う ・最高情報システム統括責任者を技術面で補佐する。
最高情報セキュリティ統括責任者（総務部を担任する副区長）	・情報セキュリティインシデント対応チームに対し、状況報告を求め、必要な措置をするよう命ずる。
情報セキュリティインシデント対応チーム	情報セキュリティインシデント対応チーム設置要綱に規定の以下を実施する。 ・インシデントの検知及び連絡の受付 ・影響度の判定 ・インシデント対応 ・報告及び公表 ・事後対応

５　緊急時対応・復旧計画

（１）参集ルール等

ア　参集ルール

前提として、本区における情報システム環境は、「２　情報システム環境の現状とリスク」に記載しているように、サーバを外部のデータセンターに移行していることや、端末の個別設定作業が不要になっていることなどから、情報システム課が実施すべき確認作業は、以前に比べ減少している。

また、情報システム課では、情報システムの稼働監視サービスを利用し、異常の検知が即時に把握できるようになっていること、異常を検知した際は職員各自が保持する業務用スマートフォンに連絡が来るようになっていること、当番制で端末を持ち帰っており、システムの稼働状況をいつでもどこからでも確認できるようになっていることなど、来庁しなくても情報システムに係る問題の有無について確認できる体制になっている。

なお、参集対応については、事前の取り決めに基づき運用事業者も参集し対応を実施することになる。

これらを踏まえ、以下のように参集ルールを整理する。

（ア）地震の場合

全庁BCP〈地震編〉に規定のとおり、震度６弱以上で全職員が参集し、震度５強以上で災害対策本部が設置された場合においては全体の40％の職員が参集する。

（イ）風水害の場合

全庁BCP〈水害編〉に規定のとおり、風水害が発生する恐れがあり、区長の指示により災害対策本部が設置される場合には全職員が参集する。

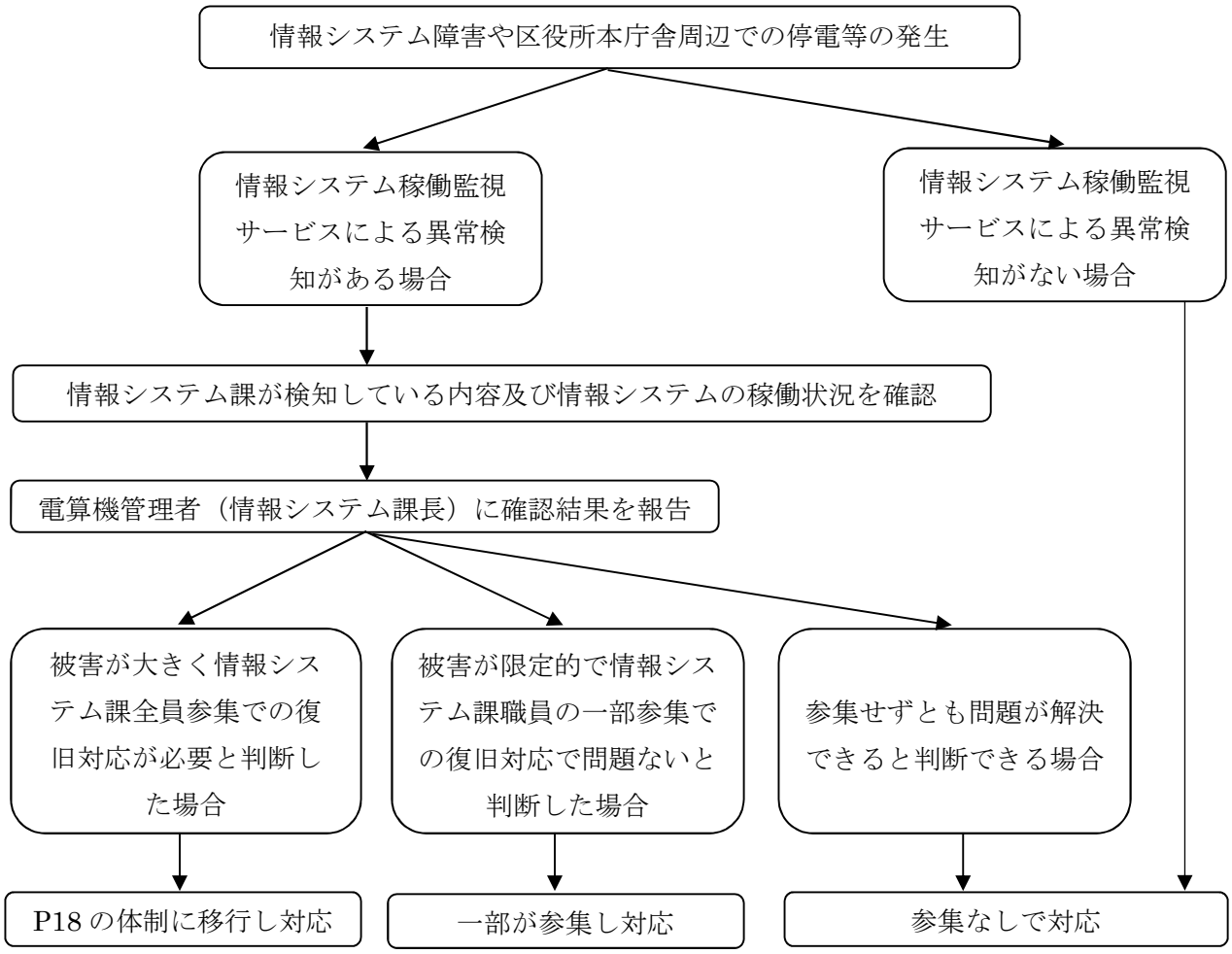
（ウ）情報セキュリティ事象の場合

サイバー攻撃や情報システム障害等が発生した場合は、被害状況次第で参集し対応を行う必要がある。参集条件は、情報システムの利用が脅かされ、庁内の業務継続に支障が出てしまう場合（可能性を含む。）で、参集しなければ問題を解決できないときとする。

この場合において、基本的には電算機管理者の指示により参集することとするが、判断に当たっては、情報システムの稼働監視サービスの状況等を踏まえることとする。また、この場合における情報システム課の対応は小さなエラーから情報システム障害など多岐に渡る。影響が小さいものであれば情報システム課の対応で完結するが、実際に住民影響や全庁に影響が出る大きな障害が発生した場合には、P18「（３）情報セキュリティ事象発生時の体制と役割」に則った対応に移行する。

これらを踏まえた参集ルールフロー図を以下に示す。

〈参集ルールフロー図〉



なお、電算機管理者と連絡が取れない場合は、代行者１がその役割を担当する。責任者及び代行者１のいずれとも連絡が取れない場合は、代行者２がその役割を担当し、代行者２とも連絡が取れない場合は、代行者３がその役割を担当する。

役割	
電算機管理者	情報システム課長
代行者１	情報システム課調整係長
代行者２	情報システム課管理係長
代行者３	電算機管理者があらかじめ指名する情報システム課職員

（エ）その他の脅威の場合

被害の内容により、（ア）～（ウ）に準じて対応することとする。

イ　運用・保守事業者への復旧協力依頼

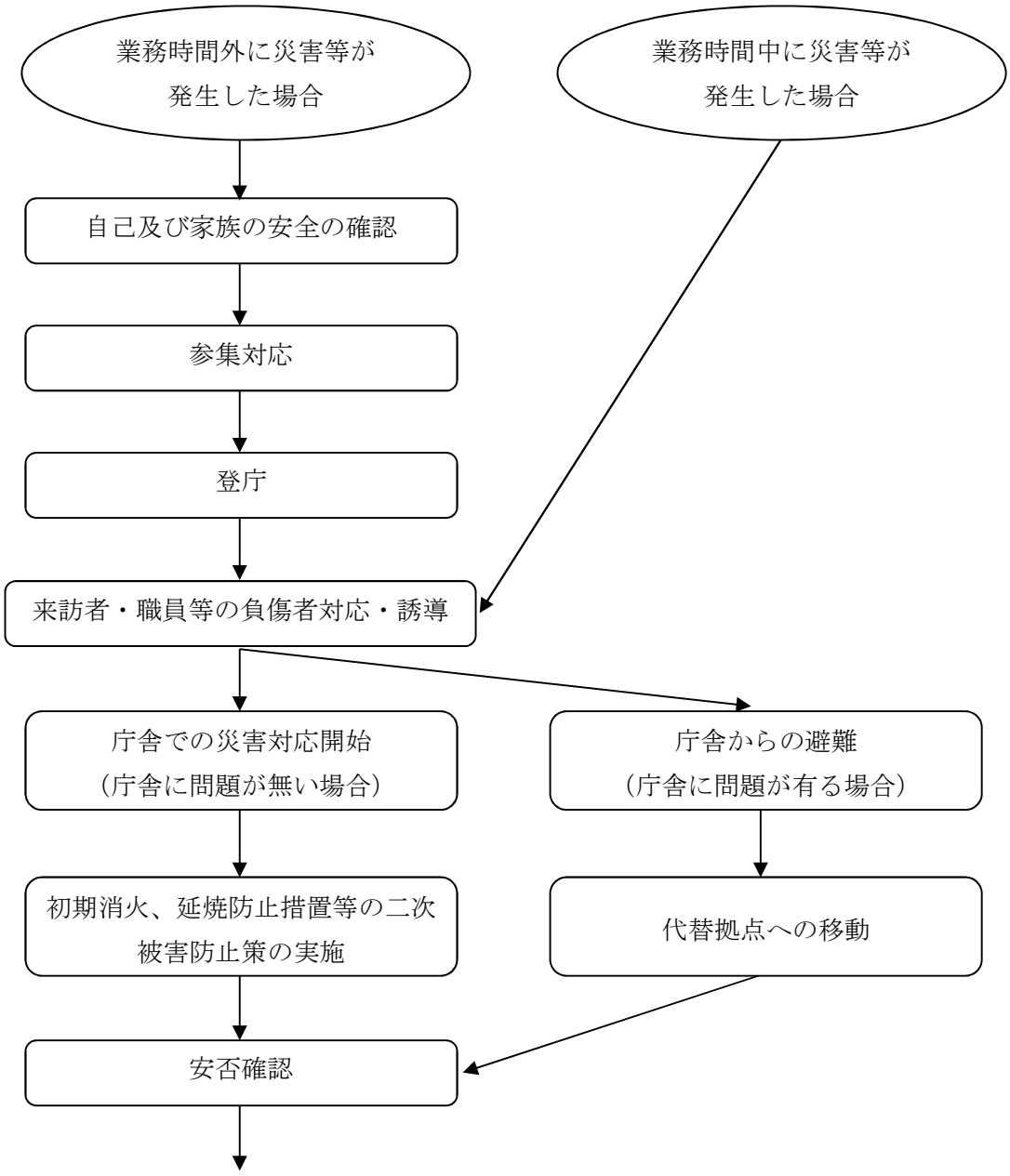
災害や情報セキュリティ事象が発生した場合は、まずは情報システム課職員及び運用事業者による被害状況の確認を行い、障害等の原因を特定するよう努めることとする。その結果、保守事業者での対応が必要と判断した場合には、保守事業者に復旧へ向けた協力依頼を行うこととする。

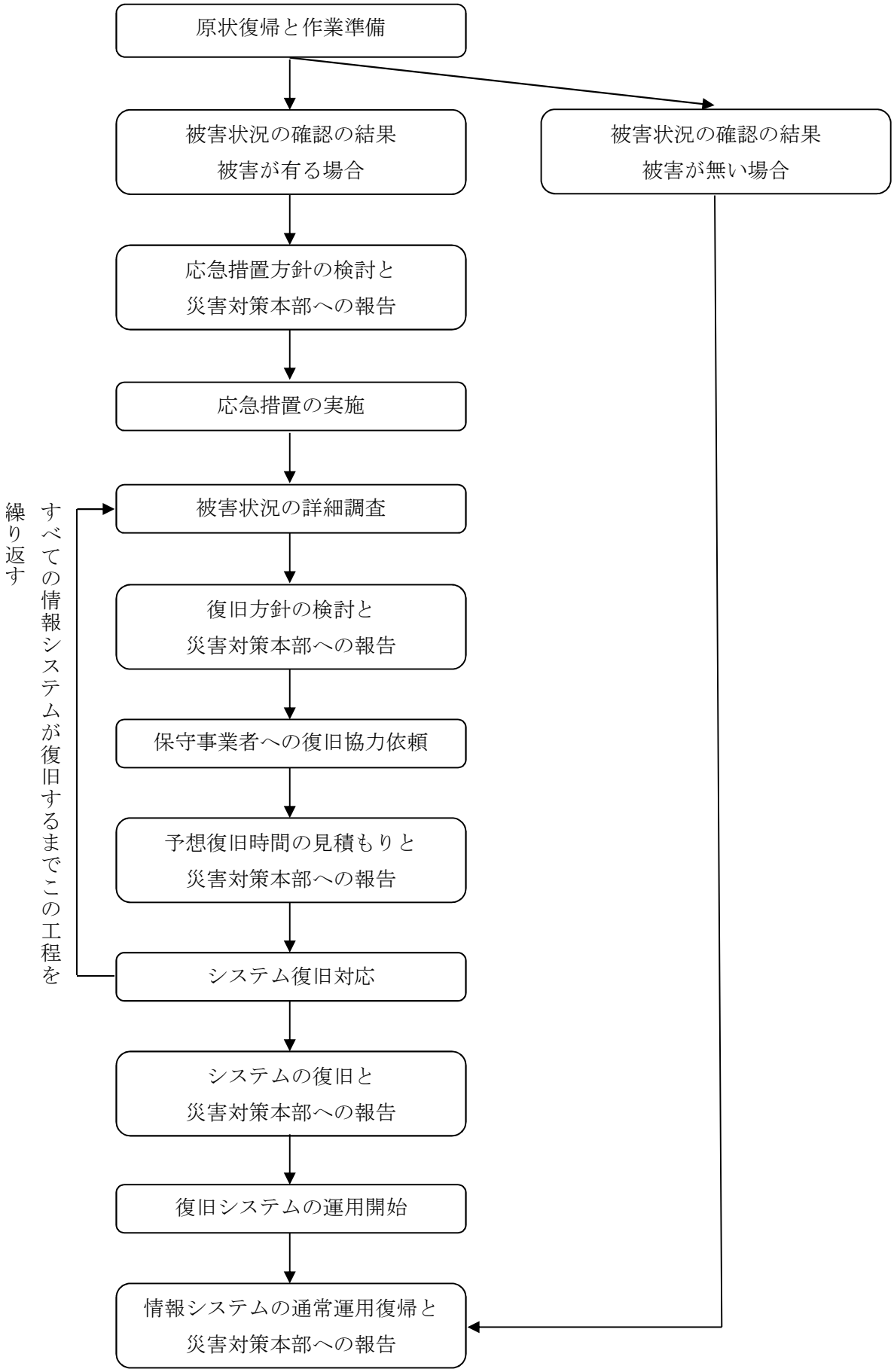
（2）行動計画

ICT部門における基本的な行動計画について、行動の概要をフロー図で以下に示す。なお、詳細については、別途作成のマニュアルで対応する。

〈行動計画フロー図〉

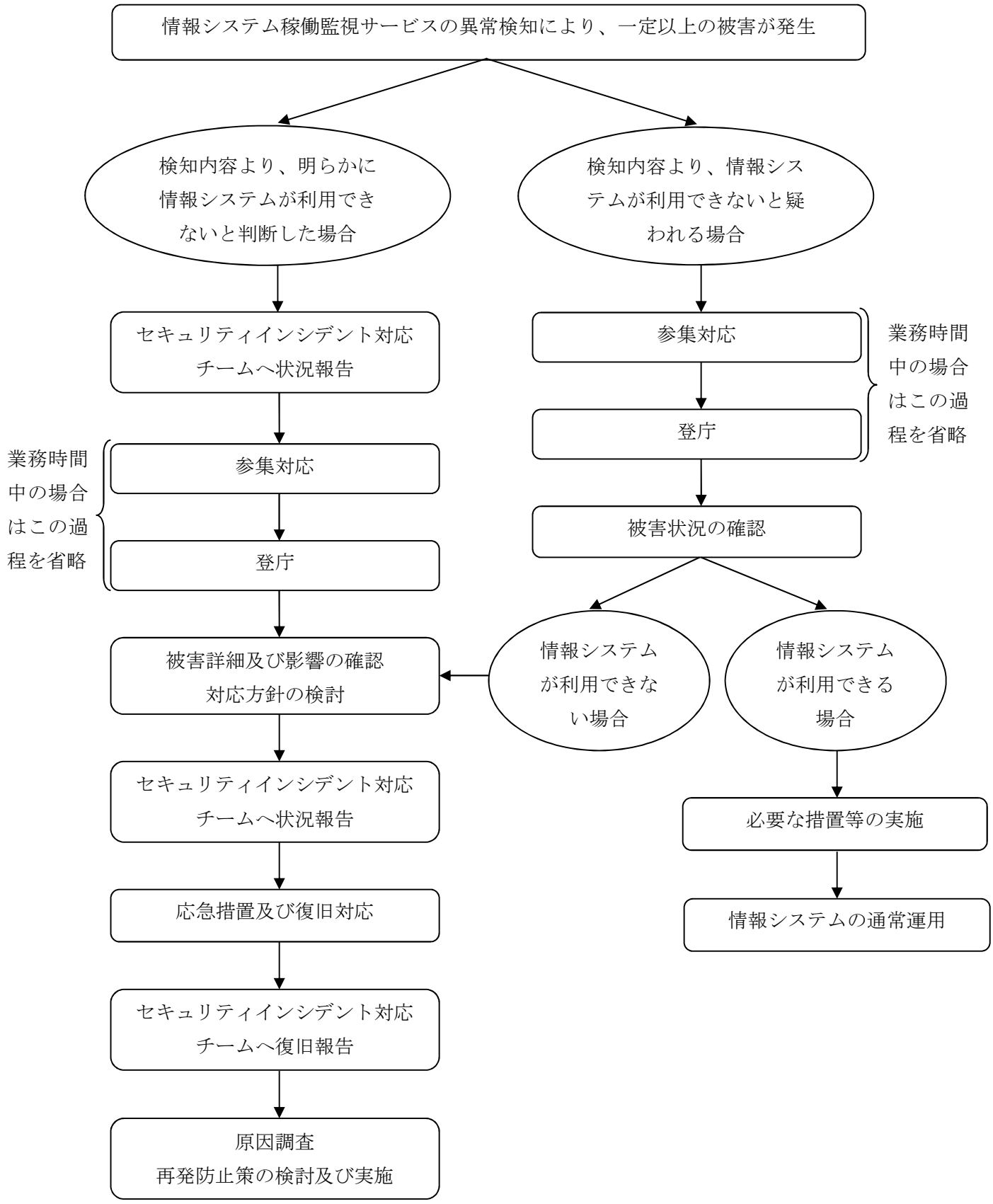
ア　地震・風水害の場合




原状復帰と作業準備
被害状況の確認の結果
被害が有る場合
被害状況の確認の結果
被害が無い場合
応急措置方針の検討と
災害対策本部への報告
応急措置の実施
被害状況の詳細調査
復旧方針の検討と
災害対策本部への報告
保守事業者への復旧協力依頼
予想復旧時間の見積もりと
災害対策本部への報告
システム復旧対応
システムの復旧と
災害対策本部への報告
復旧システムの運用開始
情報システムの通常運用復帰と
災害対策本部への報告
すべての情報システムが復旧するまでこの工程を
繰り返す

イ　情報セキュリティ事象の場合

セキュリティインシデント対応チームの動きは、「葛飾区情報セキュリティインシデント対応チーム設置要綱」に基づくものとする。



６　計画の運用

（１）本計画を踏まえたマニュアルの整備

本計画の下に整備するマニュアルは事象別とする。想定する事象は本計画で取り上げているものとし、以下の６つを事象別対応マニュアルとして整備する。

・地震編
・風水害編
・情報セキュリティ事象編
・自然災害（異常気象・火山噴火等）編、大規模事故（爆発・危険物事故等）
・武力攻撃事態、緊急対処事態（テロ等）編
・新型インフルエンザ等、健康危機（食中毒、感染症等）編

さらに、事象別対応マニュアルに沿った行動を行う中で参照する資料も別途用意する。その種類や概要等について、以下にまとめる。

種類	名称	概要
リスト（一覧）	・事業者連絡先一覧 ・職員安否確認票（参集予測票） ・被害・復旧見込みチェックリスト ・職員参集時指揮者優先順位及び役割 等	事業者の連絡先や参集時の役割についてまとめたものや、職員の安否確認や被害状況の確認結果を記録するものなどをリストや一覧として整備する。
手順	・電源復旧手順（停電対応） ・データセンター通信確認・原状回復手順 ・電算センター空調機確認・原状回復手順 ・庁議室通信暫定原状回復手順 等	停電時など、設備や機器の確認順序を記載し、回復作業の手順を明確にしたものを整備する。
図	・ネットワーク機器配置情報 ・電算センターラック配置図 ・CVCF（※）室レイアウト図 ・執務室配置図及び周辺図 等	庁舎内のネットワーク機器や電算センターラックの配置状況、情報システム課に関係する機器や執務室のレイアウトなどについてまとめたものを整備する。
帳票	・作業計画書 等	被害状況に応じて各種作業を行う際に作成する内部書式などを整備する。
その他	・作業にあたっての留意事項 ・災害等対応時参集職員の役割分担 ・職員・事業者が参集できない場合	その他、想定されない事態が発生した場合に備え、復旧に当たる

	の対応 等	考え方を整理・検討したものを整備する。

（２）本計画及びマニュアルの見直し

本計画及びマニュアルは、情報システムの新規導入や更改等環境が変化した場合や訓練結果、新たに整備するマニュアル等との関連性を踏まえて、見直しを行う。なお、見直しは、年１回以上実施することとする。

（３）承認ルール

本計画を改訂する場合は、情報システム統括責任者が承認し、「計画の新規制定／改訂一覧」に記述する。

また、マニュアルを整備又は改訂する場合は、電算機管理者が承認し、改訂の主な内容と承認日を各マニュアルに記述する。

（４）訓練

本計画の実効性を担保するため、以下のとおり定期的に訓練を行う。

訓練名称	訓練の概要	実施者	時　期
机上訓練	本計画及びマニュアルを読み、緊急時にすべき行動を確認したうえで、想定シナリオをもとに訓練を行う。	情報システム課職員、運用事業者等	毎年１回
緊急連絡・安否確認訓練	緊急時を想定し、緊急連絡先リストにより情報システム課職員等の安否確認連絡を行う。	情報システム課職員、運用事業者等	毎年１回 例：４月の人事異動後、任意のタイミングで実施する。
システム復旧訓練	災害発生に伴う停電時を想定した情報システム機器の起動方法等の確認及び配線、ネットワーク、業務システム等の稼働状況の確認を行う。	情報システム課職員、運用事業者等	毎年１回 例：区庁舎の停電日に合わせて実施する。

7　用語集

本計画内で「※」で示している用語の解説について、アルファベットで表記されているものはアルファベット順で、漢字やカタカナ表記のものは五十音順でそれぞれ以下に示す。

〈アルファベット順〉

用語	解説等
ASP	Application Service Provider の略。業務ソフトウェアをはじめとする各種システム機能をネットワーク経由で提供する事業者やサービスのこと。
CIO	Chief Information Officer の略。最高情報システム統括責任者のこと。
CIO 補佐官	「葛飾区デジタル技術を活用した区政の推進及び情報システムの管理運営に関する規則」に規定されている外部専門家のこと。CIO を専門的見地から補佐する。
CVCF	Constant Voltage Constant Frequency の略で「定電圧定周波数装置」のこと。一般的なコンセントで利用する電気（商用電源）は電圧や周波数の変動があり、精密機械に不具合が生じることがある。これを防ぎ、安定した電圧や整流した周波数を供給する。本区では、庁舎地下に設置されている。
DoS 攻撃	情報システムに過剰な負荷をかけて、サービスを提供することを妨げてしまうこと。
DDoS 攻撃	攻撃 DoS 攻撃の攻撃元が複数で、標的とされた情報システムがひとつといった形で、標的とされる情報システムに DoS 攻撃より大きな負荷をかけるもの。
ICT-BCP	以下の用語を組み合わせたもの。 ICT:Information and Communication

	Technology の略。情報通信技術のこと。 BCP: Business Continuity Plan の略。業務継続計画のこと。
IPA	Information-technology Promotion Agency の略。独立行政法人情報処理推進機構のことで、経済産業省が所管する独立行政法人である。
OS	Operating System の略。機器の基本的な管理や制御のための機能や、多くのソフトウェアが共通して利用する基本的な機能などを実装した、システム全体を管理するソフトウェアのこと。

〈五十音順〉

用語	解説等
インシデント	本計画においては、（事故の一歩手前の）重大な結果に繋がりかねない出来事や状況、異変、危機、もしくは発生してしまった事故の意味で用いる。
インフラ	インフラストラクチャーの略であり、身近な例としては、電気や水道、ガスなどの生活の基盤となるものを指す。本計画においては、ICTインフラの意味で用い、業務システムが稼働する前提となる基盤や環境（データーセンター、ネットワーク等。）を指す。
運用・保守事業者	運用事業者は、情報システムの利用における日々の問い合わせ対応（ヘルプデスク業務）や通常の管理業務等を行う事業者を指す。保守事業者は、情報システムに問題がある場合の修正等を行う事業者を指す。
仮想化	ハードウェアやソフトウェアなどを物理的構成に拠らず柔軟に分割したり統合したりする技術のこと。１台のサーバを分割してあたかも複数台の仮想的なサーバとして使用できる「仮想サーバ」や、サーバで動かしているデスクトップ画面をネットワーク経由で端末に表示させる「仮想デスクトップ」などの技術がある。

葛飾区情報セキュリティポリシー	本区では、「葛飾区情報セキュリティに関する規則（令和２年区規則第11号）」及び「情報セキュリティ対策基準（学校含む。）」を総称してセキュリティポリシーという。
サイバー攻撃	情報システムに対し、ネットワークを通じて破壊活動やデータの窃取、改ざんなどを行うことをいう。
情報セキュリティインシデント対応チーム	「葛飾区情報セキュリティインシデント対応チーム設置要綱」に規定されるインシデント対応チームのこと。チームは総務課を中心とする関係課で構成される。
情報セキュリティ10大脅威	各年発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約160名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものであり、毎年行っている。個人編と組織編がある。
総合行政ネットワーク（LGWAN）	地方公共団体を相互に接続する行政専用のネットワークのこと。
データセンター	サーバやネットワーク機器を設置することに特化した建物のこと。冷却装置、大容量電源なども兼ね備える。庁外にある民間のもの。
電算センター	精密機械であるネットワーク機器やサーバには最適となる一定範囲の温度や湿度があり、それを保つための空調機などを備えた空間のこと。
バッチ処理	一定量のデータや複数のプログラムを一括して自動で処理することを指す。本区では、主に日中に更新されたデータを業務システム内や他の業務システムに夜間連携する際に活用されている。
標的型攻撃	メール等を利用し特定組織のパソコンをウィルスに感染させ内部に潜入し、組織の機密情報の搾取や情報システムの破壊を行う攻撃のこと。
不正アクセス	情報システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと。
ミドルウェア	OS と実処理を行うアプリケーションを仲介しそれぞれを補佐するソフトウェアのこと。

ランサムウェア	Ransom（身代金）＋Software（ソフトウェア）２つを組み合わせた造語。感染すると身代金を支払うまでファイル暗号化やパソコンがロックされるウィルスのこと。身代金を支払っても情報が復旧できないことが多い。

葛飾区ICT部門業務継続計画
（ICT-BCP）

発 行 日　令和4年9月
発　　行　葛飾区
葛飾区立石5－13－1
電話:03－3695－1111（代表）
編　　集　葛飾区政策経営部情報システム課