第２章　行政データに係るバックアップ・リストア基準の策定に向けた提言

前章においては、データ管理の必要性の観点からの調査を行った。本章では、その調査結果を踏まえ、行政データのバックアップ・リストア方策及び日常的運用に係る課題に対して解決方策を検討し、バックアップ・リストア基準の策定を行う。

バックアップ・リストア基準を策定する前提条件として、既存のデータ管理に関わる規則・規程等を収集・分析し、参考とした。

第１節　情報セキュリティポリシー及び ICT - BCP 等に係る調査

既存のデータ管理に関わる規則・規程等として、情報セキュリティポリシー及び ICT - BCP 等について調査した。

１　情報セキュリティポリシーガイドラインの概要

地方公共団体における情報セキュリティポリシーに関するガイドライン[35]（以下「情報セキュリティポリシーガイドライン」という。）の概要を以下に示す。

（１）情報セキュリティポリシーガイドライン（平成 22 年 11 月版）の概要

ア　ガイドラインの目的

情報セキュリティポリシーとは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書をいう。

地方公共団体における情報セキュリティは、各地方公共団体が保有する情報資産に自ら責任を持って確保すべきものであり、情報セキュリティポリシーも各地方公共団体が組織の実態に応じて自主的に策定するものである。

ガイドラインは、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したものである。

したがって、ガイドラインで記述した構成や文例は、参考として示したものであり、各地方公共団体が独自の構成、表現により、情報セキュリティポリシーを定めることを妨げるものではない。

---

35 詳細は、下記（総務省ホームページ）を参照のこと。
http://www.soumu.go.jp/main_content/000087555.pdf

イ　地方公共団体における情報セキュリティの考え方

地方公共団体の業務の多くが情報システムやネットワークに依存していることから住民生活や地域の社会経済活動を保護するため、地方公共団体は、情報セキュリティ対策を講じて、その保有する情報を守り、業務を継続することが必要となっている。

情報セキュリティの確保に絶対安全ということはないことから、情報セキュリティに関する事故の未然防止のみならず、事故が発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要である。

情報セキュリティ対策は、個人情報保護対策と内容的に重なる部分も多い。また、自然災害時や大規模・広範囲にわたる疾病における対応という意味では防災対策とも重なる。

情報セキュリティを対策する部署とこれらを担当する部署は、相互に連携をとって、それぞれの対策に取り組むことが求められる。

ウ　情報セキュリティポリシーの必要性と構成

地方公共団体においては、情報セキュリティ対策を徹底するには、対策を組織的に統一して推進することが必要であり、そのためには組織として意思統一し、明文化された文書として、情報セキュリティポリシーを定めなければならない。

情報セキュリティポリシーの体系は、**図－３１**に示す階層構造となっている。

各地方公共団体の情報セキュリティ対策における基本的な考え方を定めるものが、「基本方針」である。

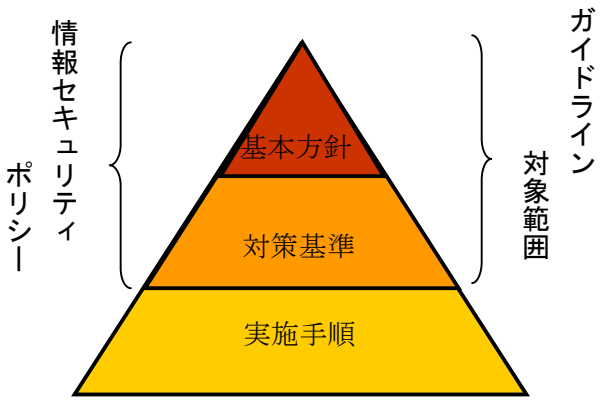
この基本方針に基づき、すべての情報システムに共通の情報セキュリティ対策の基準を定めるのが「対策基準」である。

この「基本方針」と「対策基準」を総称して「情報セキュリティポリシー」という。

この「対策基準」を、具体的なシステムや手順、手続に展開して個別の実施事項を定めるものが「実施手順」である。

このように、情報セキュリティポリシーは、情報セキュリティ対策の頂点に位置するものであることから、地方公共団体の長をはじめ、すべての職員等及び外部委託事業者は、業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負う。

ガイドラインの対象とする範囲は「情報セキュリティポリシー」を構成する「基本方針」及び「対策基準」であり、「実施手順」は含まれない。



図－３１　情報セキュリティポリシーに関する体系図

出典：情報セキュリティポリシーガイドライン

エ　組織体制の確立

情報セキュリティポリシーの策定には、幹部職員の関与が不可欠である。

また、情報セキュリティポリシーは、組織内の様々な部局の情報資産に係る問題を取り扱うことから、責任の所在を明確にするため、すべての部局の長、情報システムを所管する課室長及び情報セキュリティに関する専門的知識を有する者などで構成する組織又はこれに代わる組織が行う。

小規模の団体の場合には、新たに、組織を立ち上げるのではなく、「情報化推進委員会」等の既存の類似する組織が行う場合もありえる。組織が有機的に機能するために全組織横断的な指示、連絡可能な役割及び権限を明確にすることが望ましい。

オ　情報セキュリティ基本方針の策定

情報セキュリティ基本方針においては、情報セキュリティ対策の目的、体系等、各地方公共団体の情報セキュリティに対する基本的な考え方を示す。

カ　リスク分析の実施

リスク分析とは、各地方公共団体が保有する情報資産を明らかにし、それらに対するリスクを評価することである。

様々なリスク分析方法があるが、例えば、次図のとおり、次の手順で行う。

（ア）各地方公共団体の保有する情報資産を調査の上、重要性の分類を行い、この結果に基づき、要求されるセキュリティの水準を定める。

（イ）各地方公共団体の情報資産を取り巻く脅威の調査を行い、その発生可能性及び発生した際の被害の大きさからリスクの大きさを求める。

なお、一般的に両者の積をリスクの大きさとしている。

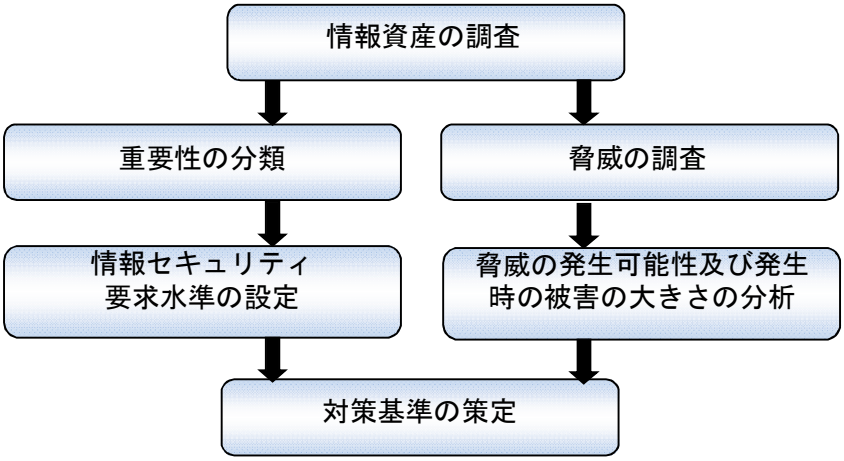
（ウ）リスクの大きさがセキュリティ要求水準を下回るよう対策基準を策定し、適切なリスク管理を行う。

情報資産や情報資産に対するリスクに大きな変化が生じたときには、関係する情報資産についてリスク分析を再度行い、その結果、情報セキュリティポリ

シーの見直しが必要と判断される場合にはその見直しを行う。

定期的な情報セキュリティポリシーの評価・見直しの際にもリスク分析から再検討することが必要である。

リスク分析に関する資料は、情報セキュリティポリシー策定の基礎資料として保管する必要があるが、当該資料には情報資産の脆弱性に関する事項が記載されているため、厳重な管理が必要である。



図－３２　リスク分析の事例

出典：情報セキュリティポリシーガイドライン

キ　情報セキュリティ対策基準の策定

リスク分析の結果得られる情報セキュリティ要求水準に対して、それを実現するための遵守事項や判断基準等を定める情報セキュリティ対策基準を策定する。

情報セキュリティ対策基準は、想定される情報リスクに十分に対処し、情報セキュリティ要求水準を満たすものでなければならない。

ク　実施手順の策定

実施手順は、職員等関係者が、各々の扱うネットワーク及び情報システムや携わる業務において、どのような手順で情報セキュリティポリシーに記述された内容を実行していくかを定めるマニュアルに該当する。

このマニュアルには、主要な情報資産に対するセキュリティ対策実施手順も含まれる。

実施手順は、個別の目的のために作成し、見直し等を柔軟に行っていくため、業務部門において情報システムや情報資産を管理する者等が策定することが適当である。

ケ　運用

情報セキュリティポリシーを確実に運用していくため、情報システムの監視や情報セキュリティポリシーにしたがって対策が適切に遵守されているか否かを確認し、情報資産に対する侵害や情報セキュリティポリシー違反に対し、適正に対

応しなければならない。

このため、緊急時対応計画の策定、同計画に基づく訓練、同計画の評価・見直し等を実施する。

コ 〔基本方針〕情報セキュリティ基本方針の目的

情報セキュリティ基本方針は、各地方公共団体における情報セキュリティ対策の基本となる事項を定めるとともに、地方公共団体が積極的に情報セキュリティ対策に取り組み、情報セキュリティの確保を図ることを住民に示すものである。

サ 〔基本方針〕情報セキュリティ基本方針の形式

情報セキュリティ基本方針の記載形式には、地方公共団体が実施する情報セキュリティ対策の基本的事項を項目立てて規定する形式のものと、民間企業等で情報セキュリティ対策を明らかにする際に多く使われる宣言書形式のものがある。

（ア）基本的事項を規定する形式の構成

基本的事項を記載する形式の情報セキュリティ基本方針では、地方公共団体において情報セキュリティ対策に取り組む基本的事項として、セキュリティ対策を実施する目的、対象とする脅威、情報セキュリティポリシーが適用される行政機関や情報資産の範囲、職員等の義務、必要な情報セキュリティ対策の実施、情報セキュリティ対策基準及び情報セキュリティ実施手順の策定等について規定する。

（イ）宣言書形式の構成

宣言書形式の情報セキュリティ基本方針は、地方公共団体の長又は最高情報統括責任者が、情報セキュリティ対策に積極的に取り組むことを対外的に宣言するところに特色がある。

宣言書形式の情報セキュリティ基本方針では、冒頭で情報セキュリティ対策に取り組む必要性や理念を記載し、全庁的な推進体制、情報セキュリティ対策基準及び情報セキュリティ実施手順の策定、主要な情報セキュリティ対策の実施、職員等のセキュリティポリシー遵守義務等を規定している。

地域全体の情報セキュリティ基盤の強化に積極的に貢献していくことを宣言に含めることも考えられる。

なお、宣言書形式の基本方針とする場合、情報セキュリティ対策基準に用語の定義、対象とする脅威、実施手順書の非公開に関する規定等を設ける必要がある。

シ 〔対策基準〕対象範囲

情報セキュリティポリシーを適用する行政機関及び情報資産の範囲を明確にする。

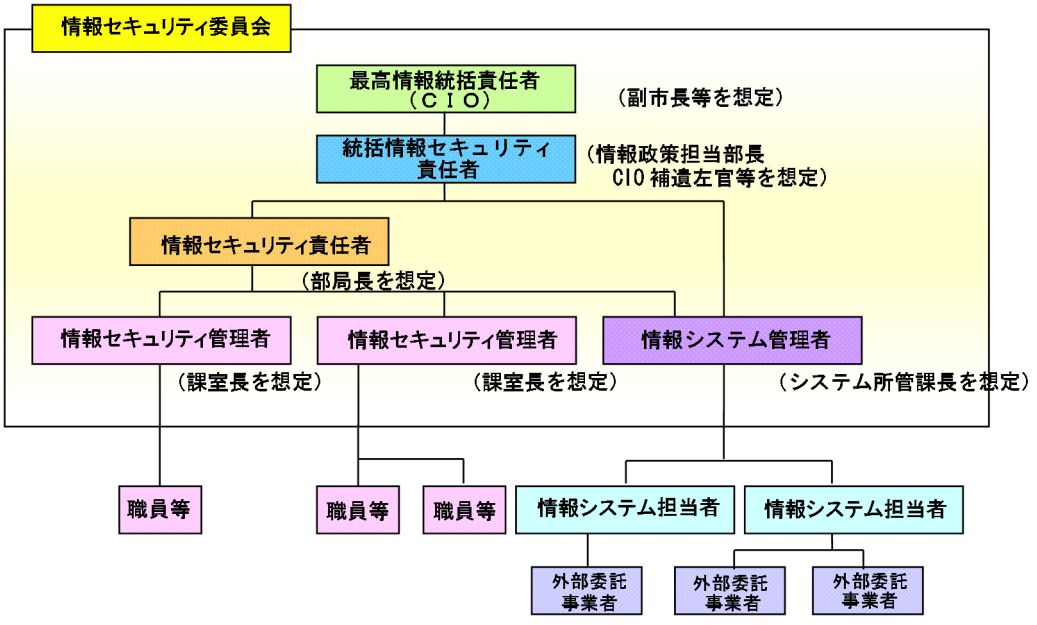
表－２５　情報資産の種類と例

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルータ等の通信機器
情報システム	サーバ、パソコン、汎用機、オペレーティングシステム、ソフトウェア等
これらに関する施設・設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル
電磁的記録	CD-R、DVD-R、フロッピディスク、MO、DLT（Digital Linear Tape）、USBフラッシュメモリ等
ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ（これらを印刷した文書を含む。）
システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

出典：情報セキュリティポリシーガイドライン

ス　〔対策基準〕組織体制

組織として、情報セキュリティ対策を確実に実施するには、情報セキュリティ対策に取り組む十分な組織体制を整備し、一元的に情報セキュリティ対策を実施する必要がある。このことから、情報セキュリティ対策のための組織体制、権限及び責任を規定する。



図－３３　情報セキュリティ推進の組織体制例

出典：情報セキュリティポリシーガイドライン

セ　〔対策基準〕情報資産の分類と管理方法

情報資産を保護するには、まず情報資産を分類し、分類に応じた管理体制を定める必要がある。

情報資産の管理体制が不十分な場合、情報の漏えい、紛失等の被害が生じるおそれがある。そこで、機密性・完全性・可用性に基づく情報資産の分類と分類に応じた取扱いを定めた上で、情報資産の管理責任を明確にし、情報資産のライフサイクルに応じて取るべき管理方法を規定する。

（ア）情報資産の分類[36]

情報資産は、機密性、完全性及び可用性[37]により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

a　機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・私物パソコンでの作業禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の外部記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・外部記録媒体の施錠可能な場所への保管
機密性２	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
機密性１	機密性２又は機密性３の情報資産以外の情報資産	

b　完全性による情報資産の分類

分類	分類基準	取扱制限
完全性２	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される、又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・外部記録媒体の施錠可能な場所への保管
完全性１	完全性２情報資産以外の情報資産	

36 情報セキュリティポリシーガイドライン 30 頁を参照のこと。

37 利用者が必要なときに情報資産にアクセスできることを確実にすること。

ｃ　可用性による情報資産の分類

分類	分類基準	取扱制限
可用性２	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される、又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・外部記録媒体の施錠可能な場所への保管
可用性１	可用性２の情報資産以外の情報資産	

ｄ　重要性に基づく情報資産の分類[38]

重要性分類
Ⅰ　個人情報及びセキュリティ侵害が住民の生命、財産等へ重大な影響を及ぼす情報。
Ⅱ　公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報。
Ⅲ　外部に公開する情報のうち、セキュリティ侵害が、行政事務の執行等に微妙な影響を及ぼす情報。
Ⅳ　上記以外の情報。

（イ）情報資産の管理

ａ　管理責任

情報資産の管理は、その情報資産に係る実務に精通している者が行う必要があり、ガイドラインでは、情報資産の管理責任者を情報セキュリティ管理者（課室長等）と想定している。

管理に当たっては、重要な情報資産について目録を作成することが望ましい。これにより、情報資産の所在、情報資産の分類、管理責任が明確になる。また、情報資産の管理について、管理不在の状態や二重管理にならないように留意することが重要である。

ｂ　情報資産の分類の表示

情報システムについて、当該情報システムに記録される情報の分類を規定等により明記し、当該情報システムを利用するすべての者に周知する方法もある。

機密性2以上、完全性2、可用性2の情報資産についてのみ表示を行い、表示のない情報資産は、機密性1、完全性1、可用性1とする運用もある。

38 情報資産の分類は、機密性、完全性及び可能性に基づき、分類することが望ましいが、職員の理解度等に応じ、本項目のような重要性に基づき分類することもありうる。

c　情報の作成

d　情報資産の入手

e　情報資産の利用

f　情報資産の保管

（a）情報セキュリティ管理者又は情報システム管理者は、利用頻度が低い外部記録媒体や情報システムのバックアップで取得したデータを記録する外部記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。【推奨事項】

（b）情報セキュリティ管理者又は情報システム管理者は、機密性2以上、完全性2又は可用性2の情報を記録した外部記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

g　情報の送信

h　情報資産の運搬

i　情報資産の提供・公表

j　情報資産の廃棄

上記cからjにおける情報資産の取扱いについて遵守すべき事項は、情報のライフサイクルに着目し定める。情報のライフサイクルには、作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等の局面がある。これらの局面ごとに、情報資産の分類に応じ取扱制限を定める。

ソ　〔対策基準〕物理的セキュリティ

（ア）サーバ等の管理

サーバ等のハードウェアは、情報システムの安定的な運用のために適切に管理する必要があり、管理が不十分な場合、情報システム全体に悪影響が及んだり、業務の継続性に支障が生じたりするおそれがある。

このことから、サーバ等の設置や保守・管理、配線や電源等の物理的セキュリティ対策を規定する。

サーバ等の機器が緊急停止した場合にも、業務を継続できるようにするために、バックアップシステムを設置することが有効である。

ただし、ハードウェアやソフトウェアが二重に必要となるほか、運用面でデータの同期化等が必要となり、多額の費用を要するので、これらの費用とサーバ等の緊急停止による損失の可能性を検討した上で、冗長化を行うか否かを判断する必要がある。

（イ）管理区域（情報システム室等）の管理

情報システム室等は、重要な情報資産が大量に保管又は設置されており、特に厳格に管理する必要がある。

情報システム室等が適切に管理されていない場合には、盗難、損傷等により重大な被害が発生するおそれがあり、このことから、情報システム室等の備えるべき要件や入退室管理、機器等の搬入出に関する対策を規定する。

ただし、対策によっては建物の改修を必要とするなど多額の費用を要するものもある。対策の実施に当たっては、費用対効果を考慮して行う必要がある。

（ウ）通信回線及び通信回線装置の管理

ネットワーク利用における通信回線及び通信回線装置が適切に管理されていない場合は、ネットワークそれ自体のみならず、ネットワークに接続している情報システム等に対しても損傷や不正アクセス等が及ぶおそれがある。

このことから、外部ネットワーク接続等の通信回線及び通信回線装置の管理にセキュリティ対策を規定する。

（エ）職員等のパソコン等の管理

職員等が利用するパソコン等の端末が適切に管理されていない場合は、不正利用、紛失、盗難、情報漏えい等の被害を及ぼすおそれがある。

このことから、これらの被害を防止するために、職員等のパソコン等の盗難及び情報漏えい防止策、パソコン等の持ち出し・持ち込み等に関する対策を規定する。

タ　〔対策基準〕人的セキュリティ

（ア）職員等の遵守事項

職員等が情報資産を不正に利用したり、適正な取扱いを怠った場合、コンピュータウイルス等の感染、情報漏えい等の被害が発生し得る。このことから、情報セキュリティポリシーの遵守や情報資産の業務以外の目的での使用の禁止等、職員等が情報資産を取り扱う際に遵守すべき事項を明確に規定する。

職員だけでなく、非常勤職員及び臨時職員、外部委託事業者についても、遵守事項を定めなければならない。

情報漏えい事案の多くが、職員等の故意又は過失による規定違反から生じており､職場の実態等を踏まえつつ､職員等の遵守事項を適正に定めるとともに、規程の実効性を高める環境を整備することが重要である。

（イ）研修・訓練

情報セキュリティを適切に確保するためには、情報セキュリティ対策の必要性と内容を幹部を含めすべての職員等が十分に理解していることが必要不可欠である。

情報セキュリティに関する事故の多くが、職員等の規定違反に起因している。情報セキュリティの向上は、利便性の向上とは、必ずしも相容れない場合があり、職員等の意識として業務優先で情報セキュリティ対策の軽視につながることもある。

また、情報セキュリティに関する脅威や技術の変化は早く、職員等には常に最新の状況を理解させることが必要である。

実際に事故が発生した場合に的確に対応できるようにするため、緊急時に対

応した訓練を実施しておくことが必要である。

これらのことから、職員等に情報セキュリティに関する研修・訓練を行うことを規定する。

（ウ）事故、欠陥等の報告

情報セキュリティに関する事故や情報システム上の欠陥の発生の予防が重要なことはいうまでもないが、完全な予防は事実上困難であることから、実際に事故や欠陥が発生した場合に、責任者に報告を速やかに行うことにより、被害の拡大を防ぎ、早期に回復を図れるようにしておく必要がある。

このことから、情報セキュリティに関する事故、欠陥があった場合の報告義務について規定する。

（エ）ID 及びパスワード等の管理

情報システムを利用する際の ID 及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（IC カード等）の管理が適切に行われない場合は、情報システム等を不正に利用されるおそれがある。

このことから、ID及びパスワード等の管理に関する遵守事項を規定する。認証情報等は、人的な原因により漏えいしやすい情報である。情報システム管理者からの認証情報等の発行から職員等での管理に至るまで、人的な原因で情報の漏えいするリスクを最小限にとどめる必要がある。

チ　〔対策基準〕技術的セキュリティ

（ア）コンピュータ及びネットワークの管理

ネットワークや情報システム等の管理が不十分な場合、不正利用による情報システム等へのサイバー攻撃、情報漏えい、損傷、改ざん、重要情報の詐取、内部不正等の被害が生じるおそれがある。

このことから、情報システム等の不正利用を防止し、また不正利用に対する証拠の保全をするために、アクセスログの管理やシステム管理記録の作成、バックアップ、無許可ソフトウェアの導入禁止、機器構成の変更禁止等の技術的なセキュリティ対策を規定する。

緊急時に備え、ファイルサーバ等に記録される情報について、バックアップを取ることが必要である。

なお、バックアップを行う場合には、データの保全を確保するため、バックアップ処理の成否の確認、災害等による同時被災を回避するためバックアップデータの別施設等への保管、システムを正常に再開するためのリストア手順の策定及びリストアテストによる検証が必要である。

（イ）アクセス制御

情報システム等がアクセス権限のない者に利用できる状態にしておくと、情報漏えいや情報資産の不正利用等の被害が発生し得る。

そこで、アクセス制御を業務内容、権限ごとに明確に規定しておく必要がある。

また、不用意なアクセス権限付与による不正アクセスを防ぐために、アクセス権限の管理は統括情報セキュリティ責任者及び情報システム管理者に集約することが重要である。

このことから、利用者登録や特権管理等を用いた情報システムへのアクセス制御、ログイン手順、接続時間の制限等不正なアクセスを防止する手段について規定する。

（ウ）システム開発、導入、保守等

システム開発、導入、保守等において、技術的なセキュリティ対策が十分に行われない場合は、プログラム上の欠陥（バグ）によるシステム障害等により業務に重大な支障が生じるおそれがある。

このことから、システム開発、導入、保守のそれぞれの段階における対策を規定する。なお、本規定にはシステムの更新又は統合時の十分な検証等も含まれる。

（エ）不正プログラム対策

情報システムにコンピュータウイルス等の不正プログラム対策が十分に行われていない場合は、システムの損傷、情報漏えい等の事故が発生するおそれがある。

不正プログラム対策としては、不正プログラム対策ソフトウェアを導入するとともに、パターンファイルの更新、ソフトウェアのパッチの適用を確実に実施することが基本であり、被害の拡大を防止することになる。

これらを踏まえ、不正プログラムの感染、侵入を予防し、更には感染時の対応として取るべき手段を規定する。

（オ）不正アクセス対策

情報システムに不正アクセス対策が十分に行われていない場合は、システムへの攻撃、情報漏えい、損傷、改ざん等の被害を及ぼすおそれがある。このことから、不正アクセスの防止又は被害を最小限にするため、不正アクセス対策として取るべき措置、攻撃を受けた際の対処及び関係機関との連携等について規定する。

（カ）セキュリティ情報の収集

ソフトウェアにセキュリティホールが存在する場合、システムへの侵入、改ざん、損傷、漏えい等の被害を及ぼすおそれがある。

また、情報セキュリティを取り巻く社会環境や技術環境等は刻々と変化しており、新たな脅威により情報セキュリティ事件、事故等を引き起こすおそれがある。

これらのことから、セキュリティホールをはじめとするセキュリティ情報の収集、共有及び対策の実施について規定する。

ツ 〔対策基準〕運用

（ア）情報システムの監視

情報システムにおいて、不正プログラム、不正アクセス等による情報システムへの攻撃・侵入、部内職員の不正な利用、自らのシステムが他の情報システムに対する攻撃に悪用されることを防ぐためには、ネットワーク監視等により情報システムの稼働状況について常時監視を行うことが必要である。

したがって、情報システムの監視に係る対策について規定する。

（イ）情報セキュリティポリシーの遵守状況の確認

情報セキュリティポリシーの遵守を確保するため、情報セキュリティポリシーの遵守状況等を確認する体制を整備するとともに、問題があった場合の対応について規定する。

（ウ）侵害時の対応

情報セキュリティに関する事故、システム上の欠陥及び誤動作並びに情報セキュリティポリシーの違反等により情報資産に対する侵害事案が発生した場合に、迅速かつ適切に被害の拡大防止、迅速な復旧等の対応を行うため、緊急時対応計画の策定について規定する。

地震及び風水害等の自然災害等や大規模・広範囲にわたる疾病等の事態に備えて、情報セキュリティにとどまらない危機管理[39]規定として業務継続計画（BCP: Business Continuity Plan）[40]を策定する場合、業務継続計画と情報セキュリティポリシーの間に矛盾があると、職員等は混乱し、適切な対応をとることができなくなるおそれがある。このため、各地方公共団体において業務継続計画を策定する場合には、情報セキュリティポリシーとの整合性[41]をあらかじめ検討し、必要があれば、情報セキュリティポリシーを改定しなければならない。

（エ）外部委託

情報システムの外部委託を行う際は、外部委託事業者からの情報漏えい等の事案を防止するために、情報セキュリティを確保できる委託先を選定し、契約で遵守事項を定めるとともに、定期的に対策の実施状況を確認する必要がある。

---

39 危機管理には、大規模・広範囲にわたる疾病等によるコンピュータ施設の運用にかかる機能不全等への考慮も望まれる。

40 大地震を対象事態とした ICT 部門における業務継続計画の策定については、「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）を参照のこと。

41 整合性を検討すべき事項は、例えば、施設の耐災害性対策、施設・情報システムの地理的分散、非常用電源の確保、人手による業務処理や郵送・電話の利用を含む情報システム以外の通信手段の利用、事態発生時の対応体制及び要員計画などがある。

このことから、外部委託を行う際に、情報セキュリティ確保上必要な事項について規定する。

なお、個別団体が単独で外部委託する場合だけでなく、共同アウトソーシングやASP（Application Service Provider）[42]、SaaS（Software as a Service）[43]サービス利用の形態等により地方公共団体が共同で外部委託する場合にも対策を行う必要があることに留意する。

（オ）例外措置

情報セキュリティポリシーの規定をそのまま適用した場合に、行政事務の適正な遂行を著しく妨げるなどの理由により、これに代わる方法によることやポリシーに定められた事項を実施しないことを認めざるを得ない場合がある。

このことから、あらかじめ例外措置について規定する。

（カ）法令遵守

職員等は、すべての法令を遵守することは当然であるが、職員等が業務を行う際の参考として、情報セキュリティに関する主要な法令を明示し、法令の遵守を確実にする。

（キ）懲戒処分等

情報セキュリティポリシーの遵守事項に対して、職員等が違反した場合の事項を定めておくことは、情報セキュリティポリシー違反の未然防止に、一定の効果が期待される。

このことから、情報セキュリティポリシー違反に対する懲戒処分の規定及び懲戒に係る手続きについて規定する。

テ　〔対策基準〕評価・見直し

（ア）監査

情報セキュリティポリシーの実施状況について、客観的に専門的見地から評価を行う監査が実施されない場合は、情報セキュリティ対策が徹底されない状態や情報セキュリティポリシーが業務に沿わない状態が続くおそれがある。

このことから、監査の実施及びその方法について規定する。監査を行う者は、十分な専門的知識を有するものでなければならない。

また、適正な監査の実施の観点から、監査の対象となる情報資産に直接関係しない者であることが望ましい。

地方公共団体内の情報セキュリティ対策の監査・報告について中立性を保証され、監査に必要な情報へのアクセス等の権限が明確に与えられる必要がある。

---

42 アプリケーションソフトの機能をネットワーク経由で顧客にサービスとして提供する事業者のこと。

43 ソフトウェアの機能のうち、ユーザが必要とするものだけをサービスとして配布し利用できるようにしたソフトウェアの配布形態。近年では、サーバ上で動作するソフトウェアの機能をネットワークを介してオンラインで利用する形態が多くなっている。

監査作業に伴う情報の漏えいのリスクを最小限とするため、監査人等が取扱う監査に係る情報について、漏えい、紛失等が発生しないように保管する必要がある。

（イ）自己点検

情報セキュリティポリシーの履行状況等を自ら点検、評価することは、情報セキュリティポリシーの遵守事項を改めて認識できる有効な手段である。

自己点検は、情報システム等を運用する者又は利用する者自らが実施するので、監査のような客観性は担保されないが、監査と同様に、点検結果を踏まえ各部門で改善を図ったり、組織全体のセキュリティ対策の改善を図る上での重要な情報になる情報セキュリティ対策の評価を行い、対策の見直しに資するものである。

また、職員等の情報セキュリティに関する意識の向上や知識の習得にも有効である。

このことから、自己点検を定期的に実施する規定を設け、その活用方法と併せて規定する。

（ウ）情報セキュリティポリシーの見直し

情報セキュリティ対策は、情報セキュリティに関する脅威や技術等の変化に応じて、必要な対策が変化するものであり、情報セキュリティポリシーは、定期的に見直すことが求められる。

また、監査や自己点検の結果等から、同ポリシーの見直しの必要性が確認される場合もある。

このことから、情報セキュリティポリシーの見直しについて規定する。

２　運用体制に関する事例

地方公共団体における情報セキュリティ等に関する運用体制の事例を以下に示す。

（１）新宿区

ア　情報セキュリティ規則

（ア）体制

ａ　情報化統括管理者

ネットワーク、情報システム、情報資産及び情報セキュリティに関する最終決定権限及び責任を有する（副区長)。

ｂ　ネットワーク管理者

情報化統括管理者を補佐する（総合政策部長)。

ｃ　統括情報セキュリティ責任者

部長、会計管理者、議会事務局長、教育委員会事務局次長、選挙管理委員会事務局長及び監査事務局長

ｄ　情報セキュリティ責任者

課長及び担当課長、特別出張所長、教育委員会事務局の各課長、中央図書館長、区立学校の長　等

（イ）役割

ａ　情報化統括管理者

区の情報セキュリティの最高責任者。最終決定権限及び責任を有する。

ｂ　ネットワーク管理者

ネットワーク及び情報システムの維持及び管理並びに情報セキュリティ実施手順の総合調整を行う。

ｃ　統括情報セキュリティ責任者

部等において所管する情報システムの連絡体制の構築、部等に所属する職員等の情報セキュリティポリシーに関する意見の集約並びに部等に所属する職員等に対する情報セキュリティポリシーの遵守に関する教育、訓練、助言及び指示を行う。

情報セキュリティ対策基準に基づき情報セキュリティ対策を行うため、情報セキュリティ実施手順を定める。

ｄ　情報セキュリティ責任者

統括情報セキュリティ責任者の下に、課等における情報セキュリティポリシーの遵守に関する権限及び責任を有する。

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

（２）横須賀市

ア　情報マネジメント規則

（ア）情報マネジメント監督会議及び情報マネジメント運営会議の設置

a　位置づけ　　：庁内組織

b　監督会議委員：委員長（市長）、副委員長（副市長）、委員（教育長、上下水道局長、各部長等）

c　運営会議委員：部長等が指名した職員（概ね各部の筆頭課長）

（イ）監理担当課

総務部文書管理主管課長（監督会議を所管）

（ウ）情報マネジメント担当課

情報システム主管課長（運営会議を所管）

（エ）部内情報マネジメント責任者

部内の課内情報マネジメント責任者を統括するため、部長等が指名する課長等をもって充てる。なお、各部等に１名以上置く。

（オ）課内情報マネジメント責任者

各課長等。なお、各課等に１名以上置く。

課内情報マネジメント責任者の責務は、次のとおり。

a　情報の取扱いにおいて、滅失、き損、漏えいその他の事故等が発生した場合の対処。

b　所属の職員、非常勤職員及び臨時職員に対する「情報の取扱いに関する研修」の定期的実施とその記録の保存。

c　業務の処理等を外部に委託する際の諸事項。

（カ）課内情報マネジメント担当者

課長等が指名する職員。なお、各課等に１名以上置く。

イ　電子情報取扱規程

（ア）統括管理責任者

個別管理システムを除くすべての情報システムの安定稼働等のシステム全体に関わる責任を負う。

（イ）個別管理責任者

個別管理システムの運用に関わる管理基準を定めなければならない。

（ウ）情報管理責任者

a　所管するすべての電子情報の管理責任を負う。

b　所管する電子情報に滅失、き損、漏えいその他の事故等が生じた場合は、次に掲げる者がその管理責任を負う。

（a）すべての電子情報：情報管理責任者

（b）電子情報のうち、情報管理担当者が実際に取り扱っている情報：情報管理担当者

（エ）情報更新権限管理責任者

a　所管するすべての電子情報の更新権限及び更新する電子情報の管理責任を負う。

b　所管する電子情報を更新することにより当該電子情報に事故等が生じた場合は、次に掲げる者がその管理責任を負う。

（a）更新されたすべての電子情報：情報更新権限管理責任者

（b）更新された電子情報のうち、情報更新責任担当者が実際に更新を行った電子情報：情報更新責任担当者

３　情報分類に関する事例

地方公共団体における情報管理等に関する分類の事例を以下に示す。

（１）新宿区

ア　〔情報セキュリティ対策基準〕情報資産の重要性分類

情報資産を作成した課の情報セキュリティ責任者は、当該情報資産の機密性、完全性及び可用性を踏まえ、当該情報資産を次に掲げる重要性分類に基づき分類し、目録を作成するものとする。

（ア）重要性分類Ⅰ

a　区民の財産及びプライバシー等に重大な影響を及ぼす情報資産

b　法令又は区の条例等により守秘されるものと規定されている情報資産

c　漏えいした場合、個人又は法人その他の団体の利益を害する等区に対する信頼を害するおそれのある情報資産

d　滅失し、又はき損した場合、その復元が困難となり、区の円滑な執行を妨げるおそれのある情報資産

e　情報システムに係るパスワード及び情報システムの設定情報

（イ）重要性分類Ⅱ

重要性分類Ⅰに分類される情報資産以外の情報資産

（２）横須賀市

ア　情報マネジメント規則

情報のセキュリティ・レベルを下記の４段階に分類している。

実施機関は、保有する情報を、その重要性及び事故等が起きた場合の影響範囲を考慮し、次に掲げるセキュリティ・レベルに区分する。

情報のセキュリティ・レベルは、当該情報を所管する課の課内情報マネジメント責任者が設定し、適宜見直すものとする。

（ア）Ⅰ類

セキュリティに対する侵害及び破壊が、市民の生命、財産、プライバシー等に重大な影響を及ぼすもの

（イ）Ⅱ類

セキュリティに対する侵害及び破壊が、行政事務の執行等に重大な影響を及ぼすもの

（ウ）Ⅲ類

セキュリティに対する侵害及び破壊が、行政事務の執行等に軽微な影響を及ぼすもの

（エ）Ⅳ類

セキュリティに対する侵害及び破壊が、行政事務の執行等に影響をほとんど及ぼさないもの

４　情報セキュリティポリシーの事例

地方公共団体における情報セキュリティポリシーの事例を以下に示す。

（１）地方公共団体における情報セキュリティポリシーの策定状況

ア　〔被災県の状況〕宮城県

（ア）宮城県情報セキュリティ基本方針

基本方針は国の指針に沿った（ほぼ同様の）記述となっている。

（イ）情報セキュリティ対策基準

インターネットへの開示はなされていないが、「基本方針に対策基準及び実施手順を遵守します。」との記述があり、策定されているものと思われる。

イ　〔被災県の状況〕福島県

（ア）福島県情報セキュリティ基本方針

基本方針は国の指針に沿った（ほぼ同様の）記述となっている。

（イ）情報セキュリティ対策基準

インターネットへの開示はなされていないが、「第 7」に「情報セキュリティ実施手順の策定」との条文があり、策定されているものと思われる。

ウ　〔被災県以外の状況〕東京都

（ア）東京都情報セキュリティ基本方針

基本方針は国の指針に沿った（ほぼ同様の）記述となっている。

（イ）情報セキュリティ対策基準

インターネットへの開示はなされていないが、基本方針の記述に「情報セキュリティ実施手順」と記載されており、組織（学校等）若しくはシステム（税総合システム等）ごとに定められているものと思われる。

エ　〔被災県以外の状況〕神奈川県

（ア）神奈川県情報セキュリティポリシー（要綱）

要綱であるが、記述内容は「基本方針」である。

（イ）情報セキュリティ対策基準

要綱の「8」において情報セキュリティ対策基準の策定を位置づけ、「9」で情報セキュリティ実施手順の策定を位置づけており、策定されているものと思われる（上記 2 点については、インターネット上への開示はされていない）。

オ　〔被災県以外の状況〕新宿区

（ア）新宿区情報セキュリティ規則

第１節１（1）において既に調査した内容。区では基本方針に該当する部分を「規則」として定めている。

（イ）新宿区情報セキュリティ対策基準

同上

カ　〔被災県以外の状況〕横須賀市

情報マネジメント規則及び電子情報取扱規程をもって、情報セキュリティポリシーとしているものと思われる。

キ　〔被災県以外の状況〕西宮市

（ア）西宮市情報セキュリティポリシー

情報セキュリティマネジメントシステム（ISMS）を基盤にした各種対策を実施している（ISMS をもって代替えしているものと思われる）。

（２）地方公共団体における情報セキュリティポリシーの事例

地方公共団体における情報セキュリティポリシーの事例として、仙台市と神戸市の事例を以下に示す。

なお、比較のため、仙台市の基本方針－1 から対策基準－10 の項番に対応させているので、神戸市の項番には空欄等が存在する。

ア　〔仙台市の事例〕基本方針と対策基準の項目

（ア）情報セキュリティ基本方針

基本方針－1：目的
基本方針－2：定義
基本方針－3：情報セキュリティポリシーの位置づけ
基本方針－4：情報セキュリティポリシーの対象範囲
基本方針－5：職員の責務
基本方針－6：管理体制
基本方針－7：情報資産の分類
基本方針－8：情報資産への脅威
基本方針－9：情報セキュリティ対策
基本方針－10：情報セキュリティ対策基準の策定
基本方針－11：情報セキュリティ実施手順（運用マニュアル）の策定
基本方針－12：評価・見直し

（イ）情報セキュリティ対策基準

対策基準－1：管理体制
対策基準－2：権限、役割及び責任
　　最高情報セキュリティ責任者

局（区）情報管理者
情報管理者
システム管理者
ネットワーク管理者
副情報管理者

対策基準－3：情報資産の分類と管理
・行政情報の分類：4段階に分けて定義している
重要性分類Ⅰ：機密、非開示情報　等
重要性分類S:Ⅰに分類される行政情報のうち､滅失又はき損した場合、行政の円滑な執行に重大な支障をきたす行政情報
重要性分類Ⅱ：市の情報公開条例の条文で定義された非公開情報
重要性分類Ⅲ：重要性分類S、Ⅰ及びⅡ以外の行政情報
・情報システムの分類
・行政情報の管理方法：管理及び取扱い、外部記録媒体の管理、重要性分類S、Ⅰ及びⅡのバックアップ　等
具体的管理方法は「共通実施手順」による
・情報システムの管理方法
対策基準－4：人的セキュリティ
対策基準－5：セキュリティ教育
対策基準－6：物理的セキュリティ
対策基準－7：技術的セキュリティ
対策基準－8：運用
対策基準－9：法令等順守
対策基準－10：評価・見直し等

イ　〔神戸市の事例〕基本方針と対策基準の項目

（ア）情報セキュリティ基本方針

基本方針－1：目的
基本方針－2：定義
基本方針－3：情報セキュリティポリシーの位置づけ及び構成
基本方針－4：適用範囲
基本方針－5：職員等の責務
基本方針－6：情報セキュリティ管理体制
－
基本方針－8：情報資産への脅威
基本方針－9：情報セキュリティ対策
基本方針－10：情報セキュリティ個別基準の策定
基本方針－11：情報セキュリティ実施手順の策定
基本方針－12：情報セキュリティ監査及び自己点検の実施
基本方針－13：情報セキュリティポリシーの見直し

（イ）情報セキュリティ対策基準

・目的

・適用範囲

対策基準－1：情報セキュリティ管理体制

・体制

情報セキュリティ最高責任者
情報セキュリティ統括責任者
情報セキュリティ責任者
情報セキュリティ管理者
情報基盤管理者
基幹系ネットワーク管理者
情報系ネットワーク管理者
情報責任者
情報管理者
業務システム責任者
業務システム管理者
大型汎用機器管理者
情報セキュリティ監査統括責任者
神戸市情報課推進会議

－

対策基準－3：情報資産の分類と管理

・機密性：3 段階

・完全性：3 段階

・可用性：3 段階

・リスク分析の実施

・情報資産の管理方法：情報資産の管理、データの作成、情報資産の入手、情報資産の利用、情報資産の保管、情報資産の提供・公表、情報資産の廃棄

・文書の管理

・記録の管理

－

対策基準－6：物理的セキュリティ

対策基準－4：人的セキュリティ（セキュリティ教育を含む）

対策基準－7：技術的セキュリティ

対策基準－8：運用面のセキュリティ

・情報セキュリティ個別基準の策定

・情報セキュリティ実施手順の策定

対策基準－9：情報セキュリティポリシー等に関する違反に対する対応

対策基準－10：評価・改善・見直し

５　ICT - BCP ガイドラインの概要

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[44]（以下「ICT - BCP ガイドライン」という。）の概要を以下に示す。

（１）ICT - BCP ガイドライン（平成 20 年 8 月版）の概要

ア　当該ガイドラインの目的

地方公共団体は、災害時において、地域住民の生命、身体の安全確保、被災者支援、企業活動復旧のために、被害応急業務、復旧業務及び平常時から継続しなければならない重要な業務を実施していく責務を負っており、役所の業務全般において業務継続計画を策定する動きが未だなくても、率先して「情報システムに関する業務継続計画」を策定し、業務の継続力を高めていかなくてはならない。

このような問題意識から、総務省では、情報システムを所管する ICT 部門の業務継続計画（BCP）策定に向けた地方公共団体の取組を支援するため、ガイドラインを作成した。

イ　当該ガイドラインの基本的考え方

当該ガイドラインでは、下記の3点を対象としている。

・ICT部門を対象とする
・大地震を主たる対象事業とする
・あらゆる規模の地方公共団体を対象とする

当該ガイドラインでは、多数の対応可能な職員がいる大規模な団体だけでなく、小規模な団体でも実際に使用できるようにするという現実的な観点から、ステップアップ方式を採用している。

ウ　業務継続計画とは

「業務継続計画」とは、災害・事故で被害を受けても、重要業務をなるべく中断させず、中断してもできるだけ早急に（あるいは許容される中断時間内に）復旧させる「業務継続」を戦略的に実現するための計画である。

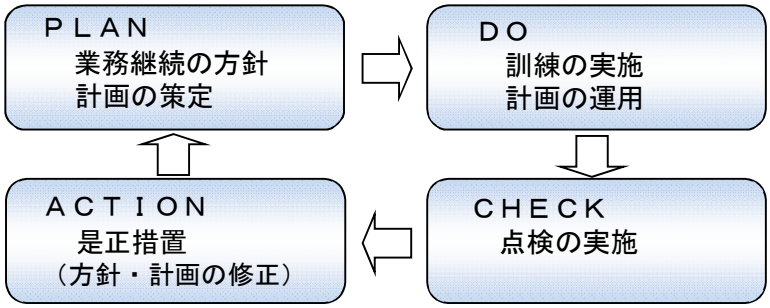
エ　計画の継続的改善

最初から完璧な業務継続計画を策定しようとしても困難である。

まずは対象範囲を限定して、可能な範囲で検討することが重要であり、業務継続の取組の全体を「BCM（Business continuity Management : 業務継続管理）」という。

---

44 詳細は、下記（総務省ホームページ）を参照のこと。
http://www.soumu.go.jp/main_content/000145527.pdf



図－３４　業務継続計画のマネジメントサイクル

出典：ICT - BCP ガイドライン

オ　業務継続計画の必要性

当該ガイドラインでは、下記の5点を業務継続計画の必要性として整理している。

（ア）地方公共団体の社会的責任
（イ）危機管理に対する市民の意識の高まり
（ウ）業務継続計画と地域防災計画との関係
（エ）業務継続に関わるガイドライン策定の動き
（オ）リスクの発生懸念の増加

カ　地方公共団体における ICT 部門の取組のあるべき姿

当該ガイドラインでは、下記の8点を地方公共団体におけるICT部門の取組のあるべき姿として整理している。

（ア）最低限のバックアップの実施
（イ）ICT部門としての緊急時対応体制の検討
（ウ）災害時の行動を指揮できる管理者の育成
（エ）外部事業者との連携・協力関係の構築
（オ）情報通信機器の固定措置の実施
（カ）地方公共団体間の協力関係の構築
（キ）既存のマネジメントとの整合
（ク）遠隔地で運用しているサービスの利用

表－２６　情報セキュリティ対策と ICT 部門における業務継続計画の比較

	情報セキュリティ対策	ICT部門の業務継続計画
活動視点	機密性、完全性、可用性	可用性、継続性
管理対象	保護資産 （電子的記憶媒体上のデータ、通信回線上のデータ、プログラムコード、利用主体（ユーザ）、情報処理システム、ネットワークシステム、情報機器等）	重要業務と重要資産（建物、要員、データ、設備、電気、備品等）
活動目的	対象資産の保護	業務継続とそのための重要資源の確保
想定脅威	サイバーテロ、情報システム障害、人為的な犯罪行為、オペレーションミス等（周辺のリソースは平常どおり使用できる状況を想定）	地震、水害、新型インフルエンザ、情報システム障害等（周辺のリソースに被害がある状況）
主要活動領域	防犯領域	防災・危機管理領域

出典：ICT－BCP ガイドライン

表－２７　ASP、SaaS の長所と留意事項

長所	・サービス提供事業者の情報通信機器設置環境は一般的に堅牢であり、地方公共団体が通常負担できるレベルを上回る。 ・地方公共団体の庁舎内で、設備の耐震性の確保等の業務継続上の対策の必要性が少ない。 ・外部のリソースを活用するため、要員増大の抑制が可能である。
留意事項	・ネットワークが切断されるとサービスが停止するため、ネットワーク機能の継続ができる仕組みも検討していく必要がある。 ・地方公共団体の庁舎内での端末の稼働は不可欠なので、庁舎の耐震性、電力確保の対策等の必要性はあまり変わらない。 ・堅牢とはいえ、事業者の拠点の災害リスクを考慮する必要がある。 ・サービス内容によっては外部のサーバに重要な情報を保存することとなるため、導入に当たっては機密保持契約、情報漏洩対策等セキュリティ面での対策を実施する必要がある。

出典：ICT－BCP ガイドライン

キ　ICT 部門の業務継続計画策定に当たっての留意点

（ア）当該ガイドラインでは、下記の4点を地方公共団体においてICT部門の業務継続計画の策定を検討するに当たっての留意点として整理している。

a　地域条件

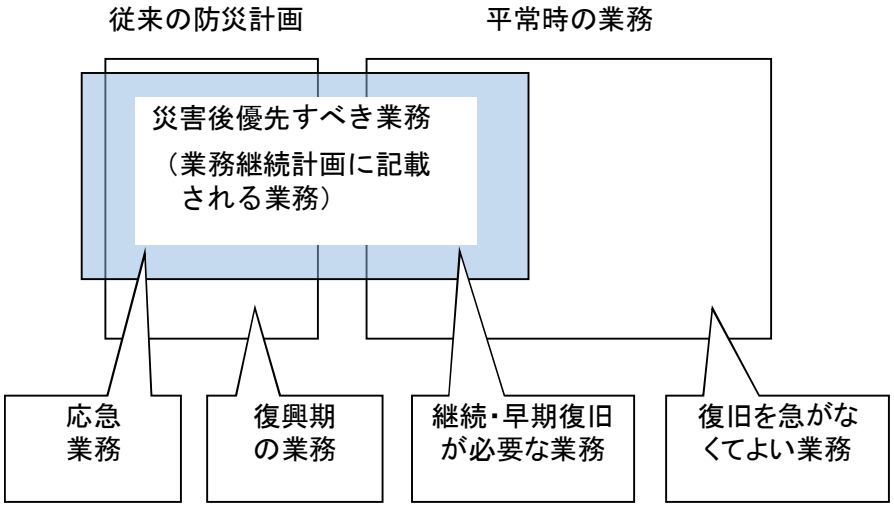
b　外部への依存

c　災害対策実施状況の格差

d　サーバ設置場所

（イ）業務視点での整理

地方公共団体における被害後の業務範囲のイメージは**図－３５**のとおりである。



図－３５　行政機関の防災計画、平常時の業務

出典：丸谷浩明著「事業継続の意義と経済効果」

ク　ガイドラインの構成

ガイドラインでは、3 部構成のステップアップ方式を採用し、全庁的な判断が必要な投資等の抜本的な対策の提案・実施に進むことが可能となるような工夫をしている。

（ア）第 1 部　BCP 策定の基盤づくり

ICT 部門が主導して検討や実施が可能な範囲での課題を取り上げ、各種の対策の実施計画及び災害時の行動計画を策定する。

（イ）第 2 部　簡略な BCP の策定

第 1 部を発展させて、業務部門（情報システムを業務で利用する各部門）を含めた検討体制を構築し、業務部門の意向も踏まえた簡略な業務継続計画を策定することを目的とする。

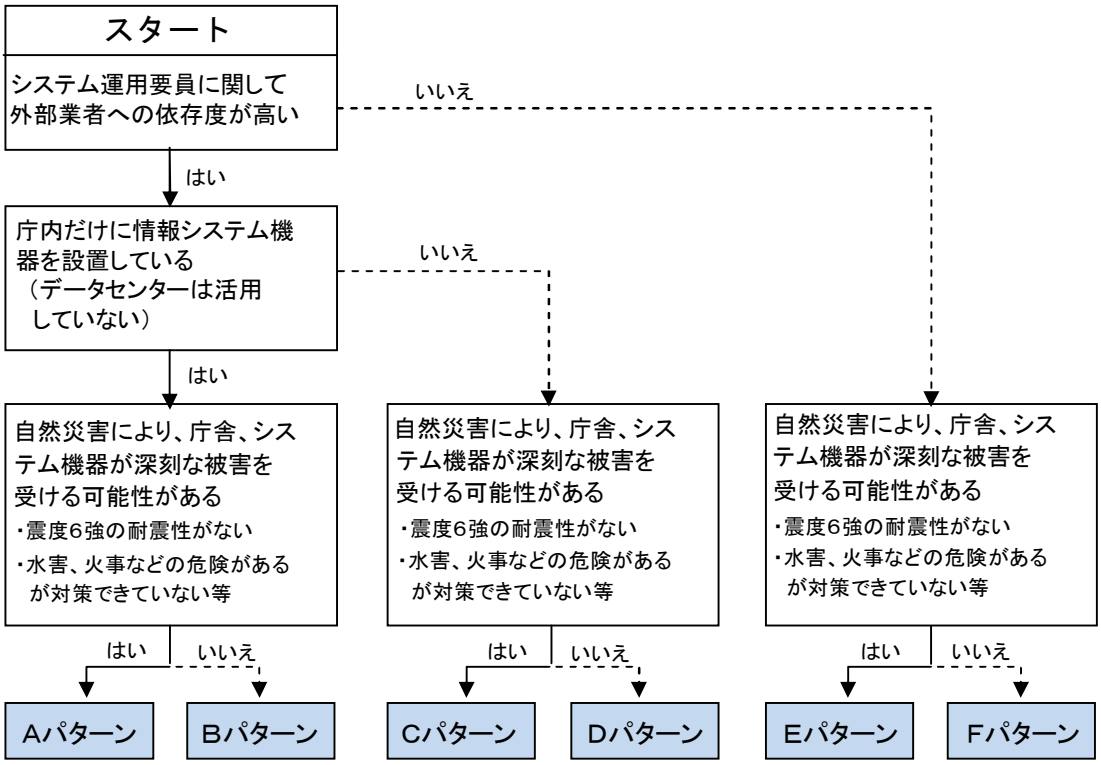
（ウ）第 3 部　本格的な BCP の策定と全庁的な対応との連動

本格的な ICT 部門の業務継続を追求するためには多額の投資判断を要する事項も検討し、業務継続計画に位置づけ、着実に実施していく必要があり、そのような本格的な業務継続計画の策定を目的とする。

ケ　自らの状況の理解

地方公共団体によって、災害・事故時に情報システムの機能を継続、早期復旧するための条件・環境は多様であるため、各々の状況に合った業務継続計画を検討することが必要である。

次図の分岐フローで自らがどのパターンにあるかを把握し、どういった事項を中心に検討すべきかを理解することが必要である。



図－３６　パターン把握

出典：ICT－BCP ガイドライン

以下の表では、前頁の各パターンについて、下記の３点を説明している。

（ア）被災した場合の実態を把握すべき範囲

（イ）最優先して実施すべき対策

（ウ）その次に実施すべき対策

表－２８　中心的に検討すべき項目

	中心的に検討すべき項目
A	(ア)被災した場合の庁舎、情報システム、要員（外部事業者を含む。）の実態を把握する。 (イ)大きな物理的被害が懸念されるので、早急に低コストの減災対策及び情報システムの機能の継続対策を実施する。 (ウ)(イ)と同時並行的に、外部事業者のシステム運用要員を含めた緊急連絡手段、参集、安否確認等の初動計画も策定する。その終了後、外部へのバックアップの搬送や代替設備の利用等の検討を行う。
B	(ア)被災した場合の庁舎、情報システム、要員（外部事業者を含む。）の実態を把握する。 (イ)災害時の情報システムの被害は比較的軽微とみられるため、外部事業者のシステム運用要員を含めた緊急連絡手段の整備、参集、安否情報等の初動計画を整備する。 (ウ)外部へのバックアップの搬送や代替設備の利用等の検討を行う。
C	(ア)被災した場合の庁舎、外部情報センター、情報システム、要員（外部事業者を含む。）の実態を把握する。 (イ)大きな物理的被害が懸念されるので、早急に低コストの減災対策及び情報システム機能の継続対策を実施する。 (ウ)(イ)と同時並行的に、外部データセンターについても、災害耐性を確認し、外部事業者のシステム運用要員を含めた緊急連絡手段の整備、参集、安否確認等の初動計画を整備する。その終了後、外部へのバックアップの搬送や代替設備の利用等の検討を行う。
D	(ア)被災した場合の庁舎、外部データセンター、情報システム、要員（外部事業者を含む。）の実態把握を実施する。 (イ)災害時の情報システムの被害は比較的軽微の可能性があるため、外部事業者のシステム運用要員を含めた緊急連絡手段の整備、参集、安否情報等の初動計画を整備する。 (ウ)外部へのバックアップの搬送や代替設備の利用等の検討を行う。
E	(ア)被災した場合の庁舎、情報システム、要員の実態を把握する。 (イ)大きな物理的被害が懸念されるので、早急に低コストの減災対策及び情報システムの機能の継続対策を実施する。 (ウ)(イ)と同時並行的に、職員の緊急連絡手段、参集、安否確認等の初動計画を策定する。その終了後、外部へのバックアップの搬送や代替設備の利用等の検討を行う。
F	(ア)被災した場合の庁舎、情報システム、要員の実態を把握する。 (イ)災害時の情報システムの被害は比較的軽微の可能性があるため、職員の緊急連絡手段の整備、参集、安否情報等の初動計画を整備する。 (ウ)外部へのバックアップの搬送や代替設備の利用等の検討を行う。

出典：ICT－BCP ガイドライン

コ　第１部　BCP 策定の基盤づくり

（ア）ステップ１：ICT 部門のメンバーの選定

ａ　手順１　検討メンバーの選定

（ａ）業務継続計画策定プロジェクト運営責任者（１名）

（ｂ）担当者（最低限、1～2 名）

（イ）ステップ 2：情報システムの現状調査

a　手順 1　情報システム一覧の作成

既存資料等を参考に、情報システムごとに次表の事項を調査する。

表－２９　情報システム調査項目

対象情報システム	名称
	情報システムの概要（使用している業務）
	主管部門
ハードウェア	機種名
	設置場所
	保守事業者
ソフトウェア	OSの名称・バージョン、インストールされているアプリケーション →故障した場合にすぐに再インストールできるか否かを確認する
	アプリケーションのバックアップの有無
	アプリケーションのバックアップ形態
	アプリケーションのバックアップ保管場所
代替機器	ハードウェアの損壊時に代替機として使用できる機器があるか →市販されているOS（WindowsXP等）で動作しており、 どのような機器でも直ちに再インストールして動作するものは、 代替機があると同等に考える。
	代替機の設置場所
クライアントPC	クライアントPCの特殊性の有無 →市販されていない特殊なソフトウェアのインストールが必要か 否かで判断する。

出典：ICT－BCP ガイドライン

b　手順 2　ネットワークの整理

c　手順 3　外部事業者との関係整理

主要な外部事業者（保守事業者等）について次表の事項について確認することが必要である。

パターン E、F の場合は、本手順を実施する必要性は高くない。

表－３０　外部事業者との関係整理項目

契約事項	災害・事故時を含むサービス稼働率に関する取決め事項があるか
	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
	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
	一定以上の被害が起きた場合に、代替機器や場所を提供するなどのサービス継続に関する取決め事項があるか
同時被災する可能性	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。 →同時被災する地域内の判断がつかない場合は、地震を念頭に数十km離れているかどうかで判断する。
	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があるか
契約以外の協力関係について	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取決めがあるか
	電話が繋がらない場合に備えて、他の拠点の電話番号、衛星電話番号、メールアドレス等の代替連絡先を把握しているか
	複数の担当者に直接連絡できるように、電話番号、メールアドレス等を把握しているか

出典：ICT－BCP ガイドライン

（ウ）ステップ 3：庁舎・設備等の災害危険度の調査

a　手順１　庁舎、設備等の脆弱性の点検

b　手順２　庁舎、設備等の脆弱性以外に認識すべきリスク

（エ）ステップ 4：ICT 部門主導で実施できる庁舎・設備等の対策

a　手順１　庁舎の脆弱性への対策

b　手順２　情報通信機器の脆弱性への対策

c　手順３　ネットワークの脆弱性への対策

d　手順４　その他の設備等の脆弱性への対策

（オ）ステップ 5：重要情報のバックアップ

a　手順１　重要情報の把握

まず、行政として、どんな場合にも失ってはならない情報や文書、業務の継続に不可欠な情報や文書としてどのようなものを保有・蓄積しているのかを調査・把握することが必要である。

以下の２つのいずれかに当てはまる情報は、最低限守るべきものとして扱うことが重要である。

（ａ）大地震等災害・事故が発生した場合にすぐ使用するデータ、復旧に不可欠な図面や機器の仕様書等の書類

・住民記録～住民（外国人含む）の安否確認のためなど

・介護受給者情報

・障がい者情報
・道路その他の復旧に重要なインフラの図面又はそのデータ
・情報通信機器等の重要機器の修復に不可欠な仕様書

（b）地方公共団体のみが保有しており、滅失した場合に元に戻すことが不可能あるいは相当困難なデータ
・税金や水道料金等の収納状況等に関する情報
・国民健康保険業務、介護保険業務に関する情報
・許認可の記録、経過等の情報
・重要な契約、支払い等の記録の情報

b　手順 2　重要情報の喪失危険性の把握

把握した重要情報の管理の現状について、以下の項目を調査する必要がある。

（a）どの場所、どの機器に情報が格納されているか

（b）バックアップを実施しているか

（c）バックアップをしている場合は、バックアップ媒体がどのように管理されているか（別の拠点に定期的に移動しているか、耐火金庫等に格納されているかなど）

各人のパソコンに重要情報があり、バックアップを定期的に行っていない場合、パソコンが転倒したり、滑落しただけでも重要情報を喪失する可能性があることを認識すべきである。

c　手順 3　重要情報の保護に関する脆弱性への対策

（a）バックアップの実施

現時点で重要情報のバックアップが取られていない場合、情報通信機器が損壊するとデータを復旧させることが不可能となり、業務の継続が著しく困難となる状況が予想される。

まずは初歩的な方式でも定期的なバックアップを実施することが不可欠である。

一般的にはテープ媒体によるバックアップが考えられる。より簡易な方法としては、定期的にデータが蓄積されている危機とは異なる機器にリモートコピーをすることがある。

さらに、定期的に紙媒体に印刷することも最低限の対策としての一案である。

現状では、作業中の重要なデータが各人の PC の中にのみ保管されている状態にあることはかなり多いと考えられる。全庁的にこの傾向が見られる場合には、ICT 部門が率先してバックアップを実施しているサーバで重要情報を保管するように運用方法を変更し、そのノウハウを蓄積し、それを活用して他の部門も働きかけることが有効な一案である。

（b）バックアップ媒体の保管について

庁舎内に入れない被害状況となれば、同じ庁内でいくらバックアップを取っておいても意味がない。バックアップ媒体を定期的に異なる庁舎等に

移動させることでリスクは大幅に減少する。可能であれば県外等遠隔地に定期的に移動させておくことが望ましいが、同じ地域内でも耐震性の高い別の庁舎に移動させるだけでも重要情報が情報通信機器と同時被災するリスクは軽減される。

（カ）ステップ 6：初動行動計画の立案

a　手順１　ICT 部門としての行動開始基準の設定
b　手順２　ICT 部門としての緊急時対応体制
c　手順３　緊急連絡先の調査
d　手順４　緊急時の行動手順検討

（キ）ステップ 7：ICT 部門内の簡易訓練

a　手順１　訓練計画の策定
b　手順２　訓練の実施
c　手順３　訓練結果の業務継続計画への反映

（ク）ステップ 8：運用体制の構築と維持管理

a　手順１　運用体制の決定
b　手順２　見直し時期と内容、承認ルールの決定

サ　第 2 部　簡易な BCP の策定

（ア）ステップ 9：BCP 策定体制の構築

a　手順１　ICT 部門の検討メンバーの選定
（a）業務継続計画策定プロジェクト運営責任者（1 名）
（b）調査・文書作成担当（数名）
b　手順２　ICT 部門以外の検討メンバーの選定

（イ）ステップ 10：被害の想定

a　手順１　対象とする事象の特定
b　手順２　被害状況の想定

（ウ）ステップ 11：重要業務・重要情報システムの選定

a　手順１　業務影響分析
（a）インタビュー等の調査方式の決定について

表－３１　業務影響分析の調査方式

	インタビュー方式	アンケート方式
方式	各個人と直接に面談してヒアリングする	アンケート形式にして回答を求める
長所	業務継続計画の概要や必要性を直接説明できるため、的外れの回答結果になりにくい	アンケートを一斉配布すればよいため、回答者数が多いほど聞き取り時間を短縮できる
短所	回答者の時間調整が必要であり、回答者が多い場合には適さない	的外れの回答が返ってくる可能性や返答がない可能性があるため、回答者に対して質問の趣旨を説明する会合を開いたり、回答の趣旨や意図を確認したりする作業が必要 個人回答とならないように、部門長の承認欄を経て提出するよう求めることが必要

出典：ICT－BCP ガイドライン

（ｂ）調査内容について

表－３２　影響の重大性の評価基準

影響の重大性		対象とする目標レベルに到達していないことに伴う代表的な影響の内容
Ⅰ	軽微	対象とする目標レベルに対象時間までに到達しなかったことによる社会的影響はわずかにとどまる。 ほとんどの人は全く意識しないか、意識をしてもその行政対応は許容可能な範囲であると理解する。
Ⅱ	小さい	対象とする目標レベルに対象時間までに到達しなかったことにより若干の社会的混乱が発生する。 しかし、大部分の人はその行政対応は許容可能な範囲であると理解する。
Ⅲ	中程度	対象とする目標レベルに対象時間までに到達しなかったことにより社会的混乱が発生する。 社会的批判が一部で生じ、過半の人はその行政対応は許容可能な範囲であると理解する。
Ⅳ	大きい	対象とする目標レベルに対象時間までに到達しなかったことにより相当の社会的混乱が発生する。 社会的批判が発生し、過半の人はその行政対応は許容可能な範囲外であると理解する。
Ⅴ	甚大	対象とする目標レベルに対象時間までに到達しなかったことにより甚大な社会的混乱が発生する。 大規模な社会的批判が発生し、大部分の人はその行政対応は許容可能な範囲外であると理解する。

出典：中央省庁業務継続ガイドライン

（ｃ）調査内容の再確認（アンケート方式の場合）

ｂ　手順２　重要業務の選定

ｃ　手順３　重要な共通情報システムの選定

ｄ　手順４　目標復旧時間・目標復旧レベルの決定

ｅ　手順５　重要情報の目標復旧時点の整理

（エ）ステップ 12：重要情報システムの継続に不可欠な資源の把握

ａ　手順１　最低限必要となる資源の把握

ｂ　手順２　資源の準備状況の調査

c　手順３　災害発生後に必要となる時期の見極め

（オ）ステップ 13：ICT 部門が中心に検討すべき事前対策

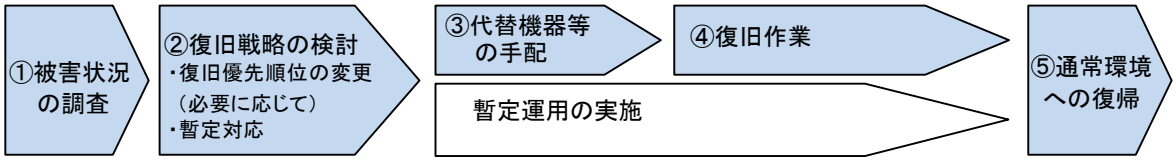
a　手順１　事前対策の検討

（カ）ステップ 14：外部事業者との運用保守契約の見直し

a　手順１　必要不可欠な外部事業者の把握
b　手順２　緊急時対応計画策定の要求
c　手順３　契約内容の見直し

（キ）ステップ 15：代替・復旧行動計画の立案

a　手順１　既存の防災計画等との整合
b　手順２　ICT 部門内のチーム編成
c　手順３　被害チェックリストの作成
d　手順４　復旧フェーズでの行動手順の検討



図－３７　一般的な復旧プロセス
出典：ICT－BCP ガイドライン

e　手順５　復帰フェーズでの行動手順の検討
f　手順６　参照する文書の整理

（ク）ステップ 16：本格的な訓練の実施

a　手順１　訓練計画の策定
b　手順２　訓練の実施
c　手順３　訓練を通した業務継続計画の課題の洗い出し・解決

シ　第３部　本格的な BCP の策定と全庁的な対応との連動

（ア）ステップ 17：ICT 部門の BCP 投資判断のための体制構築

a　手順１　首長等への報告とその参画
b　手順２　業務部門長の参画

（イ）ステップ 18：目標復旧時間・目標復旧レベルの精査

a　手順１　重要業務及び重要情報システムの見直し
b　手順２　前提事象の再検証
c　手順３　復旧見込み時間の見積

（ウ）ステップ 19：投資を含む本格的な対策

a　手順 1　対策案の洗い出し

（エ）ステップ 20：全庁的な点検・是正及び行動計画の見直し

a　手順 1　要検討課題の整理

b　手順 2　首長等による見直し

c　手順 3　本格的な事前対策の実施を踏まえた行動計画の修正

（２）平成 20 年 8 月版の ICT-BCP ガイドライン見直しの検討について

当該ガイドラインは、平成 20 年 8 月に公表されているが、東日本大震災を踏まえてどうするのか、東日本大震災の教訓をどう盛り込んでいくのかという観点での見直し作業が進められている。

検討のための組織は、「災害に強い電子自治体に関する研究会」で、「ICT 利活用 WG」と「ICT 部門の業務継続・セキュリティ WG」から構成されている。

ア　上記研究会における主な意見について

（ア）平成 24 年 2 月 21 日開催の「第 2 回合同 WG」での主な意見

a　東日本大震災で被災したある地方公共団体では、災害直後の状況を切り抜けると、次に復旧・復興のための業務が大量に発生したが、現行の ICT-BCP ガイドラインにはあまり記載がない。

b　このような業務にどのように対応するのかを明らかにするために、BCP が必要だと感じており、見直しに当たっては、このような点を重視した記載が必要だと思う。

c　現行のガイドラインは、第 2 部と第 3 部では被害想定に大きな違いがあり、第 3 部だと話が広がりすぎているような印象を持つ。

（イ）平成 24 年 4 月 23 日開催の「第 4 回合同 WG」での主な意見

a　初動にフォーカスを当てて議論をするのであれば、安否確認と情報提供が一番重要だと思う。

b　「ICT-BCP ガイドライン」のスコープについては、初動の動きは基本的に 24 時間、72 時間にしろ、被災を受けた自治体ではほぼ共通的になってくると思うので、それをできるだけイメージとして具体化し、それを支える ICT を早く復旧、継続するという観点を入れていく。

c　平成 20 年度に作成した「ICT-BCP ガイドライン」は、個別の要素としては非常にいいことがちりばめられているが、なかなか普及しなかった。今度メンテナンスしていくものに関しては、どうやって普及させていくかというやり方を踏まえた上での「ICT-BCP ガイドライン」の作り方を意識しておく必要がある。

イ　ICT-BCP ガイドライン改訂の方向性[45]

（ア）前述の検討を踏まえ、ICT-BCP ガイドライン改訂は「初動対応の支援」に焦点をあてての検討となっている。

基本的な考え方は、以下の 7 項目となっている。

a　ICT-BCP 策定の動機付けのため、最優先で取り組むべき事項として「初動を可能とするために必要となるアクション」（「事前対策」を含む）を切り出し、できるだけ具体化する。

b　「初動を可能とするために必要となるアクション」の訓練（「事前対策の点検を含む」）によって ICT-BCP の改善を促すガイドラインとすることを検討。

c　ICT-BCP の位置づけについては、災害対策基本法を中心とする防災法制の改正の方向性を踏まえながら検討していくべきではあるが、「初動を可能とするために必要となるアクション」については、地域防災計画の概念の中にほぼ収めることができれば、地方公共団体も取り組みやすいと考える。

d　「初動を可能とするために必要となるアクション」にかかる要員を非常参集要員として確保する必要性は認められると考える。

e　「初動を可能とするために必要となるアクション」部分の ICT-BCP の策定について、首長の理解を深め、策定の決断を促すために必要な具体的な取組を検討する必要がある。

f　「初動を可能とするために必要となるアクション」を提示する中で、効果的な ICT の利活用シーンを例示していくことも重要。

g　ICT-BCP ガイドラインの射程については、「初動を可能とするために必要となるアクション」部分の ICT-BCP から更に ICT-BCP 全体の策定につなげていくことが望まれる旨を明確にすべきである。

また、対象とする情報資産については、初めから一般的な ICT 部門が所管している事項に限定することなく、他の部門が所管している情報システムについても段階的に対象としていくことが望ましいことを明確にすべきである。

（イ）「初動」の範囲

ICT 部門が関連する非常時優先業務のうち、概ね 72 時間以内の初動に対応が必要となるのは、下記の 7 項目となっている。

a　情報提供のための情報システム（IP 告知、エリアメール、ホームページ等）の稼働支援など。

b　住民情報システム等の点検・稼働、安否確認に必要なデータの入手、OA 機器用電源や通信回線の確保、PC やプリンターなど OA 機器の確保・再設定作業、ケーブルや OA 消耗品の確保、ベンダーとの連絡調整など。

c　ベンダー要員の安否確認、安否確認システムの導入及び稼働支援など。

d　インターネット回線の確保・通信に必要な設定作業など。

---

[45] 出展：ICT-BCP ガイドライン改訂の方向性～「初動対応の支援」に焦点をあてて～
詳細は、下記（総務省ホームページ）を参照のこと。
http://www.soumu.go.jp/main_content/000169430.pdf

e　災害対策本部の設置に必要な PC、プリンターなどの OA 機器の確保・設定、ネットワーク（通信回線を含む）の構築及び設定、電源の確保。

f　Web サーバの点検・稼働、避難所等で運用する PC、プリンターなど OA 機器の確保・再設定作業、インターネットなど外部との通信回線の確保・設定作業、ケーブルや OA 消耗品の確保、その他 ICT ツールの確保など。

g　「初動」対応が終わった後に必要な情報システムが、そのタイミングで確実に実施できるようにするための、初動期間中の点検・再稼働、不足する OA 機器の確保・再設定など。

（ウ）被害想定

被害想定については、各地方公共団体がそれぞれの実情に応じて定める必要があるものの、当センターより例示のあった 2 つのケース（陸前高田市、宮古市＜本庁舎の倒壊、代替拠点での暫定的サービス提供、電源及びネットワークの喪失のケース＞、双葉町＜住民が行政区域から避難するケース＞）で概ね網羅していることから、地方公共団体のリソースの被害が甚大なケースを中心に以下の観点でバリエーションを考えることとしている。

a　どのような災害､脅威（又はシステムが使用不可となる可能性や被害想定）が発生するのかを想定し、当該地方公共団体の技術水準や人的リソースを勘案し、どのような対応を取ればよいか。

b　a では対応できない場合、どういう対応をとるのか。

c　更に住民ごと別の場所に避難する場合、どういう対応をとるのか。

６　運用体制に関する事例

地方公共団体における ICT-BCP に関する事例を以下に示す。

（１）藤沢市[46]

ア　ICT-BCP の策定経緯とその意義

藤沢市は ISMS 及び ICT-BCP の国際的な認証である BS25777 の認証を取得しており、セキュリティに力を入れている。

ICT-BCP 策定の背景には、災害等ではなくセキュリティ強化の一環から作成されたという経緯がある。

災害時において、民間企業と異なり、地方公共団体は災害対応業務も行うことから、ICT-BCP は災害対応業務及び業務継続業務の両方のために必要と考えている。

イ　藤沢市の ICT-BCP の経験

ICT-BCP の策定に当たっては専任の職員を確保して対応したものの、業務主管課に対するアンケートの実施や内容の説明をし、理解を得るのに時間を要したため、当初想定の 6 カ月を越え完成までに約 1 年かかった。

自治体業務の内容や優先度は自治体間であまり変わらず、情報インフラ、即ちネットワーク・電源・通信の確保等が一番重要であり、その次に住民へのサービスとなっている。

ウ　訓練、内部監査の重要性

PDCA を実施する上で一番大事なことは、訓練及び内部監査であると考えている。

障害、ウイルス等のセキュリティ事故は日常的に発生しているが、ICT-BCP に該当するような事象は非日常的な事象である。このため、訓練等を実施しておかなければ被害を想定する機会がない。

したがって訓練は重要であり、実施することで反省・見直しを実施し、次に活かすことができる。藤沢市では訓練の負担を考慮し、例えば電源の法定点検や停電時に併せて ICT-BCP の訓練を実施している。

エ　具体的な対策

災害発生時の必要最小資源として一番重要なものは人員確保である。

このため職員等緊急時連絡網を作成し、毎月訓練して、発災時すぐに職員の安否確認と参集の可否が確認できるようにしている。

職員の住所等を確認し、ICT-BCP に参集状況の想定を盛り込んでいることから、発災時に的確な人員確保が可能となる。

---

46 出展：藤沢市における BCP の概要及び災害発生時の ICT 利活用について
詳細は、下記（総務省ホームページ）を参照のこと。
http://www.soumu.go.jp/main_content/000147760.pdf

オ　ICT-BCP 策定のメリット

停電時には必要最小限の臨時端末とサーバへ電源供給が可能となるようICT-BCP に計画してあり、東日本大震災後の計画停電時には、すべて予定どおりの対策が機能した。

繰り返しの停電により UPS の機能が低下し電源が落ちたこともあったが、マニュアルの整備と日頃の訓練によりサーバのシャットダウンから再起動までの作業が迅速に行えたので、ICT-BCP が非常に有効であったことがいえる。

カ　現行のガイドラインの有効性

東日本大震災は想定外の災害であるということが言われており、ICT-BCP を策定しても意味がないという意見が多くある。

しかし、現行ガイドラインには「地震により庁舎が使用できない、情報通信の設備・危機が破損、必要な職員が参集できない、電力供給の停止などが想定される」と記載されている。現行のガイドラインには想定外の事項はない。

キ　ICT の利活用

災害時の ICT の利活用に関しては、発生前、発生時、発生直後、発生後のように時間軸により必要な ICT サービスが異なる。

平常時の予防や訓練のシステム等、災害発生時の重要インフラに関する情報提供や被災者情報の提供システム等、また発生後の復興支援システム等、適切なサービスが提供できるよう想定する必要がある。

（２）小鹿野町[47]

ア　セキュリティ対策の条例化

小鹿野町は、IT ガバナンス・セキュリティ対策を条例化している。

条例策定の経緯は、小鹿野町は小さい町であり人員が少なく財政的にも資源が限られているため、セキュリティ等に資金をかけられない、そういった中でどのようにセキュリティ対策を確保していくか、というところに起因している。

条例を策定したメリットとしては、ICT-BCP の位置づけが明確になり、職員も取組が義務付けられたことが挙げられる。

イ　庁内合意形成のための研修

一般的な職員に業務継続性確保や ICT-BCP の必要性を認識させることにより、策定段階から多くの職員の協力を得ることが重要であると考えていたが、災害発生時における人命救助等と ICT-BCP の重要性との関係の違いを説明し理解してもらうことが困難であった。

そもそも職員は全体的な BCP 等に興味を示さないため、周知の機会が必要と

---

47 出展：小鹿野町における BCP の概要及び災害発生時の ICT 利活用について
詳細は、下記（総務省ホームページ）を参照のこと。
http://www.soumu.go.jp/main_content/000147765.pdf

認識している。

このため、研修等で BCP とは何かということを認識させることが必要と考える。

ウ　小規模自治体における ICT-BCP 策定

ICT-BCP 策定に当たり半年以上の期間と 20 人日程度の実作業を要したが、これはアドバイザーの支援をいただいた上での日数であり、そのような支援がないと小さな自治体で ICT-BCP を作成することは困難である。

また、ICT-BCP 策定に当たり費用をかけられない場合が多いため、小鹿野町では費用をかけず対応できる手段を優先しており、少ない資源でできる簡単なことから実施しようと考えている。

エ　ICT-BCP 策定のメリット

東日本大震災の際は小鹿野町に被害はなかったが、非常体制がとられた。ICT-BCP を策定していたことから的確な災害時対応が実施できた。

オ　ICT-BCP 運用の課題

ICT-BCP の内容を熟知する職員は少ない。策定した ICT-BCP の周知徹底に対しては、全職員関与による定期的な見直し及び訓練が必要である。

小さな団体では費用対効果の有効性確認が難しい上、たとえ有効であったとしても財源確保が難しい。

施設や設備の整備を盛り込む ICT-BCP よりも、運用を重視したお金のかからない ICT-BCP 策定をしなくてはいけない。

カ　災害に備えた ICT 利活用と紙台帳の定期的更新

合併に伴うシステム統合に併せて、民間データセンターに住民情報系システムを置き、リカバリーシステムを自庁舎に設置することによりシステムの多重化を図った。

住民情報の紙台帳を作成し定期的に更新することで、停電等の対策を施した。この台帳を用いて証明書の手書き発行の訓練を実施したため、費用をかけず有効に活用できた。

第２節　行政データに係るバックアップ・リストア基準の策定等

前節の情報セキュリティポリシー及びICT－BCP等に係る調査を踏まえ、行政データのバックアップ及びリストアの方策として「バックアップ・リストア基準」を検討する。

１　バックアップ・リストアの必要性

システムとして管理されている電子データは、既に何らかの形でバックアップが実施されている。

しかしながら、文献調査及びヒアリング調査の結果、ICT部門により管理されているシステムと、業務部門等で管理されているシステムとでは、管理方針や管理内容に差やバラツキがある場合が多く見受けられる。

また、ローカルPC等に保存されている電子データにおいては、バックアップそのものが実施されていないケースも多く存在する。

したがって、全庁の統一的なルールの下でバックアップを実施することが必要であり、その認識が全庁に浸透していることが求められる。更に、ICT部門が、庁内全体の状況を把握することも求められる。

そして、バックアップは実施されているものの、システムやデータのリストアについて、手順書の整備や定期的な訓練等を実施している地方公共団体は少数である。

これでは、手間と経費をかけて実施しているバックアップが、非常時に活かされないことになりかねない。

リストアの重要性についても、その認識が全庁に浸透していることが求められる。

更に、紙で保存されているデータ（以下「紙データ」という）においても、滅失により、行政運営に重大な影響を及ぼすデータがあることが、被災地へのヒアリング等で明らかになった。

紙データに関しても、重要度の分類に基づき、可能な限り電子化を推進することにより、バックアップ及びリストアが可能となる。

２　バックアップ・リストア基準の位置づけ等

（１）バックアップ・リストア基準の背景及び理由

ア　情報セキュリティポリシーは、俯瞰的観点からの基本的事項を定める「上位の取り決め」であり、一般的には、対策基準や実施手順の内容や粒度にバラツキがあるなどのため、詳細までを記述するものとはなっていない。

イ　東日本大震災において、行政機関（地方公共団体の本庁舎）等が全水没するといった、これまでの想定にない事態が発生した。

ウ　当該震災で学んだ教訓を活かすためには、庁舎や機器、機材、什器及び電子データ等がすべて失われることを想定し、その事態に焦点を当てた詳細かつ具体的な対策を講じる必要があると考える。

（２）バックアップ・リストア基準の位置づけ

東日本大震災の被災状況やその後の復旧状況を調査した結果、システムとして管理されている電子データだけでなく、ローカル PC 等に保存されている電子データについても、従前からバックアップを励行し、発災後に円滑にリストアできる手続きや体制、仕組み等を整備する必要がある。

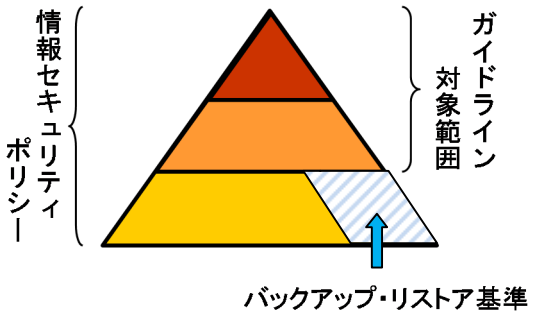
しかし、必ずしもすべての地方公共団体では、そのような従前の準備、特に被災時に即座に利用できる具体的な手順等が定められていないことが、同様に明らかになった。

調査結果を受け、本章では、災害等も視野に入れた具体的なバックアップやリストアの実施手順（基準）を検討する。

このバックアップ・リストア基準は、内容的に「情報セキュリティポリシー」の下位に位置づけられている「実施手順」の一部に該当するものである。

そのため、情報セキュリティポリシーが未策定の地方公共団体においては、速やかな情報セキュリティポリシーの策定をお願いしたい。

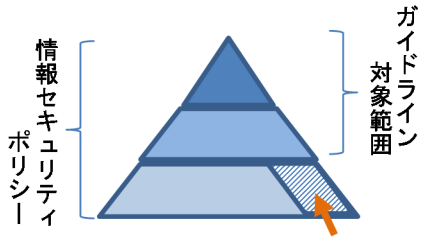
既に「情報セキュリティポリシー」が策定されている場合には、実施手順の１つとしてバックアップ・リストア基準を新たに設けていただきたい。なお、既存の実施手順を見直す場合は、本章を参考にしてほしい。



（３）バックアップ・リストア基準の作成方針

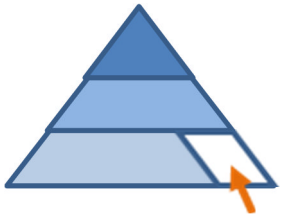
今回実施した各種調査により、情報セキュリティポリシーやその実施手順の整備状況等により、地方公共団体は次のアからウの 3 種類に区分される。

ア　既に情報セキュリティポリシーを策定し、下位の実施手順も定めているケース



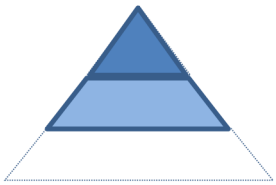
バックアップ・リストア基準〔相当〕あり

イ　既に情報セキュリティポリシーを策定しているが、バックアップ・リストアについて具体的に規定していないケース



バックアップ・リストア基準〔相当〕なし

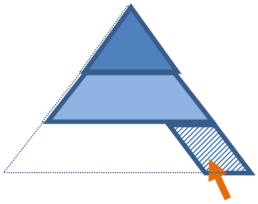
ウ　情報セキュリティポリシーを策定しているが、下位の実施手順を定めていないケース



本章では、上記イ及びウを対象にバックアップ・リストア基準案を策定する。

策定済みの情報セキュリティポリシーの下位規定として整合性がとれ、かつ災害時等を想定したバックアップ・リストア基準案のイメージは、以下のとおりである。

なお、上記アの場合は、本章を参考にすることで各団体の状況に応じた活用ができると考える。



バックアップ・リストア基準
（既存の基本方針、対策基準と整合性をとったもの）

（４）文書管理規則・規程等、情報セキュリティポリシー、ICT-BCP の位置づけ（参考）

ア　文書管理規則・規程等

前章で示したように文書管理規則・規程等は、事務の適正かつ能率的な執行に資するため、行政文書の処理等を正確かつ迅速に行うことを基本原則とし、電子情報についても「電磁的記録」として定義づけを行い、従前からの紙媒体と同じく、適正な保存・保管を位置づけている。

イ　情報セキュリティポリシー

情報セキュリティポリシーは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書であり、その位置づけは、情報セキュリティに関する全体を俯瞰的に捉え、基本的な考え方を体系的に示すものである。

ウ　ICT-BCP

ICT-BCP は、情報システムや ICT 部門の業務を継続するための対策や実施方法・手順・体制等をとりまとめたものである。

３　バックアップ・リストア基準の策定等

バックアップ・リストア基準の策定方法を以下に示す。ただし、運用に当たっては、各地方公共団体においてP（Plan 計画）、D（Do 実行）、C（Check 評価）、A（Act 改善）を着実に実施していくことが適当であると考えている。

（１）バックアップ・リストア基準の基本構成

ア　バックアップ・リストア基準の観点

バックアップ・リストア基準は、情報セキュリティポリシーに基づいて実施する際に「どのように実施するか」という「How」についての実施手順を記述するものである。

そのため、どの程度詳細なものをどこまで作成するかは、各地方公共団体の判断による。

ここでは、現場での行為の発生順に整理し、例示するとともに、システム単位での実施手順（バックアップ・リストア手順書）に記載すべき項目やバックアップ運用に係る項目等を例示する。

記述例文は、マニュアル的な内容であることに鑑み、規程等の記述形式での例示とはしない。

イ　バックアップ・リストア手順書の策定単位

（ア）特定の業務システムで運用されている場合は、業務システム単位での作成を原則とする。

（イ）特定の業務システムを持たない場合（EUC（End User Computing）等による、汎用的なソフトウェアで運用されている電子データ等）は、課単位での作成を原則とする。

ウ　バックアップ・リストア手順書の構成

（ア）業務システム単位での記述を行う。

（イ）全体の流れ（フロー図）を示した上で、作業手順等について箇条書きを基本とし、図や表等により構成される。

エ　バックアップ・リストア手順書の主な項目と内容

（ア）バックアップ手順書

a　全体フロー

b　バックアップ準備作業

c　バックアップ作業

d　バックアップ後の作業

（イ）リストア手順書

a　全体フロー

b　リストア準備作業

c　リストア作業
d　リストア後の作業

（２）バックアップ・リストア基準の策定手順

ア　基礎となるデータの整備

Step1：基本的な情報のメンテナンスの実施

電子データの重要度の分類は、情報セキュリティポリシーにおいて既に策定済みであるため、最初に紙データの重要度の分類について記述する。

なお、電子データの重要度の分類を見直す場合には、下記（エ）推奨事項を参照されたい。

（ア）紙データの重要度の分類を実施する。

【参考】被災地へのヒアリングで必要とされた主な紙データ

a　収納関連情報（申請書・領収書等）
b　課税関連情報（確定申告書）
c　財務関連情報（契約書）
d　地図情報
e　図面データ

（イ）分類に基づく紙データの電子化を実施する。

a　複合機若しくはスキャナ等による電子化の実施（ファイル形式は最もふさわしく、汎用的なものとする。例：pdf 等）
b　経費や工数等を勘案しつつ、電子化を計画的に推進する。

（ウ）古いデータ形式や特殊なデータ形式で保存されている重要情報の可読性（可用性）を確保する。

a　ワープロ専用機で作った、フロッピーディスク保管の文書等については、一旦、紙に出力した上で、紙データの電子化の推進の一環として、電子化を計画的に推進する。
b　上記 a 以外の特殊なソフトウェアで保存されている文書等については、そのソフトウェアの使用停止等が見込まれた段階で、後継のソフトウェアへのデータ変換を実施するか、一旦、紙に出力した上で、紙データの電子化の推進の一環として、電子化を計画的に推進する。
c　経費や工数等を勘案しつつ、電子化を計画的に推進する。

（エ）推奨事項

a　情報システムの棚卸を定期的に実施する。

システム構成やシステム設定等の「システム関連情報」の内容を精査し、不足があれば不足部分を整備する。

不足部分の整備に当たっては、システム提供事業者（ベンダー）の協力を得て実施する。

【調査項目の例（イメージ）】

情報システム名称	管理責任者	システム構成	システム関連文書の有無	主なデータ項目	データ更新頻度	データ参照頻度	バックアップ実施の有無	バックアップ実施の頻度	リストア手順書の有無	システム提供事業者の連絡先把握の有無
Aシステム	○課長	サーバ3台	有		毎日	毎日	有	月1回	無	有
Bシステム	△課長	サーバ1台	無		月1回程度	月1回程度	無	ー	無	無
Cシステム	□課長	サーバ1台	無		年1回程度	年1回程度	無	ー	無	無

■情報システムの棚卸結果とチェックポイントの例は 51 頁を参照

b　電子データの重要度の分類の見直しの実施

情報セキュリティポリシーに基づき実施されている電子データの重要度の分類の見直しを実施する。

（a）【参考 1】被災地へのヒアリングで必要とされた主な電子データ

・福祉関係データ（心身障がい者の医療費支給台帳、口座情報、支給実績等）
・高齢者関連データ（要介護認定のケース記録）
・障がい者関連情報（手当に係る支給先口座の一覧、ケース記録）
・子育て関連（母子相談記録）
・土地（税務）関連情報（地籍図（土地の境界））
・収納情報（処理中の情報）

（b）【参考 2】可用性による情報資産の分類[48]

分類	分類基準	取扱制限
可用性２	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される、又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・外部記録媒体の施錠可能な場所への保管
可用性１	可用性２の情報資産以外の情報資産	

（c）【参考 3】重要性に基づく情報資産の分類を 4 分類としている自治体における分類基準等[49]

Ⅰ　個人情報及びセキュリティ侵害が住民の生命、財産等へ重大な影響を及ぼす情報

・個人情報、税関連情報、介護関連情報、戸籍情報
・金融機関・口座関連情報

48 本章の「第１節－1　情報セキュリティポリシーガイドラインの概要」（1）セ（ア）を参照のこと。
49 本章の「第１節－1　情報セキュリティポリシーガイドラインの概要」（1）セ（ア）を参照のこと。

Ⅱ　公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報
・住基関連、健康管理関連、医療機関関連
・都市計画関連情報、システム関連情報
・住民サービスに係る台帳等のデータ、給付関連データ

Ⅲ　外部に公開する情報のうち、セキュリティ侵害が、行政事務の執行等に微妙な影響を及ぼす情報
・食品衛生管理、公園台帳、建築指導（いずれも登録個人情報を除く）

Ⅳ　上記以外の情報

①分類結果を参考にバックアップ頻度を見直す

②バックアップ媒体の再検討

③バックアップ媒体保管場所の再検討

基本機能	機器構成	OS	台数	容量	重要度分類	バックアップ頻度	バックアップ時期	バックアップ時間	バックアップ媒体	媒体保管場所	手順書の有無		参照先（関連ドキュメント）	
											バックアップ	リストア	保管場所	ファイル名称
住基・印鑑	DBサーバ	WindowsXXXX	△	*** GB	●類	日次	α:00～	約〇分	HDD	マシン室	有	有	〇□課共有フォルダシステムドキュメント	住基システムバックアップ・リストア手順書
							β:00～	約△時間	LTO	マシン室及び外部IDC				
	Web/APサーバ	WindowsXXXX	□	リリース時等、必要に応じてバックアップするため、容量は不定		リリース時等、必要に応じて実施	随意処理のため時刻は不定	バックアップ対象により異なる	LTO	マシン室				
	連携サーバ	WindowsXXXX	△											
	運用サーバ	WindowsXXXX	□											
	リカバリサーバ	WindowsXXXX	△											
	バックアップサーバ	WindowsXXXX	□											
	汎用〇△サーバ	WindowsXXXX	△											
	〇〇△△DBサーバ	WindowsXXXX	□											
	〇〇△△Web/APサーバ	WindowsXXXX	△											
	〇〇連携サーバ	WindowsXXXX	□											
戸籍	DBサーバ	WindowsXXXX	△	*** GB	●類	日次	α:00～	約〇分	HDD	マシン室	有	有	◇△課共有フォルダシステムドキュメント	戸籍システムバックアップ・リストア手順書
							β:00～	約△時間	LTO	マシン室及び〇△庁舎				
	Web/APサーバ	WindowsXXXX	□	上記の戸籍・印鑑に同じ		上記の戸籍・印鑑に同じ	随意処理のため時刻は不定	バックアップ対象により異なる	LTO	マシン室				
	〇〇△△DBサーバ	WindowsXXXX	△											
	〇〇△△Web/APサーバ	WindowsXXXX	□											
住基ネット	GW(ｹﾞｰﾄｳｪｲ)サーバ	WindowsXXXX	△	*** GB	●類	日次	γ:45～	約△時間	DAT	マシン室	有	有	◇△課共有フォルダシステムドキュメント	住基ネットバックアップ・リストア手順書
	CSサーバ	WindowsXXXX	□	*** GB	●類	日次	δ:45～	約△時間	DAT	マシン室				

④手順書の有無の把握と整備推進

⑤手順書の保管場所及びドキュメント名称等の明示（参照先の明示）

イ　データのバックアップ方法構築のポイント

Step2：情報セキュリティポリシーに基づくバックアップ方法の見直し

（ア）定期的バックアップが実施されている場合

a　バックアップのサイクルをデータの更新頻度や参照頻度に沿って見直す。

データの更新頻度や参照頻度が週に 2 回以上ある場合は、「日次」とするよう見直す。

b　バックアップ媒体がテープの場合は、最低でも「5 巻回し」程度とするよう見直す。

c　内容の精査や見直し作業は、システムを所管する業務部門と ICT 部門が連携して実施する。

d　バックアップの状況把握を行うため、システム監視記録や点検簿等を作成し、バックアップの監査・自己点検を定期的に実施する。

（イ）定期的バックアップが実施されていない場合

a　バックアップの取得を定期的に実施するように見直す。

b　バックアップのサイクルや監査・自己点検は上記（ア）と同じ。

c　予算等、経費が必要となるため、そのための準備を行う。

（ウ）PC レベルで運用されているデータのバックアップ

a　外部媒体装置がある場合

CD-R、CD-RW 等への定期的なバックアップを実施する。

b　外部媒体装置がない場合

課等でバックアップする PC を決め､そこに共有フォルダを作成して CD-R、CD-RW 等への定期的なバックアップを実施する。

この場合、課等に 1 台程度、外部媒体装置を整備する。予算等、経費が必要となるため、そのための準備を行う。

c　ファイルサーバ等がある場合

既存の保存ルールを、情報資産の分類の観点からの見直しを図り、データの重要度に準じたバックアップを実施する。

ウ　バックアップ媒体の保管方法構築のポイント

Step3：バックアップ媒体の保管方法の見直し

（ア）基本的事項の見直し

a　ICT 部門の役割の見直し

地方公共団体ごとに組織や役割が異なるが、バックアップデータの取扱いについては、ICT 部門の役割とし、全庁で一括して遠隔地保管することが望ましい。

（イ）短期的視点からの見直し

a　既に耐火性・防水性のある金庫等に保管している場合

（ａ）水没の危険性について検討する。

（ｂ）水没の危険性が高い場合には、高台に位置する最も堅牢な公共施設や出先機関等を分散保管先とする等の見直しを行う。

b　事務室若しくは機器等の設置場所に保管している場合

上記 a を加える方向での検討を行う。

（ウ）中長期的観点からの見直し

a　共同利用型バックアップの検討

地方公共団体が庁舎施設内に設置するシステムを、他の団体がバックアップサイトとして共同利用する検討を行う。

b　バックアップデータのデータセンター移行の検討

データセンターへのバックアップ方策の検討を行う。

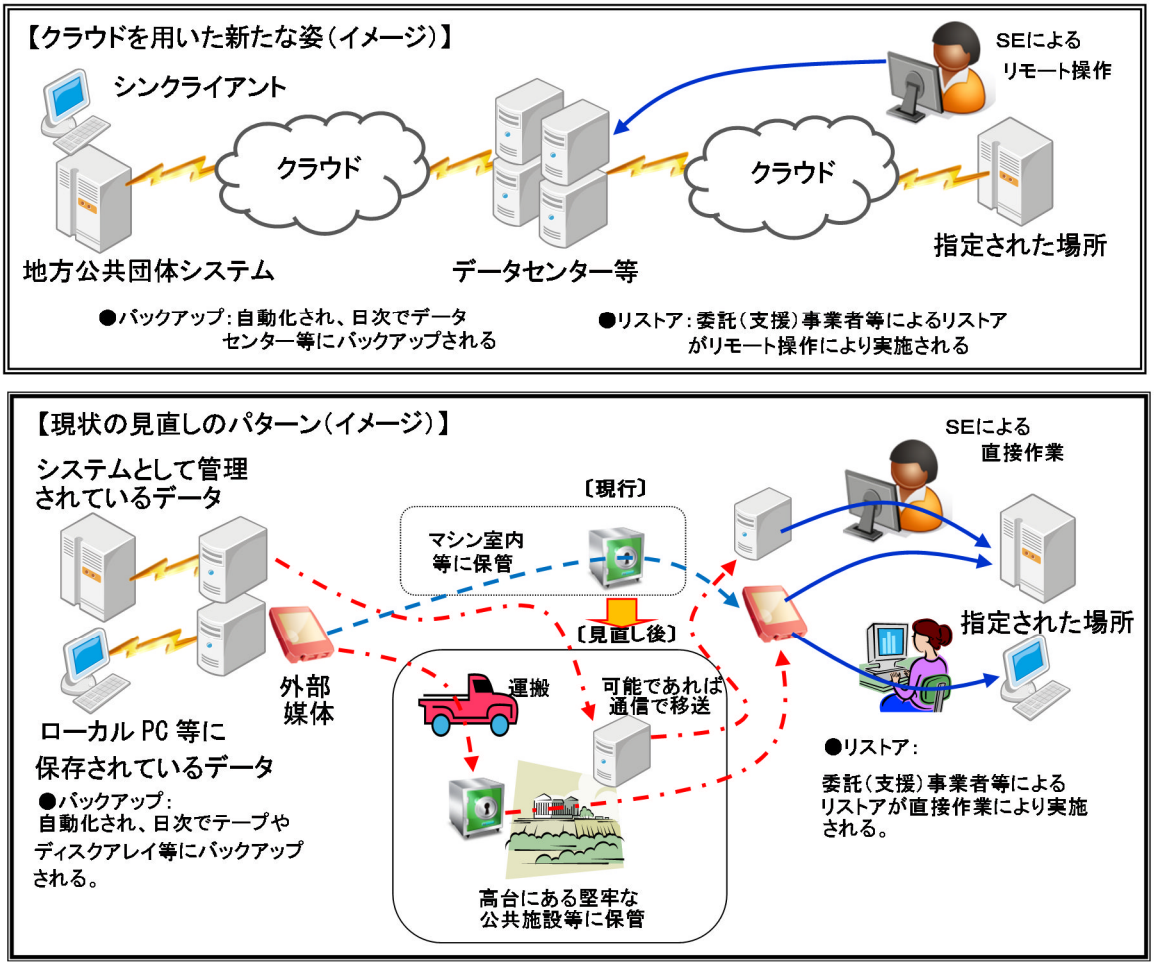
c　情報システム（システムで扱うデータを含む）のデータセンター移行の検討

（ａ）情報システムの更改や仮想化技術導入等の検討に合わせ、バックアップ方策の検討を行う。

（ｂ）地方公共団体の規模や状況によっては、被災時に最低限の業務ができるよう、データセンターからネットワーク経由で一部のバックアップデータ（住基や税等の一部）を転送し、庁舎内に保管することも検討する。

（ｃ）経費等の観点もあるため、情報システムのクラウド化や更改等の他の要素との組合せ等も検討する。

※　バックアップ・リストアの概念図は、次頁参照



図－３８　バックアップ・リストアの概念図

エ　バックアップ手順書策定におけるポイント

Step4：バックアップ手順書の整備

（ア）事前準備等の実施

a　システム提供事業者（ベンダー）が存在する場合

（a）システム提供事業者の協力を得て既存のバックアップにおける手順書を策定する（場合によっては、委託事業として整備を図る)。

（b）システム提供事業者の協力を得て既存のバックアップ方法やバックアップデータ保管場所等について事前に検討を行う。

この際の留意事項は、契約内容の見直し若しくは臨時経費等の予算が必要となるため、あらかじめシステム提供事業者との協議や調整、見積取得等を行う。

b　システム提供事業者（ベンダー）が存在しない場合

（a）職員が主体的にバックアップ作業を実施するため、あらかじめ複数の職員が手順書等により、実際に作業ができることを確認しておく。

（b）万一、職員（要員）が被災するなどした場合に備え、支援要請ができる事業者の確保に努める。

この場合は、対象となるシステムの納入事業者が既に存在しないケースが想定されるため、専門的知見等の支援を得られる事業者を探しておく必要がある。また、計画的なシステム更新の検討の実施も求められる。

※バックアップに関しては訓練ではなく、実施が求められるため、日々の作業の中から課題を整理・分析し、手順書等の見直しを実施する。

オ　リストア手順書策定におけるポイント

Step5：リストア手順書の整備

（ア）システム環境一覧データの作成

a　情報システムの棚卸で整備されたデータをリストア時に活用できる状態に整える。

b　OS（各種バージョン等を含む)、ブラウザ等のシステム環境を調査し、一覧表化して保持する。

（イ）事前準備等の実施

a　システム提供事業者（ベンダー）が存在する場合

（a）システム提供事業者の協力を得てリストア手順書を策定する（場合によっては、委託事業として整備を図る)。

（b）システム提供事業者の協力を得てリストア環境（リストアする場所等）について事前に検討を行う。

この際の留意事項は、二次被害が防止できる立地であること、電源が確保されること、地方公共団体の市民窓口（被災時のり災証明書等の発

行の窓口で、本庁舎が被災した場合は代替窓口）からリストア環境でのシステムまでの間の通信回線の確保が担保されること等である。

契約内容の見直し若しくは臨時経費等の予算が必要となるため、あらかじめシステム提供事業者との協議や調整、見積取得等を行う。

b　システム提供事業者（ベンダー）が存在しない場合

（a）職員が主体的にリストア作業を実施するため、あらかじめ複数の職員が手順書等により、実際に作業ができることを確認しておく。

（b）万一、職員（要員）が被災するなどした場合に備え、支援要請ができる事業者の確保に努める。

この場合は、対象となるシステムの納入事業者が既に存在しないケースが想定されるため、専門的知見等の支援を得られる事業者を探しておく必要がある。

また、計画的なシステム更新の検討の実施も求められる。

（ウ）手順書の作成と訓練等の実施

a　リストア手順書等の作成及び訓練等の実施

（a）リストアのための手順書等をあらかじめ作成しておく。

（b）手順書等に基づき、年１回程度の訓練等を実施する。

b　訓練等に基づく課題の把握と見直しの実施

訓練等により明らかとなった課題を整理・分析し、手順書等の見直しを実施する。

（エ）リストアの優先順位の決定

a　窓口や事務室等の環境により、復旧するサーバや PC の台数・容量等に限りがあることが想定されるため、住民サービス開始の内容や時期等を勘案し、あらかじめ、一覧表等によりリストアの優先順位を決定した上でリストアを行う。

b　被災地の状況【参考】

被災地へのヒアリングにおいて、被災直後の人命救助段階において、被災者安否確認や避難所の管理運営に住基情報が重要であるとの意見を得ている。

また、ホームページ（市の公式サイト）による情報発信も重要であるとの意見を得ている。

その後、り災証明書の発行のための税関連情報が必要となる。

（３）バックアップ・リストア手順書の項目例等

ア　〇〇業務サーバのバックアップ手順書の項目例

（ア）〇〇業務サーバ・バックアップ手順全体フロー

（イ）〇〇業務サーバ・バックアップ準備作業

a　サービス停止

b　ドメインからの切り離し

（ウ）〇〇業務サーバ・バックアップ作業

a　ネットワーク IP アドレスの設定

b　ネットワークドライブの接続

c　バックアップソフトの実行

（エ）〇〇業務サーバ・バックアップ後の作業

a　ドメインへの参加

b　サービス起動

（オ）運用管理サーバ・バックアップ手順全体フロー

（カ）運用管理サーバ・バックアップ準備作業

a　他のサーバのすべてのサービス状態の確認

b　クラスタの状態確認

（キ）運用管理サーバ・バックアップ作業

（ク）運用管理サーバ・バックアップ後の作業

a　サービス起動等

イ　バックアップ手順書の具体的構成とその内容

以下は、個々のシステムに係るバックアップの運用について整理するもので、業務システムごとに策定する。

表－３３　バックアップ手順書の構成と内容例

項目No	項目	内容
1	用語の定義	バックアップ手順書における用語の定義
2	機器構成	本番環境機器及びバックアップで使用するハードウェアを示す
3	バックアップ領域	各サーバにおけるバックアップ領域を示す
4	バックアップ管理	バックアップ準備作業及びバックアップ後の処理を含む
4-1	バックアップ処理の流れ	バックアップ処理イメージを示す
	1日のスケジュール	バックアップ処理の1日のスケジュールを示す
4-2	バックアップスケジュールと世代数	週間スケジュール及びバックアップ世代数を示す（サーバ毎）
5	バックアップ方式	
5-1	Windowsバックアップ	Windowsサーバ内データのバックアップ方式を示す
5-2	ハードディスク間（DDR）バックアップ	ディスク間コピーによるバックアップ方式を示す
5-3	一次バックアップ	日次によるバックアップの実施を示す
	二次バックアップ	月次等によるバックアップの実施等を示す
	システムバックアップ	バックアップ時期等を示す
	バックアップ容量	1世代あたりのバックアップ容量を示す
6	媒体管理方式	
6-1	バックアップ装置の媒体配置図	バックアップ装置の媒体配置図を示す
6-2	媒体管理（一次、二次、システム）	世代数に応じた媒体本数等を示す
6-3	媒体本数	媒体本数（媒体全容量を含む）及び保管場所別巻数を示す
6-4	媒体交換	媒体交換のポイントを示す
7	クリーニング管理方式	バックアップ装置のドライブクリーニングについて示す

ウ　〇〇業務サーバのリストア手順書の項目例

（ア）〇〇業務サーバ・リストア手順全体フロー

（イ）〇〇業務サーバ・リストアの準備作業

（ウ）〇〇業務サーバ・リストア作業（業務単位での実施）

a　ネットワーク IP アドレスの設定

b　ネットワークドライブの接続

c　バックアップソフトによるリストアの実行

（エ）〇〇業務サーバ・リストア後の作業

a　ドメインへの参加

b　サービス起動及び動作確認等の実施

（オ）運用管理サーバ・リストア手順全体フロー

（カ）運用管理サーバ・リストア準備作業

a　他のサーバのすべてのサービス状態の確認

b　クラスタの状態確認

（キ）運用管理サーバ・リストア作業

（ク）運用管理サーバ・リストア後の作業

a　サービス起動等

b　サービス起動及び動作確認等の実施

エ　リストアの準備作業における具体的内容

（ア）被災時を踏まえた平常時の準備作業

a　システム環境（ハードウェアや OS 等）が異なる場合の稼働確認作業等の定期的な実施

b　その時点で調達し得るシステム環境で、正常稼働が困難な場合の対処策の検討及び対処の準備

（イ）実際の被災時における準備作業

a　〇〇業務システム及びデータ等の被災状況の確認・情報収集の実施

b　バックアップデータの被災状況確認及び使用可能な状態にするための準備の実施

c　リストア環境（機器類、設置場所、電源、通信回線等）の準備及び実施のための各種調整等の実施

d　リストア開始時期、リストア対象システム、作業者確保等の調整の実施

e　リストア作業の実施後の動作確認・内容等の検証の実施