喜茂別町役場ＩＣＴ部門業務継続計画
（ＩＣＴ－ＢＣＰ）

令和７年１２月

喜茂別町役場

計画の新規策定／改訂一覧

版　数	策定／改訂年月日	策定／改訂
初　版	令和５年１２月１４日	策定
第二版	令和７年１２月２９日	改訂

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、町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。）の稼動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、町は業務を実施・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見積り、事前に備えておくことが極めて重要である。

そこで、「喜茂別町役場業務継続計画（ＢＣＰ）」に基づき、「喜茂別町役場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、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、本計画は喜茂別町役場業務継続計画（ＢＣＰ）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。

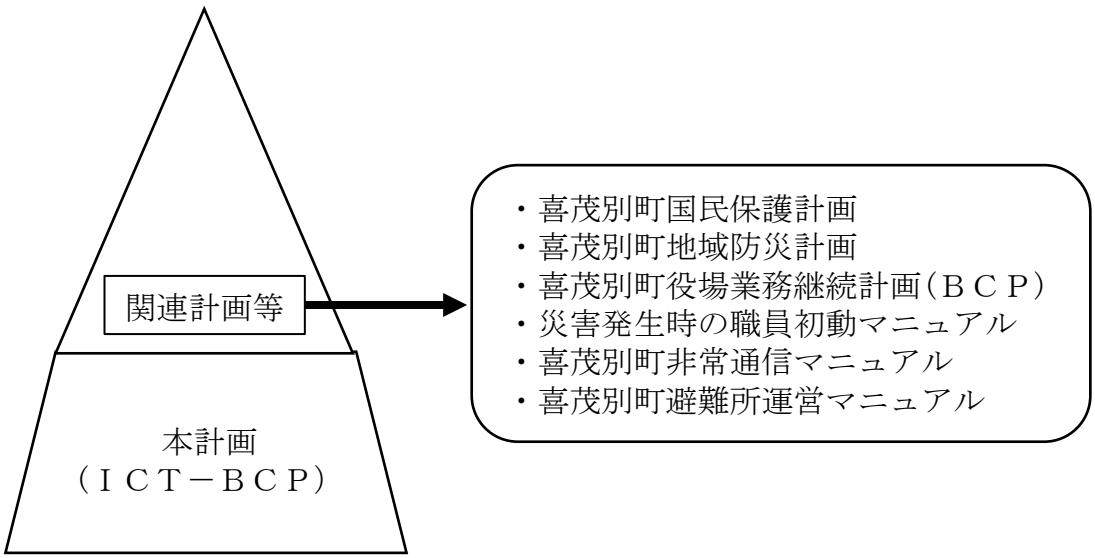


図　本計画の位置付け

(2)　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部門の責任遂行	町民の生命の安全確保や町民生活、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	可能な限り、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。

(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、まちづくり振興課が管理する端末、プリンタ及びネットワーク（機器を含む。）及び各業務所管課等が個別に管理をしている業務システムとする。

イ　喜茂別町における被害想定

災害について、地域防災計画の被害想定と同様とし、風水害において、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、ランサムウェアや標的型攻撃、情報システム障害など町の環境において発生する可能性があるものを想定する。

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利用環境（端末環境）の現状

本町の情報システムに係る利用環境（端末環境）は、端末環境の仮想化（仮想デスクトップ化）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であり、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、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、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、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。

(2)　現状におけるリスク

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動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。
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、本庁舎内で情報システムの利用ができないという事態になる。
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。
まちづくり振興課担当職員２名及び運用・保守事業者の参集不可	激しい揺れにより、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と予想される。 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）	想定されるリスク
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動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。
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。
庁舎の被災 （立ち入り不可）	庁舎１階への浸水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。
まちづくり振興課担当職員２名及び運用・保守事業者の参集不可	暴風や浸水によって、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と予想される。 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）	想定されるリスク
サイバー攻撃	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。
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、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おこなったが、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、実効性を担保しておくこととする。

(2)　想定される脅威とリスク

想定される脅威は、「喜茂別町国民保護計画」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（2）現状におけるリスク」に記載の内容に準ずる。
通信の断絶	
庁舎の被災（立ち入り不可）	
まちづくり振興課担当職員2名及び運用・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（２）現状におけるリスク」に記載の内容に準ずる。
通信の断絶	
庁舎の被災（立ち入り不可）	
まちづくり振興課担当職員２名及び運用・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（食虫毒、感染症等）の場合

事象（原因）	想定されるリスク
庁舎の被災（立ち入り不可）	「２　情報システム環境の現状とリスク（２）現状におけるリスク」に記載の内容に準ずる。
まちづくり振興課担当職員２名及び運用・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、まちづくり振興課担当者や運用・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。

(4)　重要な行政データのバックアップ

連番	システム名称
1	住基税務システム （印鑑、国民年金、国保（資格・税）、住民税、軽自、固定、収納）
2	住民税（国税連携対応機能）システム
3	e-Tax連携サービス利用料
4	e-Tax法人市町村民税/法人電子申告連携オプション
5	e-Tax申告受付支援/給報電子申告連携オプション
6	e-Tax固定資産税/償却電子申告連携オプション
7	e-Tax住民税/年金電子申告連携オプション
8	e-Tax収納消込（共通納税）電子申告対応オプション
9	共通納税税目拡大対応（国民健康保険税）オプション
１０	共通納税税目拡大対応（住民税「普通徴収」）オプション
１１	共通納税税目拡大対応（軽自動車）オプション
１２	共通納税税目拡大対応（固定資産税）オプション
１３	軽自動車ＯＳＳ対応
１４	法人市町村民税システム
１５	課税状況調システム
１６	滞納整理システム
１７	滞納整理（法人市町村民税連携機能）システム
１８	滞納整理システム預貯金取引照会連携機能
１９	選挙システム
２０	選挙（期日前投票）システム
２１	選挙システム（裁判員制度異動分把握）
２２	裁判員制度システム
２３	後期高齢者医療システム
２４	医療費助成システム
２５	児童手当システム
２６	子ども子育て支援システム
２７	データセンター処理（基本サービス）利用料（アウトソーシング）
２８	公会計システム

連番	システム名称
２９	リアルタイム仕訳
３０	固定資産管理システム
３１	人事情報システム
３２	給与システム
３３	水道料金システム
３４	統合宛名システム情報連携基盤
３５	申告受付支援システム
３６	申告受付支援システム（国税連携対応機能）
３７	健康管理システム
３８	特定健診システム
３９	国保税税率試算システム
４０	コンビニ収納システム（６科目）
４１	ＴＡＳＫクラウド基盤利用料
４２	行政区画便覧（日本加除出版）
４３	固定資産税システム登記済通知書連携機能

4　計画の運用体制と役割

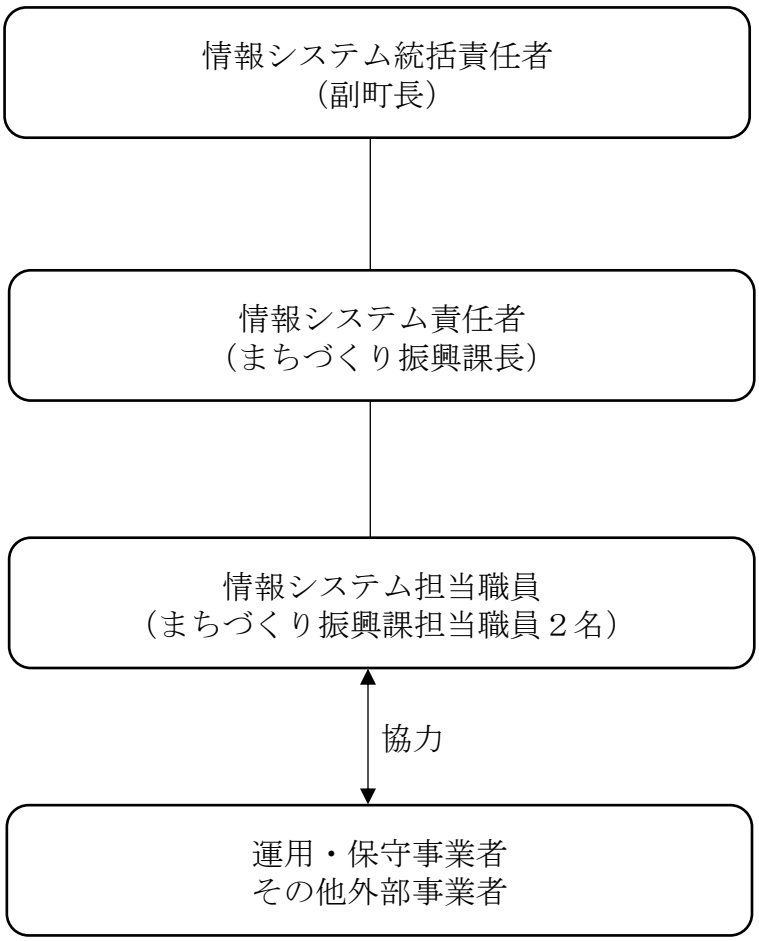
本計画の管理運用に当たり、あらゆる事態が発生した場合においても、迅速な対応が求められることから、平常時や災害時、情報セキュリティ事象発生時それぞれにおいて、必要な体制と役割をあらかじめ整備する。

なお、災害と情報セキュリテイ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＞



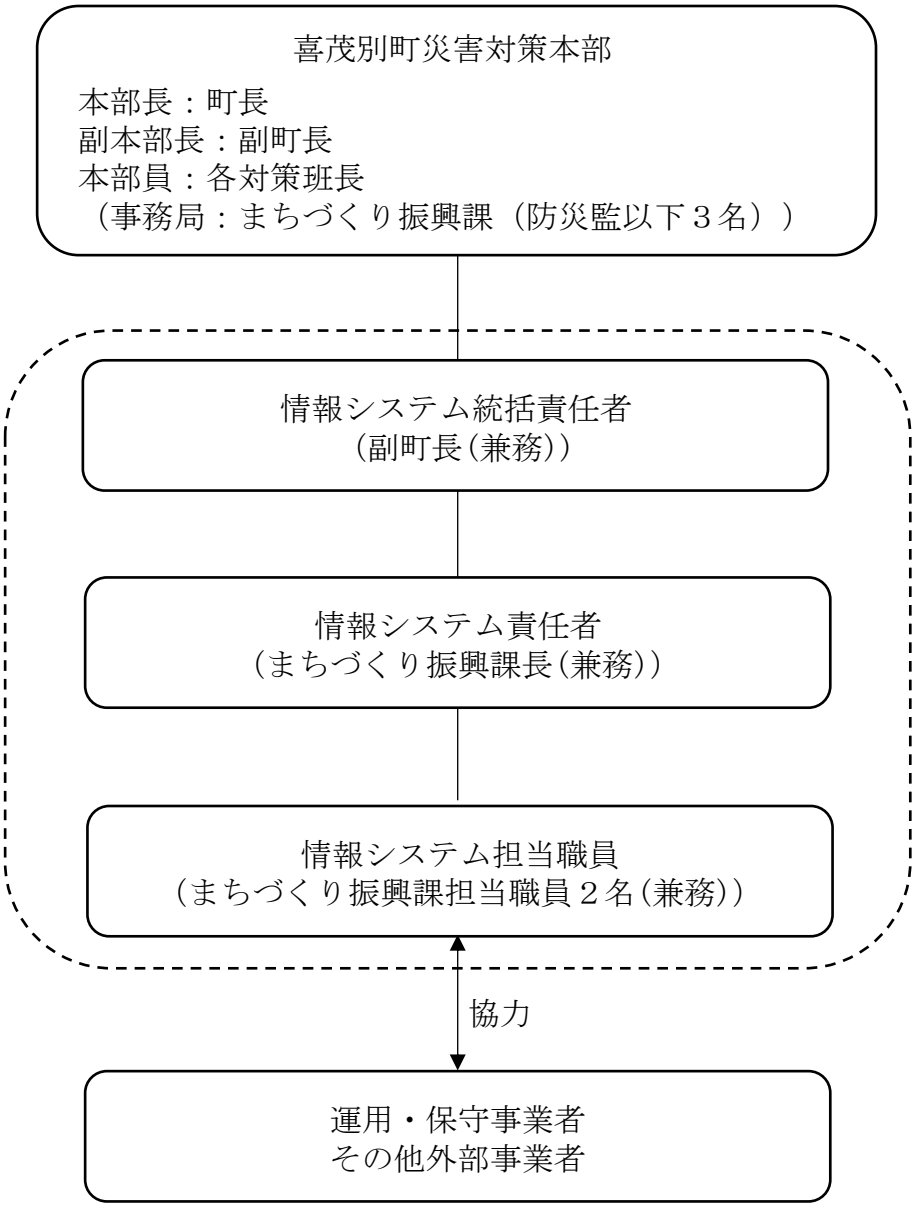
＜平常時の役割＞

組織	役割の概要	災害対策本部との関係
情報システム 統括責任者（副町長）	・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	副本部長
情報システム責任者 （まちづくり振興課長）	・まちづくり振興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	統括班長
情報システム担当職員 （まちづくり振興課 担当職員２名）	・本計画の改訂を行う ・平常時の本計画の維持管理を行う ・訓練を実施する （机上訓練、緊急連絡確認訓練及びシステム復旧訓練のいずれかの訓練を年１回以上行う	統括班員 （災害対策本部事務局を兼ねる）
運用・保守事業者 その他外部事業者	・本計画の実行時に町と協力して必要な対応を行う	

(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＞



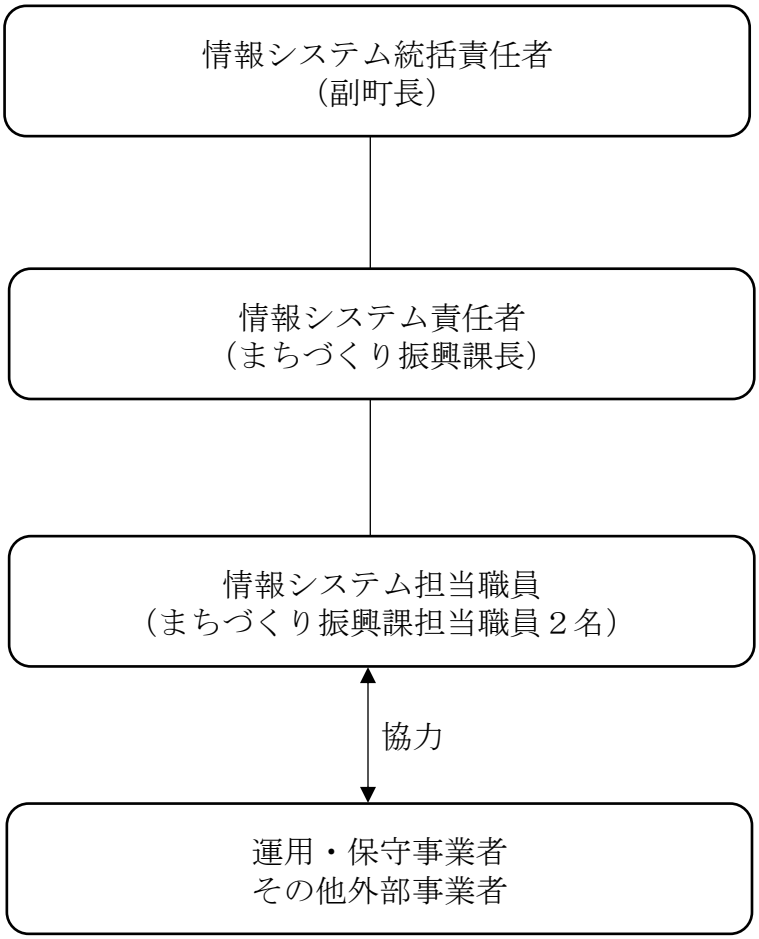
＜災害時の役割＞

組織	役割の概要
喜茂別町災害対策本部	喜茂別町地域防災計画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 ・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すること ・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
情報システム 統括責任者（副町長）	・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
情報システム責任者 （まちづくり振興課長）	・災害対策本部への状況報告と本部決定事項の部門内への伝達 ・他の業務部門との調整の統括、支援依頼
情報システム担当職員 （まちづくり振興課担当職員２名）	・庁内や出先施設等からの問い合わせ対応 ・情報システムの被害状況の把握及び情報システム責任者への報告 ・情報システムの復旧に向けた運用・保守事業者やその他外部事業者に向けた協力依頼調整
運用・保守事業者 その他外部事業者	・情報システムに係る被害状況の確認及び復旧に向けて、町と協力し必要な対応を行う。

(3)　情報セキュリテイ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、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
情報システム 統括責任者（副町長）	・情報システムの適正な運用の確保に関すること
情報システム責任者 （まちづくり振興課長）	・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）、対策遂行を行う。
情報システム担当職員 （まちづくり振興課 担当職員２名）	・庁内や出先施設等からの問い合わせ対応 ・情報システムの被害状況の把握及び情報システム責任者への報告 ・情報システムの復旧に向けた運用・保守事業者やその他外部事業者に向けた協力依頼調整
運用・保守事業者 その他外部事業者	・本計画の実行時に町と協力して必要な対応を行う

５　緊急時対応・復旧訓練

(1)　参集ルール等

以下のとおり、緊急時の職員の参集ルールを整理する。

ア　地震の場合

職員初動マニュアルの規定のとおり、震度５強で全職員が参集し、震度５弱で災害対策本部の各対策班の所要の職員が参集し、震度４で、まちづくり振興課と建設課の所要の職員が参集する。

イ　風水害の場合

広域にわたる災害の発生が予想される場合、又は被害が特に甚大であると予想される場合において町長が第３非常配備体制を指令したときには、全職員が参集する。

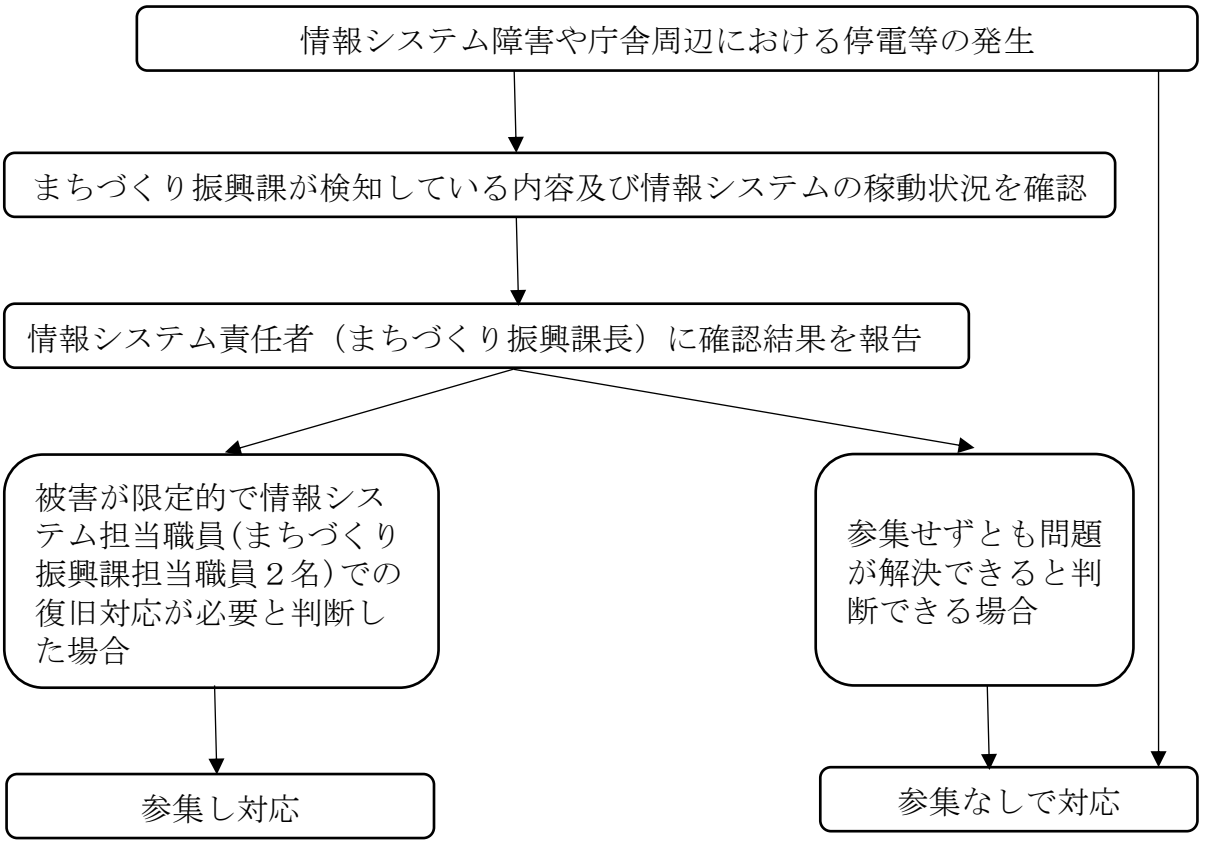
ウ　情報セキュリティ事象の場合

サイバー攻撃や情報システム障害等が発生した場合は、被害状況次第で情報システム責任者及び情報システム担当職員が参集し、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、基本的には情報システム責任者の指示により参集することとするが、この場合における、まちづくり振興課の対応は、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まちづくり振興課の対応で完結するが、実際に住民影響や庁舎全域に影響が出る大きな障害が発生した場合には、「４項（３）情報セキュリテイ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）



エ　その他の脅威の場合

被害の状況により、ア～ウに準じて対応することとする。

オ　運用・保守事業者への復旧協力依頼

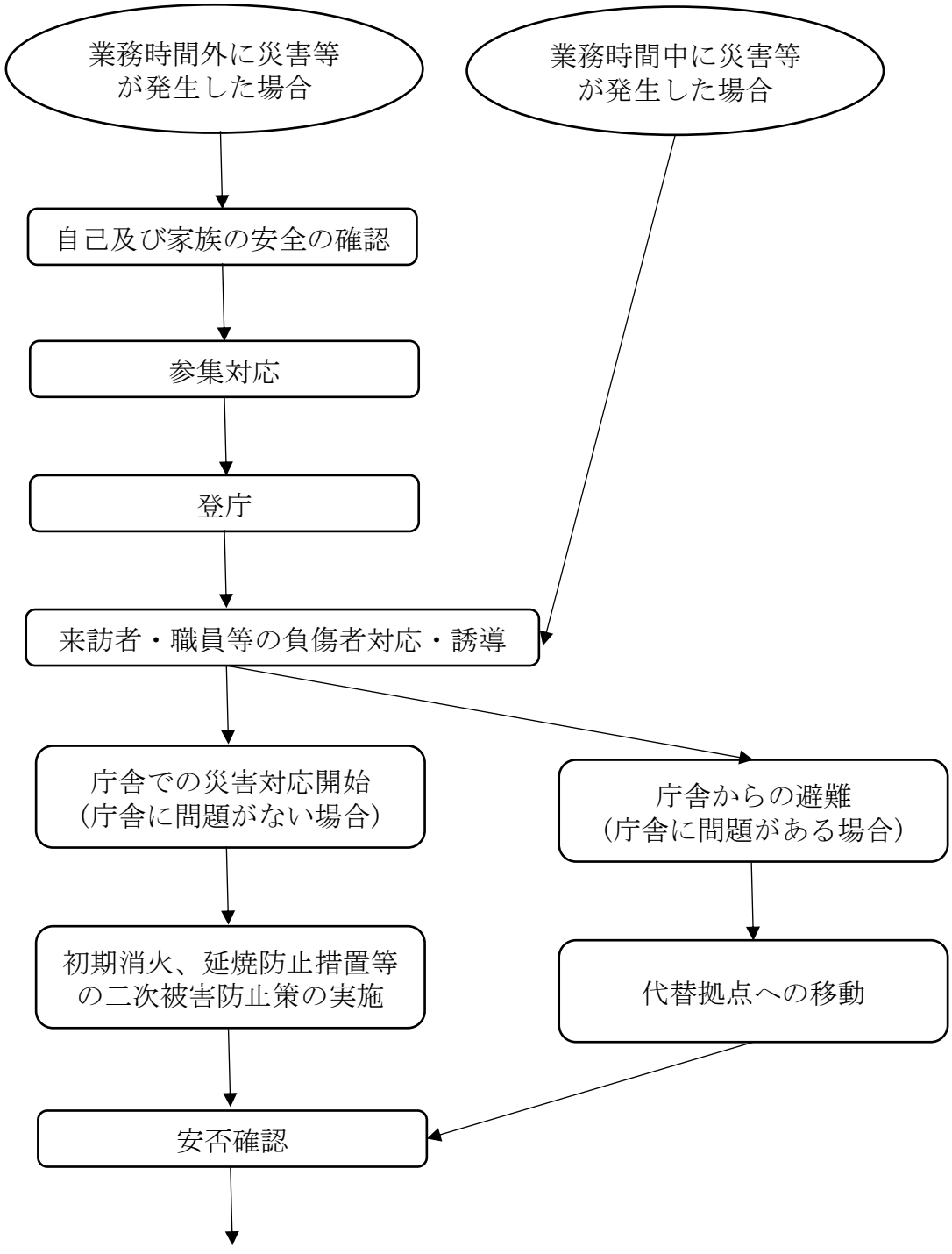
災害や情報セキュリティ事象が発生した場合は、まずは情報システム担当職員（まちづくり振興課担当職員２名及び運用事業者による被害状況の確認を行い、障害等の原因を特定するよう努めることとする。その結果、保守事業者での対応が必要と判断した場合には、保守事業者に復旧へ向けた協力依頼を行うこととする。

(2)　行動計画

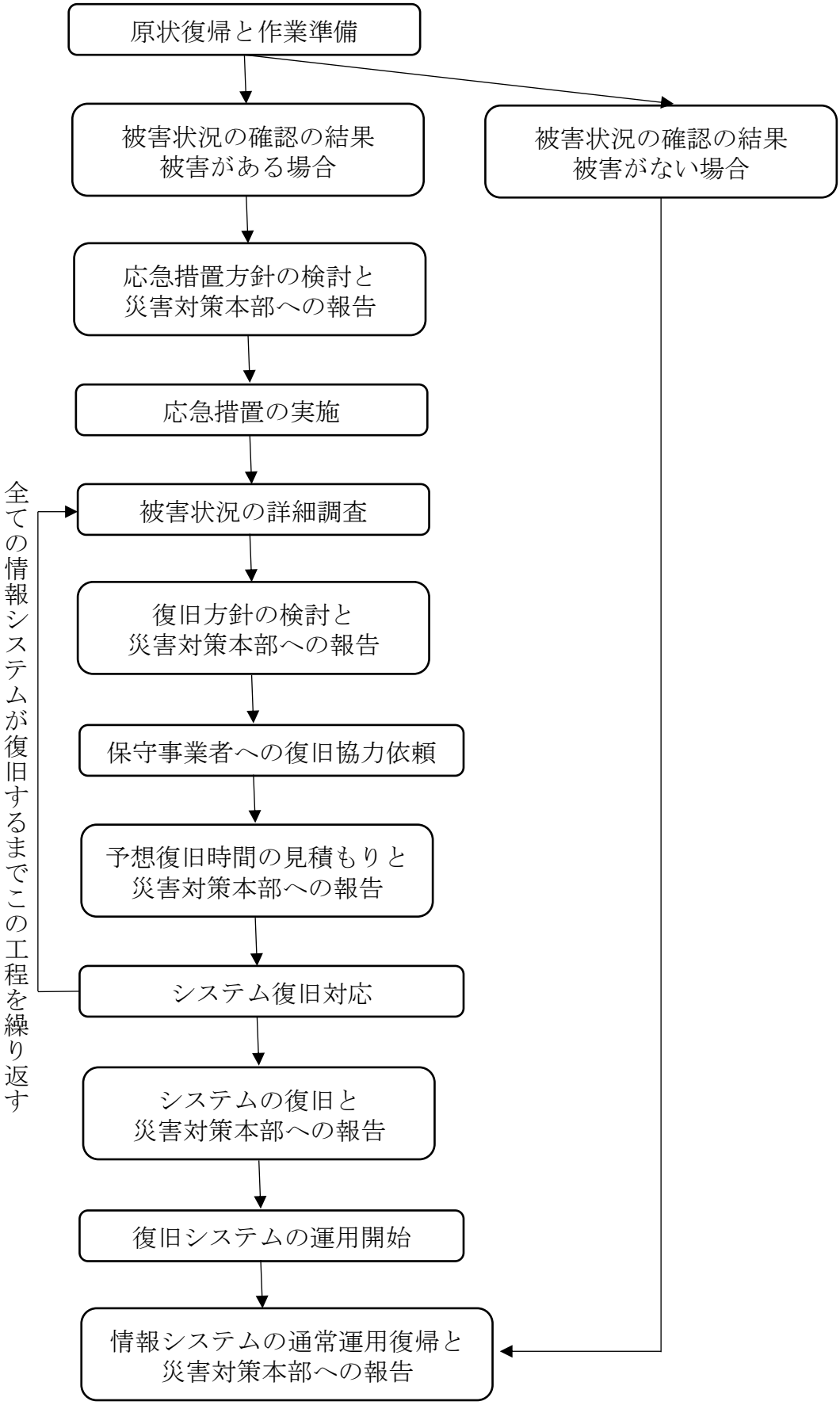
ＩＣＴ部門における基本的な行動計画について、行動の概要をフロー図に示す。

（行動計画フロー図）

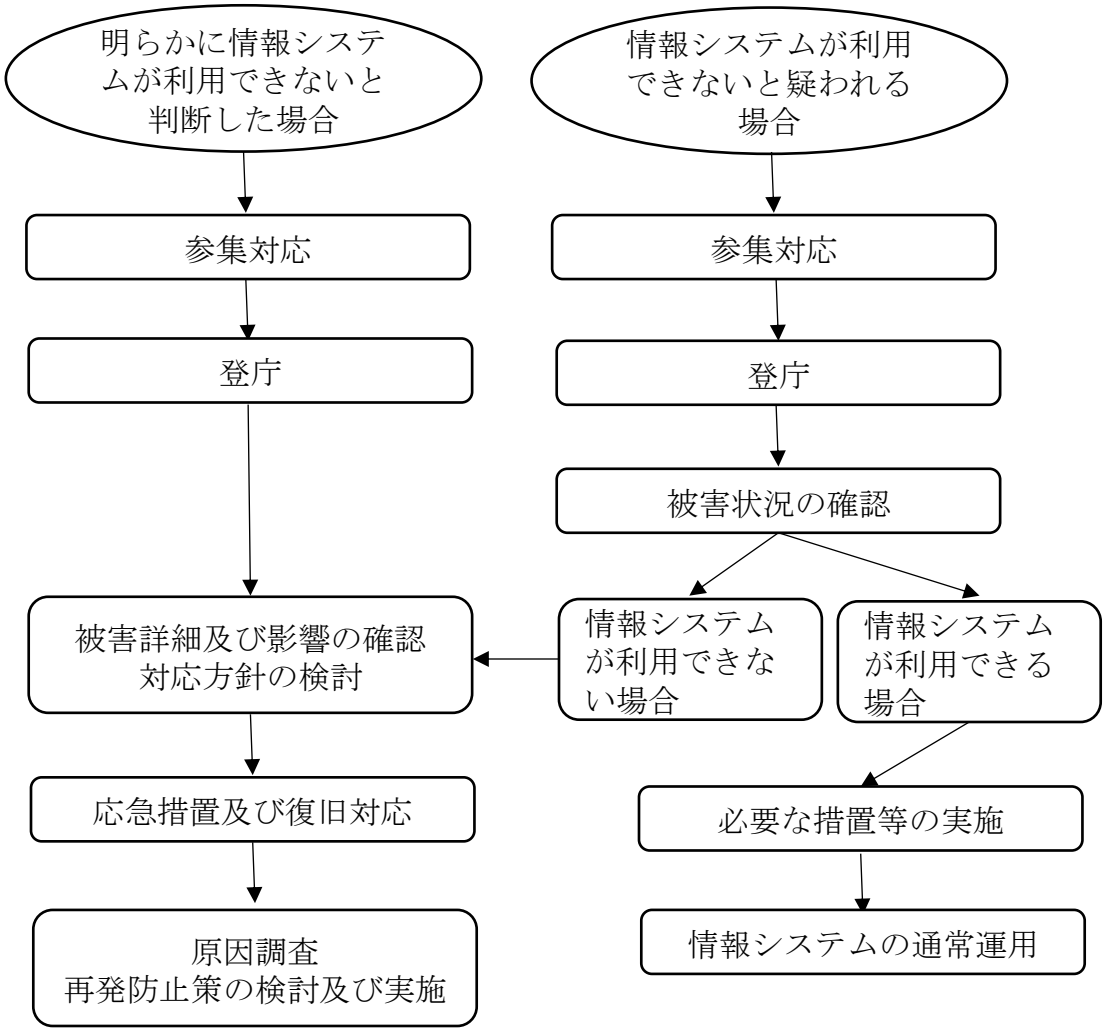
ア　地震・風水害の場合



（次のページに続く）


原状復帰と作業準備
被害状況の確認の結果
被害がある場合
被害状況の確認の結果
被害がない場合
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
全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



6　計画の運用

(1)　本計画の見直し

本計画は、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を踏まえて、次のとおり見直しを行う。

ア　組織体制に大きな変更があった場合
イ　外部事業者に大きな変更があった場合
ウ　主要な情報システムに大幅な変更があった場合
エ　国、北海道の制度変更により改訂の必要がある場合
オ　町長から改訂をするよう指示があった場合

(2)　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（副町長）が承認し、「計画の新規策定／改訂一覧」に記述する。

(3)　訓練

本計画の実効性を担保するため、次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に基づく対処行動を案出する。	情報システム責任者（まちづくり振興課長） 情報システム担当職員（まちづくり振興課担当職員２名）	毎年１回以上
緊急連絡・確認訓練	緊急時を想定し、非常呼集連絡網により情報システム担当職員の緊急連絡・確認訓練を行う		
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動状況の確認を行う。 例：庁舎の計画的な停電日に合わせて実施する。		

7　用語集

本計画に係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。

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。
ＣＶＣＦ	Constant Voltage Constsnt 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こと。
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	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。
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めソフトウェアのこと。
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示す。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）を示す。
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や通常の管理業務等を行う事業者を示す。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示す。

用語	解説等
仮想化	ハードウァアなどの物理的構成をソフトウェアを使用し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」やサーバ上にデスクトップ画面を作ることでネットワーク経由で、どの端末からでも表示させることができる「仮想デスクトップ」などの技術がある。
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。
情報セキュリテイ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イにおける事案から、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。
電源センター	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。
標的型攻撃	メール等を利用し特定組織のパソコンをウイ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、それぞれを細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イルスのこと。身代金を支払っても情報が復旧できないことが多い。