平成２４年度
研究開発事業

災害に強い地方公共団体の情報システムのあり方に関する調査研究

－行政データ管理とバックアップサイトについて－

報告書

平成２５年３月

財団法人　地方自治情報センター

はじめに

地方自治情報センターの研究開発事業は、地方公共団体が共通的に利用できる情報システム及び新技術の導入並びに新分野へのコンピュータ利用等に関して、研究・開発及び調査等を実施し、地方公共団体の ICT 化等電子自治体の推進等に資することを目的に実施しております。

平成 23 年度の調査研究では、「東日本大震災における地方公共団体情報部門の被災時の取組みと今後の対応のあり方に関する調査研究」を実施し、行政機能の継続に多大な影響を与えたのはデータの滅失であったことを踏まえ、データのバックアップ・リストア基準と管理体制を構築する必要があるとしたところです。

本年度は、平成 23 年度の成果を踏まえ、「災害に強い地方公共団体の情報システムのあり方」について、行政におけるデータ管理の必要性及びデータのバックアップ・リストア基準の策定並びに ICT 部門におけるバックアップサイトの利活用方策の調査研究を実施し、本報告書に取りまとめを行っております。

本報告書を、地方公共団体の皆様に御活用いただければ幸いと存じます。

本調査研究の実施に当たり、適切な御指導・御助言をいただいた本調査研究委員会の委員の皆様、アンケート調査及びヒアリング調査にご協力いただきました地方公共団体の皆様に、厚く御礼申し上げます。

平成２５年３月

財団法人 地方自治情報センター
理事長　　戸 田　夏 生

目　　次

序章

第１節　背景及び目的

平成 23 年度調査研究「東日本大震災における地方公共団体情報部門の被害時の取組みと今後の対応のあり方に関する調査研究」[1]の報告書によれば、行政機能の継続に多大な影響を与えたのは、データの滅失であった。滅失したデータには、住民情報や戸籍、税などの基幹系データ[2]に代表されるようなシステムとして管理されている電子データ及び各職員によりローカル PC 等に保存されている電子データや文書など（以下「行政データ」という。）があった。

基幹系データについては、上記のような甚大な被害を受けた被災団体の情報部門（以下「ICT 部門」という。）が DAT などのテープ媒体を使って日次又は週単位にデータのバックアップを実施しているが、バックアップデータの保管場所は多くの被災団体が「本庁舎内」としていた。また、業務部門がシステムとして管理されている電子データ及び各職員によりローカル PC 等に保存されている電子データや文書については、全庁で統一したバックアップ及びリストアの方策はなく、データ管理状況についても ICT 部門が必ずしも把握していなかった。

このような状況を踏まえると、すべての行政データを平常時から全庁で組織的にバックアップすることが、災害に強い地方公共団体の情報システムの実現に向けての必須要件となると考えられる。

更に、現在、紙媒体で運用・保管されている行政データについても可能な限り電子化し、バックアップ対象とすることも重要である。

よって本年度は、地方公共団体自身が被災し、制約を伴う状況下にあっても、業務を遂行できる体制、即ち、「災害に強い地方公共団体の情報システムのあり方」について、調査研究を行い、地方公共団体の取組の一助とすることを目的とする。

特に、被災時における速やかな業務継続を目指し、「行政データ管理のあり方とバックアップサイト」に焦点をあて、調査研究を実施する。

---

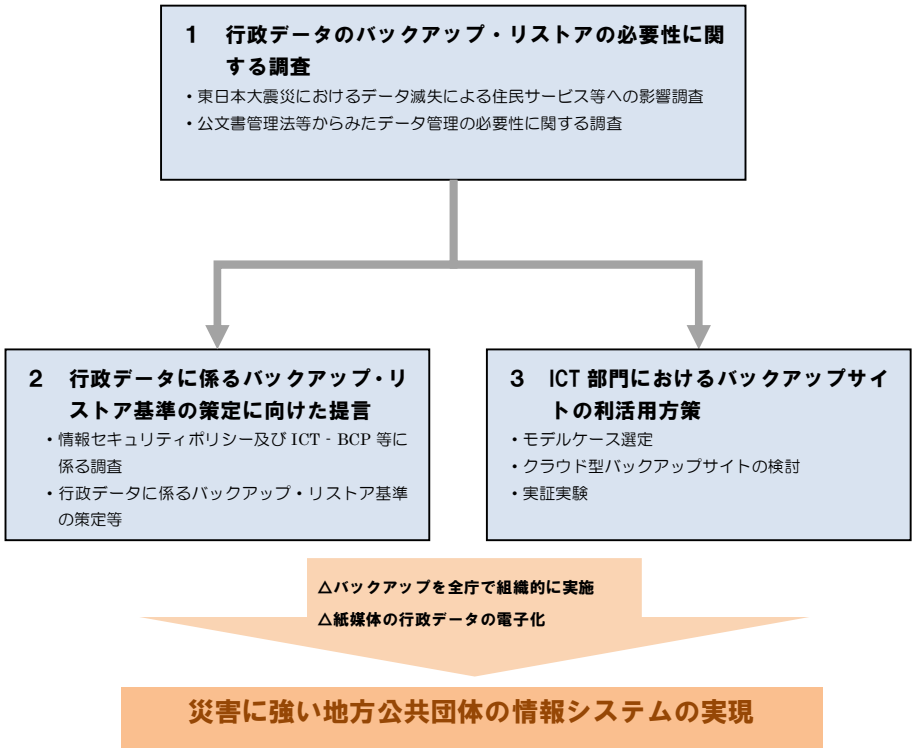
[1] 平成 23 年度調査研究は「第１章　第１節－１　文献調査」（概要）を参照のこと。

[2] 基幹系業務については、次の地方自治情報管理概要～電子自治体の推進状況（平成 24 年 4 月 1 日現在）～の 80 頁を参照のこと。http://www.soumu.go.jp/main_content/000206806.pdf

第２節　実施内容

本調査研究では、まず東日本大震災における行政データの滅失状況等を各種調査により把握し、データ管理の状況やより信頼性の高い管理の必要性等を明らかにする。

次にその結果を踏まえ、行政データのより信頼性の高い管理を行うために、管理・運用面からの方策として電子データのバックアップ及びリストアに係る実施手順（以下「バックアップ・リストア基準」という。）の策定を行うとともに、情報システムを用いた方策としてバックアップサイトの利活用方策の検討を行う。



図－１　本調査研究の実施フローとねらい

以下には、本調査研究の実施内容を個々に示す。

１　行政データのバックアップ・リストアの必要性に関する調査

地方公共団体では、行政事務において多くの団体が ICT 機器を活用しており、データ及び文書が電子化されている。しかし、行政データは、システムとして管理されている電子データを除き、各職員が個々に電子データや文書を管理している状況にある地方公共団体が存在すると想定される。本研究では、事実的側面から東日本大震災の被災団体における行政データの管理の実態やその滅失等による住民サービスに与えた影響を調査し、また、法的側面から公文書管理法等を整理・分析し、バックアップ・リストアの必要性等を研究する。

（１）東日本大震災におけるデータ滅失による住民サービス等への影響調査

ア　文献調査

東日本大震災による地方公共団体の被災状況等に関する既存の調査結果を収集・分析し、行政データの滅失状況や滅失による行政事務や住民サービス等への影響を把握・整理する。

イ　アンケート調査

東日本大震災の特定被災地方公共団体[3]に対し、平常時における行政データの管理状況、被災状況及びデータ滅失等による行政事務や住民サービス等への影響等をアンケート調査し、その状況を把握・整理する。

ウ　ヒアリング調査

上記アンケート結果を分析し、主に行政データの滅失が顕著であった地方公共団体に対してヒアリング調査を実施し、その状況等を精査する。

（２）公文書管理法等からみたデータ管理の必要性に関する調査

公文書管理法等の法令を整理・分析し、各職員が個々に管理している行政データも含め、その管理等の必要性等を再確認する。

２　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

上記調査結果を踏まえ、また、関連する情報セキュリティポリシー等の整理・分析を行い、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。

（１）情報セキュリティポリシー及び ICT - BCP 等に係る調査

情報セキュリティポリシー及び地方公共団体における ICT 部門の業務継続計画（BCP）（以下「ICT - BCP」という。）等を収集・分析し、バックアップ・リストア基準を検討する上での基礎資料とする。

（２）行政データに係るバックアップ・リストア基準の策定等

上記の調査結果に基づき、データの種類や重要度等に応じたバックアップやリストアする単位や方法、頻度（又はタイミング）等をとりまとめた実施手順をバックアップ・リストア基準として策定する。

---

[3] 福島電子力発電所事故による警戒区域、計画的避難区域等を除く

３　ICT 部門におけるバックアップサイトの利活用方策

地方公共団体自身が被災した場合の業務継続を図るため、行政データをバックアップするサイトの各種形態を、「災害に強い」を要件として、セキュリティや保守・運用の作業負荷、コスト等の点から検討する。

また、複数の地方公共団体のシステムをクラウドコンピューティングの技術を用いて一体のバックアップサイトとして管理・運用し、ネットワークを介してどこからでも利用できるバックアップサイト（以下「クラウド型バックアップサイト」という。）を一例として、その実現性及び実用性について模擬環境で実証実験を行う。

第３節　実施体制

本調査研究の実施に当たっては、本件に係る専門知識、知見を有する学識経験者、有識者、地方公共団体等で構成する研究委員会を設置し、本調査研究の方向性、的確性、適時性、網羅性、地方公共団体のニーズとの合致性等のアドバイスを頂くとともに、幅広い意見、助言等を伺い報告書を作成した。

災害に強い地方公共団体の情報システムのあり方に関する調査研究
－行政データ管理とバックアップサイトについて－
研究委員会の構成（敬称略、五十音順）

≪委員≫

池田　義博	北海道自治体情報システム協議会総務課　課長
今井　建彦	仙台市総務企画局情報政策部　部長
佐々木　豊	釜石市総務企画部広聴広報課 課長補佐兼情報推進係長
須貝　俊司	財団法人地方自治情報センター　理事
田中　秀幸	東京大学大学院情報学環・学際情報学府　教授
中山　紀雄	総務省自治行政局地域情報政策室 電子自治体推進係長
村田　新	新宿区総合政策部情報政策課　情報政策主査

≪事務局≫

株式会社三菱総合研究所（研究協力機関）
財団法人地方自治情報センター　研究開発部

第１章　行政データのバックアップ・リストアの必要性に関する調査

地方公共団体では、行政事務を実施するにあたり多くの ICT 機器を活用しており、情報システムの電子データだけでなく、文書等も ICT 機器を利用して作成している。これらの行政データの管理方法は、システムとして管理されるもの、ローカル PC 等に保存されるものなど様々である。

本章では、事実的・法的の両面から、東日本大震災の被災団体に対して、地方公共団体における行政データの管理実態や行政データの滅失等が住民サービスに与えた影響、公文書管理法等からみた行政データ管理の必要性等を調査した。

第１節　東日本大震災におけるデータ滅失による住民サービス等への影響調査

１　文献調査

東日本大震災による地方公共団体の被災状況等に関する既存の調査結果を収集・分析し、行政データの滅失状況や滅失による行政事務や住民サービス等への影響を把握・整理した。

（１）調査仕様（対象文献）

東日本大震災における地方公共団体が作成・運用するデータの滅失や、その滅失により影響を受けた行政事務や住民サービスの状況等に関する調査や関連する検討等を行った、以下の既存の文献を収集し、整理・分析の対象とした。

なお、調査対象を抽出する過程で収集したその他の文献を参考資料に示す。

■東日本大震災における地方公共団体情報部門の被災時の取組みと今後の対応のあり方に関する調査研究　報告書　平成 24 年 3 月　財団法人 地方自治情報センター、慶応義塾大学 SFC 研究所

■情報通信白書　平成 24 年 3 月　総務省

主に第 1 部 特集 ICT が導く震災復興・日本再生の道筋、第 2 節 東日本大震災と事業継続

〔参考資料〕JIIMA 政策提言プロジェクト　現用公文書の危機管理対策のために－電子化バックアップセンター構想の政策提言（骨子）　平成 23 年 8 月　社団法人 日本画像情報マネジメント協会（JIIMA）

〔参考資料〕JIIMA 危機管理を目的とした文書・記録管理ガイドライン V1.01　平成 23 年 10 月 12 日　社団法人 日本画像情報マネジメント協会（JIIMA）記録管理委員会

（２）調査結果

ア　「東日本大震災における地方公共団体情報部門の被災時の取組みと今後の対応のあり方に関する調査研究」

（ア）概観

東日本大震災の被災を受けた岩手県、宮城県、福島県内の13市町のICT部門の発災時の状況や発災後の取組及び今後の課題に対する考え方について、ICT部門への現地調査結果を取りまとめたものである。

当該現地調査では、東日本大震災における被災団体のICT部門としての行動をクローズアップし、被災前の平常時における組織体制や情報システムの状況が震災によりどのような被害、影響が出て、時間の経過とともに、それらがどのように復旧、再生に向けて動いていったか、今後の大規模災害に備えた必要な対策がどうあるべきか等について検討を行っている。

（イ）調査及び検討結果のポイント

a　被災時における ICT 部門の業務継続を含む行動計画

ICT 部門の業務継続を含む行動計画の策定がなされていた市町はなく、多様な状況を想定した柔軟なものが必要との問題提起を行っている。

b　被災状況の多様性

物理的に被災やデータ滅失、電力供給やネットワークの回復状況等によって、ICT 部門へのニーズ、復旧に向けた要件やプロセスなどに大きな違いがあった点を指摘している。

c　ICT 部門への被災後のニーズ変化

被災程度が大きかった市町では、被災直後は直接的な人命救助や避難者誘導などに忙殺され、窓口業務の復旧の優先順位が低かったケースもあった（ただし、救命オペレーション用の住民情報閲覧の緊急性は高かった。）。

ICT 部門も、災害業務へ人員を割かれたケースがあった。そのような市町でも、被災者支援などの段階では、ICT なしでは業務の遂行が困難な状態になったことから、時間の経過とともに ICT 部門へのニーズが変わることが改めて浮き彫りになった。

d　地震対策及び津波対策

津波被害や、通信ケーブル被害などの例を除き、建物の倒壊による損壊など地震そのものによる ICT 機器の物理的被害の例はほとんどみられなかった。

一方、主要な庁舎が海沿いにあった団体では、サーバなどを低層階に設置していたために津波により流出し、そのことがデータ滅失の原因であったことなどから、津波対策については一貫したポリシーがなかったといえる。

e　被災後の民間事業者の役割

情報システム委託事業者との契約の中に災害時についての定めがあったものはほとんどみられなかった。

被災時は情報システム委託事業者が契約外の作業も進んで行い、復旧に大きな役割を果たした。これらの事業者が保管していたバックアップデータにより、滅失したデータを復元した例もみられた。

f　重要データの取扱い

ICT 部門の業務継続計画を考える上でもデータバックアップの重要性が高い。しかしながら、現状では、アプリケーションやデータの管理は業務部門に委ねられている場合が多く、データバックアップの統一的な基準がないばかりか、ICT 部門でさえ、役所の中でどのようなデータがどのように管理されているかを知らない場合もあった。

制度にも問題があり、個人情報保護によって庁舎外保存が禁じられていたケースでは、重要データが津波で失われ、十分な復元が不能になったものもあった。

ハードウェアやアプリケーションの被害は復旧させることも可能であるが、データが滅失すると復元が不可能な状態に陥るばかりか、復旧プロセスのすべてがボトルネックとなる。

データこそが行政にとっての重要資産であるとの認識を再確認する必要がある。

g　電力供給と通信回線確保

ほとんどの市町が安定した電力供給の重要性を訴えていた。機器被害などがなかった団体でも、電力供給が止まることによって ICT サービスの提供ができなかった場合が多かった。

支所等を結ぶ通信回線については、自営の回線敷設の場合、回線の復旧に時間を要する場合が多かったなど、市町村が自ら回線を整備することの限界が露呈した。

今後は、市町村の枠組みを超えた中での通信回線確保が重要であると考えられる。

h　被災者支援システム[6]等の活用

被災者支援システム等のパッケージについては、被災時の状況が切迫し、システムを習得する時間がないことなどにより活用が進まず、結果としてエクセル等の簡易ソフトで代替したり、被災者支援のための対応システムを急遽準備したりする例が多かった。

6　阪神・淡路大震災を経験した兵庫県西宮市において開発された、地震や台風などの災害発生時における地方公共団体の業務を総合的に支援するための業務システムの名称。

i　クラウドコンピューティング等の取組

ICT 部門職員の間でクラウドに対する関心は、特にデータバックアップなどの面で強い一方、セキュリティに対する懸念から慎重な考えを表明する意見も多くみられた。

また、総合行政ネットワーク（LGWAN）[7]を活用したバックアップ体制を要望する声が高い一方で、現状の回線速度ではそれが非現実的であることを指摘する声などもある。

なお、クラウドコンピューティングを含めたシステムの共同利用については、関心は高いものの、データ形式の標準化などに課題があり、トップダウンによる一本化した標準化への取組を求める声が強い。

j　バックアップ・リストア基準策定と管理体制構築等の必要性

災害時対応の手順の検討に入る前に、まずは全庁におけるデータのバックアップ・リストア基準を確立するべきである。調査団体から提供された貴重な教訓を生かすためにも、まず合理的なバックアップ・リストア基準と管理体制を構築する必要がある。

その際には、今回、情報システム委託事業者がデータ復旧に果たした役割を考慮することも必要である。また、今後の課題として、バックアップ・リストア基準の整備にあたって、個人情報の外部保管に関する取扱いのガイドラインも含めた議論を行う必要性が高い。

このバックアップ・リストア基準の策定及び管理体制について、庁内論議の旗振り役には、ICT 部門が担うことが望ましい。

（ウ）調査結果の概要

次表には、データの滅失や業務状況等を中心に調査結果をまとめ、以降の頁にはその内容を整理した。

---

[7] 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。Local Government Wide Area Network を略し LGWAN と呼ばれる。LGWAN は、地方公共団体相互間のコミュニケーションの円滑化、情報の共有による情報の高度利用を図るための基盤として整備され、府省間ネットワークである霞が関 WAN との相互接続により、国の機関との情報交換も行える。セキュリティレベルが高く、ASP を利用し様々な行政用アプリケーションサービスも提供されている。

表－１　東日本大震災の被災地方公共団体におけるデータ滅失及び業務等の状況（１／２）

団体名称		データの種類	データ滅失の状況【本庁舎被害】	バックアップデータの滅失状況	データバックアップの状況			平常復帰の時期			滅失データ回復の状況		
					頻度	保管方法	保管場所	日付等	日数	概要・サービス内容	日付等	日数	データ回復・復旧の内容
岩手県	宮古市	住民情報システム（住基・戸籍・税・福祉）	喪失無し	喪失無し	日次	テープ	本庁舎内	3/14～	3	サーバ類移設			
								3/20～	9	り災証明発行			
								3/27～	16	本庁舎での業務開始			
								4/27～	16	義援金と被災者生活再建支援制度の申請受付			
		PC端末	本庁舎1 階、宮古保健センターで流失										
	陸前高田市	住民情報システム（住基・税・福祉）	滅失【水没】	利用不可（水没）DATテープからのデータ復旧はできなかった	日次	テープ	本庁舎内	3/20～	9	住民票発行、死亡届受	3/23～	12	仮設庁舎仮サーバ運用
								3/23～	12	住基システムと財務会計システムの仮運用を開始	⇒	⇒	この事業者が持参した2 月末時点のデータを使用 財務会計データは、1月23 日時点のデータを使用
								3/29～	18	税務関係証明発行	4/下旬	45	委託事業者持参のデータを使用
								4/ 5～	25	戸籍謄抄本発行	上記以降	46	サーバのHDDから復旧させたデータを使用
								4/27～	47	り災証明発行			
								5/10～	60	印鑑登録			
								5/16～	66	災害義援金、災害弔慰金及び被災者生活再建支援金の申請受付を開始	5/16～	66	第一仮庁舎移転
								5/24～	74	住民異動届手続	7/25～	136	本サーバでの運用開始
		PC端末	流出								7/25～	136	施設の移転とともに随時支援や新規購入により調達
	釜石市	住基システム（戸籍・税・福祉システムは別管理だが、被災状況や復旧工程は同じ）	喪失なし	喪失なし	日次	テープ	本庁舎内	4/1～	21	住民票・印鑑証明の発行、転入・転出届、出生・死亡・婚姻届など（受付のみ）、国民健康保険業務、国民年金業務、税証明などを再開	4/1～	21	教育センターでの業務提供
								4/11～	31	り災証明書及び被災証明書の発行業務等再開（教育センター1 階） 生活再建支援相談窓口（災害弔慰金の案内、被災者生活再建支援金の申請等）開始（シープラザ釜石1 階）	4/18～	38	教育センター（1 階、5 階）で実施していた窓口業務の端末をシープラザ釜石2 階に移設し業務を開始
		PC端末	第2、第3、第4 庁舎で浸水により流失	ファイルサーバ水没（本庁舎B1F設置）									流失分は最終的に機器更新
	大槌町	住民情報システム（住基・戸籍・税・福祉）	発生【水没】完全に喪失	完全に喪失	日次	テープ	本庁舎内	3/17	6	安否確認用として、住基ネットの県サーバから出力した住民データのCD と紙が、県から提供された			
								3/下旬	14	町民課窓口を中央公民館に開設			
											4/8	28	被災した役場庁舎のサーバ室から回収したハードディスクから復元した住基データ（3 月11日時点）を使用して、中央公民館に第2 仮サーバを設置
								4/13～	33	印鑑登録、住民票発行	4/13～	33	仮サーバによる業務開始：住基・税仮復旧
								4/27～	47	り災証明発行	4/末	50	戸籍復旧
								5/9～	59	災害義援金や被災者生活再建支援金の申請受付を開始	5月頃	51	総合福祉サーバ稼働開始
											9/20～	193	本番サーバによる運用開始、戸籍システムのみ本番サーバへの移行は11月
											12月	265	福祉復旧
		PC端末	すべて水没										色々な組織から提供を受けた
宮城県	仙台市	住民情報システム（住基・税・福祉）	喪失なし	喪失なし	日次 月次（市外）	テープ	本庁舎内	3/14～	3	窓口業務再開	3/13～	2	情報システムセンターの主電源回復
								5月連休明け	56	り災証明書の発行を開始	3/17～	6	オンラインシステム稼働再開
		PC端末	被害なし（一部施設で流出）								3/12～	1	本庁舎復電に伴い復旧
	石巻市	住基・税システム（福祉・戸籍システムは別管理）	一部喪失あり（雄勝地区の確定申告データ等）	利用可能	週次 月次	サーバHDD テープ	本庁舎内 図書館（月次）	3/28～	17	本庁舎で、住民票（3 月11 日時点、続柄なし）の写しの交付を再開	3/26～	15	本庁舎の商用電源が復旧
								4/11～	31	窓口業務（住民票・戸籍に関する諸証明、住民票の異動、戸籍届出、印鑑証明・登録、税諸証明等）は、基幹系システムの稼働再開に合わせて再開	4月中旬	35	サーバ回収するも復旧不可能
								4/14～	34	被災証明書・り災証明書、被災者生活再建支援制度、災害弔慰金等の申請受付を開始 被災者生活再建支援制度や災害弔慰金等の受付業務開始			
								5月連休中	53	被災者支援システム本格稼働を開始			
		PC端末	一部出張所で流失・損壊								6月中旬	96	購入（総務省第一次補正予算を活用）
	気仙沼市	住基・税システム（福祉・戸籍システムは別管理）	喪失なし（住民情報系及び内部情報系）※一部部署や公共施設での個別管理機器は損傷あり	喪失なし（住民情報系及び内部情報系）※一部部署や公共施設での個別管理機器は損傷あり	日次（住民情報系及び内部情報系）	テープ（住民情報系及び内部情報系）	本庁舎内（住民情報系及び内部情報系）	3/11～	0	安否確認受付及び死亡届受付は、継続して実施	3/15～	4	非常用発電装置による仮復旧
											3/17～	6	通常稼働
								3/22～	11	住民票の写しの発行再開	3/22～	11	戸籍稼働
								3/23～	12	税証明の交付業務を再開	3/31～	20	市立本吉病院内の医事システム復旧
								3/28～	17	印鑑証明等の交付業務を再開	4/14～	34	同病院内財務会計・給与システム復旧
								4/18～	38	り災証明書の交付開始	5/31～	81	生活保護システム復旧
								5/16～	66	被災者生活再建支援金の申請受付を開始	6/7～	88	公営企業会計システム復旧
		PC端末	一部公共施設で流失								3/17～	6	本庁舎及び電算センター復電 流失分は一部新規購入

表－１　東日本大震災の被災地方公共団体におけるデータ滅失及び業務等の状況（２／２）

団体名称		データの種類	データ滅失の状況【本庁舎被害】	バックアップデータの滅失状況	データバックアップの状況			平常復帰の時期			滅失データ回復の状況		
					頻度	保管方法	保管場所	日付等	日数	概要・サービス内容	日付等	日数	データ回復・復旧の内容
宮城県	東松島市	住基・税・福祉システム（戸籍システムは別管理）	喪失なし	喪失なし	日次(異動分) 週次(全体)	テープ	本庁舎内	3/14～	3	死亡届の受付開始	3/16～	5	システムが再稼動
								3月下旬	14	被災証明書の発行開始			
								4/4～	24	り災証明書の受付・発行、災害弔慰金、災害障害見舞金、災害援護資金の申請受付を開始	4/18～	38	「り災台帳システム」の稼働開始
								4月初旬	25	市民課窓口で、戸籍関係など各種証明書の発行や転入・転居などの受付を開始			
								4/20～	40	被災者生活再建支援制度の申請受付を開始			
		PC端末	一部の出張所等で流失								3/15～	4	本庁舎内復電 流出分は支援や新規購入
	南三陸町	住基、税、福祉（戸籍システムは別管理）	発生 【流出】	喪失	週1～2回	テープ サーバHDD	本庁舎内	3/28～	17	一部窓口業務（住民票・印鑑証明書・転出等の届出・死亡届の受付等）を再開	3/22～	11	仮庁舎で業務開始後、仮サーバにより仮復旧
								4/3～	23	11か所の避難所において、順次、「り災証明書・被災証明書」の申請受付を開始	3月末	20	データ処理等を委託している事業者が3月4 日時点の住民情報を格納した仮サーバ等を持参。 一部窓口業務に利用（内部情報系システムのデータはすべて喪失）
								4/14～	34	被災者生活再建支援金の申請受付開始	4月下旬	45	平成23 年1 月下旬までのデータを法務局において再製、そのデータを使ってシステムを復旧
								5月上旬	55	り災証明書の発行開始			
								5/17～	67	災害義援金の申請受付開始			
								5/25～	75	窓口業務開始	7～8月	112	データセンターへ仮サーバを移設
								6/1～	82	災害弔慰金の申請受付開始	H24.1～	299	新システム稼働
		PC端末	流出										情報システム委託事業者の支援でプリンタ5 台・パソコン20 台程度、そのほかはレンタル（順次、支援や購入により増設）
福島県	いわき市	住基システム（戸籍・税・福祉システムは別管理）	喪失なし	喪失なし	月次(異動分) 週次(全体)	テープ	本庁舎内	3/14～	3	窓口業務の一部再開（本庁舎での臨時窓口）	9月 9/16～	174	サーバ室を庁舎外に移転 原発避難者特例法に基づく指定市町村となった
								4/4～	24	り災証明書の発行開始	11月末	264	「被災者支援システム」稼働
		PC端末	流出（パソコン端末10 台未満）										
	南相馬市	住民情報システム（住基・戸籍・税・福祉）	喪失なし	喪失なし	日次	テープ	本庁舎内	4/25～		り災証明書の発行開始（地域自治区ごとに順次発行を開始）	9/16～		原発避難者特例法に基づく指定市町村となった
		PC端末	被害なし										ICT 支援応援隊からパソコン40 台、事業者から10 台ほどの貸与を受けた
	双葉町	住基、税、福祉（戸籍システムは別管理）	無 【無（原発事故移転）】	喪失なし	日次	テープ	本庁舎内	3/20～	9	被災証明発行	3 月末及び4月初旬	20～25	一時的に役場庁舎に戻った際に持ち出し、仮システム構築時に使用
								4/18～	38	窓口業務開始	4/18～	38	旧埼玉県立騎西高校移転後に仮復旧
								6/22～	103	り災証明発行	4/22～		町内全域が警戒区域となった
											9/16～		原発避難者特例法に基づく指定市町村となった
		PC端末	被害なし										さいたまスーパーアリーナ移転時に新潟県刈羽村からプリンタ及びパソコン各10 台寄贈、旧埼玉県立騎西高校移転後、民間事業者による支援
	浪江町	住基・税・福祉システム（戸籍システムは別管理）	無 【無（原発事故移転）】	喪失なし	日次	サーバHDD テープ	町外保管(日次) 本庁舎内	3/22～	11	被災証明発行			
								4/4～	24	住民票・印鑑証明書・税証明書の発行を、二本松事務所（二本松市東和支所内）で開始	4/4～	24	簡易サーバ設置 バックアップデータは簡易サーバ上で使用
								4/中旬～	35	「り災証明書」の発行を開始	4月下旬	45	いわき市内データセンターサーバと接続
		PC端末	被害なし								12/9	273	一時的に庁舎に戻った際、120 台ほどを二本松事務所へ順次運び出した ICT 支援応援隊からの支援（ノートパソコン20 台）を含め、新たに60～70 台のパソコンを調達 業務に必要なパソコンは、確保済み

日数：3/11の翌日から起算　上旬：5日　中旬：15日　下旬：25日　としてそれぞれを算出

ａ　本庁舎の被災状況と ICT 機器・設備、データバックアップの状況

（ａ）窓口業務の移転

・本庁舎における窓口業務の移転を行ったのは、13市町中8団体であった。

・上記の内、津波被害があったのは、陸前高田市、釜石市、大槌町、気仙沼市、南三陸町の5団体である。

・5団体のうち、水没又は流失して一時的に行政機能が失われた団体は、陸前高田市、大槌町、南三陸町となっており、同時に、ICT部門の職員が被災し、データの滅失が発生している。

・津波被害には遭わなかったものの、窓口の一部移転を実施したのは、いわき市の1団体である。

・本庁舎の被災がないにも関わらず移転を余儀なくされたのが双葉町及び浪江町の2団体であった。

－2団体については、東京電力福島第一原子力発電所の事故（以下「原発事故」という。）による行政機能の滅失に伴う移転である。

－地震による影響については、耐震化対策の実施済みが4団体で、未実施の団体が多いにも関わらず、建物への大きな被害は発生していない。

（ｂ）サーバの設置場所状況

・13団体の内、本庁舎に設置していた団体は10団体であった。

・情報センターに外出ししていたのは1団体（仙台市）のみである。

・被災後、サーバ室を移設したのは6団体。そのうち、データセンターに移設したのは3団体である。

表－２　サーバの設置場所状況

団体名称		サーバ設置場所	サーバ室被災の有無	被災後のサーバ室移転先
岩手県	宮古市	本庁舎	無	
	陸前高田市	本庁舎の1階	**有（4Fまで水没）**	仮庁舎内に移転
	釜石市	市内公共施設の最上階	無（注）	
	大槌町	本庁舎の2階	**有（2F天井まで水没）**	高台の公共施設に移転
宮城県	仙台市	情報センター（市内）	無	
	石巻市	本庁舎、支所で分散管理	**有（2F天井まで水没）**	
	気仙沼市	本庁舎、電算センターに配置	無	
	東松島市	本庁舎	無	
	南三陸町	防災対策庁舎の2階	**有（庁舎壊滅）**	データセンターに移設
福島県	いわき市	本庁舎	無	H23.9～本庁舎外に移転
	南相馬市	本庁舎	無	
	双葉町	本庁舎	無	データセンターに移設
	浪江町	本庁舎	無	データセンターに移設

注：地階の機器室の浸水により、ネットワーク機器等が使用不能

（ｃ）データのバックアップの状況

・ICT 部門の所管業務は「基幹系」と呼ばれる業務が大半を占める。
・バックアップ頻度は、大半が「日次」である。
・保管方法（媒体）は DAT 等の「テープ」である。
・保管場所は、13 団体のすべてが「本庁舎内」であり、そのうち、2 団体が別の場所にも保管している。
・データ滅失が発生しているのは、下表のうち、網掛けのある 3 団体である。

表－３　データのバックアップ状況

団体名称		ICT部門の所管業務	保存頻度	保管方法	保管場所
岩手県	宮古市	住基、戸籍、税、福祉	日次	テープ	本庁舎内
	陸前高田市	住基、税、福祉	日次	テープ	本庁舎内
	釜石市	住基	日次	テープ	本庁舎内
	大槌町	住基、戸籍、税、福祉	日次	テープ	本庁舎内
宮城県	仙台市 (注)	住基、税、福祉	日次 月次（市外）	テープ	本庁舎内
	石巻市	住基、税	週次 月次	サーバHDD テープ	本庁舎内 図書館（月次）
	気仙沼市	住基、税、福祉	日次	テープ	本庁舎内
	東松島市	住基、税、福祉	日次(異動分) 週次(全体)	テープ	本庁舎内
	南三陸町	住基、税、福祉	週1～2回	テープ サーバHDD	本庁舎内
福島県	いわき市	住基	日次(異動分) 月次(全体)	テープ	本庁舎内 本庁舎外（月次）
	南相馬市	住基、戸籍、税、福祉	日次	テープ	本庁舎内
	双葉町	住基、税、福祉	日次	テープ	本庁舎内
	浪江町	住基、戸籍、税、福祉	日次	サーバHDD テープ	町外保管(日次) 本庁舎内

注：ICT 部門はサーバ機器・設備を管理し、業務部門はシステムを管理

（ｄ）ICT部門の発災時の対応

ICT 部門の発災時の対応については、すべての調査団体において、不測の事態に迅速・的確に対処するための ICT 部門に特化した行動マニュアル等は特に定められていなかった。

情報システム委託事業者への連絡や常駐している運用委託事業者との連携など、発災時の対応に委託事業者が重要な役割を担っている。しかしながら、委託事業者との契約では、発災時の対応に関する条項を設けている例はなく、通常の運用保守契約の中でシステム障害時の対応を取り決める程度となっている。

表－４　ICT 部門の発災時の対応

団体名称		災害時の際の定め（ルール）等	具体的行動
岩手県	宮古市		・システム委託事業者への連絡 ・サーバ室確認
	陸前高田市		
	釜石市		
	大槌町		
宮城県	仙台市	主要な情報システムの運用ガイドライン	・発災時には主要な情報システムの状況を把握する
	石巻市		・汎用機の手動でのシャットダウン
	気仙沼市		・サーバ室（2か所）の状態確認
	東松島市		・サーバ及びネットワーク機器の被災状況確認
	南三陸町		・サーバ室機器類の点検（津波前の段階）
福島県	いわき市	独自の緊急連絡網を策定 （情報システム委託業者を含む）	
	南相馬市		・サーバ及びネットワーク機器の被災状況確認
	双葉町		
	浪江町	「非常時はその時点のバックアップを取る」と内規で定め	・住基データをCSV形式で出力し避難時に持ち出し
		:本庁舎水没	
		:本庁舎流出	

b　データ等の滅失の状況

（a）基幹系データの滅失の状況

前述のとおり、陸前高田市、大槌町、南三陸町の 3 団体において、基幹系データの滅失が発生した。

（b）その他システムのデータ管理の状況

多くの調査団体が基幹系システム（住基、税、福祉等）は ICT 部門で所管し、その他の情報システムはデータ管理も含め、業務部門で管理しているが、全庁で統一したバックアップ基準等は策定されていない。また、ICT 部門は、業務部門のデータ管理状況を必ずしも把握はしていない。

バックアップの統一した基準としては、仙台市が情報セキュリティポリシー及び情報セキュリティ実施手順の中で定めており、130 の主な情報システムの管理情報は、バックアップテープの有無も含め、データベース化している。

特に、重要な住民情報、税、福祉システムなどについては、別に運用ガイドラインを定めており、それに基づき、設計書及び運用手順書でバックアップ・リストアの手順を定めている。

（c）PC の状況

・宮古市

本庁舎 1 階にあった PC は、津波によりすべて流出（後にすべて回収）した。

宮古保健センターでも、一部 PC が流出（その後も行方不明）した。

－津波で流出した PC は、リースのものが多かった。リース物件の津波による損害は、動産保険が適用されないため、物件の修

繕費は市の負担となる。市では契約を継続し、リース期間満了後、物件の返還は必要ないという申し合わせをした。

－データの滅失（流出）の率については不明である。

・陸前高田市

市庁舎1階のサーバ室が津波の被害に遭ったため､PCについても、ほとんどが流出した。

被災後に外部から提供されたPCを庁内で使用するには、ネットワークへの接続やOSの設定変更等を行う必要があり、機器の性能やOS・オフィスソフトのバージョンが合わないなど、そのままでは利用できないものもあった。

7月25日からは、第3仮庁舎での業務が開始、この時点で、仮庁舎内のサーバ、通信機器、職員用PCなどのハード面は、3月11日以前に限りなく近い状態となった。

－データの滅失（流出）の率については不明である。

・釜石市

第2庁舎～第4庁舎の1階は津波で浸水し、PC等の機器が流出したり、使用不能となったりした。

流出・損傷した機器は、全庁舎の合計で、PC約80台、コピー機8台（リース)、プリンタ5台であった。

－第1庁舎地階に置いていたファイルサーバ等の機器は､すべて水没して使用不能となった。

・大槌町

大津波に襲われ、役場庁舎内にあったコピー機、PC、サーバは、利用不可能となった。

そのため、PCは、いろいろな組織から提供していただいた。ただし、提供前に一定の設定は実施していただいたが、LANの設定等は役場で行う必要があった。また、必要なソフト（ウイルス対策ソフトやJava等）のインストールは、事業者へ委託した。

財務会計システムのサーバ、ラック及びセットアップ費用等は、委託事業者から支援を頂いたが、住基ネットで使用する機器は、新たに購入した。

なお、総務省からもPCの提供があり、いずれはすべてのPCを置き換える予定である。

・仙台市

津波被害のあった施設（学校・保育園・南蒲生下水処理場）では、機器が流失した。

市役所本庁舎内の PC 等業務機器へは給電がない状態であったため、サービスを停止しデータをバックアップした後、サーバを停止させた。

・石巻市

公共施設を含む市役所全体で稼働している PC は、約 3,000 台であり、情報政策課では、本庁舎や総合支所等で使用する 1,300 台を管理していた。学校関係については、教育委員会が管理していた。

本庁舎では、PC23 台、プリンタ 13 台、イメージスキャナ等 12 台が損壊し、総合支所等では、PC193 台、プリンタ 50 台が、流失又は落下により損壊した。

－これらの損壊した機器は、総務省の第一次補正予算を活用して、6 月中旬に購入。

－10 月ころから、組織改編があったり、他都市からの応援職員が急激に増えたりしたほか、地元の被災者を窓口対応などのために臨時的に雇用したことから、コンピュータの利用者が 200～300 人程度増えたことにより、アカウント発行や PC 設置の事務が頻発した。

・気仙沼市

本庁舎、電算センター、唐桑総合支所及び本吉総合支所では、ハードウェアの損傷はなかった。しかし、本庁舎に隣接する分庁舎「ワン・テン庁舎」では、大津波により一階部分が浸水したため、PC をはじめとするハードウェアは、大きな被害に遭った。また、内部情報システムに接続している公共施設（公民館・児童館等）では、情報化推進室で管理している PC 約 500 台のうち 100 台以上が流出・損傷した。

PC 等機器の支援については、貸与期間が設けられている場合が多く、その後の代替機器の用立ての見通しが立たない状況では、受け入れにくかった。

OS のライセンスに関しても、同様に期限が設けられている場合があり、復興業務が長期間に及ぶことを考慮し、貸与ではなく現物支援として提供された機器を優先的に利用することとし、不足する分は新たに購入した。

・東松島市

本庁舎及び鳴瀬庁舎（分庁舎）にあった PC に被害はなかった。

本庁舎内の復電（3 月 15 日）と同時に稼働したが、出張所等の一部では、大津波による機器の流失等があった。

－外部からの支援を受けたものもあるが、平成 23 年 6 月に策定の「東松島市震災復興基本方針」に基づく公共施設の復旧に併せて、復旧させる予定。

・南三陸町

地震の揺れにより、サーバラックが倒れ、その後、大津波が襲来し、防災対策庁舎の屋上を超えた（防災対策庁舎には、非常用発電装置が整備されていた)。本庁舎は、地震発生直後に停電した。また、庁内ネットワークは、利用できなくなった。

大津波の来襲により、本庁舎は倒壊し、防災対策庁舎は鉄骨だけが残った状況であるため、相当数の PC の流出があったものと推測されるが、その数等までは把握されていない。

仮庁舎（1 棟目）の設置時に、情報システム委託事業者から、仮サーバ、PC（20 台程度)、プリンタ（5 台）の提供があり、そのほかは、レンタル等で対応した。機器のセットアップは、役場職員と情報システム委託事業者で実施し、その後、仮庁舎の増設に合わせて、支援や新規購入により機器を整備した。

・いわき市

津波による被害のあった地区では PC 等が流出した。流出した台数は、10 台未満であった。

・南相馬市

津波で浸水した地域以外、市内の停電はなく、庁内ネットワーク（業務系と情報系は分離）も問題なく稼働した。本庁－区役所間は、自営の光ファイバ網でつないでいたが、この線は生きていた。また、PC の被害はなかった。

－ICT 支援応援隊から PC40 台、事業者から 10 台ほどの貸与を受けた。

・双葉町

役場庁舎内のコピー機やプリンタ、PC 等の機器については、利用上障害となる大きな被害はなかった。

さいたまスーパーアリーナから旧埼玉県立騎西高校への移転時は、寄贈を受けた PC 及びプリンタ各 10 台を持ち運んだ。民間事業者からは、事務用として 40 台、避難者貸し出し用として 40 台、計 80 台の寄贈があった。すべて OS がインストール済みの状態であった。そのほか一般の方からの支援もあった。セットアップは、役場職員と PC 提供元の事業者とで行った。

なお、役場庁舎へ一時的に戻った際は、業務に使っていた PC を持ち出した。

・浪江町

役場には、約 300 台の PC があったが、地震・津波で損壊したもの

はなかった。役場から津島支所への避難の際、PC を 3 台持ち出し、その後、二本松市東和支所へ移動した際は、その 3 台と津島支所にあったものとを合わせて、10 台ほど持っていった。

一時的に庁舎に戻った際、120 台ほどを二本松事務所へ順次運び出した。ICT 支援応援隊からの支援（ノート PC20 台）を含め、新たに 60～70 台の PC を調達した。なお、12 月 9 日現在、業務に必要な PC は、確保済みである。

c　データ等の被災による実務上の影響

（ａ）宮古市

窓口の閉鎖、再開の状況は把握できるが、実務上の影響の詳細については、不明である。

本庁舎は津波に襲われ、総合窓口が置かれていた 1 階部分が、完全に水没した。サーバ室は、ぎりぎりで被災を免れ、床が海水でぬれた程度で済み、機器やデータは守られた。住基／戸籍／税／福祉システムの機器は無事で、データの損失もなかったが、1 階総合窓口の PC が流出・全壊した。

地震発生直後、市内全域で停電が生じ、本庁舎にある小型の非常用発電装置（2 台）は照明等への給電にとどまっていた。そのため、大型の非常用発電装置を備えた新里総合事務所へ、最小限のサーバを移設して稼働させることを決め、同日のうちに、移設作業を行い、23 時ごろには新里総合事務所でシステムを稼働できる状態になり、3 月 14 日には、新里総合事務所では、朝から通常どおり総合窓口業務を実施している。

庁舎間を結ぶ専用回線（地域イントラネット）は、地震後もつながっていたが停電のため実際には使用しなかった。本庁舎の復電は、本庁舎周辺が津波被害のための電柱が倒れ、部材調達の遅れにより 3 月 26 日となった。

このように、システム復旧だけでなく、復電及び通信回線網等の復旧も実務やサービス提供に大きく影響している様子が覗える。

（ｂ）陸前高田市

窓口の閉鎖、再開の状況は把握できるが、実務上の影響の詳細については、不明である。

データに関しては、サーバの HD からの復旧や、他の場所に残っていたデータからの復旧を試みたが、復旧できないデータもあった。復旧不可能なデータをいかに埋めるかが、重要な課題となっている。

今回の震災で、テープからはデータの復旧ができなかったこと、テープだと定期的な交換作業が必要なこと等により、現在では、データのバックアップにテープは使っていない。

震災前、市の情報システムは、業務部門毎にシステムの仕様が決められ、ストレージ（外部記憶装置）や UPS 装置（無停電電源装置）は、サーバ

毎に設置していた。設置スペースも限られていたため、新しいシステムを導入する際は、セキュリティや、機器の重量等の問題で、その都度既存の機器の配置替えを行う必要があり、手間と費用がかかっていた。今後はそうしたことを避けたいと考え、仮庁舎への移転後は、サーバ室全体を担うUPS 装置を導入し、ストレージも共有化した。

（ｃ）釜石市

窓口の閉鎖、再開の状況は把握できるが、実務上の影響の詳細については、不明である。

サーバは無事であった（データ滅失はなかった）が、窓口業務を行う PC の電源と、PC からサーバ室までの回線が不通であることにより、情報システムを使用した各種窓口業務が再開できない状況であった。このため、電気が復旧した地域にある施設に窓口を開設（PC を置き、その施設からサーバ室への回線を敷設）するという方針で、再開準備が進められた。

バックアップに関しては、外部記録媒体として、原則としてサーバ室で保管していたが庁舎外で保管しているバックアップデータもあった。データの性質によって庁舎外へ持ち出すことが難しいシステムもあるため、庁舎外にバックアップ媒体を保管するかどうかは､システムによって異なる。なお、バックアップ頻度は、システムによって毎日から毎月まで様々であった。

非常時に電源が確保できない問題が大きかったことから、非常用発電装置の追加購入を検討している。データの復旧だけでなく、電源の確保も実務上の影響が大きく、重要な課題となっている。

（ｄ）大槌町

窓口の閉鎖、再開の状況は把握できるが、実務上の影響の詳細については、不明である。

総務課の金庫に納められていたバックアップテープも、サーバ室の住基サーバにセットしていたバックアップテープも､ともに残っていなかった。津波に襲われ亡くなってしまった情報担当の職員が、取り出して、持って避難しようとしたものと考えられる｡財務サーバのバックアップテープは、取り出す時間がなかったのだろう、DAT 装置内に残っていた。

データの復旧手順は、システムによって異なる。住基サーバと税サーバのデータは、HD から復旧できたが、総合福祉サーバのデータ（一部）は復旧できなかった。戸籍は、管轄法務局で保存していた戸籍の副本等に基づき、平成 23 年 2 月中旬までのデータを法務局において再製（平成 23 年 4 月下旬完了)、そのデータを使ってシステムを復旧させた。

サーバ室に残存していた HD の、データ復旧に至るまでの流れは、以下のとおりである。

①情報システム委託先の 1 つである事業者の担当者が、役場庁舎が流

されなかったことから建物内にサーバが残っているのではと考え、岩手県政策地域部市町村課に連絡。県職員から職員情報班長に連絡を取り、サーバを回収することを連絡。

②3 月 25 日、職員情報班長、県職員、この事業者の担当者でサーバ室に入る。ラックから機器を取り外してみると、機器内部まで泥やがれきが入っている状態だった。基幹系システムのサーバ等 8 台（総合福祉サーバ、住基サーバ、税サーバ、介護サーバ、照会発行サーバ、運用サーバ、財務会計サーバ 2 台）を回収し、各ハードウェアメーカに、データの復旧を依頼。

③住基サーバ、税サーバ及び介護サーバのデータは、HD から復旧できたが、財務会計サーバのデータは、復旧できなかった。財務会計サーバについては、サーバ室内に残されていたバックアップテープからデータを復旧。

－平成 24 年 1 月現在、住基・戸籍・税・総合福祉の各サーバは、冗長構成にしている。住基については、総合行政ネットワーク（LGWAN）経由で情報システム委託事業者のデータセンター（遠隔地）へ 30 分毎にバックアップを行うサービスを、平成 23 年 12 月から利用している。

（ｅ）仙台市

本庁舎も情報システムセンターも、情報システム自体には大きな被害はなかった。

情報システム委託事業者は仙台市内に事業所があり、障害発生時には数十分で駆け付けられること、情報システムセンターには、情報システム委託事業者が常駐していたことなどから、仮に被害にあったとしても、その復旧にあたる人員の確保に奔走しなければならないような事態は、避けられたであろうと想定される。

窓口業務は、停電による情報システムの停止後も、紙による申請書・届出書については受付を継続していたが、担当職員の多くが避難所の運営にあたるなど、通常よりも少ない人数で、最小限の対応しかできない状況であった。窓口に住民が訪れ始めたのは 16 日ころからで、3 月中は窓口の大きな混乱はなかった。

住基／戸籍／税／福祉業務データは、毎日、情報システムセンター内でバックアップを取得しており、毎月、遠隔地（市外）にバックアップテープを保管している。

（ｆ）石巻市

窓口の閉鎖、再開の状況は把握できるが、実務上の影響の詳細については、不明である。

データ復旧については、サーバ室のフリーアクセスフロアの水抜きを行い、本庁舎での商用電源復電後（3 月 26 日）は、「ディスクチェック等の

実施」、「データに滅失がないことを確認」、「3 月 11 日に実施予定であった処理を実行し、その処理結果を確認」、「3 月 11 日以降の異動分のシステムへの反映」の順に作業等を実施した。

サーバ室のフリーアクセスフロア下が浸水し、ネットワークケーブル等が水没した。フリーアクセスフロアは、津波により床下が 20～30cm ほど浸水し、電源、ネットワーク、ケーブル等、フロアの下にあったものは、すべて水没した。サーバ機器そのものは水没しなかったが、付随するケーブルや電源関係は、すべて交換が必要になった。

異動データの反映が終了した後に、個別システムとの情報連携を開始した。データの整合性の確認は、各業務部門で実施した。

情報政策課では、ハード及びシステムの面から、業務再開のめどを各業務部門へ伝えた。津波により庁舎が全壊した雄勝総合支所の申告支援システム用サーバは、4 月中旬に回収を行ったが、サーバが錆びついており、データの復旧はできなかった。総合支所等は、復電次第、情報政策課の職員が現地に赴き、システムの確認と復旧を行った。雄勝総合支所では、3 月 11 日は確定申告相談受付会場となっていたため、申告支援システム及び申告開始日から被災当日までの雄勝地区の申告データ等が滅失した。

ーデータのバックアップについては以下のとおりであった。

- メインフレームのデータバックアップは、週一回サーバに保管するとともに、月に一回、本庁舎近くの高台にある図書館へ磁気テープを保管。
- 基幹系システム（メインフレーム上で稼働している住基と税）のデータは、週 1 回サーバ上にバックアップを行い、3 世代まで保存。
- サーバは本庁舎と河北総合支所に分散配置し、ファイルサーバは本庁舎と渡波支所でレプリケーション[8]構成としていた。
  渡波支所を使用していたのは、スペースや電源容量の都合である。
- そのほか、バックアップデータ（磁気テープ）は、本庁舎近くの高台にある図書館へ、月 1 回運んでいた。
- 戸籍については、月 1 回程度の間隔で、データ保存したテープ等を法務局へ送付。
- 総合福祉システムについては、業務部門の管理となっているため、情報政策課では詳細を把握していない。
- 全庁的なバックアップデータの保管に関する全庁統一ルールは存在しない。
- 毎週金曜日の夜に実施していたバックアップ処理は実行できなかった。

[8] データベース管理システムが持つ機能の一つで、あるデータベースとまったく同じ内容の複製（レプリカ）を別のコンピュータ上に作成し、常に内容を同期させる機能。負荷分散や耐障害性の向上などを目的に行われる。

（ｇ）気仙沼市

窓口の閉鎖、再開の状況は把握できるが、実務上の影響の詳細については、不明である。

地震発生直後、本庁舎及び電算センターは停電したが、本庁舎及び電算センターは、地震の揺れによる建物の損壊もなく、津波による浸水もなかった。住民情報システムのデータは、毎日テープでバックアップを行い、サーバ室内に保管していた。住基／戸籍／税／福祉業務データのバックアップは、毎日夜間に行っている。

- 1 週間を 1 サイクルとして、曜日ごとに使用するスロットを指定（オートチェンジャを利用）している。
- バックアップデータは、電算センター内に保管している。
- 遠隔地では保管していない。

（ｈ）東松島市

窓口の閉鎖、再開の状況は把握できるが、実務上の影響の詳細については、不明である。

本庁舎は、津波による浸水を免れ、建物及び事務用機器への大きな被害はなかった。サーバ室は、地震の揺れによりラックが歪んだが、それ以外の被害はなかった。発災直後は、市内全域で停電となった。サーバは、UPS 装置（無停電電源装置）からの給電に切り替わったのち、自動でシャットダウンした。

サーバ機器の被災はなかったため、住民情報等データの滅失はなかった。バックアップは、日々の差分を、週一回全件、それぞれ DAT テープに保存し、本庁舎 1 階の金庫で保管していた。

新システムが稼働した平成 23 年 7 月以降は、メディアが LTO に変わり、バックアップメディアは、サーバ室で保管するようになった。なお、平成 23 年 11 月現在、サーバ室以外での保管を検討している。

（ｉ）南三陸町

窓口の閉鎖、再開の状況は把握できるが、実務上の影響の詳細については、不明である。

電算室は、防災対策庁舎の 2 階にあったため、サーバ及びバックアップテープも滅失した。住基／戸籍／税／福祉業務データのバックアップは、フルバックアップが週 1～2 回、差分バックアップは毎日、テープ及びストレージ上に保存し、電算室内で保管していた。システムによっては、業務部門がバックアップを行っているものもあった。

戸籍は、管轄法務局で保存していた戸籍の副本等に基づき、平成 23 年 1 月下旬までのデータを法務局において再製（平成 23 年 4 月下旬完了）、そのデータを使ってシステムを復旧した。庁舎内の台帳や申請・届出書も、津波により流出したが、可能なものから順次再開しようとの判断だった。

滅失分の住民情報や戸籍情報等は、住民の協力（届出等に関する申出等）により、復元を目指している。住民情報は、3 月 4 日から 11 日までの異動分のデータがなくなった。内部情報系システムは、電算室内で保管していたバックアップテープも流されたため、データの復旧は不可能となった。なお、確定申告の情報については、3 月 7 日分までは税務署へ送付していたため、3 月 8 日から 11 日までの 4 日間分がなくなった。

（ｊ）いわき市

窓口の閉鎖、再開の状況は把握できるが、実務上の影響の詳細については、不明である。

サーバ室の免震ラックが、少しずれた程度で、データの滅失はなかった。サーバ室のラックについては、職員と情報システム委託事業者で 3 月 12 日に対応を行った。4 月の余震の際は本庁舎内が停電したため、職員がすぐに対応できるシステムについては、シャットダウンをした。

住基の異動分は毎日、全体は月に 1 度、DAT テープにバックアップし、本庁舎内と本庁舎外（市内）で分散保管を実施していた。税や福祉系も、基本的には毎日バックアップを行っているが、分散保管は実施しておらず、各業務部門で保管する形となっていた。戸籍に関しては、市民課でサーバ管理を行うとともに、バックアップも市民課で実施していた。

情報システム委託事業者との契約は、原則として、情報政策課で一元管理しているが、一部例外がある。データバックアップの頻度は各業務部門で決めるが、保管場所は、情報政策課が決定していた。

（ｋ）南相馬市

3 月 11 日は、本庁内での停電はなく、機器類にも影響はなかった。ラックが少し動いたものの、情報システム自体への影響はなかった。本庁内は停電しなかったため、情報システムは稼働を続けた。

データバックアップについては、毎日テープで庁内に保管していた。ファイルサーバも同じようにバックアップを取っていた。保管場所は本庁内であった。

情報政策課では、発災以降、避難者名簿等の整理と市ホームページの管理運営業務に注力し、特に携帯電話サイトのコンテンツづくりに力を入れた。「携帯でみられる情報が少ない」という意見を受けて、携帯電話サイトに放射線量の情報などを増やした。その結果、3 月 11 日以前は月 3,000 ほどのアクセス数だったが、震災後は 60 万アクセスと 200 倍に増えた。震災 2 ヶ月後には PC 版ホームページの 2 倍のアクセスを記録した。

本庁舎に被害はなかったものの、市内は原発の影響で警戒区域、緊急避難人微区域、計画的避難区域に分かれたため（9 月 16 日、原発避難者特例

法[9]に基づく指定市町村となった）実務が混乱し、自治体窓口の閉鎖、再開の状況は把握できるが、実務上の影響の詳細については、不明である。

（ｌ）双葉町

窓口の閉鎖、再開の状況は把握できるが、実務上の影響の詳細については、不明である。

3 月 20 日には、さいたまスーパーアリーナでは、情報システム委託事業者が持参したデータを元に住民情報の閲覧が行えるようになった。3 月 31 日に旧埼玉県立騎西高校へ移転した後は、この事業者に仮システムの構築を依頼した。このデータを用いて、住民情報システムを仮サーバ（ノート PC）上に構築し、住民票の写しの交付を行えるようにした。

3 月 12 日早朝に担当職員がセットした住民情報のバックアップテープは、3 月末及び 4 月初旬に役場庁舎へ一時的に戻った際に持ち出し、業務に必要な機器や埼玉支所での業務に利用している。戸籍システムも、同時期に持ち出したデータを基に、情報システム委託事業者の支援を受けて仮復旧させた。

住民情報システム（住基／戸籍／税／福祉業務）のデータは、毎日テープにバックアップをとり、テープはサーバ室内で保管していた。なお、戸籍システムに関しては、住民生活課が担当となりバックアップを行っていた。

（ｍ）浪江町

震災前、住基・税・福祉システムのデータは、いわき市内にある情報システム委託事業者のデータセンター内のサーバへ、毎日バックアップを行っていた。戸籍データについては、庁舎内で毎日バックアップを行っていた。

戸籍に関しては、3 月 20 日ころに役場庁舎に一時的に戻った際、サーバ室のラックからサーバを取り外し、二本松事務所（二本松市東和支所内）へ持ってきた。

ｄ　復旧の時期及びプロセス

（ａ）行政機能滅失団体の窓口業務再開状況

一部のサービスは、発災後 9 日程度で再開されたが、窓口業務の再開には、1 か月半から 2 か月半程度を要している。物理的な被災を受けた団体の方が、原発事故関連で移転した団体よりも窓口業務の再開が早かった。これは、避難に関する初動の遅れ等によるものと思われる。

---

[9] 総務省「原発避難者特例法に基づく指定市町村の指定（http://www.soumu.go.jp/menu_news/s-news/01gyosei01_01000025.html）」

表－５　行政機能滅失団体の窓口業務再開状況

団体名称		本庁舎の被災	データ滅失	バックアップ	窓口業務再開の状況		
					再開日	日数	サービス内容
岩手県	陸前高田市	水没	発生		3/20～	9	住民票交付、死亡届受
					3/29～	18	税務関係証明交付
					4/5～	25	戸籍謄抄本交付
					4/27～	47	り災証明交付
					5/10～	60	印鑑登録
					5/24～	74	住民異動届手続
	大槌町	水没	発生		4/13～	33	印鑑登録、住民票交付
					4/27～	47	り災証明交付
宮城県	南三陸町	流出	発生		3/28～	17	住民票交付
					5/25～	75	窓口業務開始
福島県	双葉町	無（原発事故移転）	無	本庁舎	3/20～	9	被災証明交付
					4/18～	38	窓口業務開始
					6/22～	103	り災証明交付
	浪江町	無（原発事故移転）	無	データセンター	3/22～	11	被災証明交付
					4/4～	24	住民票・印鑑証明書・税証明書の交付を、二本松事務所（二本松市東和支所内）で開始
					4/中旬～	35	り災証明交付

注：日付が不明確な場合は概算日数

（ｂ）ネットワークの復旧状況[10]

発災直後影響を受けなかった団体は南相馬市のみであり、その他の団体は多くが本庁舎の停電や支所等の停電により利用できない状況であった。本庁舎が水没又は流失した陸前高田市、大槌町、南三陸町及び原発事故により行政機能を移転した双葉町、浪江町は、移転先でのネットワーク構築によりサービスを再開している。

いわき市では､地域イントラネットの伝送路の一部で断線が発生したが､ネットワークがループ構成のため双方向通信が可能であり、利用に影響は出ていない。釜石市の場合、停電に加え、津波被害によりネットワーク機器が水没し､利用不可となった｡復旧では､庁舎の上層階に機械室を移し、機器を新設して再構築を行っている。

仙台市は、情報システムセンターと本庁舎及び区役所や出先機関とをつなぐ地域イントラネットを構築しており、回線は、業務系ネットワークと情報系ネットワーク（庁内 LAN）があり、業務系ネットワークは二重化されていた。発災時は、市内停電が発生したが、情報システムセンターは非常用発電装置により給電が行われている。ネットワークの状況は、停電等により障害が発生した回線があり、回線を二重化していた業務系ネットワークに比べ、情報系ネットワークは不通となった出先機関が多かった。

－地域イントラネットについては、調査での聞き取り範囲において、石巻市、気仙沼市、東松島市、南三陸町、いわき市及び南相馬市が

[10] 以下、ICT 部門が管理するネットワークについて、本庁舎内の管理・業務部門で使用するネットワークを「庁内ネットワーク」、本庁舎と支所等の出先機関や図書館等の公共施設などの間を結ぶネットワークを「地域イントラネット」として区分する。

ネットワーク回線を自営としている。

－大槌町の地域イントラネットは、発災前から構築していない。

表－６　ネットワークの復旧状況

団体名称		庁内ネットワーク			地域イントラネット		
		状況	復旧日	日数	状況	復旧日	日数
岩手県	宮古市	利用不可	3/26～	15	利用不可	5/20 5/25 6/20	70 75 101
	陸前高田市	利用不可	7/23～	134	利用不可	9月以降	174
	釜石市	利用不可	7月半ば	126	利用不可	7月半ば	126
	大槌町	利用不可	4/25～	45			
宮城県	仙台市	利用不可	3/16～	5	一部利用不可	3/16～	5
	石巻市	利用不可	3/26～	15	利用不可	4/11～ 5,6,10月	31
	気仙沼市	利用不可	3/17～	6	利用不可	4/1 5/11 9/29	21 61 202
	東松島市	利用不可	3/15～	4	利用不可		
	南三陸町	利用不可	4月中	50	利用不可	5/25～	75
福島県	いわき市	利用不可	3/12～	1	**利用可**		
	南相馬市	**被害なし**			**被害なし**		
	双葉町	**発災時利用可**	4月初旬	20	発災時利用不可	9月	174
	浪江町	不明	5月	50	不明	順次	
		:本庁舎水没				:本庁舎流出	

注：日付が不明確な場合は概算日数

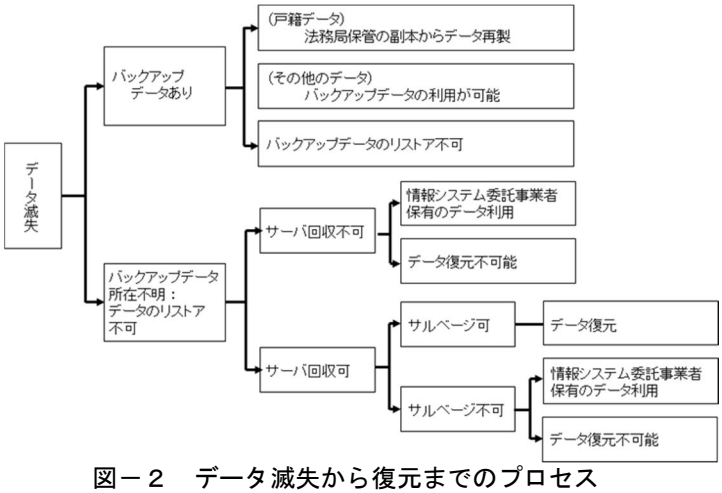
（ｃ）情報システムの復旧

本庁舎が水没又は流失し､データの滅失が発生した陸前高田市､大槌町､南三陸町は、仮庁舎でのデータ復元から始めることとなり、原発事故で行政機能を移転した双葉町及び浪江町は、移転先での復旧となった。宮古市は、バックアップテープを水没した１階の金庫室の耐震耐火金庫に納めていたため、金庫内のバックアップテープは無事であった。

個々の団体の詳細は、以下のとおりである。

表－７　情報システムの復旧

団体名称		時期	具体的内容
岩手県	宮古市	3/13	・大型の非常用発電装置を備えた施設に必要最小限のサーバを移設して稼働させることを決め、その日のうちに、移設作業を行い、総合窓口が稼働できる状態になった。
	陸前高田市	3/19	・仮設庁舎に仮サーバを設置
		3/23	・情報システム委託事業者が預かり保管していた2 月末時点の住基データ及び1 月23 日時点の財務会計データを使って、住基と財務会計システムの仮運用を開始。
		発災1 週間後	・情報システム委託事業者と、被災したサーバのハードディスク及びロッカーに保管のバックアップテープなどを回収し、データの復元を業者に依頼。 ・データの復元は、バックアップテープからはできなかったが、ハードディスクから住基、福祉システムのデータ及び税の申告データが復元できた。
		4 月下旬	・復元データを仮サーバにリストア。 ・戸籍については、管轄法務局において、保存していた戸籍の副本等に基づき再製データが作成された。
	大槌町	3/25	・情報システム委託事業者と被災したサーバ室に入り、基幹系システムのサーバ7台を回収し、データ復元を業者に依頼。
		3/29	・情報システムの復旧は、情報システム委託事業者が預かり保管していた3/1時点の住民データを元に、住民照会用の第1仮サーバを仮庁舎に設置。
		4/13	・被災したサーバのハードディスクから復元した住基データを元に仮庁舎に第2サーバを設置し、窓口業務を開始。 ・この時点で、税システムも仮復旧。 ・戸籍については、管轄法務局において保存していた戸籍の副本等に基づき再製データが作成され、そのデータを元にシステムを再構築。
宮城県	南三陸町	3/28	・情報システム委託事業者が預かり保管していた3/4時点のデータを元に、仮サーバに基幹系システムを仮復旧し、住民票の写しの交付などの一部窓口業務を開始。 ・内部情報系システムについては、すべてデータが滅失している。 ・戸籍については、管轄法務局において、保存していた戸籍の副本等に基づき再製データが作成され、そのデータを元にシステムを簡易サーバ上に再構築。
福島県	双葉町	3/20	・情報システム委託事業者が預かり保管していた3/10時点の住民情報を元に被災証明書の発行を開始。
		3月末と4月初旬	・双葉町本庁舎に戻る機会があり、業務に必要な保存データをほぼ持ち出すことができた。
		4/18	・移転先の埼玉支所でバックアップデータを使用して住民情報、戸籍等のシステムを立ち上げ、証明書発行等の窓口業務を再開。
	浪江町	4/4	・基幹系（住基、税、福祉）システムのデータを町外のデータセンターのサーバにバックアップしており、このデータを使用して二本松事務所で簡易サーバを構築。
		4月上旬	・住民票の写しの交付等の窓口業務を再開。 ・戸籍については3 月20 日頃に浪江町本庁舎に戻る機会があり、サーバを取り外し、持ち出した。
		:本庁舎水没	
		:本庁舎流出	



図－２　データ滅失から復元までのプロセス

イ　調査結果「情報通信白書」

（ア）ICT 環境に係る被災の状況

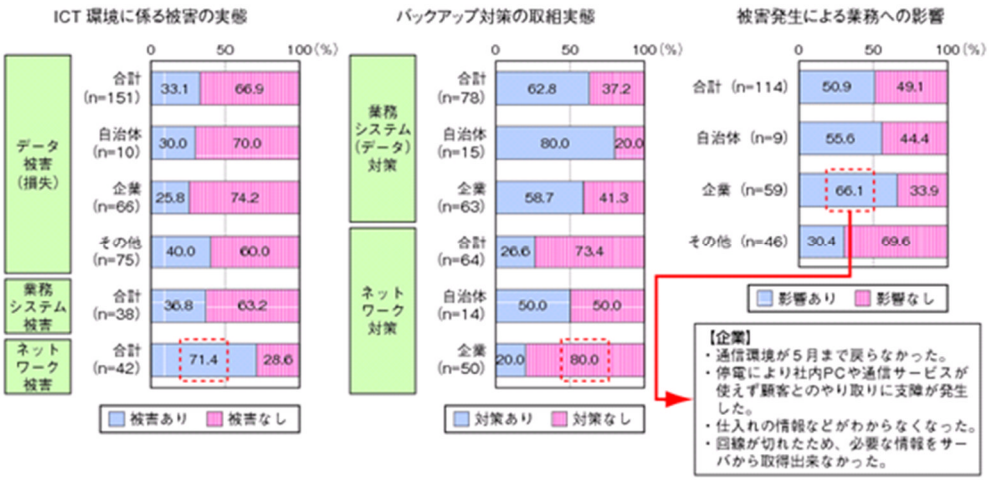
被災地におけるインタビューにより調査された震災時の被災地域における業務継続の状況を以下に示す。

まず、被災地域における ICT 環境に係る被害の実態と業務への支障についてみると、データが滅失したという被害があった企業や自治体は、全体の 33.1%であった。

組織別にみると、自治体 30.0%、企業 25.8%、その他 40.0%となっている（次図参照）。

また業務システムの被害については全体で 36.8%であった。一方、データ滅失や業務システムの被害に比べ、ネットワークに被害があったという回答は高く、全体の 71.4%となっている。ICT 環境に係るバックアップ対策の取組実態をみると、業務システムについてバックアップ対策を行っている企業や自治体は、全体の 62.8%に達した。

一方、ネットワークに関するバックアップ対策については、対策を行っている自治体は 50.0%、企業は 20.0%にとどまり、全体でも 26.6%と業務システムの対策状況と比較し対応していないケースが多かった。



出典：総務省「災害時における情報通信の在り方に関する調査」（平成 24 年）

図－３　ICT 環境に係る被害の実態

（イ）業務継続等の状況

これらの ICT 環境に係る被害によりそれぞれの業務への影響の有無についてみると、影響があったとする回答が、全体では 50.9%と半数以上となっている。

組織別にみると、自治体では影響ありが 55.6%、企業では 66.1%となり、自治体と比べ、企業のほうが業務への影響が大きかったことがわかる。

インタビューコメントをみると、「通信環境が 5 月まで戻らなかった。」「回線が切れたため、必要な情報をサーバから取得できなかった。」など、ネットワークに関するバックアップ対策が進んでいなかったことを指摘するコメントも多

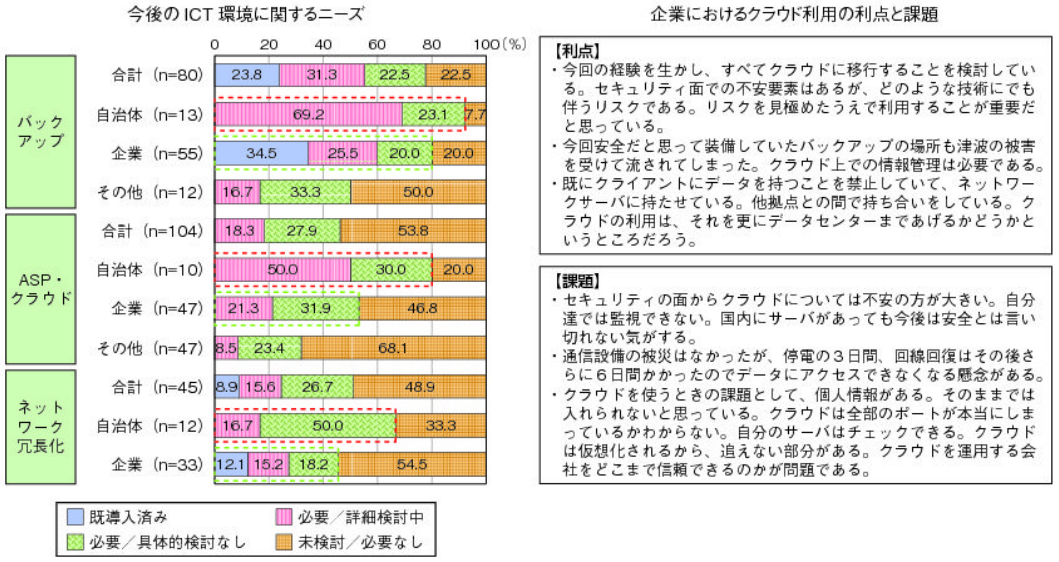
くみられた。

被災地域における今後の ICT 環境に関するニーズ（次図参照）をみると、自治体においてバックアップの必要性を指摘する比率が 92.3%、ASP・クラウドの必要性が 80.0%、ネットワーク冗長化の必要性が 66.7%とそれぞれ高い比率となっている。

企業においては、バックアップの必要性について 80.0%、ASP・クラウドの必要性が 53.2%、ネットワーク冗長化の必要性が 45.5%に達している。

しかしながら、ASP・クラウドについては具体的検討に至る比率は全体の 21.3%にとどまっていることがわかる。

クラウド利用の利点と課題についてインタビューコメントをみると、「セキュリティの面からクラウドについては不安の方が大きい。」「クラウドを使うときの課題として、個人情報がある。そのままでは入れられないと思っている。」など、主にセキュリティ面について懸念するコメントがみられた。



出典：総務省「災害時における情報通信の在り方に関する調査」（平成 24 年）

図－４　事業継続における ICT 環境に関するニーズ

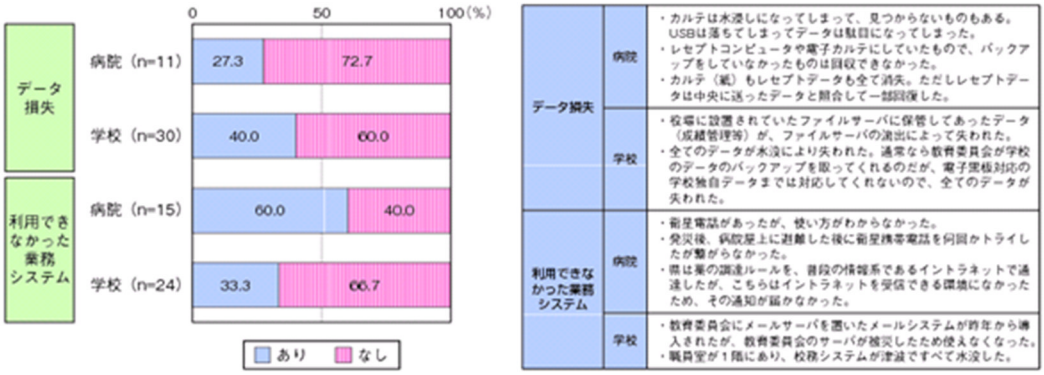
（ウ）データ滅失の状況

病院及び学校での震災によるデータ滅失等の状況をみると、データ滅失に至った比率が病院で 27.3%、学校で 40.0%に達している（次図参照）。

病院についてインタビューコメントをみると、「レセプトコンピュータや電子カルテにしていたもので、バックアップをしていなかったものは回収できなかった。」「USB は落ちてしまってデータは駄目になってしまった。」など、相当程度滅失したとの回答が複数あった。

一方、「カルテ（紙）もレセプトデータもすべて滅失。ただしレセプトデータは中央に送ったデータと照合して一部回復した。」のように、バックアップ対策により滅失を最小限にとどめたケースもみられた。

学校に関しては、校務システムを導入している学校において「すべてのデータが水没により失われた。」というコメントもみられた。



出典：総務省「災害時における情報通信の在り方に関する調査」（平成 24 年）

図－５　病院及び学校での震災によるデータ滅失及び利用できなかった業務システム

震災時に利用できなかった業務システムの有無についてみると、病院では 60.0%、学校では 33.3%が利用できなかったシステムがあると回答している。

インタビューコメントから利用できなかったシステムの詳細についてみると、病院や学校において、システムが水没等により利用できなくなったケースに加え、病院では、「衛星電話があったが、使い方がわからなかった。」「発災後、病院屋上に避難した後に衛星携帯電話を何回かトライしたが繋がらなかった。」など、緊急時のシステムが整備されていながら、実際には利用できなかったケースがみられ、事前準備の必要性が指摘されている。

ウ　参考資料「JIIMA 政策提言プロジェクト　現用公文書の危機管理対策のために電子化バックアップセンター構想の政策提言」[11]

（ア）提言の趣旨

・以下の現状等を踏まえ、公文書管理の現状と電子化の必要性を提言している。

- 我が国の行政機関では、大部分が「紙の公文書原本」として保存されている。
- 内閣官房公文書管理検討室の平成 22 年度調査によれば、政府の行政文書は 1,714 万ファイルであり、うち「96.4%が紙文書」と報告されている。
- また自治体についても総務省平成 21 年度調査では、土地・インフラ資産関係は、固定資産課税台帳を除く大部分の台帳が「紙台帳」である。

[11] 電子化バックアップセンター構想の政策提言（骨子）　平成 23 年 8 月　社団法人 日本画像情報マネジメント協会（JIIMA）

（イ）提言の骨子

・提言の骨子は以下のとおりである。

［調査研究提案―１］

－行政機関で電子化公文書として安全分散保管する必要のあるバイタル公文書[12]の選択方法や、推定数量及び必要な検索インデックス等については、各行政機関での文書管理実態の危険分散面からの調査研究が必要と考える。

「公文書の電子化バックアップセンター（公文書電子化センター）」構想

－構想の要旨：行政機関の公文書を国・都道府県・自治体間の壁を越えて、全国６か所程度に「公文書電子化センター」を設けて電子的な環境で一元的に保存・管理・運用・提供する。

［調査研究提案―２］

－電子化公文書と電子公文書とを一元的に「セキュリティの担保された公文書クラウド」環境下で、安全分散保管するために必要とされる情報セキュリティ対策について、前掲の調査研究提案―１；行政機関での文書管理実態と併せて、調査研究する必要がある。

エ　参考資料「JIIMA 危機管理を目的とした文書・記録管理ガイドライン　V1.01」[13]

（ア）ガイドラインの趣旨

・危機に対応するために文書情報管理の視点からどのような文書・記録を残さなければならないか、残すための注意点などを重点的にまとめ、災害発生時の対応方法、危機に対応できる準備を行う時の指針となることを目的とする。

（イ）ガイドラインの骨子

・ガイドラインの骨子は以下のとおりである。

バイタルレコード（事業を継続するうえで必要不可欠な記録や文書）の定義

－バイタルレコードには、設計図、見取図、品質管理資料等、災害時に直接的に必要な文書やコーポレートガバナンス・内部統制維持、法令遵守、説明責任確保のための文書、権利義務確定、債権債務確保のための文書等、間接的に必要な文書がある。

12 バイタル公文書：行政上の基本となる、行政機能維持に不可欠な公文書。

13 JIIMA危機管理を目的とした文書･記録管理ガイドライン V1.01　平成23年10月12日　社団法人 日本画像情報マネジメント協会（JIIMA）記録管理委員会

文書情報マネジメントにおけるバイタルレコード[14]

－法律で保存が義務付けられたいわゆる法定保存文書については管理されているが、その他の文書・記録類は総じて十分に管理されているとは言い難いのが現状である。

－文書情報マネジメントを実施している組織体では、管理している記録・文書の中から、バイタルレコードを選び出し、他の記録・文書とは異なる観点から保存・保管方法を決定する必要がある。

－バイタルレコード・マネジメントは、従来の文書管理に「事業の継続に重要な記録・文書を滅失から保護し、災害発生時の混乱期でも必要な記録・文書を活用できる」という観点が加わったに過ぎない。

－したがって、今までの文書管理が無駄になってしまう訳では無い。

バイタルレコード選定への指針

－各部門ではその部門の主業務を念頭に、それを実現するために必要不可欠なデータをバイタルレコードと認定するほか、業務再開には直接利用しないものでも、他から入手不可能な情報や記録類は、長期的に残すものとして選別しておく。

バイタルレコードの事前準備

－緊急時に必要な情報の整備：

従業員安否確認に必要な情報、緊急時の対応マニュアル 等

－バイタルレコードの保存：

紙、電子化、マイクロフィルム等によるバックアップ。どの形態でバックアップを行うかは、どこのフェーズで必要とするドキュメントであるかに依存する。

保護形態

－紙で残すもの：

システム障害、停電など、緊急時の対応を考え、最低限のマニュアル類や決裁権限移譲先、緊急連絡先などは電子データで作成していても紙でも管理する。

－電子化データ（紙を電子化して残すもの）：

バイタルレコードを失うことがないよう、コピーを作成し遠隔地などでの保存が必要である。

紙の書類は、紙としてのコピーも選択肢としてはあるが、その後の取り扱いやすさや保存コストなどを考慮すると、スキャニング等を実施

---

[14] このガイドラインが対象とするバイタルレコードの範囲：
基幹システムのシステム自体、そのデータ、紙文書、部門サーバとそのコンテンツ、個人が使っているPCなど、いろいろな形態の情報が存在しており、このガイドラインでは、企業に存在する「記録・文書」のすべてを対象としている。

し電子化することが望ましい。特にバイタルレコードとして選定したものは、できる限り電子化データを作成して保存する。

－電子データ：

遠隔地でのバックアップ体制や、緊急時も活用が容易なシステム化が必要である。

個人の PC などにバイタルレコードを保存することを避けるような運用基準作りが大切である。

JIIMA ステートメント

－バイタルレコードにはどのようなものがあるかを認識し、これを安全な遠隔地に電子文書化して隔離保管しておくことは、組織管理者としての義務である。

－隔離保管するバイタルレコードは、基幹系のバックアップデータシステムだけでは全く不十分であり、多くの紙の書類なども対象とする必要がある。

－PC、タブレット端末の活用も配慮しておく必要がある。このためにも、バイタルレコードである紙の書類は電子化するとともに、いつでも活用できるように準備しておくことで、PC、タブレット端末で読むことができるようになり、活用の幅が大きく広がる。

－経営者は、バイタルレコードの電子化・隔離保管などの経費は、組織を維持継続するための必須経費として認識し、年度計画に織り込むべきである。

２　アンケート調査

東日本大震災の特定被災地方公共団体に対し、平常時における行政データの管理状況、震災時の被災状況及びデータ滅失等による住民に密接に関係する行政事務や住民サービスへの影響等を調査し、その状況を把握・整理する。

（１）調査仕様

〔調査対象〕

東日本大震災における特定被災地方公共団体 167 市町村[15]の ICT 部門、業務部門に調査票[16]を配布し実施する。

・業務部門は、行政事務や住民サービスを行っていると想定される**表－８**に示す 15 部門（①から⑮）を対象とした。

・調査票は、15 部門のうち、複数の行政事務や住民サービスを一つの部門（部署）で所管している場合には、その部門（部署）に 1 部を配布する旨、調査対象団体に依頼した。また逆に、一つの行政事務や住民サービスを複数の部門（部署）で実施している場合は、複数の部門（部署）に配布することを依頼した。

なお、本調査及び次項のヒアリング調査の実施に限り、行政データを基幹系データと個別管理データという区分に分けて調査した。基幹系データと個別管理データの定義を以下に示す。

・基幹系データ　：- 上記の項においては、担当部署又は全庁で組織的に一元管理しているデータをいう。（住民情報や戸籍、税など）
　- 本章他項及び他章では、「システムとして管理されている電子データ」と表記した。

・個別管理データ：- 上記の項においては、各職員が、担当する行政事務や住民サービスを実施するために、個人で作成・管理している文書やデータをいう。保管場所や媒体は問わない（各職員が使用している PC、部署や全庁的に設けている共有フォルダ、紙媒体等）。
　- 本章他項及び他章では、「ローカル PC 等に保存されている電子データ」と表記した。

15 平成 24 年 2 月 22 日改正時（福島原子力発電所事故による警戒区域、計画的避難区域等を除く）
16 調査票については、「（付録）アンケート調査票」を参照のこと。

表－８　業務部門として想定した調査票の配布先

（以下の①から⑮の行政事務や住民サービスを実施している部門（部署））

組織のカテゴリ		担当事務・サービス・施策等の内容
部（課）相当	課（係）相当	
市民部局	①窓口サービス部門	住民票関連
		印鑑関連
		戸籍関連
		国民健康保険・後期高齢者関連
		国民年金関連
		その他
	②その他の市民部門	自治会、町内会、連合町内会等
		地縁による団体の認可及び印鑑
		市民の相談及び要望（市民相談室）
		消費生活の苦情処理
		計量器の検査
税務部局	③住民税・諸税部門	市民税、軽自動車税、入湯税、市たばこ税、及び事業所税の賦課
	④資産税部門	固定資産税、都市計画税及び特別土地保有税の課税
		国有資産等所在市町村交付金
		市税の証明に関すること
		その他
	⑤納税部門	市税の収納及び徴収
		固定資産評価審査委員会との連絡に関すること
		その他
福祉部局	⑥障害福祉部門	自立支援
		地域生活支援
		移動支援
		グループホーム整備助成
		入所施設整備支援
		障害者虐待防止
		体験雇用助成
		成年後見人支援
	⑦高齢福祉部門	独居高齢者見守り施策
		老人ホーム（特養）整備促進
		介護施設整備
		配食・入浴サービス
		認知症対策
		予防接種・ワクチン
		高齢者虐待防止
		就労支援
		買い物支援
	⑧介護保険部門	認定・給付
		保険料賦課・収納
	⑨児童福祉・子育て支援部門	私立認可保育園助成
		認証保育所助成
		一次預かり支援
		延長保育・夜間保育所開設
		病児・病後保育室設置
		保育料負担軽減
		子ども医療費助成
		発達障害児保育支援
		児童虐待防止関連
		各種手当支給
		ひとり親家庭支援
		第3子以降子支援
		母子相談
		青少年団体・施設関連
		里親の認定・登録
	⑩生活福祉部門	セーフティネット構築・拡充
		離職による住宅喪失者支援
		保護費支給関連
保健衛生部局	⑪地域医療部門	救急医療体制充実
		地域医療体制整備
		在宅療養支援
	⑫健康管理部門	感染症対策
		がん検診、普通検診
		ワクチン接種費用助成
		任意予防接種費用助成
		ひきこもり相談・支援
		自殺防止
		成人・妊婦歯科診療
	⑬生活衛生部門	食品衛生・環境衛生
		畜犬等愛護・管理
		火葬場関連
		墓地関連
		衛生試験所関連
消防・防災部局	⑭危機管理部門	災害対策の計画及び調整
		国民保護の計画及び調整
	⑮地域安全部門	防犯対策、交通安全
		自主防災組織

〔主な調査内容〕

・ICT 部門

－基幹系データのバックアップの実態

－東日本大震災による基幹系システム及び基幹系データへの影響

－個別管理データの実態

－当該部門において業務に用いている個別管理データの内容、管理・運用、震災による影響等

－電子データに関する規定

－BCP、ICT-BCP 等の策定状況

－共有ストレージ、文書管理システム、シンクライアントの導入状況

－個別管理データの管理等に関する意見・要望

・業務部門（部署）

－当該部門における東日本大震災の被災状況

－当該部門において業務に用いている個別管理データの内容、管理・運用、震災による影響等

－個別管理データの管理状況やバックアップ等に関する意見・要望

－業務を継続するために実施している（あるいは今後実施する予定）取組の内容

等

〔実施期間〕

・平成 24 年 11 月 5 日　調査票配布（投函）

・平成 24 年 12 月 31 日消印の回答迄を有効とした。

（２）調査結果

ア　回収状況

・ICT 部門

－89 票（発送数 167 票（団体あたり 1 票発送)、回収率 53.3%）

・業務部門（部署）

－942 票（発送数 2,505 票（団体あたり 15 票発送)、167 団体中 85 団体から回答有、回収率 50.9%）[17]

[17] 回収率は（回収団体数／発送団体数）からそれぞれ計算。

イ　アンケート回答

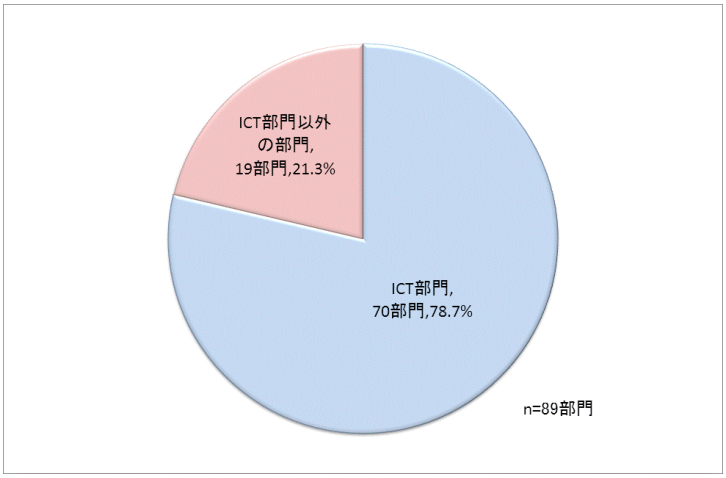
〔被災状況の概観〕

ICT 部門又は業務部門における「部門数」を単位として、被災状況を概観する。

（ア）基幹系データのバックアップを行っている部門

基幹系データのバックアップは、回答があった 89 団体の ICT 部門のうち、ICT 部門で実施しているとの回答が 78.7%（70 部門）、ICT 部門以外の部門（業務部門等）で実施しているとの回答が 21.3%（19 部門）存在した。

上記より、基幹系データをバックアップしている部門は ICT 部門が 3/4 以上であったものの、ICT 部門以外の部門がバックアップしている団体も 1/4 以下存在することが分かった。



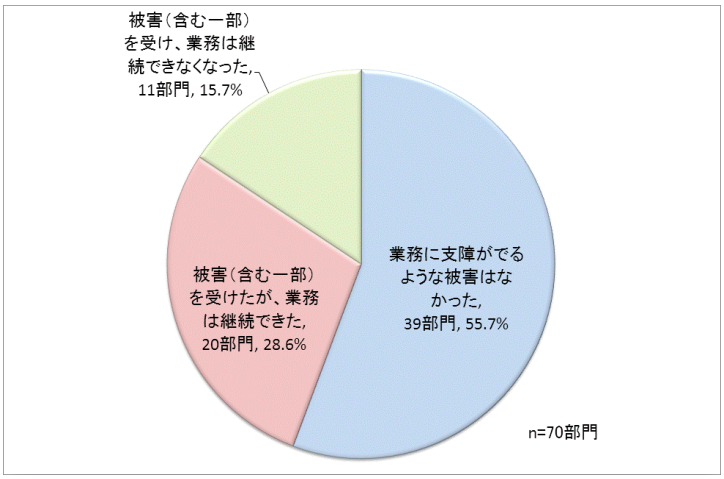
図－６　基幹系データのバックアップを行っている部門[18]

（イ）基幹系システムの被災状況

基幹系データを管理している ICT 部門（70 部門）のうち、基幹系システムに対して業務に支障がでるような被害がなく業務を継続できたとの回答が 55.7%（39 部門）存在した。その一方で、被害（含む一部）を受けたが業務を継続できたとの回答が 28.6%（20 部門）、被害（含む一部）を受け業務を継続できなくなったとの回答が 15.7%（11 部門）存在した。

上記より、基幹系データを管理している ICT 部門において、基幹系システムに対する被害が 44.3%（合計 31 部門）で発生したことが分かった。

18 図中のｎの値は、当該設問の回答数（集計の母数）を表す。以下同様。

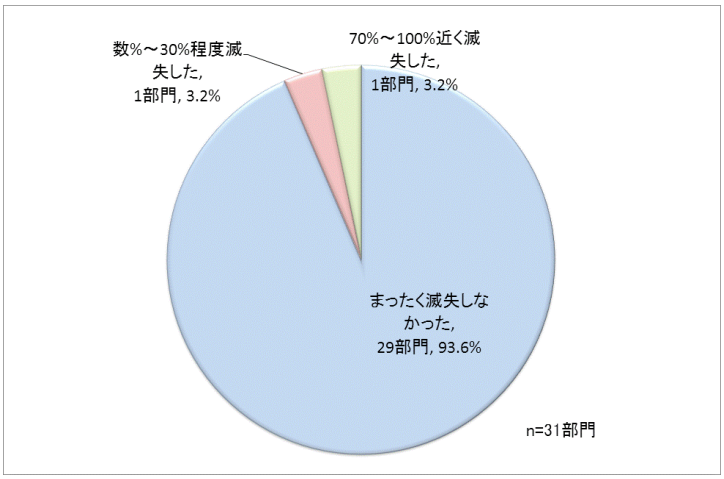


図－７　基幹系システムの被災状況

（ウ）基幹系データのバックアップデータの被災状況

基幹系システムに被害（含む一部）を受けた ICT 部門（31 部門）のうち、基幹系データのバックアップデータが滅失しなかったとの回答が 93.6%（29 部門）存在した。その一方で、基幹系データのバックアップデータが数%～30%程度滅失したとの回答が 3.2%（1 部門）、基幹系データのバックアップデータが 70%～100%近く滅失したとの回答が 3.2%（1 部門）存在した。

上記より、基幹系システムに被害（含む一部）を受けた ICT 部門の 90%以上においては、基幹系データのバックアップデータが滅失するような被害が発生しなかったものの、10%以下の ICT 部門においては、大きな被害が発生したことが分かった。



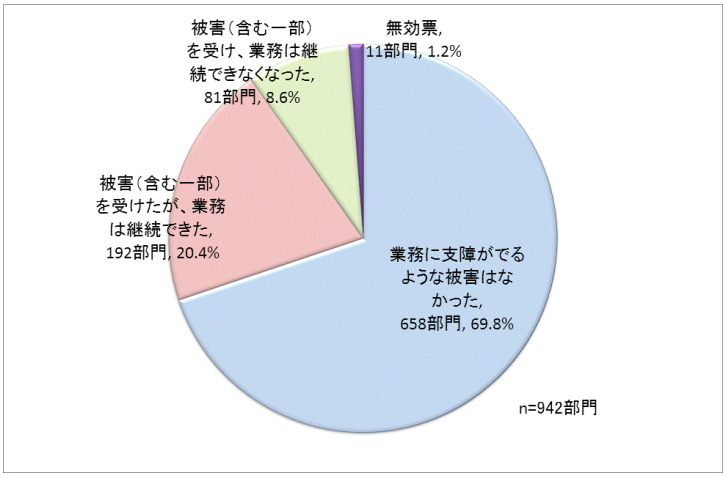
図－８　基幹系データのバックアップデータの被災状況

（エ）業務部門が使用している部屋又はスペースの被災による業務への影響

業務部門（942 部門）のうち、使用している部屋やスペースに対して業務に支障がでるような被害はなく業務を継続できたとの回答が 69.8%（658 部門）存在した。その一方で、被害（含む一部）を受けたが業務を継続できたとの回

答が 20.4%（192 部門）、被害（含む一部）を受け業務を継続できなくなったとの回答が 8.6%（81 部門）存在した。

上記より、業務部門において、使用している部屋又はスペースに対する被害が 29.0%（合計 273 部門）で発生したことが分かった。

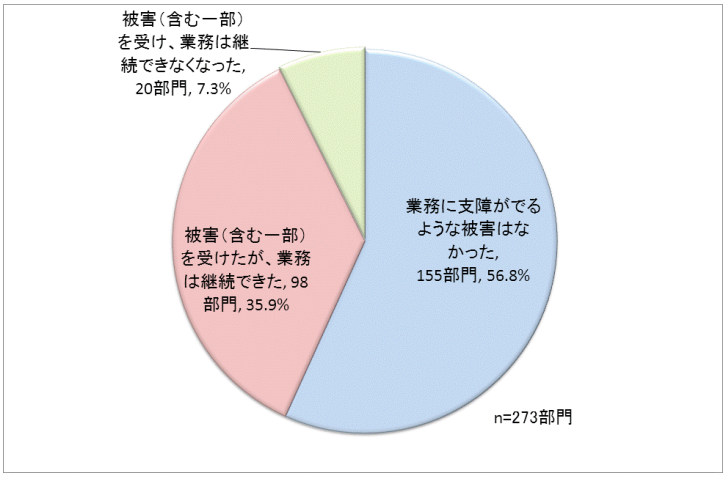


図－９　部屋又はスペースの被災による業務への影響

（オ）業務部門が使用している紙媒体の文献、資料等の被災による業務への影響

使用している部屋又はスペースの被害（含む一部）を受けた業務部門（273 部門）のうち、使用している紙媒体の文献や資料等に対して業務に支障がでるような被害はなく業務を継続できたとの回答が 56.8%（155 部門）存在した。その一方で、被害（含む一部）を受けたが業務を継続できたとの回答が 35.9%（98 部門）、被害（含む一部）を受け業務を継続できなくなったとの回答が 7.3%（20 部門）存在した。

上記より、業務部門において、紙媒体の文献、資料等に対する被害が 43.2%（合計 118 部門）で発生したことが分かった。



図－１０　紙媒体の文献、資料等の被災による業務への影響

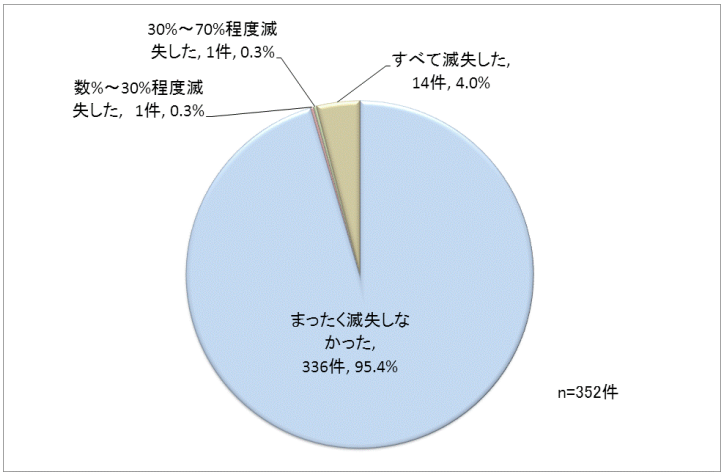
〔個別管理データの滅失状況〕

基幹系システムに被害（含む一部）を受けた ICT 部門（31 部門）及び使用している部屋又はスペースの被害（含む一部）を受けた業務部門（273 部門）の合計 304 部門における個別管理データの「件数」を単位として、個別管理データの滅失状況について分析する。

（カ）個別管理データの滅失状況

基幹系システムに被害（含む一部）を受けた ICT 部門及び使用している部屋又はスペースの被害（含む一部）を受けた業務部門（合計 304 部門）において管理・運用されていた個別管理データの件数は、352 件であった。個別管理データの滅失状況については、まったく滅失が発生しなかったとの回答が 95.4%（336 件）、データの滅失が発生したとの回答が 4.6%（合計 16 件）存在した。

このうち、すべてのデータが滅失したのは 14 件であり、全体の 4.0%の ICT 部門及び業務部門において大きな被害が発生したことが分かった。



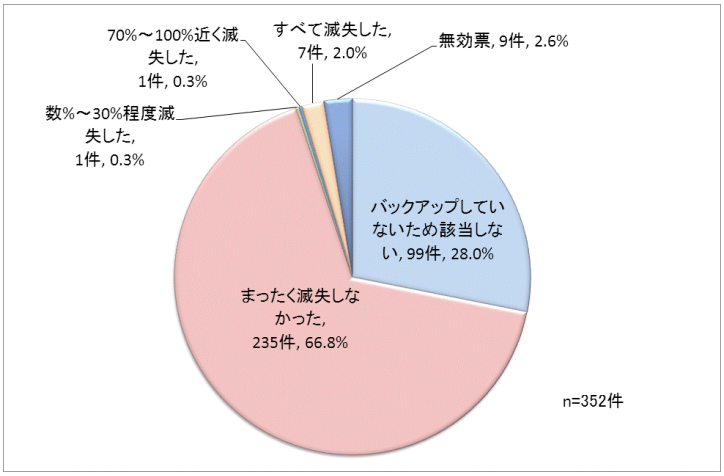
図－１１　個別管理データの滅失状況

（キ）個別管理データのバックアップデータの滅失状況

基幹系システムに被害（含む一部）を受けた ICT 部門及び使用している部屋又はスペースの被害（含む一部）を受けた業務部門（合計 304 部門）において管理・運用されていた個別管理データ（352 件）について、バックアップしていなかったとの回答が 28.0%（99 件）存在した。

また、バックアップを実施していた個別管理データ（合計 244 件）のうち、まったく滅失が発生しなかったとの回答が 66.8%（235 件）、データが滅失したとの回答が 2.6%（合計 9 件）存在した。

このうち、すべてのバックアップデータが滅失したのは 7 件であり、全体の 2.0%の ICT 部門及び業務部門において大きな被害が発生したことが分かった。



図－１２　個別管理データのバックアップデータの滅失状況

（ク）震災前のような行政事務や住民サービスが行えるまでに要した時間

基幹系システムに被害（含む一部）を受けた ICT 部門及び使用している部屋又はスペースの被害（含む一部）を受けた業務部門（合計 304 部門）において管理・運用されていた個別管理データ（352 件）のうち、1 週間以内に震災前のように個別管理データを用いて実施していた行政事務や住民サービスが行えるようになったとの回答が 53.1%（187 件）存在した。その一方で、母数を滅失した個別管理データ（16 件）に限定すると 1 週間以内に行政事務や住民サービスが行えるようになったとの回答は 6.3%（1 件）存在した。

また、個別管理データが滅失した場合には、回復に要した時間を半年程度との回答が最も多く 31.2%（5 件）存在した。なお、調査時点においても未だ回復していないとの回答も 12.5%（2 件）存在した。

上記より、データの滅失が発生することによって、震災前のような行政事務や住民サービスが行えるまでに要する時間に影響が出たと考えられる。

表－９　震災前のような行政事務や住民サービスが行えるまでに要した時間

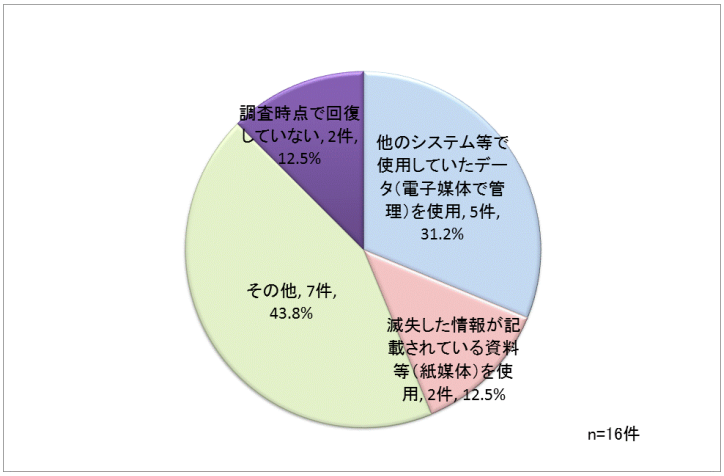
区分		震災前のような事務や住民サービス等が行えるまでに要した時間の内訳（%）								
		1週間以内	数週間程度	数ヶ月程度	半年程度	約1年程度	約1年6ヶ月程度	未だ回復していない	無効票	合計
基幹系データが被災したICT部門及び執務室やそのスペースが被災した業務部門で管理・運用していた個別管理データ		53.1%（187件）	15.1%（53件）	5.7%（20件）	3.1%（11件）	1.1%（4件）	0.3%（1件）	0.6%（2件）	21.0%（74件）	100.0%（352件）
	うち滅失が発生した個別管理データ	6.3%（1件）	18.7%（3件）	25%（4件）	31.2%（5件）	0.0%（0件）	6.3%（1件）	12.5%（2件）	0.0%（0件）	100.0%（16件）

（ケ）滅失した個別管理データの回復方法

基幹系システムに被害（含む一部）を受けた ICT 部門及び使用している部屋又はスペースの被害（含む一部）を受けた業務部門（合計 304 部門）において管理・運用されていた個別管理データ（352 件）のうち、滅失（含む一部）した個別管理データ（16 件）の回復方法は、システム等で使用していたデータ（電子媒体で管理）を元に回復した個別管理データが 5 件、滅失した情報が記載されている資料等（紙媒体）を元に回復した個別管理データが 2 件、その他の方

法により回復した個別管理データが 7 件、調査時点において回復していない個別管理データが 2 件であった。

その他の方法の内容は、「本人から聴取して作成した」「再申請してもらい作成した」「その時点から新規作成した」「県で保管していたデータ、資料を元に再生」等であった。

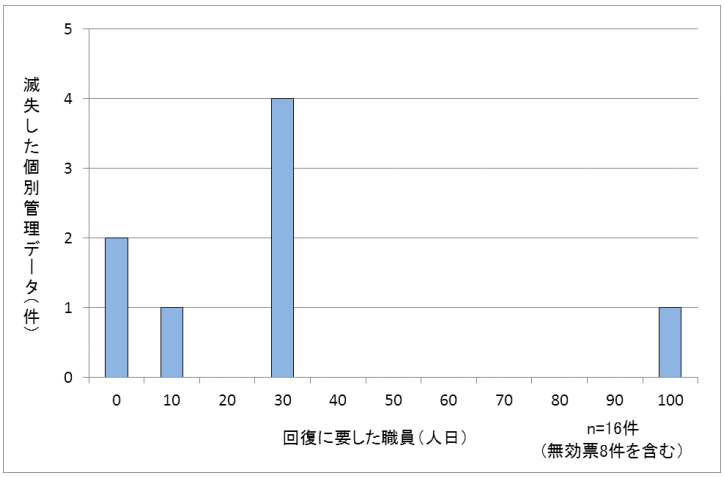


図－１３　滅失した個別管理データの回復方法

（コ）滅失したデータの回復に要した人数

滅失した個別管理データ（16 件）の回復に要した人数（人日）は、滅失した個別管理データ 1 件につき 30 人日を要したとの回答が最も多かった。

上記より、滅失した個別管理データを回復するまでに多くの作業が必要となり、業務を継続する上で大きな障害となったことが分かった。なお、データの回復に要する人数は、滅失したデータの内容が大きく影響すると考えられる。



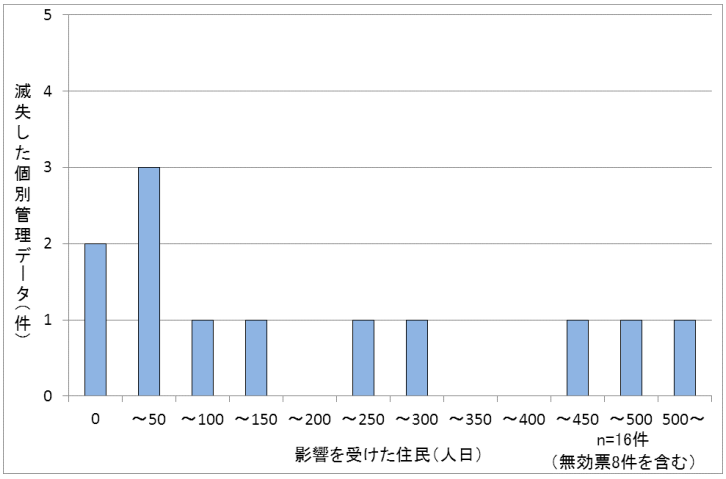
図－１４　滅失したデータの回復に要した人数

（サ）データ滅失による影響を受けた住民の人数

滅失した個別管理データ（16 件）において、行政事務や住民サービスが震災前の状況に回復するまでに、影響を受けたと考えられる住民の延べ人数は、個

別管理データ 1 件につき 1～50 名との回答が 3 件で最も多かった。また、400～450 人、451～500 人、また 500 人以上との回答もそれぞれ 1 件あった。

上記より、個別管理データが滅失したことにより、滅失したデータに基づいたサービスを受けていた住民が、大きな影響を受けたものと考えられる。なお、影響を受ける住民数は、団体の規模及び行政事務や住民サービスの内容等が大きく影響すると考えられる。



図－１５　データ滅失による影響を受けた住民の人数

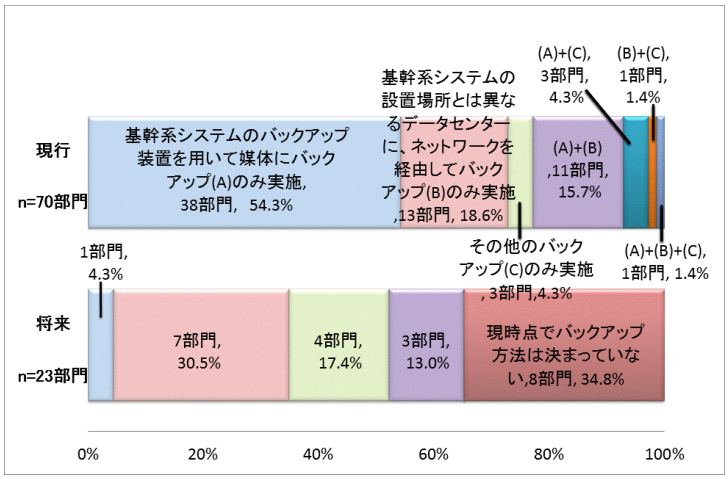
〔基幹系データの管理状況〕

ICT 部門の「部門数」を単位として、基幹系データの管理状況について分析する。

（シ）基幹系データのバックアップ方法

基幹系データをバックアップしている ICT 部門（70 部門）において、現状の基幹系データのバックアップ方法は、基幹系システムのバックアップ装置を用いて媒体にバックアップのみ実施しているとの回答が最も多く 54.3%（38 部門）存在した。

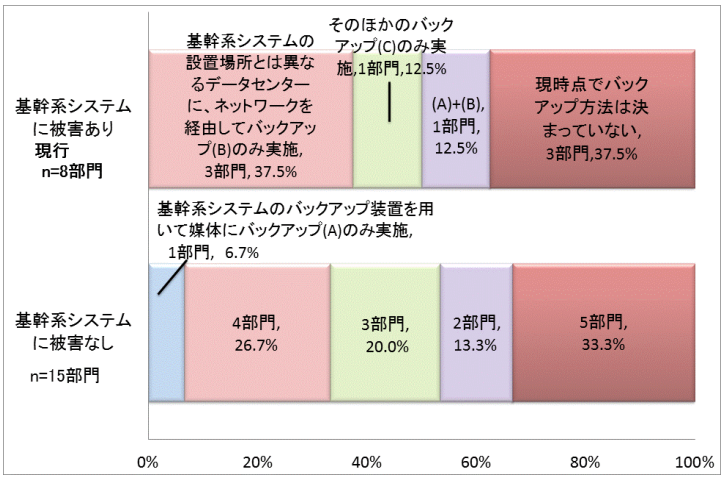
その一方で、将来的に基幹系データのバックアップ方法を検討している ICT 部門（23 部門）において、想定している基幹系データのバックアップ方法は、基幹系システムの設置場所とは異なるデータセンターに、ネットワークを経由してバックアップするとの回答が最も多く 30.5%（7 部門）存在した。



図－１６　基幹系データのバックアップ方法

次に、将来的にバックアップ方式の見直しを検討している ICT 部門（23 部門）のうち、基幹系システムに被害（含む一部）を受けた ICT 部門（8 部門）で想定している基幹系データのバックアップ方法は、データセンターを利用するとの回答が 50%（内訳：データセンターの利用のみ 37.5%（3 部門）＋データセンターの利用と媒体へのバックアップの組合せ 12.5%（1 部門））存在した。

その一方で、被害を受けなかった ICT 部門（15 部門）では、データセンターを利用するとの回答は 40%（内訳：データセンターの利用のみ 26.7%（4 部門）＋データセンターの利用と媒体へのバックアップの組合せ 13.3%（2 部門））存在した。

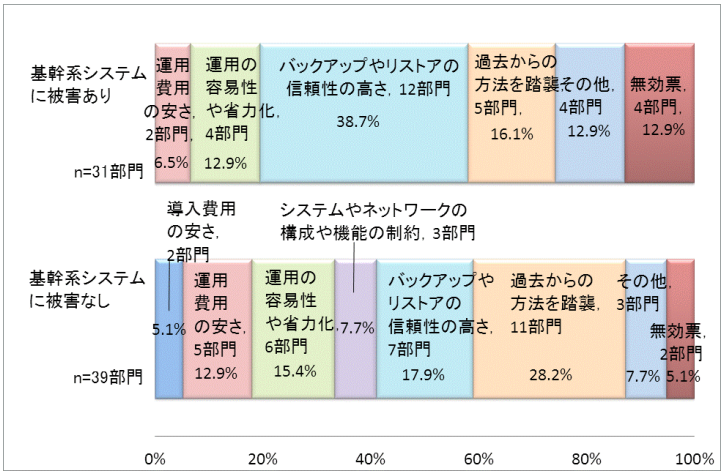


図－１７　将来想定する基幹系データのバックアップ方法の内訳

（ス）バックアップ方法の選定理由

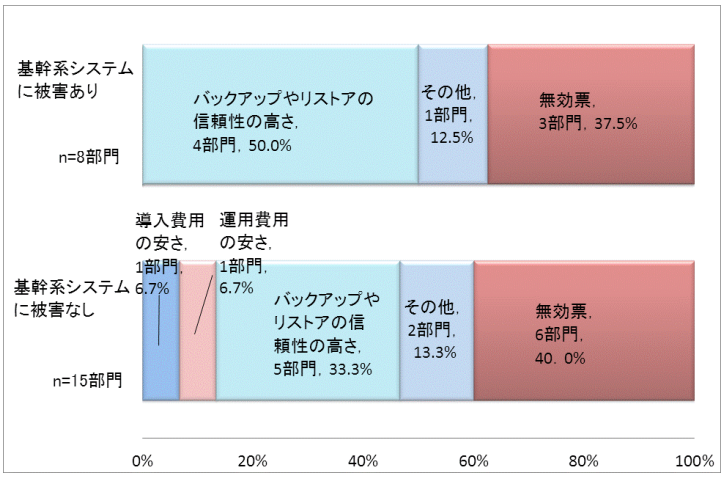
基幹系データをバックアップしている ICT 部門（70 部門）のうち、基幹系システムに被害（含む一部）を受けた ICT 部門（31 部門）におけるバックアップ方法の選定理由は、現状は信頼性の高さを理由にバックアップ方法を選定しているとの回答が最も多く 38.7%（12 部門）存在した。その一方で、被害を

受けなかった ICT 部門（39 部門）では、現状は、過去からの方法を踏襲しているとの回答が最も多く 28.2%（11 部門）存在した。



図－１８　現状のバックアップ方法の選定理由

次に、基幹系システムに被害（含む一部）を受けた ICT 部門（31 部門）のうち、将来的にバックアップ方式の見直しを検討している ICT 部門（8 部門）におけるバックアップ方法の選定理由（想定）についても、信頼性の高さを理由にしているという回答の割合が 50.0%（4 部門）存在した。また、被害を受けなかった ICT 部門（39 部門）のうち、将来的にバックアップ方式の見直しを検討している ICT 部門（15 部門）においても、バックアップ方法の選定理由（想定）については、信頼性の高さを理由に挙げる回答の割合が 33.3%（5 部門）存在した。

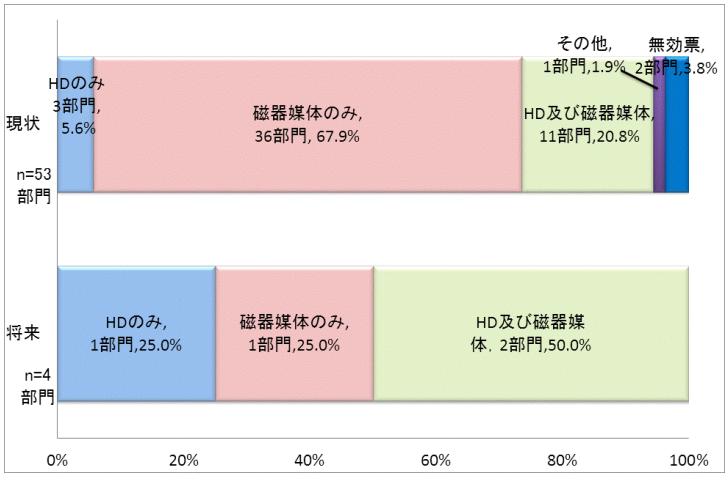


図－１９　将来想定するバックアップ方法の選定理由

（セ）バックアップ媒体の種類

基幹系データをバックアップしている ICT 部門（70 部門）のうち、現状、基幹系システムのバックアップ装置を用いて媒体にバックアップを行っている ICT 部門（53 部門）において利用されているバックアップ媒体は、磁気媒体の

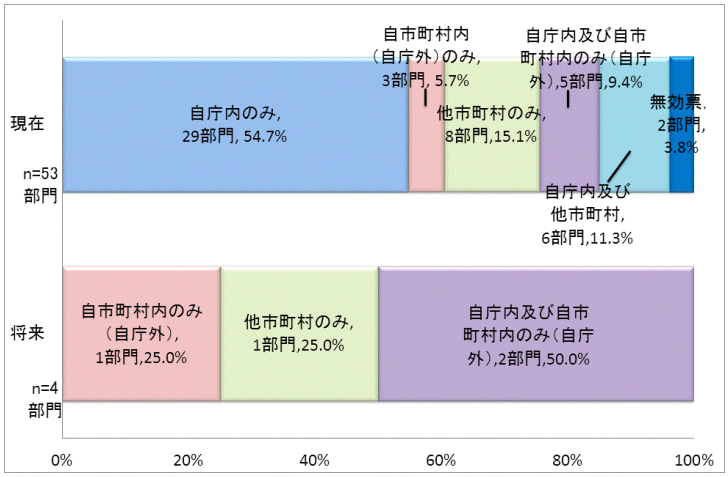
みとの回答が最も多く 67.9%（36 部門）存在した。また、将来的に基幹系システムのバックアップ装置を用いた媒体へのバックアップを検討している ICT 部門（4 部門）において想定しているバックアップ媒体は、HD 及び磁気媒体の両方との回答が最も多く 50.0%（2 部門）存在した。



図－２０　バックアップ媒体の種類

（ソ）バックアップデータの保管場所

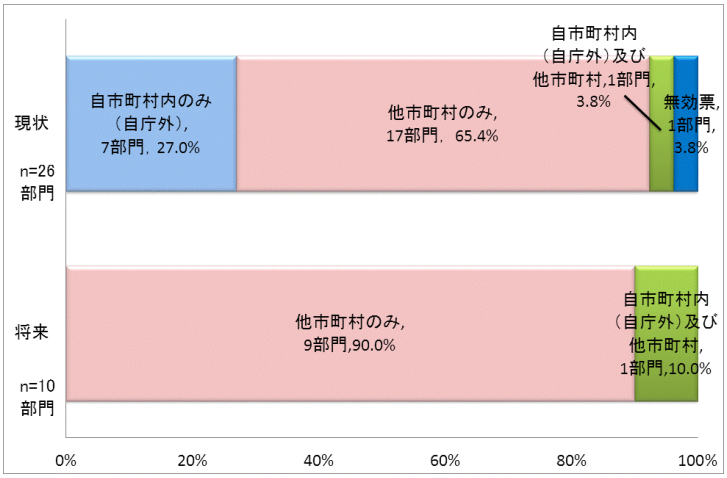
基幹系データをバックアップしている ICT 部門（70 部門）のうち、現状、基幹系システムのバックアップ装置を用いて媒体にバックアップを行っている ICT 部門（53 部門）においてバックアップデータを保管している場所は、自庁内のみとの回答が最も多く 54.7%（29 部門）存在した。また、将来的に基幹系システムのバックアップ装置を用いた媒体へのバックアップを検討している ICT 部門（4 部門）において想定しているバックアップデータの保管場所は、自庁内及び自市町村内（自庁外）の両方との回答が最も多く 50.0%（2 部門）存在し、その一方で自庁内のみに保管するとの回答は見当たらなくなった。



図－２１　バックアップデータの保管場所

（タ）データセンターの場所

基幹系データをバックアップしていると回答した ICT 部門（70 部門）のうち、現状、基幹系システムの設置場所とは異なるデータセンターにネットワークを経由してバックアップを行っている ICT 部門（26 部門）において基幹系データをバックアップしているデータセンターの場所は、他市町村との回答が最も多く 65.4%（17 部門）存在した。また、将来的に基幹系システムの設置場所とは異なるデータセンターへのネットワーク経由によるバックアップを検討している ICT 部門（10 部門）が想定しているデータセンターの場所は、他市町村との回答の割合が現状よりも増加して 90.0%（9 部門）存在した。



図－２２　データセンターの場所

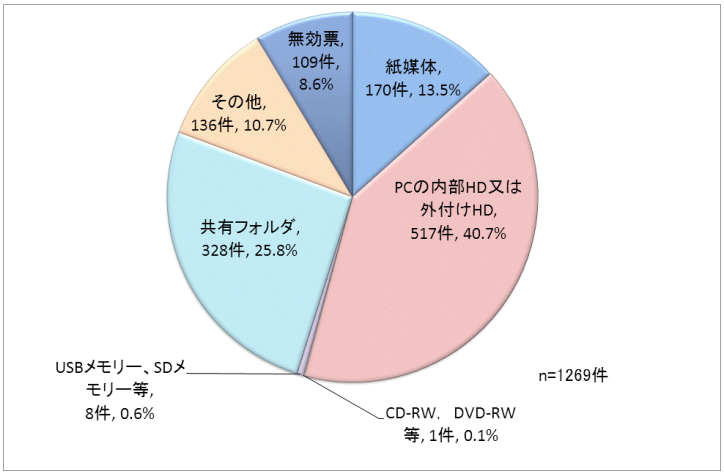
〔個別管理データの管理状況〕

ICT 部門（89 部門）及び業務部門（942 部門）の合計 1,031 部門における個別管理データの「件数」を単位とし、個別管理データの管理状況について分析する。

（チ）日常利用している個別管理データの記録媒体

ICT 部門及び業務部門（合計 1,031 部門）で管理・運用している個別管理データ（1,269 件）において、日常利用している記録媒体は、PC の内部 HD 又は外付け HD との回答が最も多く 40.7%（517 件）存在し、次いで共有フォルダが 25.8%（328 件）、紙媒体が 13.5%（170 件）存在した。その他との回答が 10.7%（136 件）存在するが、その内訳は、共有フォルダやファイルサーバ、DAT、MO、FD など多様な電子媒体が示されている。

上記より、紙媒体に記録している個別管理データも存在していることが分かった。

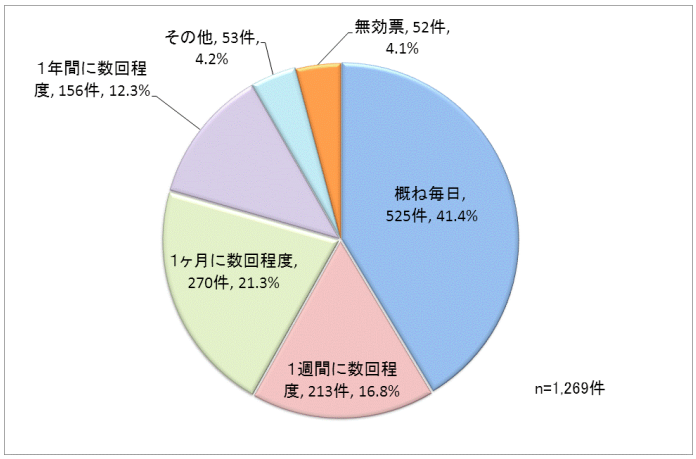


図－２３　日常利用している個別管理データの記録媒体

（ツ）個別管理データへのアクセス頻度

ICT 部門及び業務部門（合計 1,031 部門）で管理・運用している個別管理データ（1,269 件）において、アクセス頻度は、概ね毎日との回答が最も多く 41.4%（525 件）存在し、1 週間に数回程度との回答が 16.8%（213 件）存在した。また、1 年に数回程度との回答も 12.3%（156 件）存在した。

上記より、個別管理データの更新が月に数回以上であるとの回答が 3/4 以上あったことから、バックアップの頻度によっては最新のデータが滅失する可能性があると考えられる。



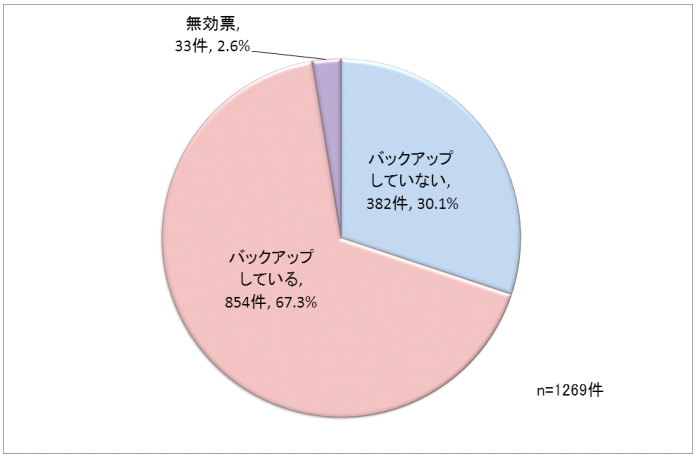
図－２４　個別管理データへのアクセス頻度

（テ）個別管理データのバックアップの状況

ICT 部門及び業務部門（合計 1,031 部門）で管理・運用している個別管理データ（1,269 件）において、バックアップ実施の有無は、バックアップしているとの回答が 67.3%（854 件）、バックアップを実施していないとの回答が 30.1%（382 件）存在した。

上記より、1/2 以上の個別管理データについてはバックアップが実施されて

いるものの、バックアップが実施されていない個別管理データも 1/4 以上存在することが分かった。

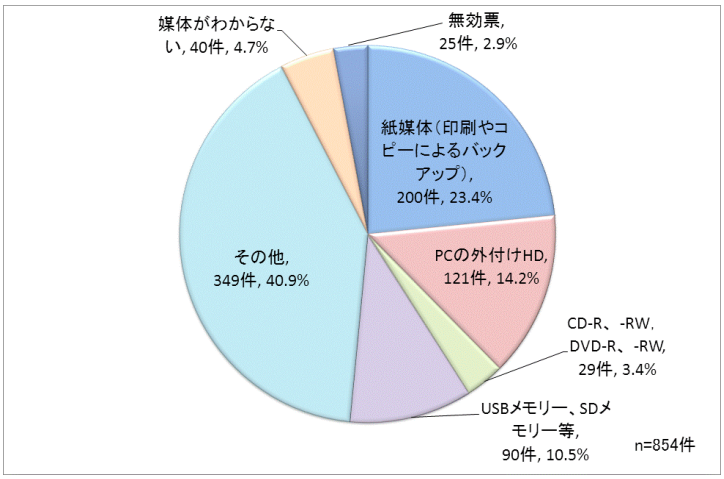


図－２５　個別管理データのバックアップの状況

（ト）個別管理データのバックアップ先

ICT 部門及び業務部門（合計 1,031 部門）で管理・運用し、バックアップを取得している個別管理データ（854 件）において、バックアップ先は、紙媒体（印刷やコピーによるバックアップ）との回答が最も多く 23.4%（200 件）存在し、次いで PC の外付け HD との回答が 14.2%（121 件）存在した。その他との回答が 40.9%（349 件）存在するが、その内訳は、共有フォルダやファイルサーバ、他の PC の HD、DAT、MO など多様な電子媒体が示されている。

上記より、バックアップを紙媒体で実施しているような個別管理データについては、被災時に元データとともに滅失する可能性があると考えられる。



図－２６　個別管理データのバックアップ先

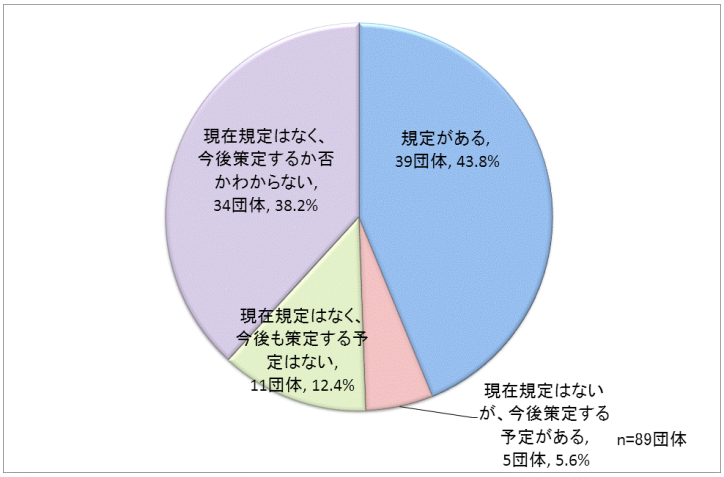
〔データ管理に関する規定等の策定状況〕

各団体における ICT 部門を窓口として調査したため、ICT 部門の回答を当該団体の回答と見なす。そのため「団体数」を単位として、データ管理に関する規定等の策定状況について分析する。

（ナ）全庁的な個別管理データの利用や管理に関する規定

本調査に回答した団体（89 団体）では、個別管理データに関する全庁的な規定を策定しているとの回答が最も多く 43.8%（39 団体）存在した。ただし、現時点で全庁的な個別管理データに関する規定が策定されていないとの回答が 56.2%（合計 50 団体）存在し、このうち、現在規定がなく今後の策定についても未定及び現在規定がなく今後も策定する予定がないとの回答が 50.6%（合計 45 団体）存在することから、導入が進んでいないことが分かった。

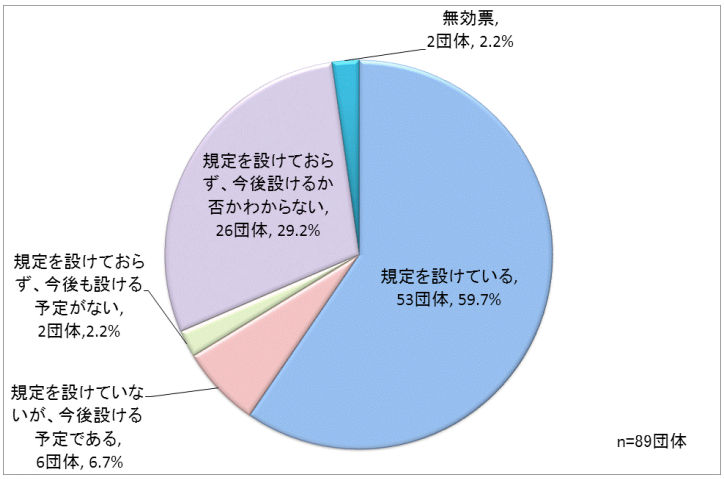
なお、別途実施したヒアリング調査では、情報セキュリティポリシー等を個別管理データの利用や管理に関する規定として認識している団体が確認されており、「規定を策定している」と回答した 43.8%（39 団体）についても、同様の認識をもった団体が含まれている可能性がある。



図－２７　全庁的な個別管理データの利用や管理に関する規定

（ニ）文書管理規定における電子データに関する規定

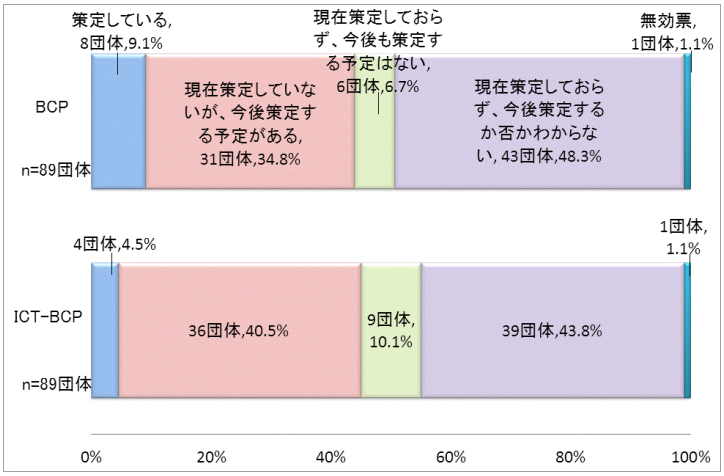
本調査に回答した団体（89 団体）では、文書管理規定において電子データに関する規定を設けているとの回答が最も多く 59.7%（53 団体）存在した。ただし、現在規定がなく今後の策定についても未定及び現在規定がなく今後も策定する予定がないとの回答が 31.4%（合計 28 団体）存在することから、導入が進んでいないことが分かった。



図－２８　文書管理規定における電子データに関する規定

（ヌ）BCP 及び ICT-BCP の策定状況

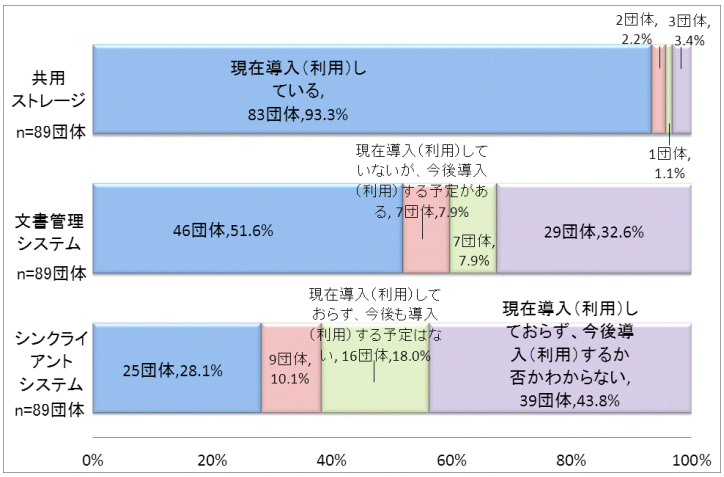
本調査に回答した団体（89 団体）では、BCP、ICT-BCP を策定しておらず今後の策定についても未定との回答がそれぞれ最も多く、BCP では 48.3%（43 団体）、ICT-BCP では 43.8%（39 団体）存在した。BCP を策定している団体は 9.1%（8 団体）、ICT-BCP を策定している団体は 4.5%（4 団体）存在するので、殆ど導入が進んでいないことが分かった。



図－２９　BCP 及び ICT-BCP の策定状況

（ネ）共有ストレージ、文書管理システム及びシンクライアントシステムの導入状況

本調査に回答した団体（89 団体）では、共有ストレージを導入しているとの回答が 93.3%（83 団体）存在することから、共有ストレージについては高い導入率であることが分かった。その一方で、文書管理システムを導入しているとの回答が 51.6%（46 団体）、シンクライアントシステムを導入しているとの回答が 28.1%（25 団体）存在することから、文書管理システムやシンクライアントシステムについては導入が進んでいないことが分かった。



図－３０　共有ストレージ、文書管理システム及びシンクライアントシステムの導入状況

（３）まとめ

東日本大震災における特定被災地方公共団体において基幹系データ[19]及び個別管理データの滅失が発生した。データ滅失が発生した地方公共団体では、データ滅失が発生しなかった地方公共団体に比べて行政事務や住民サービスの復旧に要する期間が長期化する傾向があり、調査段階において復旧できていない事例がある。

基幹系データについては、ICT 部門（70 部門）においてバックアップが実施されているものの、基幹系システムのバックアップ装置を用いて媒体にバックアップを実施しているICT部門の54.7%が､バックアップ媒体を自庁内のみに保管している。ただし、将来的に保管先を見直す場合は、自庁内のみに保管するとの回答は見当たらなくなった。また、将来的に基幹系システムの設置場所とは異なるデータセンターにネットワークを経由したバックアップを想定しているすべてのICT部門が、データの保管場所として他市町村を選択あるいは自市町村内と共に他市町村も選択している。

個別管理データについては、調査に回答した地方公共団体で管理されている個別管理データ（1,269 件）の 30.1%はバックアップが実施されておらず、バックアップが実施されている個別管理データ（854 件）の 23.4%は紙媒体（印刷やコピー）へバックアップを実施しているなど、被災時にデータ滅失の危険があるデータが多数存在することが分かった。

なお、全庁的な個別管理データの利用や管理に関する規定は、本調査に回答した地方公共団体（89 団体）の 43.8%、文書管理規定における電子データの規定についても 59.7%の導入に留まっている。

以上のように、東日本大震災におけるデータ滅失による行政事務や住民サービスへの影響と現状の基幹系データ及び個別管理データの管理状況、将来的なバックアップ方法に求めるバックアップ・リストアに係る信頼性を踏まえて、行政データ全

19 基幹系データの滅失については、「第１章　第１節―１　文献調査」を参照のこと。

体の適切な管理・運用を実現するための全庁的な統一ルールの策定もしくは既存のルールの見直し等が必要であると考えられる。

３　ヒアリング調査

前項のアンケート調査の回答から、主に行政データ（基幹系データ及び個別管理データ）の滅失が顕著であった沿岸部の地方公共団体に対してヒアリング調査を実施した。

（１）調査仕様

ア　調査対象

ヒアリング調査においては、滅失した行政データ（特に個別管理データ）の中で、どのようなデータの滅失が復旧・復興の妨げとなったのかを明らかにする。それらの行政データを「重要情報」として優先的に保全し、万が一の場合にも復元する仕組み（バックアップ・リストア基準）を策定する上でのインプットとする。

また、重要情報の滅失を避ける（若しくは最低限に止める）ための方法のひとつとして、クラウド型バックアップサイトに着目し、先進導入団体等に対してヒアリング調査を実施し、その有効性と実用性等について確認する。

ヒアリング対象の地方公共団体及び調査の目的を以下に示す。

（ア）南三陸町

アンケート調査において基幹系データの滅失が報告されている。個別管理データについては、滅失は報告されていないが、昨年度、当センターが実施した調査研究「東日本大震災における地方公共団体情報部門の被災時の取組みと今後の対応のあり方に関する調査研究」[20]において、「内部情報系システムのデータはすべて喪失」と報告を受けており、これらの行政データ等の滅失が復旧・復興に与えた影響について確認する。

（イ）陸前高田市、気仙沼市

アンケート調査において個別管理データの滅失が多数報告されている。これらの個別管理データ滅失が復旧・復興に与えた影響について確認することによって、優先的に保全すべき行政データを抽出し、バックアップ・リストア基準に反映させる。

（ウ）釜石市

アンケート調査において、基幹系システムの業務が継続できなくなる被害を受けたと報告を受けている。個別管理データについては、滅失は報告されていないが、昨年度、当センターが実施した調査研究「東日本大震災における地方公共団体情報部門の被災時の取組みと今後の対応のあり方に関する調査研究」[21]において、「PC 等の機器が流出（中略）ファイルサーバ等の機器は、すべて

---

20 「東日本大震災における地方公共団体情報部門の被災時の取組みと今後の対応のあり方に関する調査研究」の内容は、「第１節－1　文献調査」を参照のこと。

21 「東日本大震災における地方公共団体情報部門の被災時の取組みと今後の対応のあり方に関する調査研究」の内容は、「第１節－1　文献調査」を参照のこと。

水没して使用不能」と報告を受けており、これらの機器に保存されていた個別管理データの滅失が復旧・復興に与えた影響について確認する。

また、現在、総務省の被災地域情報推進事業を利用して、基幹系システムをクラウド環境に移行していることから、これまでの検討の経緯や構築にあたっての考慮点等についても確認する。

（エ）浦安市

アンケート調査において、他の地方公共団体に拠点があるデータセンターをバックアップサイトとしたプライベートクラウド環境を構築していると報告を受けている。プライベートクラウドのバックアップサイトとしての有効性について確認するとともに、作業負荷、費用及びセキュリティの観点から実用性等について確認する。

イ　主な調査内容

・被災時における重要情報
－東日本大震災において滅失した個別管理データ
－滅失したデータのうち行政事務や住民サービスへの影響が特に大きかったもの
－事前に準備すれば被災時に有用と考えられるデータ等

・重要情報の管理状況
－管理方法
－データのバックアップ
－セキュリティ対策
－データのリストア

・ICT 部門の体制及び委託事業者の支援状況等
－ICT 部門の体制
－委託事業者の支援状況等

・バックアップ方法の検討
－自治体クラウド構築の経緯
－自治体クラウドの仕様
－地方公共団体によるクラウド型バックアップサイト[22]に対する意見
－バックアップ方法の見直し

[22] 本調査研究において実証実験を行ったクラウド型バックアップサイトの枠組み及び基本コンセプトについて説明し、実際に現場で作業する地方公共団体職員としての立場からの意見をヒアリングした。詳細については、「第３章　ICT 部門におけるバックアップサイトの利活用方策」を参照のこと。

ウ　調査実績

・平成 25 年 1 月 15 日（火）陸前高田市
　－ICT 部門　総務課
　－業務部門　市民環境課、長寿社会課、社会福祉課、健康推進課、税務課

・平成 25 年 1 月 16 日（水）釜石市
　－ICT 部門　広聴広報課
　－業務部門　税務課、子ども課、地域福祉課、地域包括支援センター

・平成 25 年 1 月 17 日（木）南三陸町
　－ICT 部門　復興企画課

・平成 25 年 1 月 18 日（金）気仙沼市
　－ICT 部門　震災復興・企画課
　－業務部門　震災復興・まちづくり推進課、社会福祉事務所

・平成 25 年 1 月 18 日（金）浦安市
　－ICT 部門　情報政策課

（２）調査結果

ア　調査結果概要

調査内容に対するヒアリング結果を以下に示す。

表－１０　ヒアリング項目[23]

○:ヒアリングを実施した項目

調査内容		陸前高田市	釜石市	南三陸町	気仙沼市	浦安市
1. 被災時における重要情報	(1)東日本大震災において滅失した個別管理データ	○	○	○	○	
	(2)滅失したデータのうち行政事務や住民サービスへの影響が特に大きかったもの	○	○	○	○	
	(3)事前に準備すれば被災時に有用と考えられるデータ等	○	○	○	○	
2. 重要情報の管理状況	(1)管理方法	○	○	○	○	○
	(2)データのバックアップ	○	○	○	○	○
	(3)セキュリティ対策	○	○	○	○	○
	(4)データのリストア	○	○	○	○	○
3. 委託業者の体制等	(1)ICT部門の体制	○	○	○	○	○
	(2)委託業者の体制等	○	○	○	○	○
4. バックアップ方法の検討	(1)自治体クラウド構築の経緯		○			○
	(2)自治体クラウドの仕様		○			○
	(3)地方公共団体によるクラウド型バックアップサイトに対する意見	○	○	○	○	○
	(4)バックアップ方法の見直し	○	○	○	○	○
5. その他		○	○	○	○	○

[23] 調査実施時においては、ICT 部門と業務部門を同時にヒアリングした場合もあるため、ヒアリング結果については ICT 部門と業務部門を区別せずにまとめて記載する。浦安市は「個別管理データに関する被害はなかった」との回答を得たため、個別管理データの滅失に係る質問を省略した。自治体クラウド構築の経緯及び仕様は、実際に自治体クラウドを構築・運用している釜石市と浦安市に対して質問した。

イ　被災時における重要情報

（ア）東日本大震災において滅失した個別管理データ

a　陸前高田市

・庁舎が津波の被害を受けて、あらゆる行政データが滅失してしまった。
・システム構築事業者、保守事業者の連絡先が滅失し、復旧時にどこに連絡したらよいかが分からなくなった。
・規程集及び要綱等が滅失し、行政の継続性があやしくなった。また、復旧時に書類を作成するにあたり、一つ一つ書類の雛形を作り直す作業が発生した。
・福祉関係を始めとする高齢者や障がい者等に係る住民情報も滅失してしまった。対象者も不明のため、再調査ができない。
・障がい者関連の手当に係る支給先口座の一覧が滅失してしまい、直前に指定金融機関に振り込んだ口座を確認して対象者を特定した。
・障がい者のケース記録が滅失してしまい、事情を知る保健師の方も亡くなってしまったので、ゼロベースで情報を収集した。避難所等からの相談に応じていく過程で記録を作成した。
・要介護認定者のケース記録も滅失してしまい、ゼロベースで情報を収集した。
・母子相談の記録も滅失してしまい、ゼロベースで情報を収集した。
・予防接種の記録も滅失してしまった。震災の発生した年の１月時点のデータを業者がバックアップしていたので、それをもとに情報を更新している。
・土地の境界を記載した地籍図が滅失してしまい、相続手続に支障をきたした。後ほど、法務局からデータを提供してもらうことができた。
・当日、窓口で受け付けた分の申請書や領収書等の紙媒体が滅失してしまったことで、収納した事実を確認できない事例がある。

b　釜石市

・鵜住居地区生活応援センターが津波により全流出してしまい、納付書や金庫等が流出した。税に限らず、納付金及び収納金については不明確な部分があると思う。
・地下１階の書庫に保管していた税関係の申請及び申告書類（紙媒体）が浸水被害を受けた。現在、国文学研究所の協力のもと、復元作業を行っている。
・地下 1 階に置いていたファイルサーバが浸水して、データが滅失した。ファイルサーバ内に保管していたデータは復元できなかった。
・基本的には被災者対応（避難所の運営及び被災状況の調査）を行っており、質問にあるような個別の管理データで必要になったものはなかった。
・市の管理施設である「すくすく親子教室」が津波被害を受けて、利用している障がい児のケース記録が滅失してしまった。バックアップを取っ

ていなかったので、ゼロベースで情報を収集している。
・生活保護関係の文書倉庫が浸水したため、浸水した文書を復元中である。

c　南三陸町

・電算室に住記、税、戸籍、内部系や LGWAN 等のシステムを設置していた。電算室が設置されていた施設が津波により被災したため、ホスティングしていた Web サーバ、メールサーバ以外のすべてのシステム及びデータが滅失した。
・庁内 LAN を経由したシンクライアントを導入しており、そのサーバも電算室に設置していた。個々の職員が使用する PC で作成したデータは、すべて電算室にて保管及び一括してバックアップしており、これらがすべて滅失した。このような個々の職員が作成したデータがすべて滅失したことは、非常に影響が大きかった。

d　気仙沼市

・基幹系のサーバ及びデータは、設置していた建物に津波が及ばず、また地震による損壊もなかったため、全く被害を受けなかった。ただし、ネットワークで結ばれた出先施設に設置された PC は、津波の被害を受けて流出した。
・ICT 部門として個別管理データを保有していないが、他部署またはその出先施設においては被害を受けたところがある。
・ワン・テン庁舎[24]の 1 階に事務所があり、1 階の天井まで津波が押し寄せた。通常の業務で使用するデータは、PC の HD で記録しており、避難時には PC などを持たずに逃げたため、使用していたデータはすべて滅失した。このような経験をしたため、先日避難が必要な規模の地震が発生した際には、多くの職員はノート PC を抱えて 2 階に避難した。
・所管している事業や業務の性格上、個々の職員が個別に作成・管理しているデータは多い。その多くは、基幹系システムから抽出したデータを、使いやすいように個別に Excel で加工したものであり、多くの職員がそのようなデータを持っていたはずである。元データが存在するため、このようなデータは滅失しても、それほど業務に大きな支障はないのではないかという考えもあるが、多くの職員は、USB メモリにデータをバックアップしていた。
・発災時には、津波が発生し、事務所の天井の高さまで押し寄せてくるとは思わなかった。そのため USB メモリも PC も持たずに避難した。その結果、USB メモリや PC が流出し、それらに記録したデータが滅失した。しかし、机の中に入っていた USB メモリには流されなかったものがあり、そのような USB メモリのうち約 9 割は、乾燥すると使用する

24 本庁舎に隣接する分庁舎

ことができた。そこに記録されていたデータは、業務の継続や復旧に役立った。

（イ）滅失したデータのうち行政事務や住民サービスへの影響が特に大きかったもの

ａ　陸前高田市

（ａ）発災直後から概ね 3 日間（72 時間）程度

・データはもちろん、機材、電気、通信インフラ等のすべてを失い、また職員の安否も確認できない非常に混乱した状況では、個別管理データを使える状況にはなかった。

・被災及び安否状況を把握するための連絡手段(無線や衛星携帯電話等)が必要であった。

（ｂ）発災から概ね数週間程度

・安否確認やり災証明の発行を行うために住基システム及び戸籍システム等の基幹系データが必要となった。

（ｃ）発災から概ね半年程度

・復興事務等を実施するにあたって、役所で利用していた各書類の雛形が必要になった。雛形を一つ一つ作り直す作業に手間取り、作業がなかなか先に進まなかった。

・施設の復旧を進めるにあたって、当該施設の図面データが必要になった。

・過去に工事等を施行した事業者等を把握するために、契約書等が必要になった。

・極力すべてのデータが必要。

ｂ　釜石市

・(滅失したデータではないが、業務を遂行するため影響が大きかったものとしては) 住基データが重要であった。このデータを利用して被害状況を調査した後にり災証明の発行業務を開始することができた。

・(滅失したデータではないが) 被災状況を確認するためには紙媒体の地図が重宝した。り災証明書発行のために、建物の被害状況を調査して、固定資産税の課税免除のデータとして利用した。

・発災から数週間が経過するまでには、各避難所に避難している高齢者等の調査を実施した。その調査結果がその後の業務を遂行する上でのインプットデータになった。

c　南三陸町

（a）発災直後から概ね 3 日間（72 時間）程度

・発災直後から 3 日程度は、避難所の運営等の作業に忙殺され、データや PC を使って業務を行うような状況ではなかった。人海戦術で避難所を定期的に回り、所在確認や安否確認等の把握、情報伝達等を行った。また、車もないため、歩いて回るしか手段はなかった。

・3 月頃の時点では、前述のようにシステムを使用するような状況ではなく、行政職員、住民の区別なく、自主的・主体的に行動した。窓口業務などは早期に普及させる必要があったが、本来の行政機能が回り始めたのは、5 月の連休明けであった。

（b）発災から概ね数週間程度

・発災直後から数週間程度経過すると住記や戸籍のデータが、住民の所在管理（避難所）や亡くなった方の管理などに必要となった。この時点では、内部系より基幹系のデータの滅失の影響が大きかった。

・り災証明の発行に注力した。なお、発行に際しては東京都の職員の方の支援が大きかった。

・連絡や情報発信は、避難所に掲示された紙が基本であった。タブレットを避難所に配布したが、十分に使いこなすことができなかった。一部の職員には、携帯電話が配布されたが、使用する頻度が多く通話時間も長いため、直ぐに電池が切れるような状況であった。総じて、当時は十分に連絡をとりあって復旧にあたっていたとは、言い難い状況であった。

・避難所には様々な支援団体が入って活動しており、その支援団体が情報発信を行っていた。

・物資の受入や管理等は、相当時間が経過した後であるが、HP に掲載した。また、他には人伝やマスコミを活用した。

（c）発災から概ね半年程度

・半年程度経過した時期は、PC 等が整備されてきた。しかし、内部情報系のデータが滅失したため、一つの作業を処理しようとしても、過去の処理の経緯等が不明なため、滅失したデータを再生できずに苦労した。

・3 月 11 日の週に確定申告を行ったデータを送信する前に被災した。復旧に際しては、数回に分けて申告をやり直した。

・業務の綴り、台帳、契約書、地図などの紙ベースのデータも滅失したため、影響が大きかった。契約書は相手方からコピーをもらうなどにより対応した。

d　気仙沼市

・発災直後には、各種データを用いて業務を実施している状況ではなく、実施した業務の多くは避難所に関するもの、支援等であった。被災の状況等を把握するために必要となったデータは、自治会長等へ問い合わせるための連絡先情報であったが、滅失してしまった。

・発災直後は、避難や救命等など一刻を争う業務に注力しており、この時点でどうしても必要というデータは少なかったように思う。また、行政機能がすべて麻痺しているような状況であり、データを使った業務等は必然的に後回しになった。事態が落ち着きはじめ、復旧活動に着手できるようになって初めて、そのような業務を開始するようになった。

・本来であれば基幹系システムに入っていてもおかしくないデータを個人が管理している場合があった。そのデータが滅失したために、他の施設の倉庫に保管されていた紙ベースの資料からデータを起こしたり、ご本人に問い合わせたりして対応したが、毎月の支払いが滞ったり遅延したケースが発生した。

なお､ICT 部門が全庁的にシステムの復旧を取りまとめて業者に委託し、被災後 3 か月程で復旧した。

ただし、今回の災害はあまりにも大規模かつ広域に及んだため、当時は金融機関自体が機能停止していた。仮に市側の事務ができていても、金融機関において振り込みや引き落とし等の処理ができなかった可能性もある。

（ウ）事前に準備すれば被災時に有用と考えられるデータ等

a　陸前高田市

・緊急時における行政と地域住民との連絡網（自主防災会、地域の防災担当等の地域の窓口となる人）が整備されていると被災状況を把握しやすい。ただし、通信手段の確保が大前提である。

・住基システムのデータを何かしらの形で閲覧できるようにしておく必要がある。

・基幹系システムを再構築するためのハードウェア・ソフトウェアの調達及び設定方法などが分かるような書類を準備しておく必要がある。

b　釜石市

・災害時に要援護者名簿及び要介護認定者の紙媒体で出力した名簿があれば、電源が落ちてしまった場合にも業務を継続できる。ただし、先の震災においては、このような情報が必要になったのは、発災後数週間が経過した後だったため、その際には電源が復旧していた。

・(データという観点とは異なるが) 発災直後には、まずは情報収集が必要なので、緊急連絡手段（無線、衛星携帯電話)、報道発表の手段、職員の安否確認手段を確保しておくことが重要である。

c　南三陸町

・発災初期の安否確認、り災証明の発行、死亡の確認等のために、住記、戸籍、税務のデータが必要である。
・職員間の連絡網のようなものは構築される可能性がある。しかし、要介護者などの特定の住民を除き、一般の住民に対する連絡網的なものの構築は難しいであろう。
・今後、発災時における連絡等は、J-ALERT 情報を一斉配信するとか、HP に連動させる等が考えられる。発災後における避難所との連絡等については、今後の検討課題である。
・正確な行政情報を伝えるためには、災害 FM が有用であり、何度も再放送した。多くの被災者は、この FM 放送を聞いていた。

d　気仙沼市

・基幹系のシステムが生きていたため、データは損失しなかったが、り災証明書を作成する機能を備えていなかった。そのため急遽、新たに短期間で作成し、り災証明書を発行した。上記のような被災状況のため、ICT 部門として特に事前に準備しておくと有用と考えられるデータは思いつかない。
・事前に準備しておくことで、復旧や復興に有用な情報については、特に思いあたらない。しかし、今回の震災による PC の流失で痛感したのは、前述の自治会長の連絡先や当部署が所管している施設の連絡先であった。
・職員に関しては、発災時に庁舎内に居た人にはその場で連絡がとれ、他に個人の携帯に連絡先が登録されていた人にも連絡ができた。しかし、そのうちに携帯が使えなくなったので、結局連絡がつかなかった人も何名かいた。また、当日休んでいた人の中にも、連絡がつかない人がいた。
・基幹系システムに入っていてもおかしくないデータが、諸事情により個人が Excel や Word を用いて管理･運用していた。このようなデータは、災害等の影響を受けないように保管するべきである。
・今回の震災では、幸運にも紙ベースの資料が残っていたり、システムが復旧できたりしたため、結果的に救われたが、滅失したり、復旧できない場合も十分想定される。その場合は、データやシステムの復旧には、相当、労力や費用を費やすことになるであろう。基幹系システムやそのデータの保全のためには、クラウド等の利用が考えられるが、個別管理データについては、まずは一定のルールを定めて管理する必要があると考えている。

ウ　重要情報の管理状況

（ア）管理方法

a　陸前高田市

・基幹系データと個別管理データのうちファイルサーバに格納されたものは、サーバルームに設置したストレージサーバで一元的に管理している。
・バックアップは自動で処理実行するので、職員の作業負荷は殆どかかっていない。

b　釜石市

・基幹系システムは委託事業者のデータセンター（クラウド環境）にて管理している。
・内部情報系システムのサーバ及び住基ネットのサーバは本市施設内のサーバルームに管理している。
・税務課で独自に管理している申告支援システムは、基幹系システムとは別に 2 台のサーバに同じソフトが入っており、それぞれの中身の同期をとっている。（1 台は申告会場に持参し、専用の PC から入力した情報を収集する。その上で、外部媒体（USB メモリ）を用いて 2 台のサーバの間で同期をとって保管している。）
・税務課ではこの他に滞納管理システム、固定資産税の課税システム等を管理しているが、これらのシステムによって収集した申告情報、課税情報及び収納情報は自動的に基幹系システムに連携される仕組みとなっている。
・税務課で管理しているサーバ機器等は、すべて同じフロアに保管している。
・（全般的に）サーバ等の機器は建物の上層階に設置している。津波がきたのは地下 1 階までだったため、先の震災においても浸水被害を受けることがなく、データを滅失することがなかった。
・身体障がい者台帳は職員の PC に Excel で管理している。
・介護保険関連の情報のサーバは鍵の掛かった部屋に保管している。
・健康管理システムの情報は介護保険関連の情報と同様の管理を行っている。
・介護保険関連の情報は専用のサーバで管理している。
・特に広聴広報課の職員に負荷は発生していない。住基ネットのバックアップを取得する程度である。

c　南三陸町

・現在は、基幹系システム、内部系システムともに、データセンターに預けている。庁内にはネットワーク関連、防災系のシステムのみ設置している。

ｄ　気仙沼市

・現在、特に重要度に応じた区分を設けていない。ただし、基幹系システムに入っている住記や税などのデータが、実質的に重要度の高いものと考えられる。それらの管理は、ICT 部門で一元管理している。個別管理データに関しては、前述のように、部門内で検討しているような状況であるが、責任者を配置してバックアップを実施するようになれば、情報をランク付けして、管理するようになるのではないか。

・社会福祉事務所は、災害対応の急先鋒であり、遺体の搬送から始まり、炊き出しや義援金・弔慰金の処理、仮設住宅の整備等も実施した。現状やっと落ち着いてきて、本来業務に本腰が入ってきているような状況である。市として、今後の防災対策も併せて、早期に検討を始めることができれば良いが、現状は、個々の部署においてやっと検討が始まった状況である。

ｅ　浦安市

・データセンター（市外・民間）へのバックアップを実施している。

・当該方式の選択の理由は、「運用の簡易性・省力化」及び「バックアップやリストアの信頼性の高さ」である。

・処理サイクルは、毎日、業務終了後（夜間）である。

・運用は、データセンター側が実施しており、職員は一切タッチしていない。

・処理の確認（正常終了している等の確認）も、データセンター側が実施している。

・月 1 回程度、データセンター職員が市に来る形で、運用定例会（報告会）を開催している。

（イ）データのバックアップ

ａ　陸前高田市

・バックアップはサーバルーム内に設置した別のストレージサーバに取得している。性能はバックアップ用の方がやや劣る。

・費用等との兼ね合いから、遠隔地へのバックアップは行っていない。

・住基ネットは他の情報システムと運用が異なり、テープ媒体にバックアップを取得している。

・市庁舎の建て替え等に合わせてサーバルームの設置場所を改めて検討し、更に市内の別施設（支所等）にバックアップする仕組みを構築したいと考えている。

・先の震災においては、通信インフラの断絶が長く続いた。遠隔地へのバックアップが安全なのは理解できるが、たとえ行政データが滅失しなくても利用できないことを懸念している。

b　釜石市

・基幹系システム（クラウド環境）のバックアップデータは、自庁及び遠隔地に取得している。
・住基ネットのバックアップデータはテープ媒体に取得している。
・申告支援システムは、システムのサーバ（2 台）とは別のサーバにバックアップを取得している。
・個別システムである児童扶養手当システムについては専用端末にバックアップデータを取得している。
・児童扶養手当システムのバックアップを取得する処理サイクルは決まっていない。
・児童扶養手当システムは、専用の PC にのみ閉じたシステムで、その端末が流出した場合にはデータを復元することができない。
・身体障がい者台帳はファイルサーバにもバックアップを取得しているが最新版は個人の PC で管理している。
・身体障がい者の台帳について、バックアップの頻度については不明である。
・生活保護に係る情報は専用のサーバで管理している。
・生活保護に係る情報は専用のサーバに蓄積された情報を日次のバックアップを外付け HD に取得している。
・介護保険関連の情報は専用のサーバに蓄積された情報を日次のバックアップを外付け HD に取得している。
・内部情報系システムのバックアップデータは日次で外付け HD に取得している。
・取得した内部情報系システムのバックアップデータはサーバルーム内に保管している。

c　南三陸町

・基幹系データ、内部系データともに、一般的なバックアップソフトを用いて、差分をバックアップ・ストレージ（HD）と媒体にバックアップしている。
・バックアップしたデータは、データセンターと、大手通信会社と連携してオンライン・バックアップを行っている。
・オンライン・バックアップは、実証試験として実施しており、本年度で終了する予定である。継続しない理由は、通信回線やシステムのコストである。媒体を輸送する方が安価であり、また他にも様々な方法が想定されるからである。
・バックアップデータはバックアップサーバに保管しており、オンライン・バックアップはこれらを補完する「保険の保険」的な位置づけであることから、継続して年間数百万のコストをかけるのであれば、安価な別な手法などを検討する必要もあると考えられる。

・将来的には、被災時でも窓口業務の一部を実施できるようにしたいと思っている。自庁内に基幹系のバックアップサーバを置き、ネットワーク障害等の際には使用することも想定される。その際には、バックアップデータは、手元にあった方が良い。
・内部系のデータは、テラの規模になるため、このような大量のデータを庁内にバックアップすることは困難である。内部系については、データセンターとの間の通信回線を二重化するなどして、信頼性を高めて使用することを将来的に考えたい。

d　気仙沼市

・基幹系のデータのバックアップは、毎日夜間に自動で媒体（LTO,DAT テープ）に記録し保管している。データはフルバックアップである。住民系のデータは LTO 一つに収まっている。LTO の交換はチェンジャーを用いて行っている。そのため一週間分をセットしておき、週一回手動で交換する。前週の分を、サーバを設置している建物内の耐火保管庫に収納している。現状、バックアップはこれのみである。
・部署内で、バックアップする方法やそれを実施する担当者等について特にルール化していない。市としても、そこまで明確に決めたものはない。データを所管する担当者が自分の PC に保管し、管理しているのが実態であり、個人に任せている。USB メモリ等を用いて、バックアップしている職員もいた。もしそのようなバックアップデータがなかったら、業務の復旧はもっと大変であったろう。
・現時点における個別管理データのバックアップは、震災前と変わりなく、個人が行っているのが実態であり、個々の職員任せになっている。その背景には、事務所自体が高台に移転したことにより、少し安心してしまっている点があるのかもしれない。
・個別管理データの管理等については、現在、個々の部署毎ではなく、ICT 部門において、全庁的な視点から検討が進められているという認識である。しかしその一方で、例えば社会福祉事務所には係が 4 つあるが、各係で 1 名ずつ管理者を配置し、係単位で PC に記録したデータを共有化したり、外付け HD に保存をしたり、あるいはバックアップを取るということも必要ではないかと考えている。今はまだ構想段階であり、ICT 部門と詰める段階には至っていないが、個別管理データについては、バックアップを含めそのような管理・運用になるのではないか。

e　浦安市

・データセンター（市外・民間）へのバックアップを実施する方式を選択している理由は、「運用の簡易性・省力化」及び「バックアップやリストアの信頼性の高さ」である。運用における作業負荷は、「ウ　重要情報の管理状況　（ア）管理方法」で説明したとおり、事実上何もない。

・仮想化により、サーバ数を圧縮し、経費縮減を図った。加えて、サーバ室の拡張が予想され、それらの想定経費等を含めての比較を行った。
・セキュリティ面とコスト面で有利であることを説明し、了承された。
・データセンターへの移行は平成 23 年 2 月（平成 22 年度末）である。
・データセンターの委託にあたり、委託事業者におけるセキュリティ資格取得を必須要件とした。
・汎用機のアウトソーシング（外出し）を今から 5 年前に実施しており、その際に外部にシステムを出すことの許可を得ているため、今回のために特別な手続き等は行っていない。
・汎用機業務についても、順次、クラウドへの移行を進めており、住基システムは既に移行済みである。現在、税システムを来年目途に移行すべく、作業中である。

（ウ）セキュリティ対策

a　陸前高田市

・業務を遂行する上での重要な作業内容については、すべてストレージサーバに格納するように運用ルールを定めている。
・ストレージサーバはレイド構成で冗長化している。
・サーバルームのラックは床に固定している。
・ネットワークを一部冗長化している。
・ネットワーク機器の代替機を準備している。性能はバックアップ用の方がやや劣る。

b　釜石市

・住基ネットのサーバルームの場所を公表していない。
・地域包括支援センター（介護保険関連の情報等）と健康推進課（健康管理システム）のサーバは鍵のついた別室で管理している。
・内部情報系及びファイルサーバの保管場所は公表していない。

c　南三陸町

・主要なネットワーク機器の二重化を行っている。
・基幹システムのデータセンター内は、耐震、耐火、防水、空調、免震床構造、24 時間 365 日有人監視、自家発電機等を実施または整備している。
・内部系システムのデータセンター内は、耐震、耐火、防水、空調、自家発電機、生体認証を実施または整備している。

d　気仙沼市

・サーバをラックに搭載しているが、ラックは耐震用の架台の上に設置し

ている。被災時には、物理的な損傷はなく、一定の効果があったと認識している。

・サーバの設置場所と本庁舎（含む一部近隣の庁舎）の間のみ、バックアップ用の回線を設けている。他の出先施設との間には、バックアップ用の回線はコストの問題もあり設置していない。

・被災時には、ネットワークに被害はなかったため、この冗長化したネットワークは、使用しなかった。ただし停電した期間が長かったために、回線は生きていても、通信することができなかった。

・復電するまでに一週間弱かかった（3 月 17 日に復電）。復電前の 2 日程度､大型の発電機を借りて使用した(初日に 3 時間､次の日 7 時間使用)。

・サーバやネットワークが生きていても、停電するとシステムが使用できない。そのため停電対策として、停電時に自動で切り替わる非常用電源設備を整備することとし、現在調達中である。この非常用電源は、業務時間帯に稼働させることを想定し、3 日間程度使用できれば良いと考えている。消防法や予算の都合で、燃料の備蓄までは現時点では計画していない。

e　浦安市

・データセンターの場所は、ソフトウェアの保守業者に対しても必要がない限り場所を公表していない。

・ソフトウェアの保守業者との契約書にもデータセンターの正確な住所は明記していない。

・通常は遠隔操作で保守を行うが、どうしてもデータセンターでないと作業ができない場合のみにデータセンターの場所を教えることとしている。

（エ）データのリストア

a　陸前高田市

・行政データが滅失した際にリストアする手順を定めている。

・障害が発生した場合等には、職員で対応できるものについては対応し、対応が難しいものについては委託事業者に対応を依頼している。

・委託事業者は内陸部に拠点を構えており、システムを遠隔サポートしてもらっている。

・遠隔サポートで対応できない部分については、実際に役所まで来て対応してもらっている。委託事業者から庁舎までの所要時間は概ね 1 時間半程度である。

・非常時を想定した運用要件は契約上、特に定めていない。

・被災時において、委託事業者が早急に対応することは現実的に難しいと思う。

・どこに誰がいるか（生存しているか）も分からない状況において、情報システムを復旧させるために職員を配置する余裕はないと思う。

・先の震災においては、委託事業者に依頼して住基システムのデータを紙出力したものを届けてもらった。
・発災から約 2 週間後に、委託事業者が住基システムと財務会計システムを仮運用できるようにしてくれた。
・同じような状況におかれた場合には、委託事業者とその場にいる職員で対応せざるを得ないと思う。

b　釜石市

・データはデータセンターで管理しているので、作業環境さえ整えば、自庁でなくても業務を継続できる。

c　南三陸町

・データのリストアは、データセンターにおいて委託事業者が対応することとなる。

d　気仙沼市

・リストアの手順や方法等について、特に定めたものはない。リストアする場合には、現在締結している保守契約の中で、委託事業者にその作業を依頼することになる。
・窓口で使用する基幹系システム（住記・税・保険・福祉等）は、統合パッケージを使用しており、保守業務を委託しているのは一つの業者である。
・リストアについて具体的な方法等の取り決めはない。まずは、バックアップの方法等を決めることが肝要である。前述したように個別管理データは、外付け HD 等によって定期的なバックアップが必要であろう。そのデータを利用して、システムが損壊した時にリストアを行うような形態になるのでないか。

e　浦安市

・バックアップについては、各システムにおいて、各ベンダーがバックアップ手順を作成しており、その手順に基づき、データセンターでバックアップ取得を実施している。
・リストアについては、データセンターが各ベンダー向けのマニュアルを作成しており、それに基づき、各ベンダーがリストアを実施する。
・リストアは、市からの遠隔操作にて、ベンダーの SE が実施する。
・市の職員は、リストア作業は行わない。（立ち合いのみである。）
・市からリモートでリストアする理由は、データセンターはセキュリティ面から入室が大変なためである。（原則、データセンターへの出入りは行わない）
・データセンター内でリストアできない場合は、市のサーバ室を復元場所

と考えている。
・リストアの訓練等は実施していない。
・非常用電源は、3 日分を確保している。ただし、発電施設の対象は、サーバ室と防災無線であり、一般事務室の PC まではカバーできていない。
・シンクライアントであるため、電源、無線 AP 及びネットワーク回線があれば、業務は遂行可能である。
・具体的に、市としての BCP は今のところない。
・仮に、データセンターが大きな被害を受けた場合や、データセンターから市役所間の通信回線の復旧の見込みが立たない場合であっても、バックアップデータは、データセンターだけでなく、市側にもあるので、復旧可能である。
・もちろん、代替機器等の物理的サーバ等の機器を用意する必要があるが（現状、機器の準備ができている訳ではない）、庁舎にマシン室があるので、マシン室内にリストア環境を構築することができる。

エ　ICT 部門の体制及び委託事業者の支援状況等

（ア）ICT 部門の体制

a　陸前高田市

・総務課の中で情報システム担当は 2 名のみである。昨年度は他団体の職員を含む 4 名が情報システム担当だった。
・被災時における ICT 部門のマンパワーは足りていないと思う。
・先の震災のような非常時においては、委託事業者からの支援があると効率的な復旧が見込める。
・ICT 部門の専門職員を採用するわけにはいかないので、将来的には委託事業者に完全に委託して、職員が対応するのは情報システムの調達等に限定するのが現実的だと思う。
・委託事業者に支払う費用を考慮すると、常駐と比較して費用の安い遠隔サポートによる対応が現実的だと思う。
・非常時に備えて職員を情報システム専門に配置する（増員する）のは不可能である。
・被災時には、被災者対応などを優先させる必要があるため、たとえ ICT 部門の職員であったとしても、情報システムの復旧に主体的に取り組むのは難しいと思う。

b　釜石市

・広聴広報課の職員は 7 名。昨年度と比べると減員傾向にある。
・広聴広報課も人員を削減されている状況にあり、情報システムに特化した職員を育成する余裕はない。
・自庁にサーバを置いて職員が管理を行うよりも、業者にサーバを置いて障害対応も含めて管理してもらう方が業務効率は高い。

c　南三陸町

・ICT 部門は、情報推進係であり、3 名で組織されている。
・現在は、データセンターを利用していることもあり、システム担当は実質 2 名の体制である。

d　気仙沼市

・情報化推進室 5 名、そのうち 1、2 名でシステムの管理等を行っている。
・データ復旧サービスを専門とする業者に依頼して、壊れた HD からデータの復旧を実施した。依頼したすべての PC が復旧できたわけではないが、一部は復旧できた。
・ワン・テン庁舎で被災した PC で復旧の依頼があったのは、22 台であった。そのうち専門業者によってデータが復旧できたのは、6 台であった。ただし、その 6 台に記録されたデータがすべて復旧できたわけではない。
・滅失した自治会長の連絡先情報は、発災の数日前にメールで他の部署に送信していた。受信した PC に、運良くその情報が残っていたため、その情報をもとに復旧させることができた。
・紙しか残っていない情報については、業務を実施する際に、もう一回入力し直した。その場ですぐ必要な情報はある程度限られるため、業務を実施する過程で、不足するデータが発覚した都度、対応方法を検討し実施した。例えば去年の資料を見ながら入力し直した。
・書類も津波の被害にあったものが多数あり、それらを拾い集めた。それらの中には、使用できずに処分したものもあるが、利用できるものもあった。

e　浦安市

・基本的には、職員はリストアを実施しないので、各ベンダーがリストアを行う際は、別途契約が必要と考えている。今後保守契約のなかに、盛り込めるよう各ベンダーと協議したいと考えている。
・立会者としての市職員は、情報政策課職員であれば、誰でも可能としている。

（イ）委託事業者の支援状況等

a　陸前高田市

・先の震災においては、地元事業者が主体的に復旧を支援してくれた。
・PC、プリンタ等の必要最低限の OS 機器の貸与、機器の敷設、設定等の作業も対応してもらい、大変有り難かった。
・被災時においては、委託事業者も被災している可能性があるため、たとえ被災時の要件を定めたとしても、その内容が担保されるかどうかは、その時になってみないと分からないと思う。

・被災時には、如何に被災者を速やかに支援するかが重要であり、情報システムは、被災者を支援するための手段として考えていかなくてはならない。情報システムの復旧は、その点を踏まえ、優先順位をつけて対応する必要があると思う。

b　釜石市

・ハードウェア、ソフトウェアともに事業者が一元的な窓口となって対応。
・システム導入から運用・保守まで担当 SE が一貫した対応を行う。

c　南三陸町

・建屋やハードウェアがすべて流出したため、システムの部分的な修繕等の対応では済まなかった。プレハブの仮庁舎ができた後、委託事業者からサーバと端末を数台、無償支援して頂いた。一部残っていたデータがあったため、これらを活用して、震災前と同様な窓口業務ができるように、システムを再構築してもらった。
・何から手をつけて良いのか全く判らない状況下で、機材の調達から、システムの再構築まで一貫して支援して頂き、当時の対応には非常に感謝している。
・現在は、システム（住記、戸籍、財務等）毎に保守運用を委託している。システムは、パッケージもあれば、スクラッチ[25]で開発したものもある。

d　気仙沼市

・委託事業者は、被災後に駆けつけて来てくれ、また支援物資を提供して頂き、大変お世話になった。ただし、現課からは、現場に対するフォローがもっと欲しかったという意見を聞いている。被災した状況で、何をどのようにしたら良いのか、業務面のフォローがもっと必要であった、とのことであった。なお、委託事業者の事務所は仙台にあり、交通事情が極度に悪化していた状況下では頻繁に通うことは難しかった。
・被災後、データは生きているが停電により使用できない時に、まずバックアップしていたデータを委託事業者に託し、仙台で住民のリストを作成してもらい活用した。
・委託事業者との連絡は、電話に頼らざるを得なかったが、非常に取り難かった。

e　浦安市

・被災時の委託事業者のレスポンスや人手の充足度はきちんとしていた。問題なく対応ができた。現時点でも同様である。
・震災以降に契約等の見直しは、特には実施していない。

[25] システムを新たに独自開発すること。

・委託事業者との取り決め等においては、特に課題は思い当たらない。

オ　バックアップ方法の検討

（ア）自治体クラウド構築の経緯

ａ　釜石市

・平成 23 年 7 月頃、復興支援で北九州市から派遣されていた職員から、北九州市がもつクラウド基盤を利用しないか提案を受けた。北九州市とは、日本における近代製鉄の歴史遺産をテーマとして、共同でユネスコ世界遺産への登録に取り組んでいたおり、以前から人事交流があった。

・当初、北九州市からは以下の 3 案が示された。①北九州市のクラウド基盤を利用し、北九州市と同じ基幹系システムを利用する案、②釜石市の基幹系システムを北九州市のクラウド基盤に載せる案、③北九州市のクラウド基盤を釜石市の基幹系システムのバックアップサイトとして利用する案である。検討の結果、双方に負担の少ない③を検討することとした。

・発災から数か月が経過した頃（平成 24 年 1～2 月）、総務省の職員が釜石市を訪問し、首長に対して総務省が推進する被災地域情報化推進事業の説明を行った。その中で、システムをクラウド化する場合には、構築費用の 3 分の 1 を総務省からの補助金で負担する旨が示された。（構築費用の残り 3 分の 2 は震災復興特別交付税を充てることができたため、実際に発生する負担は運用費用だけになった）

・時期を同じくして、業者 3 社に対して基幹系システムをクラウド化して再構築した場合の構築・運用費用（平成 24 年 2 月）について情報提供依頼（RFI）を実施するなど、職員もクラウド化について情報収集を始めた。

・岩手県沿岸市町村復興期成同盟会の中で、大槌町を事務局とした ICT まちづくりワーキンググループを設置した。大槌町は内部情報系も含めたクラウド化を検討していたが、釜石市は内部情報系の更新時期ではなかったことから、最終的には釜石市単体で基幹系システムのみのクラウド化を実施することに決めた。

・平成 23 年度の第 3 次補正予算で基幹系システムの構築・運用費用を予算計上した。

・平成 24 年 4 月、釜石市が単独で基幹系システムをクラウド化することを決定した。

・平成 24 年 4 月、総務省から被災地域情報化推進事業に係る補助金の交付が正式に決定した。

・補助金の交付が正式に決まった頃から、新しい基幹系システムの仕様を詳細に検討し始めた。

・平成 24 年 6 月、議会において基幹系システムをクラウド化することが正式に決定した。

・クラウド化を推進した背景には、やはり首長の影響が大きかった。
・震災前は、行政データを自庁外に保管することは想像もつかなかった。
・今回の基幹系システムの自治体クラウドの構築においては、北九州市の存在が大きかった。北九州市の提案が大前提であった。
・北九州市は釜石市の他にも、近隣の団体の行政データを自らのクラウド基盤で保管している。

b　浦安市

・経緯等の詳細は、ネット上で開示しているのでそれを参考とされたい。（情報システム及びサーバの管理・運用にかかるアウトソーシング可能性検討調査報告書 http://www.city.urayasu.chiba.jp/secure/18906/saishuhokoku.pdf）
・クラウド方式を採用した理由は、セキュリティ及びデータセンター化のメリット（安定性、冗長性、継続性等）のすべて。
・クラウド方式の課題はない。強いて言えば、帳票のデリバリの時間（主管課にとって、帳票出力の外部委託は、スケジュール的に厳しくなる）である。
・ホストコンピュータにおいては元々、市原市及び佐倉市と 3 市共同利用であったが、平成 24 年 12 月に終了し、個々の運用となった。クラウドの共同利用については考えなかった。プライベートクラウドを念頭に考えた。

（イ）自治体クラウドの仕様

a　釜石市

・委託事業者の管理するデータセンター内にプライベートクラウドを構築している。
・仕様上では、遠隔地（北九州市のクラウド基盤）と自庁の 2 拠点にバックアップすることを要件とした。
・北九州市へはすべての基幹系データをバックアップするが、自庁のバックアップサーバは、データだけでなく最低限の業務を実施するためのシステムを稼働できる仕様とした。これは、ミニ住基機能に近いイメージで、先の震災における経験をもとに釜石市で独自に考えた仕様である。なお、最低限の業務とは、「住民票の写し・印鑑証明書・転入・転出届、出生・死亡」「税証明（所得証明・納税証明）の発行」等である。
・り災証明の発行機能は基幹系システムに標準装備されているわけではないが、住民基本台帳のデータがあればり災証明は発行可能である。
・データ移行に際しては、中間標準レイアウト[26]を採用することにした。

[26] 地方公共団体の業務システムの切り替えに伴うデータ移行時に、全国の自治体が共通的に利用できる、総務省が作成した標準的なレイアウト仕様のこと。
（http://www.soumu.go.jp/main_sosiki/jichi_gyousei/c-gyousei/lg-cloud/）

・データ通信中の秘匿性はVPNサービスで担保することにした。
・旧システムの機能はすべて新システムでも利用可能とした。
・自庁からデータセンターまで、データセンターから北九州市までは、フレッツVPN（ベストエフォート型）で繋いでいる。
・データセンターから自庁及び北九州市に対しては、日次でデータのバックアップを行っている。（翌日更新）
・釜石市における基幹系システムの全データ（3.9GB）をデータセンターから北九州市にバックアップするのにかかった所要時間は5分程度である。
・北九州市のクラウド基盤にバックアップできるデータ量は、北九州市との話し合いの上で10GBとした。バックアップデータとしては2世代の管理である。（7年契約、必要経費のみ）
・委託事業者（自治体クラウド）との契約は5年間のサービス契約である。
・実質的に負担している費用は、旧システムよりも若干高くなっている。今回の基幹系システムの再構築においては、費用の削減よりも行政データを安心安全に管理すること、時代の流れに則したシステムを構築することを考慮した。

b　浦安市

・前提として、浦安市のシステムはイメージバックアップを毎週、データバックアップは毎日とっており、それぞれ共有ストレージのバックアップ領域に保存している。
・そのデータを、RDX（外付型HDの一種）で外部メディアに保存して、耐火金庫に保管している。
・耐火金庫はデータセンター内にある。
・上記にあるRDXが市側にもあり、そこにもバックアップデータを保存している。
・市側のバックアップ処理サイクルは、データは日次で、イメージバックアップは週次である。
・差分バックアップ若しくはフルバックアップの実施サイクルは、各システムによって異なる。
・日次でバックアップサーバに保存するデータは、各システムベンダーが指定したフォルダの中身すべてなので、そこに入れるデータがDB丸ごとなのか、差分なのかは決まっていない。イメージは丸ごと（フルバックアップ）である。
・データというよりもファイル数に依存することが多いとは思うが、一番遅いもので処理時間は12.3MB／SEC、一番速いもので41MB／SEC、平均30MB／SECとなる。なお、イメージバックアップは実施するのに時間がかかっている。

（ウ）地方公共団体によるクラウド型バックアップサイトに対する意見

a　陸前高田市

・紹介してもらったバックアップサイトのコンセプト自体は理解できる。
・先の震災において、通信インフラの復旧に時間を要したため、行政データは物理的にどこに保管されているかを承知していたい。
・バックアップした行政データが格納されている場所は把握しておきたい。
・ネットワーク経由だと運用費用が高くなることが懸念される。
・自庁のサーバに他団体のデータを保管する場合のセキュリティをどう担保するかが懸念される。また、自庁のデータを預かる他団体におけるセキュリティレベルも同様。
・自分たちが相手に預けるデータ量と、相手から自分たちが預かるデータ量が異なると不平等が生じることが懸念される。

b　釜石市

・行政データの滅失を防ぐための選択肢のひとつになり得ると思う。
・導入に際して、費用対効果がどの程度見込めるかが懸念される。
・規模が大きい団体と小さい団体でどのようにデータを持ち合うか、運用ルールを定める必要があると思う。
・業務によって、バックアップを取得するタイミングは異なる筈なので、実際の運用にあたっては、各団体において運用ルールを定める必要があると思う。
・リスク分散の手段として評価できる。
・団体の規模が異なる場合には、データの持ち合いに不平等が生じない仕組みにする必要がある。
・規模の大きな団体のバックアップデータを預かることになった場合には、追加でストレージを準備する必要が生じることが懸念される。
・他の団体のデータを預かることによる責任の所在を明確にする必要がある。
・データを保管してある場所は明確にしないと、住民や首長が納得しないと思う。
・データは責任をもって管理してくれるところに預けたい。
・自治体間を繋ぐのであればLGWANを利用すべきと考える。

c　南三陸町

・他の自治体のデータを預かることについては、その責任が気になる。またセキュリティの確保も重要である。
・導入の可否は、コストに大きく左右されるであろう。仕組みもしっかりしていて安価であれば検討の余地はある。ちなみに、10 年程前は基幹系のデータをMTに記録し、県外に輸送をしていた。
・リストアするときには、そのデータをどのようにして入手するのか。バ

ックアップデータは、差分を圧縮するなどして、比較的データ容量は小さくできるが、リストアするときには、全データが必要なため、回線の性能が心配である。またバックアップ時にも、多くの自治体が相互にデータを授受することになるため、回線の性能が心配である。

d　気仙沼市

・自治体間でデータを預かる例は、既にあることは認知している。現在検討中のサイトは、それが１対１ではなく複数の自治体間で持ち合い、かつネットワークを使用するものになっている、と認識している。１ヵ所にデータを預けるのではなく、複数箇所に預けることは、データの保全という点から評価できる。
・預けるデータは、個人情報で、それを複数箇所に保管することは、法令上の点からも心配であり不安がある。また、他の自治体のデータを預かる場合、情報漏洩等の問題が発生する可能性は皆無ではなく、責任の所在やその範囲等について不安がある。
・当該サイトに係るコストが気になる。自団体の経費に加えて、他の団体のデータを預かるための費用も掛かることになる。それだけ負担できるか心配である。
・他の自治体にデータを預けるのではなく、民間に預ける方法もあるのではないか。
・地理的にかなり離れた自治体間でデータを持ち合う必要があろう。
・データに共通性があれば、データを預けた先で処理することができることが望ましい。
・預けたデータの機密性が担保され、また基幹系システムにベンダーの制約（特定のベンダーのシステムで作成されたデータしか預けることができない）がないのであれば、コスト的にどうかは不詳であるが、確実性が高いバックアップの仕組みではないか。
・特に複数箇所に保管し、かつ一つのバックアップデータからだけでは、データを復元することができないのであれば、かなり確実性が高いと思われる。
・一つの自治体が被災した場合、他の自治体でバックアップデータを活用して、業務継続するには、基本的にカスタマイズされていない同じパッケージを使用する必要があるなど難しさがあろう。よって、単にデータを保管することを目的とするのであれば、大いに導入に向けた検討の余地があるものと考えられる。

e　浦安市

・バックアップに限定せず、自治体クラウドの方向性を出す動きの延長線上で、バックアップについても考えればよいと思う。
・浦安市は災害協定を複数の自治体と結んでいるが、相互バックアップと

いう観点ではなく、災害時の職員支援等の観点である。

（エ）バックアップ方法の見直し

a　陸前高田市

・現在運用している情報システムはリースではなく購入している。暫くは現行のままの運用が続くと思う。クラウド化を含めて、将来的にどこに行政データを保管するかについては､次回のリプレース時に検討したい。

b　釜石市

・将来的に、内部情報系システム等についてもクラウド化するかは不明である。非常時に業務を遂行するのに必要な情報（内部決裁の文書等）はクラウドに載せる必要があるかもしれない。

c　南三陸町

・現在はデータセンターを活用している。現在の庁舎は仮庁舎という位置づけであり、仮庁舎のうちは、そこにサーバを設置する等は考えられない。よって当面は、バックアップ方法を含めたシステムの形態及び運用を見直すことは考えていない。

d　気仙沼市

・現在はサーバと同じ建物内にバックアップを保管しているため、別の場所に保管すべきと考えている。例えば、媒体を民間のデータセンターに預けることや、クラウド･バックアップ･サービスも検討した。しかし、データを搬送する場合、頻度にも左右されるが、特に個人情報の搬送は非常にコストが高くつくことが課題であった。ネットワーク経由の場合は、通信時間がかかることが課題である。大分以前に検討した際には、次の日の始業までに通信が終わらない見込みであった。よって未だ具体的な実施方法が見出せないでいる。

e　浦安市

・バックアップ方法の見直しの結果、現在の RDX となった。
・これから、さらに見直しは考えていない。
・RDX は耐ショック性、容量性を検討した結果、採用に至った。

カ　その他

（ア）シンクライアント方式の採用

a　陸前高田市

・個人の PC で作成した個別管理データについてもストレージサーバでバックアップしているため、特にシンクライアントにする必要性を感じない。

・シンクライアントは費用が高い。
・シンクライアントに対応していないソフトウェアが多い。

b　南三陸町

・震災の 7 年程前に、出始めであったシンクライアントを導入した。将来的に、PC の普及とともに情報漏洩やウィルス感染の危険性が高まることが予想されたため、セキュリティを確保することを目的に導入した。
・導入に際しては、使い勝手が悪い、業務に特化したソフトが使えない、生産性が低下する等の意見もあった。しかし、セキュリティを確保するために、やらざるを得ない状況があった。
・震災後には支援の職員が増えたこともあり、接続する PC が増え、また迅速かつ柔軟に業務を進める必要があり、使い方に制限があるシンクライアントは使用していない。

c　気仙沼市

・シンクライアントは、十分に検討していない。例えば CAD のように、現課が個々の業務に応じたシステムを必要としている。シンクライアントを導入するためには、内部系として機能や用途を絞り込みつつ、それ以外の利用ニーズには個々にシステムを整備する必要がある。しかし、現状内部系として多様なシステムが存在する中で、クライアントの利用を制限し、絞り込むことは容易ではない。上手く絞り込めれば、シンクライアントも有用であろうが、少なくとも短期間では難しい。
・ファイルサーバについては検討したが、実現までには至っていない。導入した場合には、ICT 部門として当然管理責任が発生する。しかし、責任を全うするためには、冗長化構成をとった上で、バックアップできる仕組みを整備する必要がある。しかし、全庁的に使用するとなると必要となる容量も相当であろう。また、そのような大規模容量を媒体にバックアップしようとすると、一晩では終わらないという話もあった。また、運用にもよるのであろうが、記録しようとするデータ量が肥大化することも懸念される。以前一度、安全性を重視した構成を検討し、予算化しようとしたが、非常に高価なものとなってしまい、認められなかった。
・共有フォルダとして、例えば課単位に一つの PC に記録したデータを共用するような利用形態は認めており、現状かなり利用されている。
・今回の震災を経験して、全庁で一元的にデータを記録・保管する方法は良いと思う。そのような仕組みが導入されていれば、津波から逃げる際には、何も持たずにすぐに逃げることができる。サーバで、一元的にバックアップしていれば安心して逃げることができ、データとともに生命も守ることができる。
・ファイルサーバ等を導入し、個別管理データも一元的に管理する可能性や有用性はあると思う。ただ、個人のファイルとなると Excel とか Word

を用いて作成されたものが主であり、その書式等は個人毎に異なるものが多い。ファイルをそのままサーバに保管するだけであれば問題ないが、一定の形式や書式で入力することが求められ、自分が使いやすいように作成できるというような柔軟性が損なわれる可能性が危惧される。また、制度の改正等も頻繁にあり、それに柔軟に対応できるか心配である。まずは前述したように、部署単位でデータを管理・運用し、コスト面等も含めて検討してみてはどうか。

d　浦安市

・一人あたりの容量上限等は決めていない。各課分についても容量上限等は決めていない。
今は、いくらでも保存が可能となっている。
・基本的には、課共有フォルダに保存するよう促しているが、個人用フォルダ（20MB）も設けている。
・ファイルサーバの容量は、5 年後を見据えての容量（10TB 程度）を用意しているためデータ保存に制限はかけていない。
・保存ルールについても特段の定めはない。
・紙ベースでは「ファイリング基準」があるが、電子ベースではない。
・ファイル名称やフォルダの階層等（年度別、事業別等）も、各主管課に任せている。
・仮想サーバの方式である。
・シンクライアントのメリットは、セキュリティ面、個別の対応がなくなったことによる工数減等。
・ログイン方式は ID、パスワード方式である。
・ファイルサーバは毎日フルバックアップを行っている。
・月 1 回、OS のイメージバックアップも取っている。

（イ）文書管理システムの利用

a　陸前高田市

・文書管理は LGWAN が敷設された機会に利用し始めたが、使い勝手が悪かったために実際の業務では利用しなかった。
・現在、被災した文書をスキャナーで電子化しており、この流れの中で文書管理システムを導入する可能性はある。

b　南三陸町

・未だ庁内の体制等が落ち着いていない。支援の職員が多く、年度末や一定の時期に、人の入れ替え、増減が大きい。このような状況では、長期的な検討が難しく、今後導入するか否か見通せない状況である。

c　気仙沼市

・使用している文書管理システムでは、発番と件名管理を行っている。文書本体は別に管理している。

（ウ）バックアップ・リストア基準等

a　南三陸町

・情報セキュリティポリシーの中で、一般的なバックアップ・リストア基準を定めている。バックアップ・リストア基準に特化して、定めてはいない。
・現在定めているものは一般的な内容であるため、バックアップ・リストア基準が策定された場合には使用したい。
・防災対策や被災時の窓口業務なども、より具体的に考えておく必要がある。
・情報化推進計画の見直しもこれからである。町内には未だ仮設住宅が沢山あり、どこに何が建つのかもはっきりしない状況である。情報分野の政策を展開するにも復興や今後のまちづくりと並行して進めていく必要がある。

b　気仙沼市

・ICT-BCP は、現状策定していない。今後策定したいという考えはあるが、すぐには難しい。策定する際に、現在検討されているバックアップ・リストア基準が参考になるようであれば、参考にしたい。
・情報セキュリティポリシーは定めている。ただし、基本方針を示してはいるが、具体的な方法や手順等は定めていない。具体的な手順となるとICT-BCP に近いものになるが、セキュリティに関係するため、一般に公開されておらず、参考にするものがなくて困っている。バックアップ・リストア基準が参考になるようであれば、非常に有益である。
・情報化計画は、策定していない。

（エ）情報管理の仕方や意識の変化

a　南三陸町

・メディアで取り上げられると、全国からの注目度が格段に上がり、HP のアクセス数が急激に増える。そのような経験を経て、情報の出し方、扱い方について十分意識し、また留意するようになった。特に、肖像権なども含め、個人情報について十分意識するようになった。
・震災を経験して感じたのは、「機械が無くなってもデータさえあれば、なんとかなる」ということである。特に基幹系のデータは、絶対なくしてはならない。
・ペーパーレスという言葉が流行り、電子化できれば便利だが、データが滅失すると大変である。
・これまで業務はシステムに依存して実施してきたが、これが無くなると、

何もできなくなる。どうやって処理したら良いのか判らず、手がつけられない。しかし、ベテランの人は、手で仕事を覚えており、手書きで処理した経験と知識があるので、特に窓口業務の復旧には、ベテランの寄与が大きかった。

b　気仙沼市

・前述のように、ICT 部門として管理対象となっているシステムやデータに滅失や大きな被害はなかったが、現課が被ったようなデータや施設の滅失が生じないよう、今後取り組んで行かなければならないと考えている。

・震災の影響により、意識は大きく変化した。先日起きた地震の際には、職員は皆最初に PC を持って避難した。自分の PC の他に、その時に不在であった何人かの職員の PC まで抱えて避難した。PC さえ持って逃げれば、最低限自分の業務は継続できるという意識が、強く根付いたようである。

・個人によって状況は異なると思うが、総じて今まではバックアップの必要性に関する認識や、実施しようとする意思が稀薄であったのではないか。しかし実際に災害を経験し、災害の影響を痛いほど経験したため、PC と USB メモリなどを用いて、何ヵ所にも保管している者が多い。ただし、USB メモリでバックアップすることの是非はあるが。

（オ）個人情報の扱い

a　気仙沼市

・個人情報ということで情報を囲ってしまうと、本当に必要な情報まで囲ってしまうことになるのではないか。例えば、我々の部署が所管する自治会長の連絡先を、必要としている他の部署に開示することができないとすると、その部署の仕事に支障をきたすことになる。共有できるものは、ある程度共有していく必要があるのではないか。囲うことで、結果的に困るのは被災者である。

・例えば、最初に被災者の情報を得るのが、義援金の担当者であったため、担当者のもとには他部署からその情報の提供依頼が来る。しかし、この情報は個人情報に属するものであり、当然すぐに USB メモリに記録して渡すというようなことはできない。個人情報については市の取り決めがあり、所定の手続きを経てから情報を提示することになる。そのため情報の受け渡しに時間を要し、業務処理全体にも時間を要することになる。秘密を保持する必要はあるが、もう少し円滑な使い方ができるようにする必要があるのではないか。なお、義援金の処理に伴う個人情報とは、被災したかどうか、被災したのであればその程度、振込先の口座情報、連絡先などである。

・個人情報の運用の仕方は、事前に詰めておく必要がある。できるだけ早

く義援金を支払う必要があるなど、被災時の対応にはスピードが求められる。基幹系システムが利用できれば、個人情報の管理・運用はシステムを用いてできるが、被災時には各担当者が個々に行わなければならなくなるため、事前にルール決め等を行う必要がある。

・現状、被災者に関する様々な情報を、各部署が個々に管理・運用している。その弊害が小さくないため、被災者の支援システムとして統合することを現在進めている。このシステムは、今後また震災等が発生したときにも大いに活用できるのではないかと期待しているところである。

（カ）アンケート調査結果に対する質問への回答等

a　陸前高田市

・「介護予防ケアマネジメントシステム」「飼犬管理システム」は個別管理データではなく、ホストないしサーバで管理している情報である。

・障がい者手帳はデータを県でも管理していたので復旧が早かった。比較的早い段階で、陸前高田市における手帳所持者の名簿や再交付に必要な様式を県の職員に持って来てもらった。

・妊婦の記録（カルテ等）は「いーはとーぶ」（岩手県が試験的に運用する妊婦に係る情報の管理システム）に入っていたため滅失を免れた。

b　釜石市

・地震によって作業が継続できないような被害が生じたと報告したのは、主に電気を始めとするインフラ（ガス、水道）も、電話もつながらない状況だったので、業務を継続することができなかったからである。

・床に PC が落下するような被害報告は受けていない。恐らく職員が転倒しないように押えたのだと思う。

（３）まとめ

ア　被災時における重要情報

（ア）滅失した行政データ

・ヒアリング調査対象団体のうち、庁舎が壊滅的な被害を受けた団体（陸前高田市、南三陸町）においては、殆どの行政データ（システムとして管理されている電子データ及びローカル PC 等に保存されている電子データ）が滅失した。

・その他の団体（釜石市、気仙沼市）においても、庁舎の１階が浸水したり、出張所が壊滅的な被害を受けたことによって、PC 等に保管していた個別管理データが滅失した。

・基幹系データについては、一部はサルベージによってリストアできたが、完全に滅失してしまったデータも存在する。

・個別管理データについても、一部は送信メールの添付ファイルや USB メモリ等からリストアできたが、殆どのデータは完全に滅失してしまった。

・ヒアリング調査で滅失が報告された行政データ（基幹系データ及び個別管理データ）を以下に示す。

表－１１　滅失データの具体的内容と住民サービス等への影響

データ属性	滅失した行政データ等	
	業務等名称	個別のデータ名称等
システムとして管理されている電子データ	住基、税、戸籍関連	住民の所在管理（避難所）及び死亡者の管理データ
		安否確認・り災証明関連データ
	広聴広報関連	ファイルサーバ内のデータ
	内部系システム関連（シンクライアント関連）	ファイルサーバ内のデータ、一般文書、各課業務データ
	福祉関係	－
	高齢者関連	要介護認定のケース記録
	障がい者関連	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
	保健衛生関連	予防接種記録
	規程集・要綱等	書式情報（帳票フォーマット）
ローカル PC 等に保存されている電子データ	障がい者関連	障がい者児童のケース記録
	自治会長等への連絡	連絡先情報
	EUC 関連	－
	福祉関係	心身障がい者の医療費支給台帳 口座情報、支給実績等

データ属性	滅失した行政データ等	
	業務等名称	個別のデータ名称等
紙で保存されているデータ	書庫に保管していた文書	ー
	土地（税務）関連	地籍図（土地の境界）
	施設復旧関連	図面データ
	収納関連	申請書・領収書等の紙媒体
		納付書及び現金
	課税関連	確定申告書
	財務関連（施行経験のある事業者等の把握）	契約書
	業務綴り	台帳
	ー	地図

注：上記はヒアリング調査において聞き取りした結果
（実際に滅失したデータの一部）である。

（イ）発災直後から概ね３日間に必要だった行政データ

・被災直後（発災直後から概ね 3 日間）はいずれの団体も被災者対応（避難所の設営等）に追われ、データや PC を使って業務を行うような状況ではなかった。
・必要なのは特定の行政データではなく、何よりも緊急連絡・安否確認手段（無線、衛星携帯電話）だった。
・職員たちは各避難所を回るなどして、地域住民の被災状況等の把握に努めた。
・特に被害が大きかった団体では停電や回線寸断等が発生しており、情報システムが被害を免れたとしても利用することができなかった。
・比較的被害が小さかった団体においても、停電によりシステムが利用することができなかった。
・被災直後は停電等により電子データの検索、閲覧ができなくなってしまうため、紙媒体の重要性が示唆された。

（ウ）発災から概ね数週間後に必要だった行政データ

・発災後数週間が経過すると、まずは住基データや戸籍データを始めとする基幹系データが必要になった。用途はり災証明の発行や亡くなった人の把握等であった。
・住基データと戸籍データが最も重要なデータであり、これらのデータの滅失が免れたことで業務を継続できた。

（エ）発災から概ね数カ月後に必要だった行政データ

・発災後数か月が経過すると、必要な情報は多岐にわたってくる。例えば、被災した施設の復旧を進めるための図面データ、支払事務等に係る契約書などである。
・内部文書の様式が滅失したことにより、事務処理を回す際に一つ一つ様式を作成する手間が発生し、作業が遅延した。
・普段付き合いのある業者等の連絡先などが滅失した場合には、どこに作業を依頼してよいかが分からず、そのような小さな作業が山積みして、復興作業を進める上での妨げになった。
・滅失した情報の多くは、データ及びバックアップ媒体を庁内に保管していたものである。例えば、外部機関にデータを連携していたものについては、その外部機関から後にデータの提供を受けて、発災直前までの情報をリストアできた場合もあった。

（オ）事前に準備すれば被災時に有効と考えられる行政データ等

・職員間、市が管理する各施設、報道機関等との通信手段
・住基・戸籍等の基幹系データ
・緊急連絡先やシステムの復旧方法等を紙媒体に出力したもの
・災害時要援護者及び要介護認定者の一覧（紙媒体）

イ　重要情報の管理状況

・現時点における重要情報の管理方法については、被災した団体によっては運用が異なっている。
・基幹系データについては、陸前高田市と気仙沼市は庁内にデータを保管し、バックアップも庁内に保管している。
・釜石市と浦安市は外部のデータセンターにデータを保管している。南三陸町は、庁舎外のデータセンターへ、ネットワークを利用したバックアップを実証実験として行っている（実証実験後の管理方法については未定である）。
・ネットワークによるデータの遠隔地保管には、自庁舎にデータを媒体等で保管するよりもコストが高いことが、普及を妨げる要因となっている。
・陸前高田市では、震災後に構築したシステムにおいて新たにファイルサーバを設置して、職員が扱う情報のうち、業務に係わるものをそこに格納するように周知している。
・個別管理データの管理について明確な運用ルールを定めず、基本的には職員個人の判断に任している団体が存在する。
・情報システムの管理作業については、日次等でバックアップを取得するのみで、職員の作業負荷は殆ど発生していない。
・バックアップデータのリストアは事業者に委任している団体が多い。

ウ　ICT 部門の体制及び委託事業者の支援状況等

・陸前高田市や釜石市では、業務効率を考慮すると、将来的に ICT 部門の業務を事業者に委託することも選択肢のひとつと考えている。

・先の震災においては、何の取り決めもなかったものの、運用保守事業者が主体的に OS 機器を貸与し、システムを復旧したことが迅速な復旧に繋がったとのことで、いずれの団体においても職員は運用保守事業者に感謝していた。

エ　バックアップサイト

（ア）自治体クラウドの仕様

・釜石市と浦安市で構築されている自治体クラウドにおいては、行政データを遠隔地に保管するだけでなく、自庁にも一部のデータを保管する仕様を採用している。これにより、「イ　被災時における重要情報」で述べた重要情報（特に住基データ等の最低限のデータ）を庁舎内に保管し、回線が遮断されたとしても、発電機さえあれば業務を継続できる体制を構築している。

（イ）地方公共団体によるクラウド型バックアップサイトに対する意見

・地方公共団体によるクラウド型バックアップサイトについては、コンセプトについては理解できるが、実際の運用での相手先との調整を懸念する声も聞かれた。

・団体にとっては、住民に対して説明責任を果たす必要があるため、どこにデータを保管しているかということは明確であった方がよい。

第２節　公文書管理法等からみたデータ管理の必要性に関する調査

公文書管理法等の法令に基づいて行政データの管理等に係る必要性を検討した。

１　国における文書管理に係る法令等

（１）公文書等の管理に関する法律等の概要

ア　行政文書の定義

第 2 条第 4 項において、この法律において「行政文書」とは、「行政機関の職員が職務上作成し、又は取得した文書（図画及び電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。以下同じ。）を含む。第十九条を除き、以下同じ。）であって、当該行政機関の職員が組織的に用いるものとして、当該行政機関が保有しているものをいう。」とされている。

【参考】多くの自治体においても、ほぼ同様の定義となっている。

仙台市　行政文書取扱規程

行政文書　職員が職務上作成し、又は取得した文書、図画及び電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。以下同じ）であって、職員が組織的に用いるものとして、市が保有しているものをいう。ただし、官報、公報、白書、新聞、雑誌、書籍その他不特定多数の者に販売することを目的として発行されたものを除く。

釜石市　文書管理規程

文書　職務上作成し、又は取得した書類、図画及び電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。以下同じ。）をいう。

イ　公文書等の管理に関する法律における電子情報

上記のとおり、「電磁的記録」は「行政文書」に含める形で位置付けされている。都道府県や市区町村においても同様の記述、扱いとなっている。

従って、システムとして管理されている電子データはもとより、ローカル PC 等に保存されている電子データも「行政文書」として位置付けられる。

ウ　行政文書の管理・保存

公文書等の管理に関する法律（以下「文書法」という。）第 6 条において、「行政機関の長は、行政文書ファイル等について、当該行政文書ファイル等の保存期間の満了する日までの間、その内容、時の経過、利用の状況等に応じ、適切な保存及び利用を確保するために必要な場所において、適切な記録媒体により、識別を容易にするための措置を講じた上で保存しなければならない。」とされている。

同条第 2 項においては、前項の場合において、「行政機関の長は、当該行政文

書ファイル等の集中管理の推進に努めなければならない。」とされている。

従って、システムとして管理されている電子データはもとより、ローカル PC 等に保存されている電子データも「行政文書」として、適切な保存が義務付けられている。

エ　行政文書管理規則

（ア）規定のポイント

「文書法」第 10 条において、「行政機関の長は、行政文書の管理が第四条から前条までの規定に基づき適正に行われることを確保するため、行政文書の管理に関する定め（以下「行政文書管理規則」という。）を設けなければならない。」とされている。

同条第 2 項において、「行政文書管理規則には、行政文書に関する次に掲げる事項を記載しなければならない。」とされている。項目は 7 項目あり、以下のとおりである。

一　作成に関する事項
二　整理に関する事項
三　保存に関する事項
四　行政文書ファイル管理簿に関する事項
五　移管又は廃棄に関する事項
六　管理状況の報告に関する事項
七　その他政令で定める事項

（イ）策定状況

各省庁等において「行政文書管理規則」を設けている。[27]

一例として、内閣官房行政文書管理規則の構成等を以下に示す。

規則は、公文書等の管理に関する法律（平成 21 年法律第 66 号。以下「公文書管理法」という。）第 10 条第 1 項の規定に基づき、内閣官房における行政文書の管理について必要な事項を定めることを目的とする。

・第 2 章 行政文書ファイル等の管理体制（第 3 条－第 5 条）
  - 管理責任者を規定（3 条）
  - 文書管理者の設置（4 条）
  - 行政文書を適正に管理しなければならない（5 条）
・第 5 章 行政文書ファイル等の保存（第 8 条）
  - 行政文書ファイル保存要領の作成
  - 2(1)保存する行政文書ファイル等の媒体の種別及びその保存場所・方法[28]

---

[27] 参考：行政文書の管理に関する定め（行政文書管理規則）一覧
http://www8.cao.go.jp/chosei/koubun/about/kikan/kanrikisoku_ichiran.html
[28] 内閣官房行政文書管理規則の詳細は次を参照のこと。
http://www.cas.go.jp/jp/koukai/yosiki/kisoku_110401.pdf

オ　行政文書の管理に関するガイドライン

前出規則の詳細を定めるため、当該ガイドラインが設けられている。構成は以下のとおりである。

〔行政文書ファイル保存要領〕

- 総括文書管理者は、行政文書ファイル等の適切な保存に資するよう、行政文書ファイル保存要領を作成するものとする。
- 行政文書ファイル保存要領には､次に掲げる事項を記載しなければならない。「紙文書の保存場所・方法」､「電子文書の保存場所・方法」､「引継手続き」､「その他適切な保存を確保するための措置」

〔紙及び電子文書の保存場所・方法〕

・行政文書の管理に関するガイドライン（平成 23 年 4 月 1 日　内閣総理大臣決定）（平成 24 年 6 月 29 日　一部改正）（以下「行政文書ガイドライン」という。）に、○○省行政文書ファイル保存要領（例）[29]として、紙及び電子文書の保存場所・方法の記述がある。

・正確性を期するため、当該記述を原文のままの内容で、以下に転載する。

＜電子文書の保存場所・方法＞

○ 電子文書について、①改ざん、漏えい等の不適切な取扱いを防止、②一定期間経過後の集中管理、③移管のための長期保存フォーマットへの変換など、時の経過、利用の状況等に応じ、適切な保存及び利用を確保するための場所、記録媒体等についての考え方を記載する。なお、記載に当たっては、各府省庁の情報セキュリティポリシーに留意する。

○○省行政文書ファイル保存要領（例）

2 電子文書の保存場所・方法

- 電子文書の正本・原本は、文書の改ざんや漏えい等の防止等の観点から、文書管理システムで保存する。
- 保存期間が○年を経過した電子文書については、副総括文書管理者が管理する。
- 保存期間満了時の措置を移管としたもので、電子文書で移管するものは、適切な方式で保存する。
- 文書管理システム以外で保存する電子文書がある場合には、適切なアクセス制限を行う。
- 長期に保存する電子文書については、国際標準化機構（ISO）が制定している長期保存フォーマットの国際標準等で保存するなど、利活用が可能な状態で保存する。

・電子文書は、情報セキュリティポリシーの規定に従い、必要に応じ、パスワードの設定、暗号化、電子署名の付与を行うとともに、バックアップを保存する。

---

[29] 行政文書ガイドラインの 20 頁から 22 頁を参照のこと。
http://www8.cao.go.jp/chosei/koubun/hourei/kanri-gl.pdf

（２）法令からみた公文書管理の必要性

「文書法」に基づき、行政文書管理規則や管理に関するガイドラインが制定され、適切な管理が行うことのできる体制、制度となっている。

電子文書については、「行政文書の管理に関するガイドライン」においてバックアップの保存が位置付けられているが、具体的な方法等についてまでは触れられていない。

（３）紙文書の取扱いに係る再検討の必要性

行政文書ガイドラインに、○○省行政文書ファイル保存要領（例）[30]として、紙及び電子文書の保存場所・方法の記述がある。

正確性を期するため、当該記述を原文のままの内容で、以下に転載する。

1 紙文書の保存場所・方法

⑴事務室における保存

・年度ごとにまとめられた行政文書ファイル等（保存期間が○年以上のもの）について、事務室においては、「①現年度の行政文書ファイル等」と「②前年度の行政文書ファイル等」とを区分して保存する。この場合、①の保存場所を職員にとってより使いやすい場所（例：ファイリングキャビネットの上段等）とするよう配意する。

・年度末においては、新年度の行政文書ファイル等の保存スペースを空けるために、行政文書ファイル等の移動を行う（例：ファイリングキャビネットの上段から下段への移動等）。ただし、「継続的に利用する行政文書ファイル等」にあっては、現年度の保存場所で保存することができる。

・個人的な執務の参考資料の収納場所は、職員各自の机の周辺のみとする。

⑵書庫における保存

・「前々年度以前の行政文書ファイル等」については、副総括文書管理者に引き継ぎ、書庫で保存する。ただし、「継続的に利用する行政文書ファイル等」にあっては、事務室で保存することができる。

・「継続的に利用する行政文書ファイル等」として継続して事務室で保存されている行政文書ファイル等については、年度末に、文書管理者が利用状況等を勘案し、書庫への移動を再検討する。

・個人的な執務の参考資料は書庫に置いてはならない。

⑶機密性の高い行政文書ファイル等

・上記⑴及び⑵にかかわらず、機密性の高い行政文書ファイル等については、施錠のできる書庫・保管庫に保存し、不正な持出しや盗難を防ぐ必要がある。

⑷ファイリング用具及び書棚の表示と所在管理

・ファイリング用具（バインダー、保存箱等）の見出しや背表紙の表示については、別添様式のとおりとする。

---

[30] 行政文書ガイドラインの 21 頁を参照のこと。
http://www8.cao.go.jp/chosei/koubun/hourei/kanri-gl.pdf

・書棚は、行政文書ファイル等の所在を明らかにするため、棚番号を付すとともに、行政文書ファイル等にも同一の番号を付し、所在管理を行う。

このように、紙文書の保存場所・方法として、具体的かつ必要な記述がなされているが、先の震災のような事態が生じた際には滅失する可能性が否定できない。

そのため、万一の滅失に備え、重要度の分類に伴い必要と判断された紙文書の電子化を推進し、前頁にある電子文書の一環としてバックアップしておくことが重要である。

紙文書の電子化の推進については、後段のバックアップ・リストア基準の策定の中で示す。

２　地方公共団体における文書管理に係る規則・規程等

（１）文書管理に係る規則・規程等の概要

調査対象を、被災地については 3 県、13 市町とし、被災地以外については以下の理由から 1 都 2 県、4 市とした。

－自治体として最も大規模である東京都と東京都下にあって、電子自治体としての先進性を持つ三鷹市を対象とした。

－文書管理システムを早い時期に導入した（平成 11 年 4 月から電子決裁を含め運用開始）横須賀市と、横須賀市が位置する神奈川県を対象とした。

－阪神淡路大震災の被災経験を持つ兵庫県と神戸市、西宮市を対象とした。

ア　都道府県における規則・規程等の概要

（ア）被災地

ａ　岩手県

「紙」と「フォルダ（紙をまとめた綴り）」を基本とした規定である。文書管理システムを前提とした文書管理規程とはなっていない。また、データのバックアップに関する規定はない。

表－１２　岩手県における文書管理に係る規則・規程等[31]

団体名称	規則・規程等の種別	名称	整理保管に係る規定（主に電磁的記録に係る箇所の概要）	文書管理システム前提の有無	バックアップ関連	
					記述	記述内容
岩手県	規程	行政文書管理規程	行政文書の管理は、ファイル（同様の方法で区分され、若しくは利用される関連した簿冊又は簿冊に編てつすることが適当でないものにあっては、他の適当な方法により整理したものをいう。以下同じ。）を単位として行うものとする。 職員が、検討資料を作成するために収集した関係資料、起案等に際しての下書き、業務の参考に供するために保有しているコピー等の個人文書は、行政文書と明確に区分して保管しなければならない。 電磁的記録の保存方法：文書管理者の承認を得た後に、他の媒体に変換する前の媒体に録されている行政文書を廃棄すること。	無	無	無

ｂ　宮城県

規則と規程を設けており、文書管理システムを前提とした文書管理規程となっている。規程において、「災害に際しいつでも持ち出すことができるようにあらかじめ準備し、紛失、火災、盗難等に対する予防措置を講じなければならない。」との規定はあるものの、データのバックアップにまでは言及されていない。

31 文書管理システム前提の有無：文書の管理は、「原則として文書管理システムによるものとする。」との趣旨の記載が条文化されている場合を言う。

表－１３　宮城県における文書管理に係る規則・規程等

団体名称	規則・規程等の種別	名称	整理保管に係る規定（主に電磁的記録に係る箇所の概要）	文書管理システム前提の有無	バックアップ関連	
					記述	記述内容
宮城県	規則	行政文書管理規則	職員は、県がその諸活動を説明する責務を有することを認識し、常に行政文書の所在を明確にする等行政文書を適正に管理しなければならない。 電磁的記録については、前四条の規定にかかわらず、その種別、情報化の進展状況等を勘案して別に定める方法により管理するものとする。	有	無	無
	規程	文書規程	文書は、別に定めがある場合又は特に支障のある場合を除き、総合文書システムにより取り扱うよう努めなければならない。 本庁において保管されている完結文書の保存は、総合文書システムにより決裁された文書及び保存年限が一年のものにあつては主務課長が、保存年限が三年以上のものにあつては県政情報公開室長が行わなければならない。 文書(電磁的記録を除く。)を未完結文書又は完結文書に区分してその所在箇所及び処理状況を明らかにしておかなければならない。 重要な文書は、災害に際しいつでも持ち出すことができるようにあらかじめ準備し、紛失、火災、盗難等に対する予防措置を講じなければならない。			

c　福島県

規則を設けており、文書管理システムを前提とした文書管理規則となっている。規定そのものは、紙を前提とした管理内容が基本となっており、データのバックアップに関する規定はない。

表－１４　福島県における文書管理に係る規則・規程等

団体名称	規則・規程等の種別	名称	整理保管に係る規定（主に電磁的記録に係る箇所の概要）	文書管理システム前提の有無	バックアップ関連	
					記述	記述内容
福島県	規則	福島県文書等管理規則	本庁機関における電子文書である完結文書は、文書管理システムにより保管するものとする。 完結文書(本庁機関における電子文書でない完結文書に限る。)は、当該完結文書に係る事案の処理が完結した日から当該日の属する年度の翌年度の末日までの期間(保存期間が一年未満のものにあっては、当該保存期間を経過する日までの期間)、保管するものとする。	有	無	無

（イ）被災地以外の地域

ａ　東京都

文書管理システムを前提とした文書管理規則となっている。

規則において、「文書等の保存に当たって、常に紛失、火災、盗難等の予防の措置を講ずるとともに、重要な文書等は、非常災害に際し、いつでも持ち出せるようあらかじめ準備しておくものとする。」との規定はあるものの、データのバックアップにまでは言及されていない。

表－１５　東京都における文書管理に係る規則・規程等

団体名称	規則・規程等の種別	名称	整理保管に係る規定（主に電磁的記録に係る箇所の概要）	文書管理システム前提の有無	バックアップ関連	
					記述	記述内容
東京都	規則	東京都文書管理規則	別に定めのある場合を除き、文書等の管理は、文書総合管理システムにより行うものとする。 同種の文書等を定例的に処理する場合においては、主務課長は、局の庶務主管課長の承認を得て、文書総合管理システムによる管理に代えて当該文書等を管理するための帳票(以下「特例管理帳票」という。)を使用して当該文書等の管理を行うことができる。 特例管理帳票を使用する場合において、記載すべき事項をパーソナルコンピュータ(以下「パソコン」という。)に入力し、記録する方式により当該帳票を調製することができる。 文書等(電子文書を除く。以下この条及び次条において同じ。)は、必要に応じて利用することができるように、分類記号別に、かつ、一件ごとに整理しておくものとする。 主務課長は、文書等の保存に当たって、常に紛失、火災、盗難等の予防の措置を講ずるとともに、重要な文書等は、非常災害に際し、いつでも持ち出せるようあらかじめ準備しておくものとする。	有	無	無
	－	東京都文書管理規則の解釈及び運用について	逐条解説的な内容	有	無	無
	要領	東京都文書保存委託要領	倉庫業法(昭和31年法律第121号)第3条に規定する許可を受けた事業者に保存委託するもの	－	－	－

b　神奈川県

文書管理システムを前提とした文書管理規則・規程となっている。

特に、規則においては電子化されたデータが、行政文書の中核をなしている現実を踏まえた規定の記述となっているものの、データのバックアップにまでは言及されていない。

表－１６　神奈川県における文書管理に係る規則・規程等

団体名称	規則・規程等の種別	名称	整理保管に係る規定（主に電磁的記録に係る箇所の概要）	文書管理システム前提の有無	バックアップ関連	
					記述	記述内容
神奈川県	規則	神奈川県行政文書管理規則	行政文書は、事務を適正かつ円滑に処理するため、その所在等に関して常時把握が可能な状態を維持する等、適正に管理しなければならない。この場合において、電子文書及び電子情報に関しては、法令等に別に定めのあるものを除き、総務局情報統計部文書課長（以下「文書課長」という。）が別に定めるところにより、取り扱うものとする。 文書課長及び所（給与事務センター等を除く。次項及び第3項において同じ。）の文書担当課の長は、保存文書を整理し、書庫等に保存するものとする。	無	無	無
神奈川県	規程	神奈川県行政文書管理規程	事務は、文書又は電子文書によって処理することを原則とする。この場合において、電子文書によって処理できる範囲は、総務局情報統計部文書課長（以下「文書課長」という。）が別に定める。 行政文書事務（行政文書の収受、整理及び保管、文書及び電子文書の作成等に関する事務をいう。以下同じ。）は、統合文書処理システムの利用により行うことを原則とする。 文書の整理及び保管は、ファイリングキャビネット等の収納用じゅう器（以下「キャビネット等」という。）に収納することにより行わなければならない。ただし、キャビネット等に収納することが不適当なものは、あらかじめ別に定める場所に置くことにより行うことができる。 電子文書（グループウェアシステムを利用して作成したものを除く。以下この条において同じ。）の整理及び保管は、統合文書処理システムへの登録により行わなければならない。 同一の処理済み電子文書でファイル基準表の2以上の個別フォルダーに関係があるものは、最も関係の深い個別フォルダーに収納し、関連する他の個別フォルダーを関連フォルダーとして指定するものとする。 電子情報の整理及び保管は、当該電子情報の処理サイクル及びシステム運用を考慮し、適切に行わなければならない。この場合において、当該電子情報の内容に関する文書又は電子文書を併せて保管しなければならない。 文書、電子文書及び電子情報以外の行政文書に関しては、その媒体等の性質に応じて、適切に整理及び保管しなければならない。この場合において、統合文書処理システムに必要事項が登録されている場合を除き、索引目録等を整備しなければならない。	有	無	無
神奈川県	規程	神奈川県電子情報等の利用に係る行政文書事務の特例を定める規程	行政手続オンライン化システムによる電子情報等及び文書の保管及び保存	－	無	無

c　兵庫県

文書管理システムを前提とした文書管理規則・規程となっている。

特に、規則においては電子化されたデータが、行政文書の中核をなしている現実を踏まえた規定の記述となっているものの、データのバックアップにまでは言及されていない。

表－１７　兵庫県における文書管理に係る規則・規程等

団体名称	規則・規程等の種別	名称	整理保管に係る規定（主に電磁的記録に係る箇所の概要）	文書管理システム前提の有無	バックアップ関連	
					記述	記述内容
兵庫県	規則	文書管理規則	本庁等の職員は、文書等を正確かつ迅速に取り扱うとともに、文書等を良好な状態で保存し、常にその所在を明らかにしておくこと等により、文書等を適正に管理しなければならない。 文書等の収受、起案、決裁、保存、廃棄その他文書管理に関する事務の処理は、原則として、文書管理システムにより行うものとする。	有	無	無
	規程	本庁文書管理規程	電磁的記録は、磁気ディスク、光ディスク、磁気テープ等（以下「磁気ディスク等」という。）に録して取り扱うものとする。 本庁等の職員は、文書等を良好な状態で保存するために必要があるときは、当該文書等について、記録媒体を変換することができる。 電磁的記録である完結文書等前項の規定により難い完結文書については、規則第７条第１項の規定により作成した文書等の分類基準に基づいて一定のまとまりごとに整理して保存し、常に所在を明らかにしておかなければならない。 文書管理システムに記録されている電磁的記録は、保存期間中文書管理システムで保存するものとする。 第22条第１項第３号に掲げるシステムに記録されている電磁的記録については、保存期間中当該システムの管理者が定める方法で保存するものとする。 前２項に規定する電磁的記録以外の電磁的記録は、保存期間中主務課の事務室において保存するものとする。	有	無	無

イ　市町村における規則・規程等の概要

（ア）被災地

a　岩手県下４市町

「紙」と「フォルダ（紙をまとめた綴り）」を基本とした規定である。文書管理システムを前提とした文書管理規程とはなっていない。また、データのバックアップに関する規定はない。

表－１８　岩手県下市町村における文書管理に係る規則・規程等

団体名称		規則・規程等の種別	名称	整理保管に係る規定（主に電磁的記録に係る箇所の概要）	文書管理システム前提の有無	バックアップ関連	
						記述	記述内容
岩手県	宮古市	規程	宮古市文書取扱規程	完結した文書は、文書分類表により分類し、ファイリングキャビネットの該当フォルダーに収納しなければならない。 キッビネットに収納することが不適当な文書の整理及び保管は、簿冊につづることその他適当な方法により鋼製書庫等の用具を用いて行わなければならない。	無	無	無
	陸前高田市	規程	陸前高田市文書管理規程	保存文書は、書架に分類整理しておくこと。 保存文書の保存状況を定期的に点検すること。	無	無	無
	釜石市	規程	釜石市文書管理規程	文書は、課を中心に常に整理し、重要なものは非常災害時に際して支障がないようあらかじめ適当な処置を講じておかなければならない。 文書は、係を単位として分類表の記号により整理保管しなければならない。	無	無	無
	大槌町	規程	大槌町文書取扱規程	文書は、各課ごとに整理し、重要なものは、非常災害時に際して支障がないようあらかじめ適当な処置を講じておかなければならない。 各所属長は、その主管に係る保管文書の登録、保管状況等について調査するなど、常にその所在、保存状態についての管理を怠ってはならない。	無	無	無

b　宮城県下５市町

仙台市を除き、「紙」と「フォルダ（紙をまとめた綴り）」を基本とした規定である。文書管理システムを前提とした文書管理規程となっているのは仙台市である。（気仙沼市は目録レベルでの規定と思われる。）

いずれの都市においてもデータのバックアップに関する規定はない。

－石巻市においては、例規データベースは開示されているが、文書に係る掲示がなかった。

表－１９　宮城県下市町村における文書管理に係る規則・規程等

団体名称		規則・規程等の種別	名称	整理保管に係る規定（主に電磁的記録に係る箇所の概要）	文書管理システム前提の有無	バックアップ関連	
						記述	記述内容
宮城県	仙台市	規程	行政文書取扱規程	完結文書(簡易起案によるものを除く。)の完結日を文書管理システムに登録すること。この場合において、紙決裁起案にあっては、起案用紙に記入すること。 行政文書ファイルのうち電磁的記録によるもの(文書管理システムに保管するものを除く。)については、完結年度又は完結年、行政文書ファイル名、保存期間及び主務課名が容易に確認できるよう適宜の表示の措置をして保管するものとする。ただし、表示が困難なものにあっては、この限りでない。	有	無	無
	石巻市		文書・公印　掲示なし				
	気仙沼市	規程	気仙沼市公文書管理規程	文書は，常に整然と分類して整理し，必要なときに直ちに取り出せるよう保管し，又は保存しておかなければならない。 文書の保管及び保存に当たっては，常に紛失，火災，盗難等の予防に努めるとともに，重要な文書は，非常災害時に際しいつでも持ち出せるように，あらかじめ準備しておかなければならない。	△ 決裁後の電子目録登録か？	無	無
	東松島市	規程	東松島市文書取扱規程	文書は、常に整理し、紛失、災害、盗難等を防止するとともに、重要なものについては、非常災害時に際して支障がないよう、あらかじめ適当な措置を講じておかなければならない。 職員は、文書の整理、整とんに心がけるとともに、担当者において保管する文書は、常に保管場所を明らかにし、私有化してはならない。 第46条　電磁的記録の保存、保管及び整理並びに原本性については、この訓令の規定にかかわらず、その種別、情報化の進展状況等を勘案し、総務課長が復興政策課長と協議し別に定める。	無	無	無
	南三陸町	規程	南三陸町文書取扱規程	主務課長は、文書(電磁的記録を除く。以下この章において同じ。)を未完結文書又は完結文書に区分して、その所在箇所及び処理状況を明らかにしておかなければならない。 重要な文書は、災害に際しいつでも持ち出すことができるように、あらかじめ準備し、紛失、火災、盗難等に対する予防措置を講じなければならない。	無	無	無

c　福島県下４市町

双葉町を除き、文書管理システムを前提とした文書管理規程となっている。

いずれの都市においてもデータのバックアップに関する規定はない。唯一、いわき市において「消滅、改ざん、漏えい等が生じないよう適切に保管しなければならない。」との規定があり、データのバックアップを示唆する役割があるものと思われる。

－浪江町においては、文書に係る情報の開示がなかった。

表－２０　福島県下市町村における文書管理に係る規則・規程等

団体名称		規則・規程等の種別	名称	整理保管に係る規定（主に電磁的記録に係る箇所の概要）	文書管理システム前提の有無	バックアップ関連	
						記述	記述内容
福島県	いわき市	規程	いわき市文書等管理規程	文書等の管理は、文書管理システムにより行うことを原則とする。 取扱責任者は、編冊した完結文書が電子文書であるときは、当該電子文書を文書主管課に引き継ぐまで消滅、改ざん、漏えい等が生じないよう適切に保管しなければならない。 取扱責任者は、編冊した完結文書が紙文書であるときは、保存文書カード（第13号様式）を作成し、当該完結文書及び保存文書カードを文書主管課に引き継ぐまで最良の方法で管理しなければならない。	有	△	消滅、改ざん、漏えい等が生じないよう適切に保管しなければならない。
		規程	いわき市マイクロフィルム文書取扱規程	総務課長は、マスターフィルム文書を長期保存に支障がないように、かつ、安全な方法により管理しなければならない。	無	無	無
	南相馬市	規程	南相馬市文書管理規程	完結文書は、文書管理システムにより保管する。 文書管理システムにより保管できない文書は、課内で保管する。	有	無	無
	双葉町	規則	双葉町文書等管理規則	完結文書のうち電磁的記録は、第1項の規定にかかわらず、保存期間を経過する日までの期間、保管するものとする。	無	無	無
	浪江町		関連情報の掲示なし				

（イ）被災地以外の地域

a　東京都三鷹市

文書管理システムを前提とした文書管理規程となっている。

文書管理としては、データのバックアップにまでは言及されていない。

－三鷹市では、平成 16 年 1 月に ISO27001（ISMS）[32]の認証を取得しており（現在 11 部署(課)）、文書管理とは別の詳細な取り決めを行っている。ISMS の性格上、詳細は公開されていないがすべての情報システムの棚卸等が実施されている。

表－２１　東京都三鷹市における文書管理に係る規則・規程等

団体名称		規則・規程等の種別	名称	整理保管に係る規定（主に電磁的記録に係る箇所の概要）	文書管理システム前提の有無	バックアップ関連	
						記述	記述内容
東京都	三鷹市	規程	三鷹市文書取扱規程	別に定めるものを除き、文書の管理は、総合文書管理システムにより行うものとする。 定例的に処理する同種の文書で相当数量に及ぶものについては、当該文書を管理する課の長（以下「主管課長」という。）は、文書事務主管課の承認を得て、当該文書の管理に当たり、総合文書管理システムによらず帳票（以下「特例帳票」という。）を使用することができる。	有	無	無

[32] 情報セキュリティマネジメントシステム。組織（企業、部、課など）における情報セキュリティを管理するための仕組み。情報セキュリティ管理システムともいう。組織の情報資産について、機密性、完全性、可用性をバランスよく維持し改善することが、情報セキュリティマネジメントシステムの基本コンセプトである。

b　神奈川県横須賀市

関連する規則 2 つと規程 2 つを設けている。

文書管理における全庁の体制とほぼ同等レベルの体制を構築し、統括管理システム、個別管理システム、ネットワーク端末（PC）の管理運用（データ保護等を含む）を行っている。

端末機（PC）レベルでのバックアップの実施を規定しているが、統一的な方法等までは定義されていない。

－横須賀市では、過去に ISO9001[33]の認証を取得した経緯があり、現段階では認証継続はしていないが、情報システム全般に関わる基本ポリシーやドキュメント等の整備を進めて来た経緯がある。

表－２２　神奈川県横須賀市における文書管理に係る規則・規程等

団体名称		規則・規程等の種別	名称	整理保管に係る規定（主に電磁的記録に係る箇所の概要）	文書管理システム前提の有無	バックアップ関連	
						記述	記述内容
神奈川県	横須賀市	規則	公文書管理規則	公文書の作成、保存及び廃棄に関する基本的な事項を定めることにより、公文書の適正な管理を図ること。 事務を適正かつ円滑に処理するために、公文書の所在は把握できる状態にしておかなければならない。	無	無	無
		規程	公文書管理規程	文書管理システム　公文書の起案、決裁、保存等の公文書の管理を行うための電子情報処理組織で総務部行政管理課長(以下「行政管理課長」という。)が管理するものをいう。 文書管理システムに登録した公文書は、文書管理システム内に保存するものとする。この場合において、第1種の公文書は、文書管理システムから印刷物として出力したものを併せて保存しなければならない。	有	無	無
		規則	情報マネジメント規則	セキュリティポリシーとしての規則。 この規則に定めるもののほか、情報システムを用いる場合の運用及び管理の詳細については、別に定める。	無	無	無
		規程	電子情報取扱規程	情報マネジメント規則に定めのあるもののほか、電子情報及び情報システムの管理及び運用については、この規程の定めるところによる。 第3条：情報システムの管理責任 第4条：電子情報の管理責任等 第16条：端末機等の運用管理 第17条：端末機等の管理責任者の業務	－	有	統括管理責任者は、統括管理システムで作成した磁気ファイル中の電子情報のうち、必要があると認めるものについて、バックアップデータを作成しなければならない。 統括管理責任者は、磁気ファイルのうち重要と認めるものについては、耐火金庫等に保管し、予備ファイルを作成し、又はミラーリング等を行って分散保管することができる。 個別管理責任者は、個別管理システムで作成した磁気ファイル中の電子情報のうち、必要があると認めるものについて、バックアップデータを作成することができる。 個別管理責任者は、磁気ファイルのうち重要と認めるものについては、耐火金庫等に保管し、予備ファイルを作成し、又はミラーリング等を行って分散保管することができる。 端末機等の管理担当者は、次に掲げる事項を実施しなければならない。 (1)適時、適切なバックアップデータの作成 (2)保存されている情報の媒体形式、媒体の保管場所、各媒体内のファイル名称の整理、把握

[33] 品質マネジメントシステム関係の国際標準化機構による規格。「ISO 9000s」などとも言う。製造物や提供されるサービスの品質を管理監督するシステムである。

c　兵庫県神戸市

文書管理システムを前提とした文書管理規程となっているが、データのバックアップにまでは言及されていない。

文書管理規程とは異なる「電子計算機処理に係るデータ保護管理規程」について、「保護データ」を定め、それを保全するための諸規程が定められている。

－神戸市では、平成 20 年に ISO27001（ISMS）に準拠したセキュリティポリシー（神戸市情報セキュリティ基本方針）を策定しており、文書管理とは別の詳細な取り決めを行っている。

表－２３　兵庫県神戸市における文書管理に係る規則・規程等

団体名称		規則・規程等の種別	名称	整理保管に係る規定（主に電磁的記録に係る箇所の概要）	文書管理システム前提の有無	バックアップ関連	
						記述	記述内容
兵庫県	神戸市	規程	公文書管理規程	公文書は，常に整理し，紛失，盗難，損傷その他の事故を防止するとともに，重要なものについては，非常災害時の保護にも支障がないよう準備しておかなければならない。 公文書は，原則として，文書管理システムにより公文書の収受，起案，決裁，保存，廃棄その他公文書の管理に関する事務の処理を行うこと等により，適正に管理し，かつ利用しなければならない。 完結公文書(保存期間が1年未満であるものを除く)は，決裁等に係る年月日その他の必要な事項の登録を確認の上，遅滞なく文書管理システムに完結の登録をしなければならない。 完結公文書は，文書管理システムにより保存しなければならない。 ただし，文書管理システムにより保存することができない完結公文書は，次に掲げるところにより速やかに成冊(文書を冊子状に取りまとめることをいう)をしなければならない。	有	無	無
		規程	電子計算機処理に係るデータ保護管理規程	本市の電子計算機処理に係る管理運営について必要な事項を定めることにより，データの保護その他の適正な管理を図り，もって行政の円滑な運営と信頼を確保することを目的とする。	無	有	保護データの指定等:保護管理者は，協議により当該データを保護すべきデータとして指定するものとする。 (1) 個人情報に関するデータ (2) 法令の規定により秘密を守る義務を課されているデータ (3) 部外に知られることが適当でない法人その他の団体に関するデータ (4) 部外に漏れた場合に行政の信頼を著しく害するおそれのあるデータ (5) 滅失し，又は損傷した場合にその復元が著しく困難であるため行政の円滑な運営が妨げられるおそれのあるデータ 保護データに係る記録媒体の管理:保護責任者は，保護データに係る記録媒体の管理については，次に掲げるところによる。 (1) 保管については，帳簿に記録するとともに，施錠して保管した上で，必要に応じて予備ファイルを作成して別個の施設に保管することその他の必要な措置を講ずること。 (2) 公文書管理規程に規定する保存期限の経過等により保管の必要がなくなったときは，速やかに記録の内容を復元できない状態にしての廃棄その他の必要な措置を講ずること。

ｄ　兵庫県西宮市

文書管理システムを前提とした文書管理規程となっているが、データのバックアップにまでは言及されていない。

－西宮市では、ISO27001（ISMS）の認証を取得しており、文書管理とは別の詳細な取り決めを行っている。

表－２４　兵庫県西宮市における文書管理に係る規則・規程等

団体名称		規則・規程等の種別	名称	整理保管に係る規定（主に電磁的記録に係る箇所の概要）	文書管理システム前提の有無	バックアップ関連	
						記述	記述内容
兵庫県	西宮市	規程	西宮市文書取扱規程	文書管理者は、保管文書を文書管理システム又はオープンファイルシステムにより、文書分類表に基づき整理し、保管しなければならない。 収受登録を行った文書等又は起案登録を行った文書若しくは起案した文書で完結したものは、文書管理システムにより作成された電子的なファイルにより編集し、保管しなければならない。 保管文書については、当該文書の完結日の属する年度の翌年度の4月末日までに、保管する保管文書の冊数及び保管場所を文書管理システムに登録しなければならない。 文書（電磁的記録を除く。）のうち、文書管理者が当該文書を保存するうえで適当と認めるものについては、その文書を撮影したマイクロフィルムをその文書に代えて保存することができる。 保存文書は、その保存期間中、総務課長が文書管理システム及び総務課の書庫において、保存し、及び管理する。	有	無	無
		規程	マイクロフィルム方式による文書管理に関する規程	マイクロフィルム方式による文書・図面・図書・資料等の管理について定め。	－	－	－

（２）現行の規則・規程等における特徴

本調査研究において、被災地と被災地以外の地域における現行の規則・規程等における特徴は、次のとおりである。

ア　被災地

現行の「文書管理」制度は、従前からの「紙」をベースとした内容に、電子情報（電磁的記録）の条文を付記しただけの内容となっている。

イ　被災地以外の地域

現行の「文書管理」制度は、従前からの「紙」をベースとした管理を残しつつも、文書管理システムにおける管理を基本として位置付けているとおり、ICT 部門が全庁のデータ（電子文書）の管理・保全に対し、積極的に関与している（ISMS の認証取得や ICT 部門としての規則・規程等の策定等）。

このような地方公共団体にあっては「ICT 部門が、役所の中でどのようなデータがどのように管理されているか」の把握に努めている。

しかしながら、両者ともに文書管理規則・規程等では、データとして存在する文書の保全に関する記述がなく、文書管理主管部局におけるデータ保全への認識が希薄となっている。そのため、文書管理主管部局におけるデータ保全への認識を新たにし、文書管理規則・規程等に定める検討や見直しが必要となる。

（３）現行の規則・規程等における課題

地方公共団体における既存の「文書管理」制度には、バックアップに関する観点

がないことに課題（限界）がある。

文書管理システムが運用されている場合には、ICT 部門等がバックアップ等を実施している自治体が多いが、未導入の自治体においては、PC の管理を含め、基準等が曖昧であり、個別の PC レベルまでを網羅した「データバックアップの統一的な基準がない」点が課題となっている。

当該調査により、「東日本大震災における地方公共団体情報部門の被災時の取組みと今後の対応のあり方に関する調査研究　報告書」で指摘されている「データバックアップの統一的な基準がないばかりか、ICT 部門でさえ、役所の中でどのようなデータがどのように管理されているかを知らない場合もあった。」との内容を、規則・規程面からも裏打ちすることとなった。

３　まとめ－バックアップ・リストア基準の策定－

（１）国における文書管理に係る法令等においてのバックアップの必要性

電子文書は、情報セキュリティポリシーの規程に従い、必要に応じ、パスワードの設定、暗号化、電子署名の付与を行うとともに、バックアップを保存すると定めており、バックアップの必要性が明示されている。

（２）被災地におけるデータのバックアップと被災の状況

被災地においては、住基や税システム等の ICT 部門において管理されているデータは、日次の頻度でテープ等に保存されていたものの、ほとんどが庁舎内保管であったため、庁舎の水没等により、バックアップデータそのものが使用不能となる事態が生じた。

住基や税システム以外の個別システム等の ICT 部門以外の各業務部門において管理されているデータに関しては、各業務部門に管理が委ねられており、ICT 部門が全体を把握することが困難な状況にあった。

また、ローカル PC 等に保存されているデータについては、データバックアップに関する明確な基準がないため、滅失による業務の継続が困難な状況が生じた。

（３）バックアップ・リストア基準の策定の観点

被災の状況を踏まえたバックアップ・リストア基準を策定する際の観点は、以下のとおりである。

－バックアップ媒体等及び保管場所を見直すこと。

－紙データの電子化の推進にあたり、「重要情報」の分類を行うこと及び電子データの「重要情報」の分類の見直しを行うこと[34]。

－バックアップデータ保存の対象を拡げる若しくは明確化すること。

－上記を、全庁的な統一ルールとし、既存の運営体制の機能強化若しくは運用・チェック機能を有する責任体制を構築すること。

（４）新たなバックアップ・リストア基準の対象

ア　システムとして管理されている電子データ

前述したとおり、自治体における既存の「文書管理」制度には、バックアップに関する観点がないことに課題（限界）があるため、既存の文書管理規程等を見直すこと及び情報の更新頻度等を踏まえたバックアップ頻度を明記することなど、バックアップデータの取得方法や保管場所、保管方法等についての見直しを図ることが必要である。

また、今回の調査等により、業務部門が管理するシステムまでを網羅した「データバックアップの統一的な基準がない」点が課題となっているため、各業務部門において管理されているデータの状況把握を、ICT 部門がとりまとめ、定期的

[34] あくまですべてのデータをバックアップするのが望ましいが、予算等との兼ね合いで困難な場合は、重要情報レベルの高いものからバックアップする。

に把握し、その情報を更新することを義務化する規定となるよう、見直しを図ることが必要である。

イ　ローカル PC 等に保存されているデータ（シンクライアントやファイルサーバ運用団体を除く）

前述と同じく、個別の PC レベルまでを網羅した「データバックアップの統一的な基準がない」点が課題となっているため、各所属（課等）におけるデータの把握及びバックアップすべきデータの「重要情報」の分類を行い、既存の文書管理規程等を見直すことや、情報の更新頻度等を踏まえたバックアップ頻度を明記することなど、バックアップデータの取得方法や保管場所、保管方法等についての見直しを図ることが必要である。

参考資料 収集文献

（１）国

ア　総務省（LASDEC 含む）

（ア）東日本大震災を契機とした情報行動の変化に関する調査結果
http://www.soumu.go.jp/iicp/chousakenkyu/data/research/survey/telecom/2012/megaquake311-a.pdf

（イ）情報通信審議会 情報通信政策部会研究開発戦略委員会報告書（案）
～震災からの復興と日本の再生に向けたICTの研究開発戦略について～

（ウ）防災対策推進検討会議　中間報告
～東日本大震災の教訓を活かし、ゆるぎない日本の再構築を～
平成24年3月7日　中央防災会議　防災対策推進検討会議
http://www.soumu.go.jp/main_content/000156847.pdf

（エ）知識情報社会の実現に向けた情報通信政策の在り方　＜平成23年諮問第17号＞　報告書
（第一次取りまとめ）～震災からの復興と日本の再生に向けたICTの研究開発戦略について～

（オ）災害に強い電子自治体に関する研究会における主な意見・論点
http://www.soumu.go.jp/main_content/000156844.pdf

イ　文部科学省

（ア）東日本大震災からの復旧・復興の取組に関する中間的な検証結果のまとめ（第一次報告書）の概要
http://www.mext.go.jp/a_menu/saigaijohou/syousai/__icsFiles/afieldfile/2011/12/26/1314588_1_1.pdf

ウ　厚生労働省

（ア）厚生労働省での東日本大震災に対する対応について（報告書）　平成 24 年 7 月　厚生労働省
http://www.mhlw.go.jp/iken/dl/as-vol8-honbun.pdf

（２）地方公共団体

ア　岩手県

（ア）いわて復興レポート
http://www.pref.iwate.jp/view.rbz?cd=40700&ik=0&pnp=14

（イ）「東日本大震災津波に係る災害対応検証報告書」　H24.2.16　岩手県
http://ftp.www.pref.iwate.jp/view.rbz?nd=4158&of=1&ik=1&pnp=4157&pnp=4158&cd=37172

イ　福島県

（ア）東日本大震災復旧復興対策特別委員会調査報告書
http://www.pref.fukushima.jp/gikai/fu_5/02/data/201109/iken/2309tokubetuiinkaihoukokusho.pdf

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。

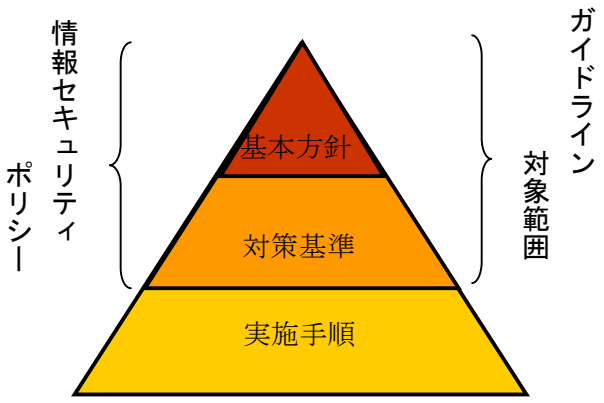
この基本方針に基づき、すべての情報システムに共通の情報セキュリティ対策の基準を定めるのが「対策基準」である。

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。

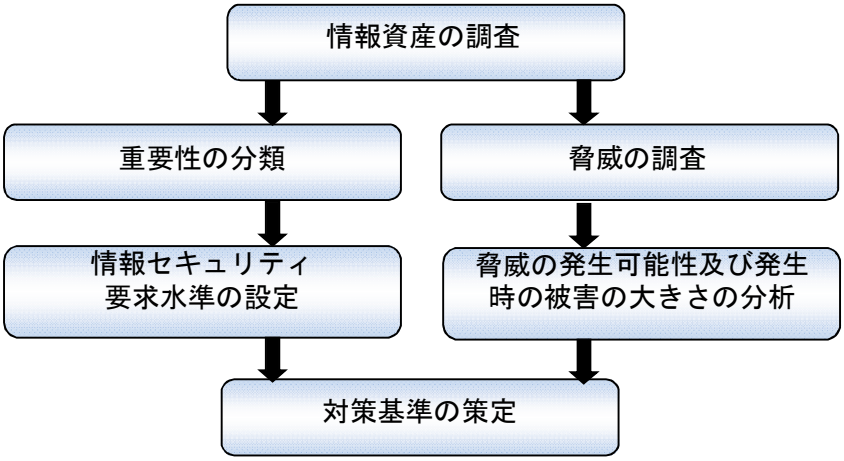
（ウ）リスクの大きさがセキュリティ要求水準を下回るよう対策基準を策定し、適切なリスク管理を行う。

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。

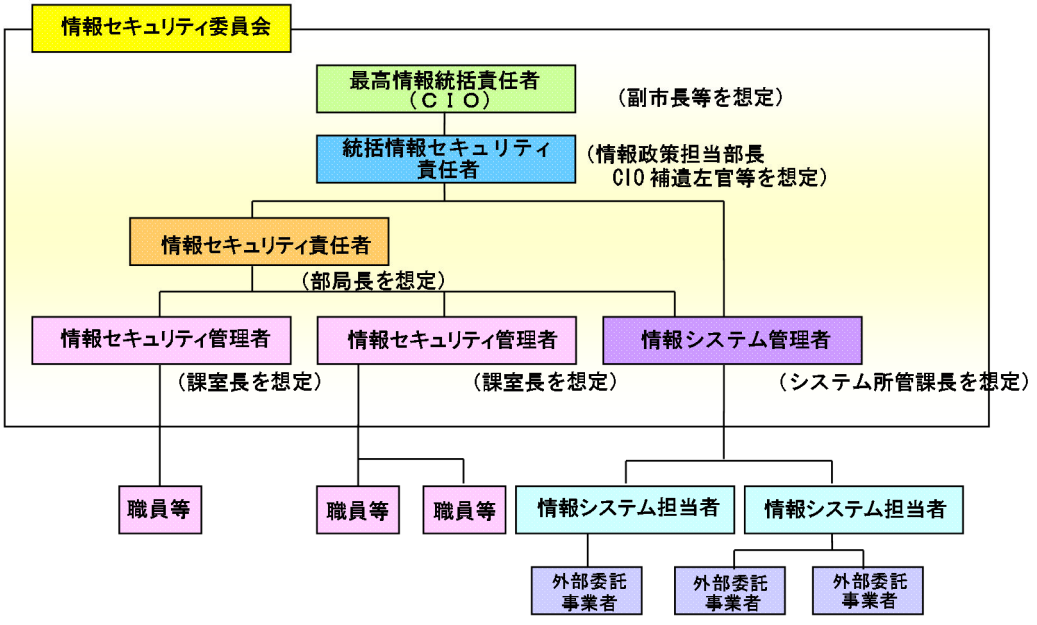
表－２５　情報資産の種類と例

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。

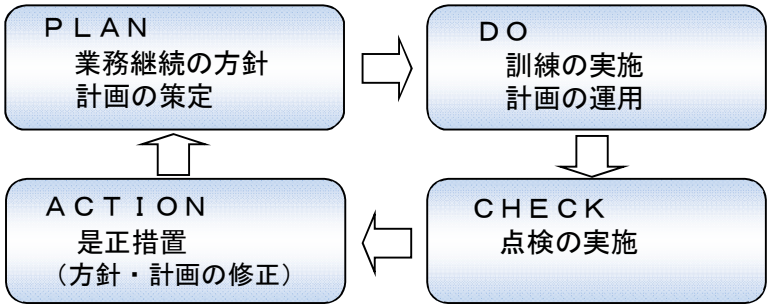
エ　計画の継続的改善

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

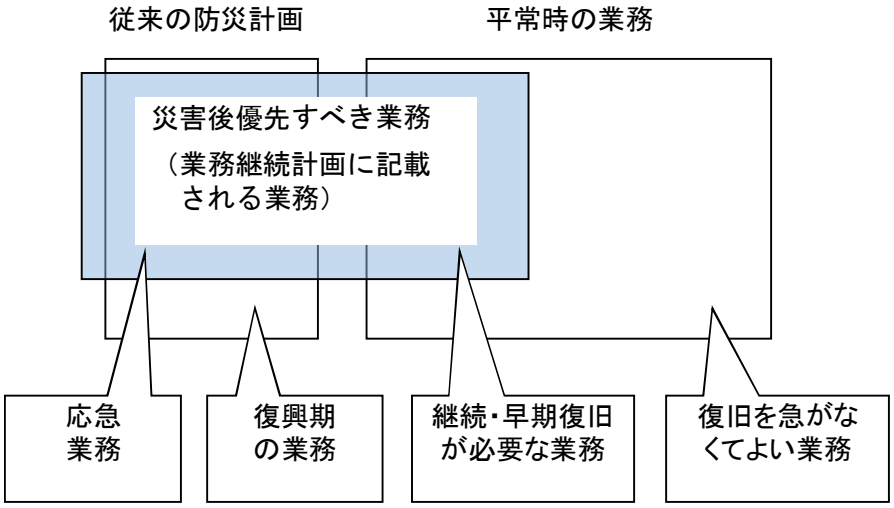
b　外部への依存

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。

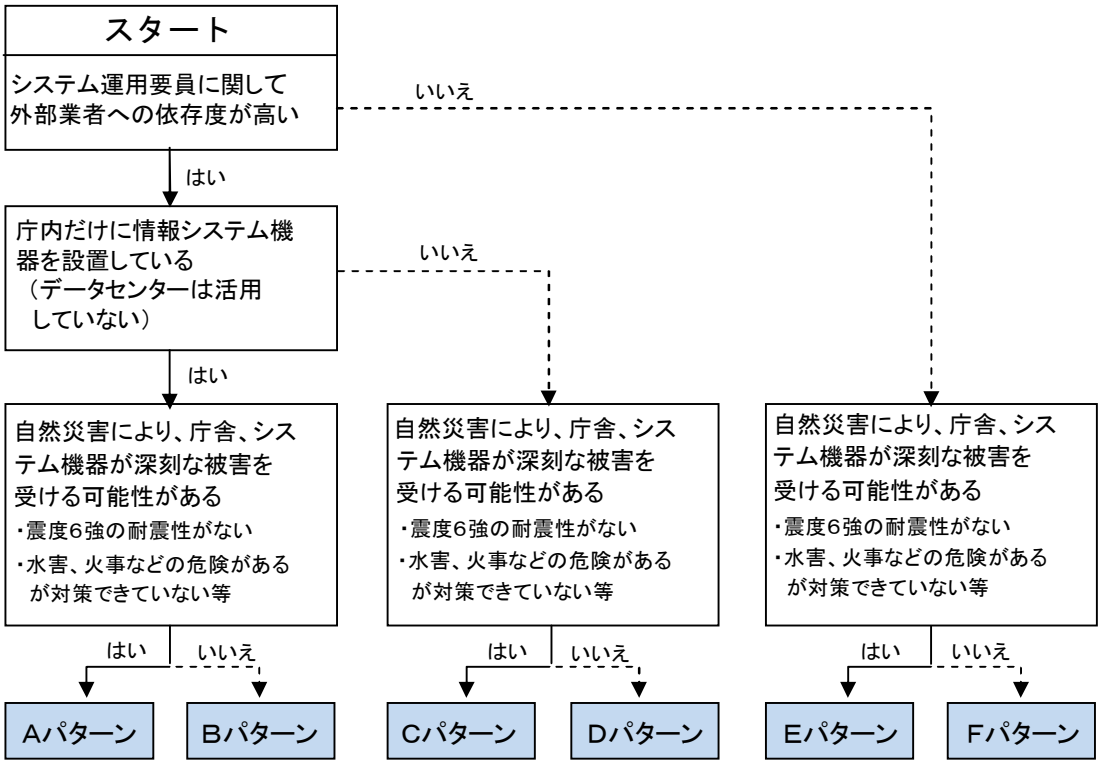
（ウ）第 3 部　本格的な BCP の策定と全庁的な対応との連動

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

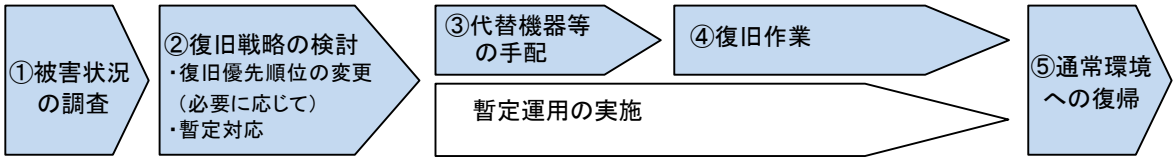
a　手順１　事前対策の検討

（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。

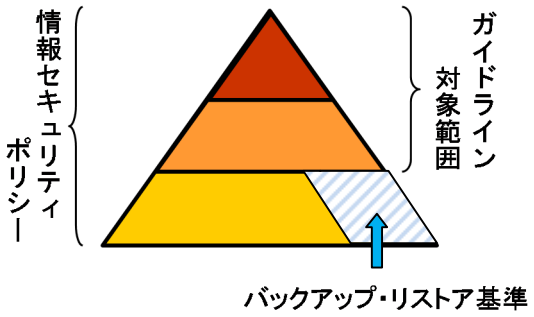
しかし、必ずしもすべての地方公共団体では、そのような従前の準備、特に被災時に即座に利用できる具体的な手順等が定められていないことが、同様に明らかになった。

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。

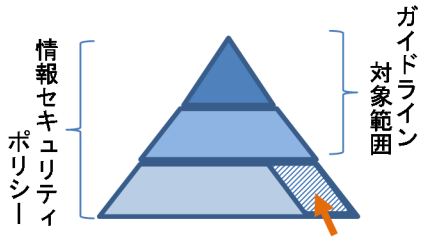
既に「情報セキュリティポリシー」が策定されている場合には、実施手順の１つとしてバックアップ・リストア基準を新たに設けていただきたい。なお、既存の実施手順を見直す場合は、本章を参考にしてほしい。



（３）バックアップ・リストア基準の作成方針

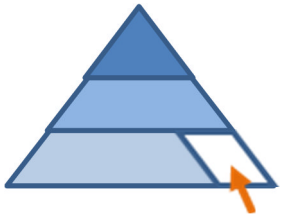
今回実施した各種調査により、情報セキュリティポリシーやその実施手順の整備状況等により、地方公共団体は次のアからウの 3 種類に区分される。

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



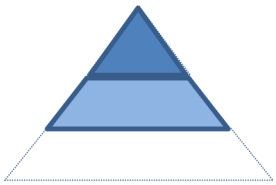
バックアップ・リストア基準〔相当〕あり

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

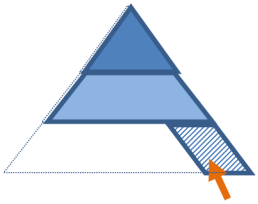
ウ　情報セキュリティポリシーを策定しているが、下位の実施手順を定めていないケース



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。

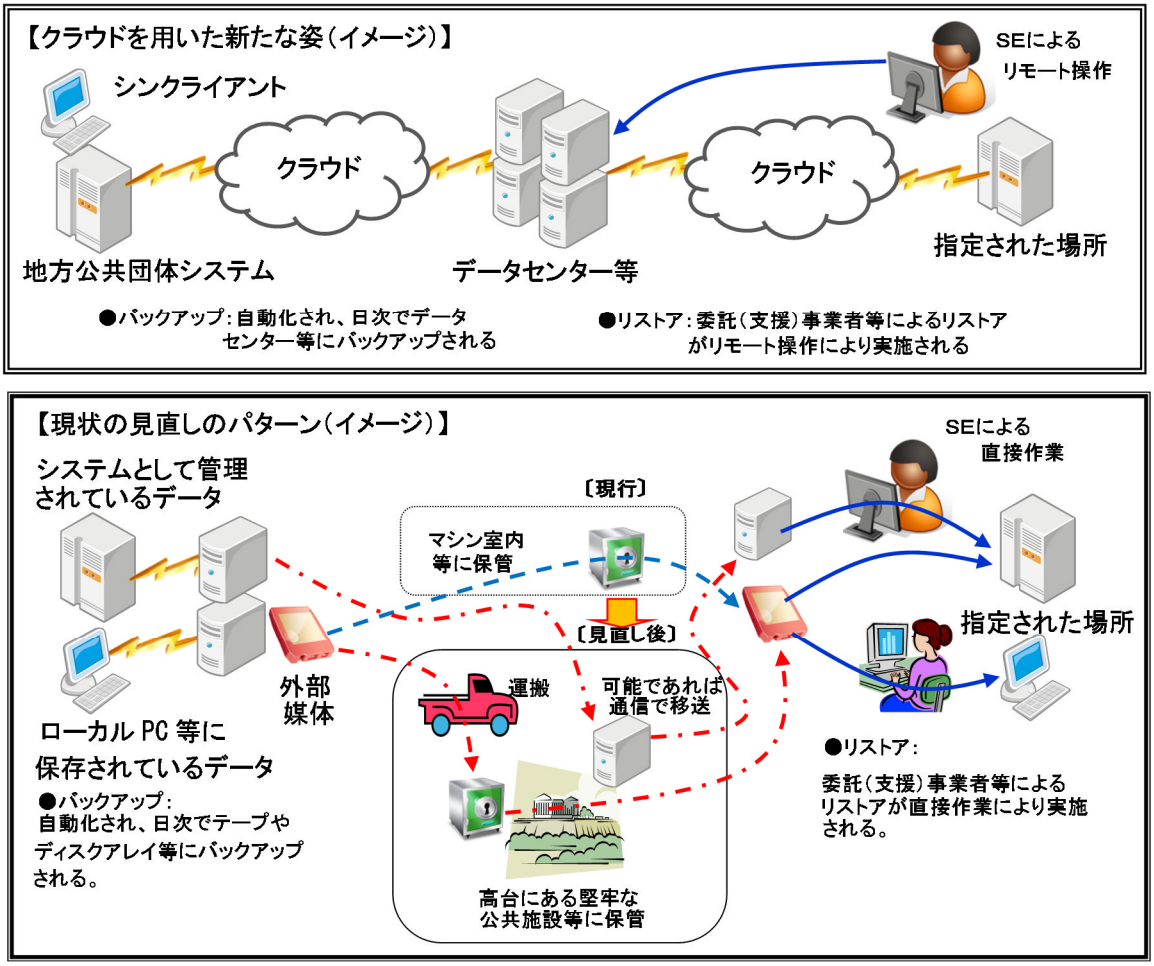
c　情報システム（システムで扱うデータを含む）のデータセンター移行の検討

（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

第３章　ICT 部門におけるバックアップサイトの利活用方策

前章では、行政データのより信頼性の高い管理を行うために、管理・運用面からの方策としてバックアップ・リストア基準の策定を行った。平常時には、このような規程に則したデータ管理が求められるが、これを支えるものとして、行政データをバックアップするインフラ及びツールが必要である。

本章では、地方公共団体自身が被災した場合の業務継続について、行政データのバックアップサイトの利活用形態及びその有効性、運用性等を検証する。なお、バックアップサイトの検証として模擬環境による実証実験を実施する。

第１節　モデルケース選定

１　地方公共団体におけるバックアップサイトの構成要素

地方公共団体においては、団体規模や財政状況等に応じ、様々な形態で行政データをバックアップしている。以下に地方公共団体におけるバックアップサイトの形態のうち、代表的な想定事例を示す。

〔想定事例 1〕本庁舎内にバックアップデータを媒体で保管する。

・本庁舎内のサーバ室又は会計課等が管理する耐火金庫等にバックアップデータを格納した媒体を保管する。

〔想定事例 2〕自地方公共団体内の支所等（本庁舎外）にバックアップデータを媒体又はネットワーク経由で保管する。

・自地方公共団体内の支所等（本庁舎外）の別施設にバックアップデータを格納した媒体を保管する。
・地方公共団体の規模や状況によっては、支所等の別施設にあるサーバ室等にネットワーク経由によりバックアップを実施し、サーバ室内等でバックアップデータを格納した媒体又はディスクを保管する。

〔想定事例 3〕他地方公共団体にバックアップデータを媒体又はネットワーク経由で保管する。

・他地方公共団体の庁舎等にバックアップデータを格納した媒体を保管する。
・地方公共団体の規模や状況によっては、他地方公共団体の庁舎等にあるサーバ室等とネットワーク経由によりバックアップを実施し、サーバ室内等でバックアップデータを格納した媒体又はディスクを保管する。

〔想定事例 4〕民間事業者にバックアップデータを媒体で保管する。

・通常は庁舎内にバックアップデータを格納した媒体を保管し、月次等のタイミングでその時点の最新のバックアップデータを格納した媒体を民間事業者の保管庫（専用の倉庫）等に保管する。

〔想定事例 5〕民間事業者にバックアップデータをネットワーク経由で保管する。

・民間事業者が提供している ASP サービス等を利用して、民間事業者のデータセンターにネットワーク経由によりバックアップを実施し、データセンターでバックアップデータを格納した媒体又はディスクを保管する。
・民間事業者が提供しているホスティングサービス等を利用して、民間事業者のデータセンターにシステムを構築し、ネットワーク経由で利用する。バックアップはネットワーク経由で処理を実行し、データセンター内でバックアップデータを格納した媒体又はディスクを保管する。
・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、庁舎内に保管しているケースもある。

〔想定事例 1〕～〔想定事例 5〕で示したバックアップサイトを構成する主要な要素を以下に示す。

表－３４　**地方公共団体におけるバックアップサイトの構成要素**

バックアップサイトの種類		構成要素			
		バックアップ方法	**バックアップデータの保管場所**	**バックアップサイトの共同利用**	**民間事業者の利用**
想定事例 1	本庁舎内にバックアップデータを媒体で保管する。	媒体送付	本庁舎内	単独利用	民間利用なし
想定事例 2	自地方公共団体内の支所等（本庁舎外）にバックアップデータを媒体又はネットワーク経由で保管する。	媒体送付又はネットワーク経由のデータ転送	自地方公共団体（支所）	単独利用	民間利用なし
想定事例 3	他地方公共団体にバックアップデータを媒体又はネットワーク経由で保管する。	媒体送付又はネットワーク経由のデータ転送	他地方公共団体	共同利用	民間利用なし
想定事例 4	民間事業者にバックアップデータを媒体で保管する。	媒体送付	自地方公共団体（庁舎外）又は他地方公共団体（庁舎外）	単独利用又は共同利用	民間利用あり
想定事例 5	民間事業者にバックアップデータをネットワーク経由で保管する。	ネットワーク経由のデータ転送	自地方公共団体（庁舎外）又は他地方公共団体（庁舎外）	単独利用又は共同利用	民間利用あり

２　ケース設定

前述の地方公共団体におけるバックアップサイトの構成要素を踏まえて、行政データをバックアップする上で、災害に強いバックアップサイトを構築するためには、以下の点が求められると考えられる。

■自地方公共団体外の遠隔地に媒体送付又はネットワーク経由のデータ転送によりバックアップサイトを置く。
（災害への強さ：他地方公共団体＞自地方公共団体（支所・庁舎外）＞本庁舎内）
■地方公共団体と同等またはそれ以上のセキュリティレベルを確保する。
（セキュリティレベルの高さ：民間利用あり≧民間利用なし）
■ネットワーク利用によりバックアップサイトの運用を省力化・迅速化する。
（バックアップ・リストア処理の柔軟さ：ネットワーク経由のデータ転送＞媒体送付）

また、上記に加えて、ネットワーク経由による災害に強いバックアップサイトの普及を推進するためには、以下の点に留意する必要がある。

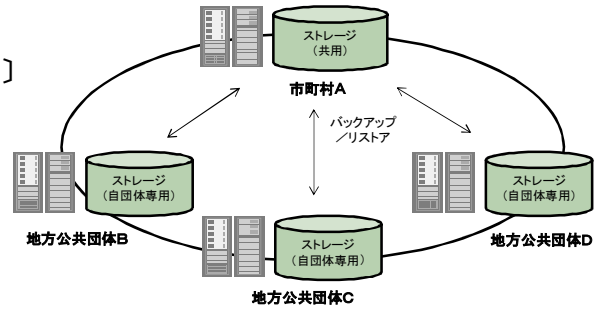
■複数の地方公共団体でバックアップサイトを共同利用する。
（コスト軽減に係るスケールメリット：共同利用＞単独利用）

上記の点を考慮すると、バックアップサイトとして使用するシステム等に応じて、以下のケースを基本型として想定した。なお、これらはあくまで、上記の点を実現することに着目し、その実現性や有効性等を比較検討するために想定した形態であり、バックアップサイトとしては、これら以外にも多様な形態[50]が考えられる。

---

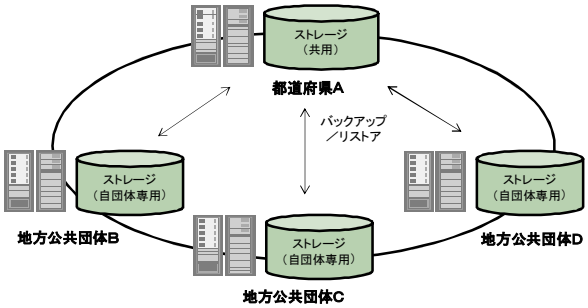
[50] バックアップサイトの実例としては、次のような事例がある。
・釜石市では、基幹系システムのバックアップサイトとして北九州市のクラウド基盤を利用している。また、被災時に最低限の業務ができるよう、データセンターからネットワーク経由で一部のバックアップデータを転送し、庁舎内に保管している。詳細は「第１章　第１節－３－（２）オ（イ）自治体クラウドの仕様」を参照のこと。
・岩手県では、県内の希望市町村に対して「行政情報データバックアップサービス」を提供するためのシステム構築を進めており、平成 25 年 4 月からサービスを開始する予定である。本サービスは、県内のデータセンターにシステムを設置し、市町村が自団体のバックアップ用サーバに格納した行政情報データを、ネットワーク経由で日次バックアップするものである。また、市町村の業務システム用サーバが被災した場合に貸し出す代替機器を配備するなど、市町村の行政機能を迅速に回復できる体制を整えている。
・新潟県聖籠町、出雲崎町、関川村のグループ（当センターの平成 24 年度自治体クラウド・モデル団体支援事業のモデル団体）では、自治体クラウドを構築したデータセンターのほかに、各団体において他の 2 団体のバックアップデータを相互保管している。それにより、被災時にどちらの団体に行っても、自団体の必要最低限の業務の運用が可能としている。

〔ケース１〕



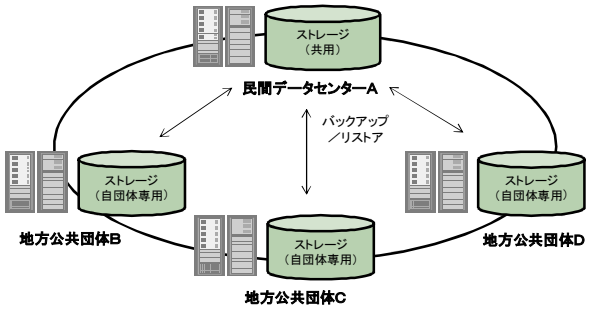
図－３９　市町村が自庁舎施設内に設置するシステムを、他の団体が
バックアップサイトとして共同利用するイメージ

〔ケース２〕



図－４０　都道府県が自庁舎施設内に設置するシステムを、当該都道府県内
の団体（市町村）がバックアップサイトとして共同利用するイメージ

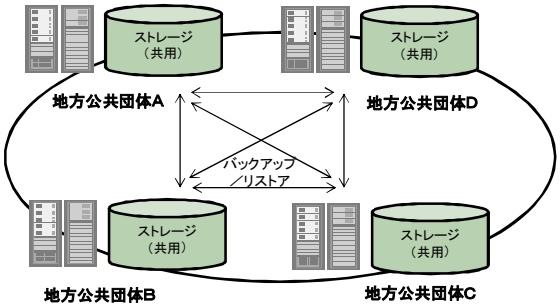
〔ケース３〕



図－４１　民間データセンター[51]を、地方公共団体がバックアップサイト
として共同利用するイメージ

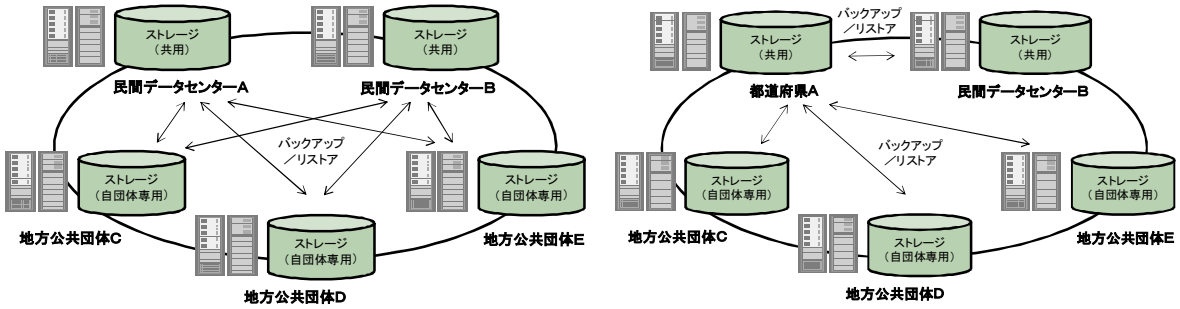
[51] 地方公共団体（都道府県あるいは市町村）が民間データセンターを利用して、バックアップサイトとして使用する場合は、データの所在の明確化、初期・運用コスト及びセキュリティレベルが自庁舎施設内に設置するシステムを利用する場合と異なることから、〔ケース３〕民間データセンターの共同利用に区分する。

〔ケース４〕



図－４２　複数の地方公共団体が自庁舎施設内に設置するシステムを、
バックアップサイトとして相互に利用するイメージ
（クラウド型バックアップサイト）

上記のケース以外に、信頼性を向上させるために同種の 2 つのバックアップサイトを利用するケース（次左図）や、異なる種類のバックアップサイトを利用し、一方はバックアップサイト全体のバックアップとするケース（次右図）など、上記の 4 つの組み合わせによる様々なケースが想定される。



図－４３　想定される様々なバックアップサイトのケース例

３　評価項目

バックアップサイトを、実際に地方公共団体が使用するためには、以下の点について考慮する必要がある。

・バックアップサイトのセキュリティ
・バックアップサイトの保守・運用に係る作業負荷
・バックアップサイト構築及び運用に係る費用
・個人情報の保管先として承認の容易さ

団体規模も財政状況も個々に事情が異なる地方公共団体に対して、バックアップサイト構築及び運用を検討する際の選択肢の一つとなるには、個人情報等の秘匿性の高い情報を保管するためのセキュリティの確保に加えて、運用及び利用が容易であることやコストの縮減に配慮することが求められる。

また、地方公共団体が扱う情報は個人情報など、特定の法令等により取扱等が規定されているものがある。そのような情報を、自庁外に保管する場合は、相応の手続きや承認等が必要であり、その対応の容易さも考慮する必要があると考えられる。

なお、複数の団体が共同利用するこのようなバックアップサイトを運用（情報システムの保守・運用を除く）するためには、特定の組織が一定の責任を負って管理する必要があると考えられる。ただし、その組織の整備や維持・運用に係るコストは、バックアップサイトの規模や具備する機能、実施する管理業務、責任範囲や内容等に大きく依存し、前出のようなサイトの形態（ケース）だけから判断することが困難なため、本評価項目には含めていない。

４　評価結果

以下では、地方公共団体（都道府県あるいは市町村）、民間データセンターそれぞれについて、バックアップサイトとして共同利用する場合の特性等を明らかにするために、前出の 4 つのケース（基本型）を評価・検討した。

その結果を次表に示す。本検討において設定した評価項目のもとでは、ケース 4 が相対的に高い評価となった。同じ地方公共団体のシステムで構成されるケース 1 及びケース 2 との評価の差は、特に運用コストが低いと推測されるためである。

地方公共団体に大規模なデータセンターを構築することとなるケース 1，2 に比べて、現行と比べて大差ない費用の範囲でケース 4 は運用することができるものと想定される（なお、本検討では、これらの初期コストは、顕著な差がないものとして同じ評価とした。精査が必要であるが、初期コストはケース 4 が少ないものと推測される）。

以上の評価結果から、複数の地方公共団体が、一つのシステム（またはデータセンター）を共同利用せずに、地方公共団体のシステムを相互に共同利用するケース 4（クラウド型バックアップサイト）を対象とした実証実験を実施し、その実現性、実用性及び運用性に関する検討を行うこととした。

表－３５　評価表

バックアップサイトの種類		評価項目				
		セキュリティ	保守・運用の作業負荷	コスト（バックアップサイト全体に係るコスト）		個人情報の保管先としての承認の容易さ
				初期	運用	
		システムやネットワークのセキュリティについては、各ケースにおける顕著な差異はないと考えられる。 しかし、その事業目的及び使用目的に特化した施設・設備を整備し、運用を行う民間のデータセンターが、市町村や都道府県が有するシステムを設置している施設やその運用に比べ、総じて相対的にレベルが高いと考えられる。	市町村や都道府県のシステムは自庁舎施設内若しくは民間データセンターに設置している、いずれの場合にも、保守・運用を、ベンダー等に委託して実施している場合が多い。これらが主体となって整備するバックアップサイトは、ケースに関わらず、外部（民間）に委託して実施されるものと考えられる。そのため当該評価項目では、ケース間に顕著な差はないものと考えられる。	民間データセンターはその利用形態により、ユーザの H/W の初期投資がほぼ不要な場合（ASP サービス等）と、必要な場合（ホスティングサービス等）により大きく異なると考えられる。また、一元的にバックアップデータを集約して保管する H/W や S/W を整備する場合（ケース 1, 2）に比べ、個別にデータストレージを整備する場合（ケース４）の方が、初期コストが小さくなる。	左記評価項目「保守・運用の作業負荷」と同様な理由により、ケース間に、基本的な顕著な差がないもとを考えられる。 なお、この運用コストには、バックアップサイト全体を管理する主体（組織）に関するものは含めていない（詳細は本文参照）。	民間データセンターと比べ、類似の条例等に基づいて、個人情報を管理・運用している他の市町村や都道府県に保管する場合の方が、民間データセンターに保管する場合に比べ、個人情報審査会や議会等の承認が得やすいものと考えられる。
ケース１	市町村が自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。	○	○	△	○	◎
ケース２	都道府県が自庁舎施設内に設置するシステムを、当該都道府県内の団体（市町村）がバックアップサイトとして共同利用する。	○	○	△	○	◎
ケース３	民間データセンターを、地方公共団体がバックアップサイトとして共同利用する。	◎	○	◎（ASP サービス等の場合） △（ホスティングサービス等の場合）	○	△
ケース４	複数の地方公共団体が自庁舎施設内に設置するシステムを、バックアップサイトとして相互に利用する（クラウド型バックアップサイト）。	○	○	○	○	◎

〔凡例〕　◎：相対的に優れている　＞　○　＞　△：相対的に劣っている

第２節　クラウド型バックアップサイトの検討

１　モデルケース設定

（１）バックアップサイトの構築及び運用に係る具体的な枠組み

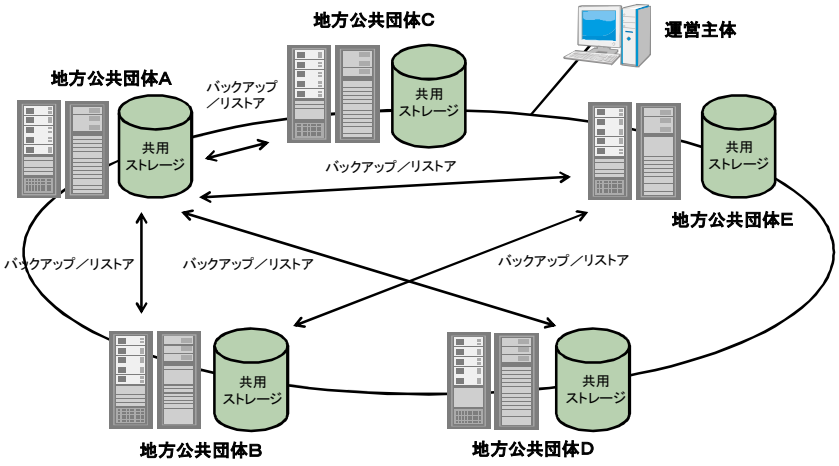
バックアップサイトの構築及び運用に係る考慮点を踏まえて、具体的な枠組みを以下のように考えた。

・地方公共団体が持つ共用ストレージの集積をバックアップサイトとしてバックアップデータを相互に保管し合う。バックアップサイトに参加できるのは地方公共団体等の行政機関に限定することで、バックアップサイトをデータセンターに委託する場合と比べて、バックアップサイトの構築及び運用に係る交渉、手続き等が容易に進むと考えられる。
・バックアップサイトに参加している地方公共団体の共用ストレージを一元的に管理する運営主体を設ける。バックアップデータの保管、履歴管理、リストア等を運営主体が実施することで、地方公共団体がバックアップサイトを利用する作業負荷は、自らバックアップサイトを運用する場合と比べて小さくなると考えられる。
・個人情報などのデータを扱うことが予想されるため、利用する技術及び運用において高い秘匿性を担保する。
・地方公共団体は、バックアップサイトとして自らが提供する共用ストレージについて、新たに専用のストレージを調達するか若しくは既存の庁内ストレージの一部を利用する。地方公共団体における責務や準備すべきストレージ容量（例えば、バックアップを依頼するのと同程度の容量を提供すべき容量とする）等の運用上の詳細は、運営主体が中心となって整備し、個々の地方公共団体と運営主体との間で覚書等による確認を実施する。

（２）モデルケースの基本コンセプト

バックアップサイトの構築及び運用に係る具体的な枠組みを踏まえて、以下のようなバックアップサイトのモデルケースを考えた。

【基本コンセプト】
- 地方公共団体は自らの共用ストレージを他の地方公共団体のバックアップサイトとして提供する。その一方で、他の地方公共団体の共用ストレージに自らのバックアップデータを保管する。
- 運営主体はバックアップサイトにおけるすべての共用ストレージを管理する。
- バックアップサイトにおいては暗号化等を施し、バックアップデータの秘匿性を担保する。



図－４４　モデルケースとするバックアップサイトの概念図

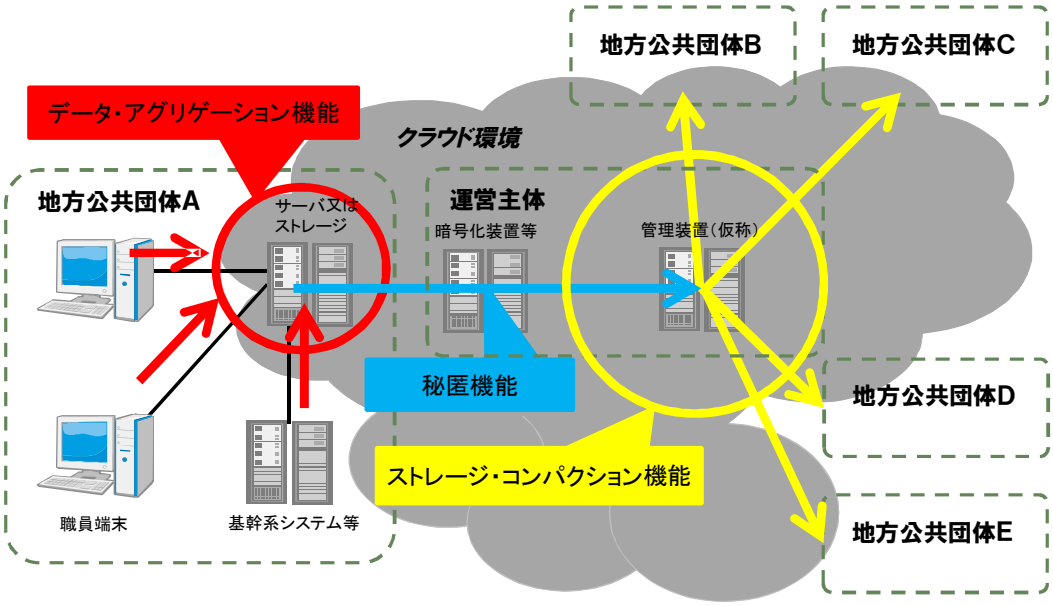
２　バックアップサイトを構成する機能

（１）基本的な考え方

地方公共団体のクラウド型バックアップサイトは、バックアップ対象のデータを設定したディレクトリに集合させてバックアップデータを作成する機能（データ・アグリゲーション（Data Aggregation）機能）と、バックアップデータの秘匿性を担保する機能（秘匿機能）、各地方公共団体のバックアップサイトの状態監視とバックアップデータの保管先を管理する機能（ストレージ・コンパクション（Storage Compaction）機能）によって構成される。

データ・アグリゲーション機能は地方公共団体に、秘匿機能及びストレージ・コンパクション機能は運営主体に実装する。

バックアップサイトを構成する機能のイメージを以下に示す。



図－４５　バックアップデータをバックアップする流れ

バックアップ時には、各地方公共団体においてデータ・アグリゲーション機能を用いて作成したバックアップデータを、運営主体において秘匿機能を用いて秘密分散技術等による暗号化を行った上で、ストレージ・コンパクション機能を用いて他の地方公共団体に分散配置する。

リストア時には、運営主体においてストレージ・コンパクション機能を用いてバックアップデータを収集し、秘匿機能を用いて暗号化を解除して、バックアップデータを復元した上で、指定する地方公共団体の空きストレージに格納（再配置）する。

（２）機能概要

ア　データ・アグリゲーション機能

（ア）機能概要

ICT 部門及び個々の職員が管理している電子データを集合させてバックアップデータを作成する。

バックアップデータの作成方法としては、設定したディレクトリに格納されたすべてのデータを抽出してバックアップデータを作成する方法と、データの作成日時等をキーとして基準日時以降に更新（追加、変更及び削除）されたデータを抽出してバックアップデータを作成する方法がある。

（イ）機能一覧

データ・アグリゲーション機能の一覧を以下に示す。

表－３６　データ・アグリゲーション機能一覧

No.	機能区分[52]		機能
	基本	付加	
1	○		バックアップの種類（フルバックアップ、差分バックアップ、増分バックアップ）を選択する
2	○		バックアップを実施するスケジュールを設定する
3		○	バックアップを実施するスケジュールをスケジュール管理ソフトウェアと連動させる
4	○		設定したサイトのディレクトリに存在するデータからバックアップデータを作成する
5	○		作成したバックアップデータを設定したディレクトリに格納する
6	○		差分バックアップ、増分バックアップの基準日時を設定する
7	○		データの作成日時等をキーとして基準日時以降に追加、更新及び削除されたデータをバックアップして設定したディレクトリに格納する
8	○		外部媒体へのデータの書出し及び読込みを行う
9	○		設定したディレクトリに格納したデータを削除する
10	○		設定したディレクトリに格納されたデータを暗号化する
11	○		設定したディレクトリに格納され、暗号化されたデータから元のデータをリストアする
12		○	秘匿処理を実施するスケジュールを設定する
13		○	秘匿処理を実施するスケジュールをスケジュール管理ソフトウェアと連動させる

[52] 基本（機能）とはバックアップサイトを実現するための必要機能、付加（機能）とはセキュリティレベル及び運用性を向上させるための機能である。

（ウ）機能の実現方法

データ・アグリゲーション機能の実現方法を以下に示す。

表－３７　データ・アグリゲーション機能の実現方法

No.	利用する製品 及びサービス	実現方法
1	アプリケーションソフトウェア	バックアップソフトウェア等の機能を利用して、バックアップ対象とするデータを抽出してバックアップデータを作成し、設定したディレクトリに格納する。フルバックアップ、差分バックアップ、増分バックアップが実施可能 （前頁の機能一覧 No.1～2、4～9 に相当、一部製品は機能 No.10～11 にも対応） 【製品例】 （バックアップソフトウェア） ・Acronis TrueImage ・Symantec Backup Exec ・CA ARC serve Backup ・JP1/VERITAS NetBackup　など
2	文書管理システム （アプリケーションソフトウェアとの組合せ）	文書管理システムで保存しているデータを利用する（文書管理システム単体で実装するとフルバックアップしか実行できなくなるため、運用性を考慮するとデータ・アグリゲーション機能を有するアプリケーションソフトウェアとの組合せが望ましい）
3	ファイルサーバ （アプリケーションソフトウェアとの組合せ）	ファイルサーバで保存しているデータを利用する（ファイルサーバ単体で実装するとフルバックアップしか実行できなくなるため、運用性を考慮した場合にはデータ・アグリゲーション機能を有するアプリケーションソフトウェアとの組合せが望ましい）
4	シンクライアントシステム （アプリケーションソフトウェアとの組合せ）	シンクライアントシステムで保存しているデータを利用する（ファイルサーバ単体で実装するとフルバックアップしか実行できなくなるため、運用性を考慮した場合にはデータ・アグリゲーション機能を有するアプリケーションソフトウェアとの組合せが望ましい）
5	クラウドストレージ	クラウド環境上にデータを保管してデータセンターでバックアップを実施する

イ　秘匿機能

（ア）機能概要

秘密分散機能等による暗号化技術によって、第三者に通信内容又は保管する文書の内容が知られないようにする。

（イ）機能一覧

秘匿機能の一覧を以下に示す。

表－３８　秘匿機能一覧

No.	機能区分		機能
	基本	付加	
1	○		設定したディレクトリに格納されたデータを暗号化する
2	○		設定したディレクトリに格納され、暗号化されたデータから元のデータをリストアする
3	○		設定したサイトのディレクトリにデータを格納する
4	○		設定したサイトのディレクトリからデータを取得する
5	○		設定したディレクトリに格納されたデータを秘匿化した上で複数のデータに分割する（秘密分散機能[53]）
6	○		設定したディレクトリに格納され、秘匿化して複数に分割したデータから元のデータをリストアする（秘密分散機能）
7	○		秘匿化する際にデータを分割する数を設定する（秘密分散機能）
8	○		リストアに必要となる分割したデータの数を設定する（秘密分散機能）

（ウ）機能の実現方法

秘匿機能の実現方法を以下に示す。

表－３９　秘匿機能の実現方法

No.	利用する製品 及びサービス	実現方法
1	アプリケーションソフトウェア	バックアップソフトウェア、暗号化ソフトウェア、秘密分散ソフトウェア等の機能を利用してバックアップデータの秘匿性を担保する 【製品例】 （バックアップソフトウェア） ・Acronis TrueImage ・Symantec Backup Exec ・CA ARC serve Backup ・JP1/VERITAS NetBackup　など （秘密分散ソフトウェア） ・SECLANCER　など

[53] 秘密分散機能については、「（章末）参考資料　秘密分散機能」を参照のこと。

ウ　ストレージ・コンパクション機能

（ア）機能概要

クラウド環境上の地方公共団体から提供されたバックアップサイトの死活状況、サーバ又はストレージの空き容量を監視する。

地方公共団体と運営主体との間でバックアップデータの取得及び再配置を行い、バックアップデータの格納先を一元的に管理する。

（イ）機能一覧

ストレージ・コンパクション機能の一覧を以下に示す。

表－４０　ストレージ・コンパクション機能一覧

No.	機能区分		機能
	基本	付加	
1	○		クラウド環境上の各地方公共団体のバックアップサイトを死活監視する
2	○		クラウド環境上の各地方公共団体のバックアップサイトに配置したサーバ又はストレージの容量を監視する
3	○		監視状況（死活状況、サーバ又はストレージ容量等）を運営主体に通知する
4	○		監視を実施するスケジュールを設定する
5	○		クラウド環境上に設定したディレクトリにデータを格納（再配置）する
6	○		地方公共団体のバックアップサイト上に設定したディレクトリからデータを取得する
7	○		クラウド環境上に設定したディレクトリに格納したデータを削除する
8	○		バックアップデータの取得・再配置の履歴を過去分にわたり履歴管理する（取得元と再配置先の地方公共団体を管理する）
9		○	履歴情報をキーワード検索する
10		○	各地方公共団体における共用ストレージを始めとするサーバ機器等の稼働環境（OS、業務アプリケーションソフトウェア等）を管理する[54]

[54] 地方公共団体ごとの稼働環境（OS、業務アプリケーションソフトウェア等）を管理することで、ある地方公共団体の業務環境が滅失した場合に、稼働環境が同一若しくは類似した地方公共団体に復元環境を構築し、業務の継続を容易とする。

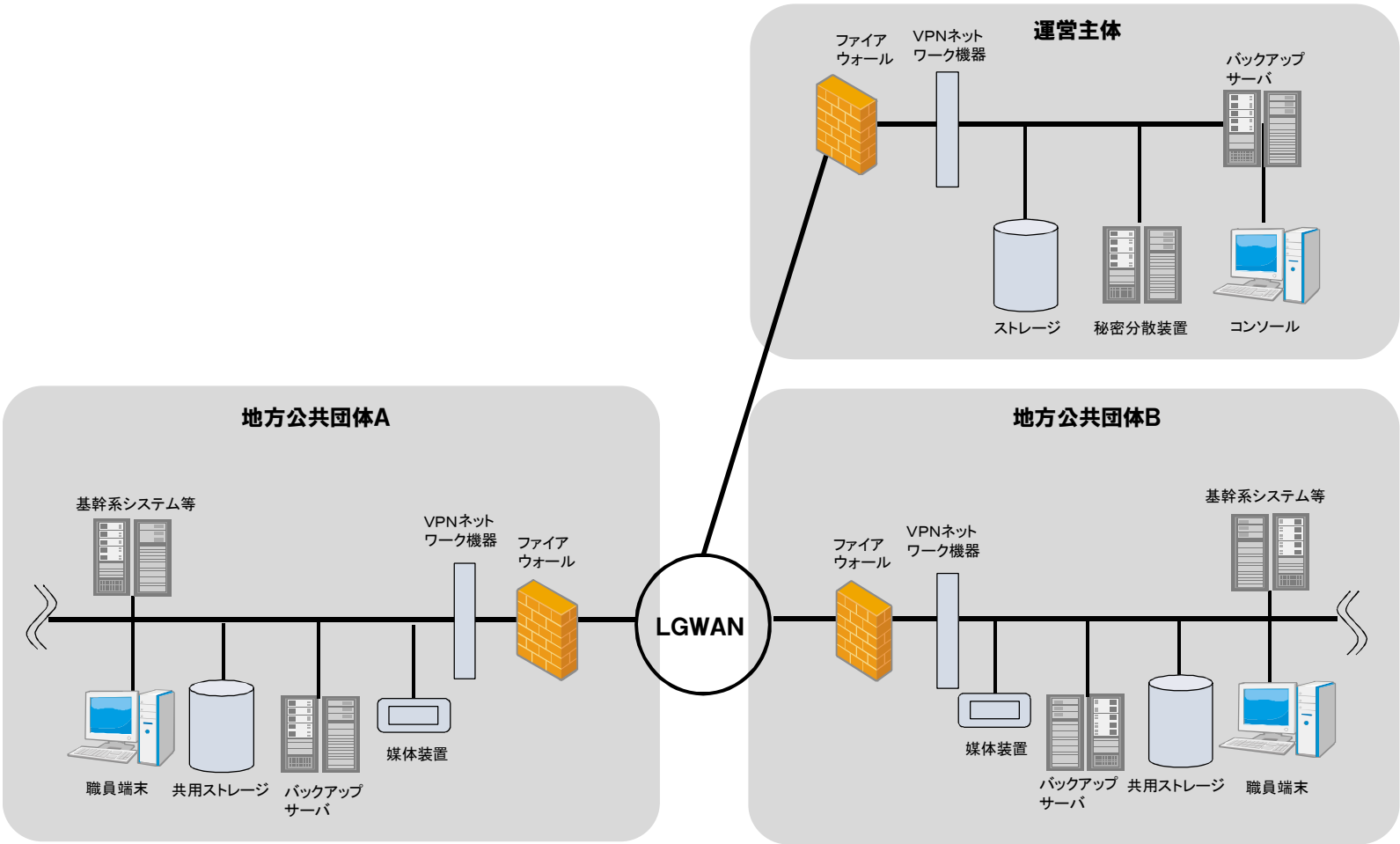
（ウ）機能の実現方法

ストレージ・コンパクション機能の実現方法を以下に示す。

表－４１　ストレージ・コンパクション機能の実現方法

No.	利用する製品 及びサービス	実現方法
1	アプリケーションソフトウェア	監視ソフトウェア等の機能を利用して死活状態やストレージ容量等を監視する （前頁の機能一覧 No.1～4 に相当） 【製品例】 （監視ソフトウェア） ・JP1/Performance Management ・Tivoli Netcool　など （バックアップソフトウェア） ・Acronis TrueImage ・Symantec Backup Exec ・CA ARC serve Backup ・JP1/VERITAS NetBackup　など
2	クラウドストレージ	クラウド環境上に各バックアップサイトの状況を監視する （前頁の機能一覧 No.1～4 に相当）
3	スクラッチ開発[55]	スクラッチ開発により機能を実装する （前頁の機能一覧 No.5～8 に相当）

[55] システムを新たに独自開発すること。



図－４６　地方公共団体のクラウド型バックアップサイトの機器構成イメージ[56]

[56] 初期費用の低減に配慮する観点からバックアップサイトを構築する上での必要最低限の機器構成。各団体におけるセキュリティ対策に重点を置く場合には、専用ストレージ及びファイアウォールの増設等が想定される。

第３節　実証実験

１　実証範囲

（１）実証実験のポイント整理

地方公共団体のクラウド型バックアップサイトの構成機能におけるポイントを以下に整理する。

・基本的な機能は市販されている製品機能で実現可能
・製品間の組合せで検証が必要な点が存在
・一部の機能について、製品化されておらず新たに開発する必要有り

表－４２　地方公共団体のクラウド型バックアップサイトの構成機能

No.		機能一覧	基本機能	実現方法有無
Ⅰ. データ・アグリゲーション機能				
	1	バックアップの種類（フルバックアップ、差分バックアップ、増分バックアップ）を選択する	○	○
	2	バックアップを実施するスケジュールを設定する	○	○
	3	バックアップを実施するスケジュールをスケジュール管理ソフトウェアと連動させる		
	4	設定したサイトのディレクトリに存在するデータからバックアップデータを作成する	○	○
	5	作成したバックアップデータを設定したディレクトリに格納する	○	○
	6	差分バックアップ、増分バックアップの基準日時を設定する	○	○
	7	データの作成日時等をキーとして基準日時以降に追加、更新及び削除されたデータをバックアップして設定したディレクトリに格納する	○	○
	8	外部媒体へのデータの書出し及び読込みを行う	○	○
	9	設定したディレクトリに格納したデータを削除する	○	○
	10	設定したディレクトリに格納されたデータを暗号化する	○	○
	11	設定したディレクトリに格納され、暗号化されたデータから元のデータをリストアする	○	○
	12	秘匿処理を実施するスケジュールを設定する		
	13	秘匿処理を実施するスケジュールをスケジュール管理ソフトウェアと連動させる		
Ⅱ. 秘匿機能				
	1	設定したディレクトリに格納されたデータを暗号化する	○	○
	2	設定したディレクトリに格納され、暗号化されたデータから元のデータをリストアする	○	○
	3	設定したサイトのディレクトリにデータを格納する	○	○
	4	設定したサイトのディレクトリからデータを取得する	○	○
	5	設定したディレクトリに格納されたデータを秘匿化した上で複数のデータに分割する（秘密分散機能）	○	○
	6	設定したディレクトリに格納された秘匿化して複数に分割したデータをリストアする（秘密分散機能）	○	○
	7	秘匿化する際にデータを分割する数を設定する（秘密分散機能）	○	○
	8	リストアに必要となる分割したデータの数を設定する（秘密分散機能）	○	○
Ⅲ. ストレージ・コンパクション機能				
	1	クラウド環境上の各地方公共団体のバックアップサイトを死活監視する	○	○
	2	クラウド環境上の各地方公共団体のバックアップサイトに配置したサーバ又はストレージの容量を監視する	○	○
	3	監視状況（死活状況、サーバ又はストレージ容量等）を運営主体に通知する	○	○
	4	監視を実施するスケジュールを設定する	○	○
	5	クラウド環境上に設定したディレクトリにデータを格納（再配置）する	○	
	6	地方公共団体のバックアップサイト上に設定したディレクトリからデータを取得する	○	
	7	クラウド環境上に設定したディレクトリに格納したデータを削除する	○	
	8	バックアップデータの取得・再配置の履歴を過去分にわたり履歴管理する（取得元と再配置先の地方公共団体を管理する）	○	
	9	履歴情報をキーワード検索する		
	10	各地方公共団体における共用ストレージを始めとするサーバ機器等の稼働環境（ＯＳ、業務アプリケーションソフトウェア等）を管理する		

製品間の組合せで検証が必要な点が存在
一部の機能について、製品化されておらず新たに開発する必要有り

（２）実証対象とする機能とその組合せ

地方公共団体のクラウド型バックアップサイトの特徴は、地方公共団体がそれぞれバックアップサイトとなって互いのバックアップデータを保管し合うこと、運営主体がバックアップデータの保管先を一元的に管理することである。

実際の運用においては、個人情報などのデータを扱うことが予想されるため、バックアップサイトの運営には、高い秘匿性を担保する必要がある。秘匿性を高める手段として秘密分散は既に確立された技術であるが、実際に地方公共団体での運用を想定した場合に、バックアップソフトウェア等が提供するデータ・アグリゲーション機能と連携して、バックアップデータを秘密分散処理することは、これまで検証がなされていない。

また、運営主体におけるバックアップデータの取得と格納（再配置）及び履歴管理の機能は独自に開発する必要があるため、実際の運用を想定して、バックアップデータの一元的な管理が可能か確認する必要がある。

上記を踏まえて、実証実験では以下の点に着目して、バックアップサイトの活用形態について、その実現性、実用性等を検証する。

・秘密分散ソフトウェアとバックアップソフトウェアの連携[57]

・運営主体でのバックアップデータの一元的な管理[58]

[57] データ・アグリゲーション機能 No.4、5、7、9、秘匿機能 No.3～6 に相当。「第２節－２－（２）機能概要」を参照のこと。

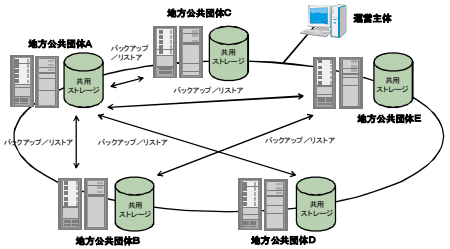
[58] ストレージ・コンパクション機能 No.5～8 に相当。「第２節－２－（２）機能概要」を参照のこと。

バックアップサイト構築時における検討ポイント

- コスト
- セキュリティ
- 作業負荷
- 自庁システムから離れていること

基本コンセプト

- ○ 地方公共団体は自らの共用ストレージを他の地方公共団体のバックアップサイトとして提供する。その一方で、他の地方公共団体の共用ストレージに自らのバックアップデータを保管する。
- ○ 運営主体がバックアップサイトにおける全ての共用ストレージを管理する。
- ○ バックアップサイトにおいては、暗号化等を施しバックアップデータの秘匿性を担保する。



地方公共団体のクラウド型バックアップサイト

地方公共団体のクラウド型バックアップサイトの構成機能

No.	機能一覧	基本機能	実現方法有無
Ⅰ.	データ・アグリゲーション機能		
1	バックアップの種類（フルバックアップ、差分バックアップ、増分バックアップ）を選択する	○	○
2	バックアップを実施するスケジュールを設定する	○	○
3	バックアップを実施するスケジュールをスケジュール管理ソフトウェアと連動させる		
4	設定したサイトのディレクトリに存在するデータからバックアップデータを作成する	○	○
5	作成したバックアップデータを設定したディレクトリに格納する	○	○
6	差分バックアップ、増分バックアップの基準日時を設定する	○	○
7	データの作成日時等をキーとして基準日時以降に追加、更新及び削除されたデータをバックアップして設定したディレクトリに格納する	○	○
8	外部媒体へのデータの書出し及び読込みを行う	○	○
9	設定したディレクトリに格納したデータを削除する	○	○
10	設定したディレクトリに格納されたデータを暗号化する	○	○
11	設定したディレクトリに格納され、暗号化されたデータから元のデータをリストアする	○	○
12	秘匿処理を実施するスケジュールを設定する		
13	秘匿処理を実施するスケジュールをスケジュール管理ソフトウェアと連動させる		
Ⅱ.	秘匿機能		
1	設定したディレクトリに格納されたデータを暗号化する	○	○
2	設定したディレクトリに格納され、暗号化されたデータから元のデータをリストアする	○	○
3	設定したサイトのディレクトリにデータを格納する	○	○
4	設定したサイトのディレクトリからデータを取得する	○	○
5	設定したディレクトリに格納されたデータを秘匿化した上で複数のデータに分割する（秘密分散機能）	○	○
6	設定したディレクトリに格納された秘匿化して複数に分割したデータをリストアする（秘密分散機能）	○	○
7	秘匿化する際にデータを分割する数を設定する（秘密分散機能）	○	○
8	リストアに必要となる分割したデータの数を設定する（秘密分散機能）	○	○
Ⅲ.	ストレージ・コンパクション機能		
1	クラウド環境上の各地方公共団体のバックアップサイトを死活監視する	○	○
2	クラウド環境上の各地方公共団体のバックアップサイトに配置したサーバ又はストレージの容量を監視する	○	○
3	監視状況（死活状況、サーバ又はストレージ容量等）を運営主体に通知する	○	○
4	監視を実施するスケジュールを設定する	○	○
5	クラウド環境上に設定したディレクトリにデータを格納（再配置）する	○	
6	地方公共団体のバックアップサイト上に設定したディレクトリからデータを取得する	○	
7	クラウド環境上に設定したディレクトリに格納したデータを削除する	○	
8	バックアップデータの取得・再配置の履歴を過去分にわたり履歴管理する（取得元と再配置先の地方公共団体を管理する）	○	
9	履歴情報をキーワード検索する		
10	各地方公共団体における共用ストレージを始めとするサーバ機器等の稼働環境（ＯＳ、業務アプリケーションソフトウェア等）を管理する		

- ○ 基本的な機能は市販されている製品機能で実現可能
- ○ ただし、製品間の組合せで確認が必要な点が存在
- ○ また、一部の機能について、製品化されておらず新たに開発する必要有（今後の課題）

実証実験のポイント

秘密分散ソフトウェアとバックアップソフトウェアの連携

○ 実際の運用を想定したデータ量、ファイル構成及びフォルダ構成のバックアップデータを用いて、バックアップソフトウェア等が提供するバック アップデータと秘密分散技術との機能連携を検証する。

【対象機能】（第2節－2－(2)機能概要を参照）
データ・アグリゲーション機能No.4,5,7,9
秘匿機能No.3～6

運営主体でのバックアップデータの一元的な管理

○ バックアップデータの取得と格納（再配置）及び履歴管理の機能は新たに開発する必要があるため、実運用を想定してバックアップデータの一元的な管理が可能か確認する。

【対象機能】（第2節－2－(2)機能概要を参照）
ストレージ・コンパクション機能No.5～8

図－４７　実証実験のポイント整理

（３）対象とするデータ[59]

地方公共団体が被災した場合の業務継続について、システムとして管理されているデータについては、汎用機からクラウドストレージへのデータ移行、データセンター間のバックアップ、被災時を想定したバックアップサイトへのアプリケーション切替え等が可能であることが、総務省の自治体クラウド開発実証事業における実証実験等によって示されている。

一方で、ローカル PC 等に保存されているデータについては、これまでに実証実験が実施された例は（システムとして管理されているデータに比べると）少なく、業務継続性については未知の部分が大きいと考えられる。

上記を踏まえて、実証実験では行政データの中でもローカル PC 等に保存されているデータに重点を置いて、バックアップサイトの活用形態について、その実現性、実用性等を検証する。

[59] 本実証実験で検証するバックアップ・リストアの仕組みは、基幹系システムのデータに対しても応用可能である。ただし、本実証実験で使用するテストデータには、基幹系システムのデータは含まない。なお、基幹系システムのデータをリストアする場合には、リストア環境の設定等が必要である。

２　実証仕様

（１）前提条件

ア　実証実験に活用する技術

・クラウドコンピューティングの技術を用いた実証実験を行う。
・データ保存の分散化（秘密分散技術等）を用いた実証実験を行う。

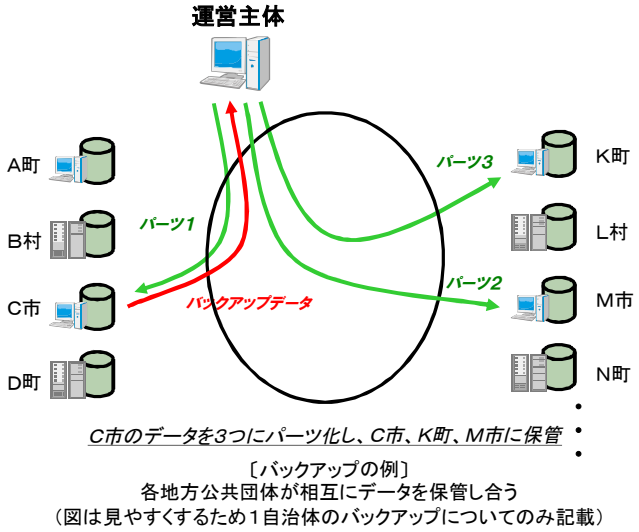
イ　バックアップ・リストア方式[60]

次に基づくバックアップ及びリストアの方法を以下に示す。

・実証実験におけるバックアップ及びリストアはネットワーク経由のデータ転送で実施する。
・バックアップデータはネットワーク上に存在する運営主体のサイトを経由した上でバックアップ及びリストアされる。

（ア）バックアップ方法

地方公共団体はバックアップデータを運営主体にデータ転送する。運営主体は秘密分散機能を用いてバックアップデータを３つのパーツに暗号化･分割し、このうち１つをバックアップ元の地方公共団体に、残る２つのパーツを、バックアップサイトを構成する２つの他の地方公共団体にそれぞれ送信する（今回の実証実験では元データを３つに分割するが、４つに分割することも可能）。

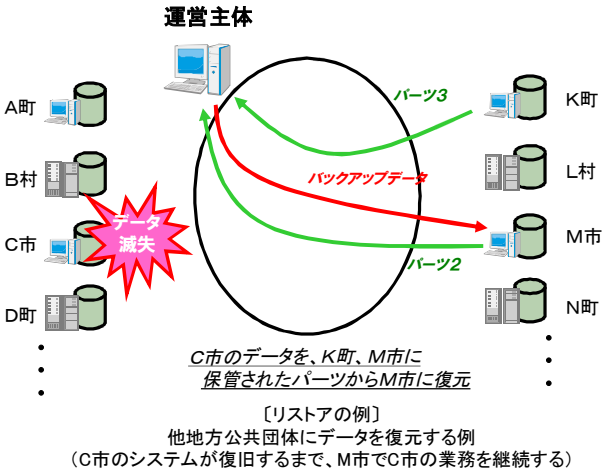


図－４８　バックアップのイメージ

60 フルバックアップとリストアでは、現時点におけるネットワーク環境を踏まえると外部媒体を用いることが一般的と考えられる。そのため、本実証実験では、増分バックアップをネットワーク経由でバックアップとリストアを行うことを検証する。

（イ）リストア方法

運営主体は秘密分散機能を用いて、バックアップデータを分割したパーツのうちの 2 つからデータをリストアする。リストア先は、バックアップ元の地方公共団体、他の地方公共団体のどちらでも設定可能である。



図－４９　リストアのイメージ

ウ　テストデータ

実証実験で使用するテストデータは地方公共団体の各職員によりローカル PC 等で保存されているデータを想定したファイル構成とする。

- 総データ量は概ね 500MB～6,000MB 程度[61]とする。
- 1 ファイルあたりのデータ量は概ね 100KB～5,000KB 程度とする。
- Word、Excel、PowerPoint、Access、Visio、PDF、テキスト、EXE[62]などの様々なファイル形式が入り混じったファイル構成（圧縮ファイルを含む）とする。
- テストデータ全体を圧縮する[63]。
- 様々な OS（Windows、Mac、Linux など）環境で作成されたファイルが入り混じったファイル構成とする。

実証実験で使用するテストデータは地方公共団体の各職員によりローカル PC 等で保存されているデータを想定したフォルダ構成とする。

- 複数の階層構造とする。
- 空フォルダを含むフォルダ構成とする。

検証項目に応じて、上記のファイル構成及びフォルダ構成等を変更することに

61 地方公共団体の職員が管理している行政データをフルバックアップする場合は、ネットワーク経由ではなくテープ媒体等にバックアップして媒体送付すると考えられるため、実証実験の実施範囲外とする。
62 EXE ファイルは「PDF Viewer.exe（≒1MB）」と「Visio Viewer.exe（≒17.5MB）」とする。
63 テストデータを圧縮しない場合は、テストデータを構成するファイル一つ一つに対して秘密分散処理及びデータ転送を実行するため、ファイルの数だけ処理が膨大に発生し、総じて処理時間がテストデータを一つのファイルに圧縮した場合よりも長くなる。このため、実証実験においてはテストデータ全体を圧縮して検証を実施する。

より、それぞれの要素が実験結果に与える影響を検証する。

エ　バックアップソフトウェア

・True Image2013 (Acronis 社)を用いる。

オ　秘密分散ソフトウェア

・SECLANCER(ケイレックス・テクノロジー社)を用いる。
・個人情報などの情報を取り扱うことを想定して、疑似乱数よりも秘匿性の高い真性乱数を用いて秘密分散処理を行う。
・実証実験に用いる秘密分散ソフトウェアの場合には、秘密分散後のデータ総容量は、元データに対して 1 つの分散データは 60%程度のサイズとなる。1GB のデータを秘密分散した場合のデータ総容量は以下のとおり。
　- 3 分散：1.8GB（=1GB＊0.6＊3）
　- 4 分散：2.4GB（=1GB＊0.6＊4）

カ　ネットワーク[64]

・ネットワークは NTT 東日本　B フレッツ 100Mbps（ベストエフォート）を用いる。

（２）実施環境

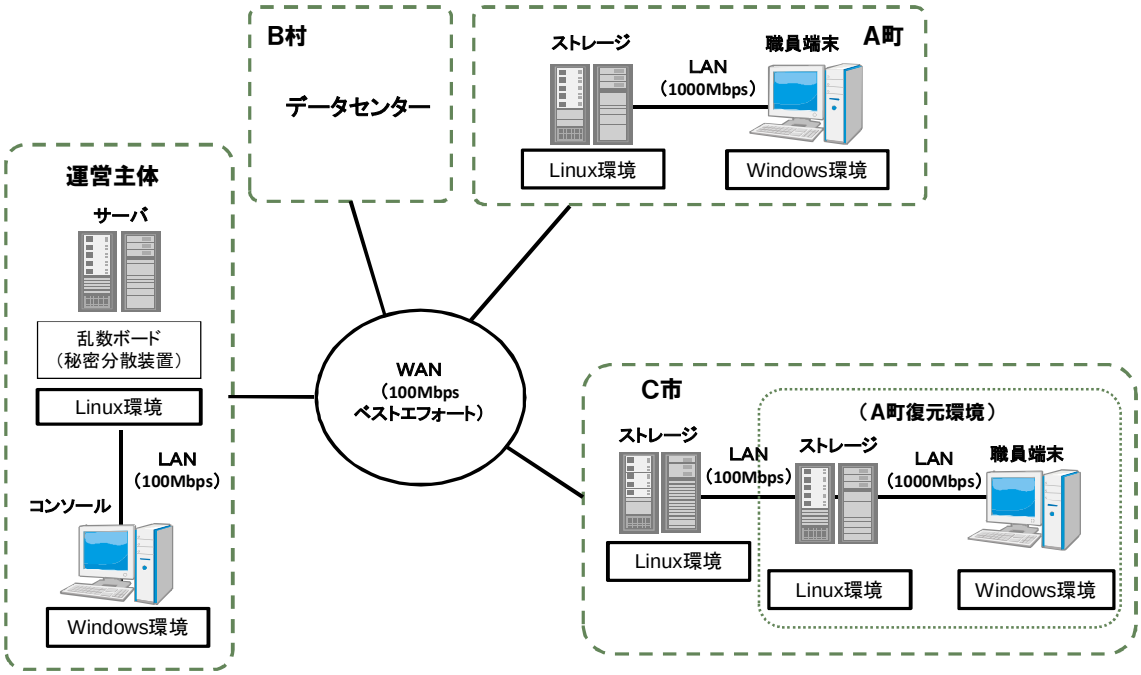
ア　基本的な考え方

・複数の地方公共団体及び運営主体に設置を想定したサーバ群によりクラウド環境を構成する。テストデータはこのクラウド上に分散して配置する。
・テストデータ自体は暗号化・分割されているため、クラウド上のどこかで断片的なデータを回収しても単独での復元を不可能とし、秘密が保全される仕組みとする。
・実証実験の実証環境は、NTT コミュニケーションズ（浜松町）のプロジェクトルームに設置する。

[64] データ転送に要する所要時間は、スループット等の影響を受けて前後する可能性がある。本調査研究において、各検証項目は 1 回ずつ検証を実施するため、より厳密に所要時間を計測するには、複数回検証を実施して平均値を算出する必要等がある。

イ　機器構成

実証実験の機器構成を以下に示す。

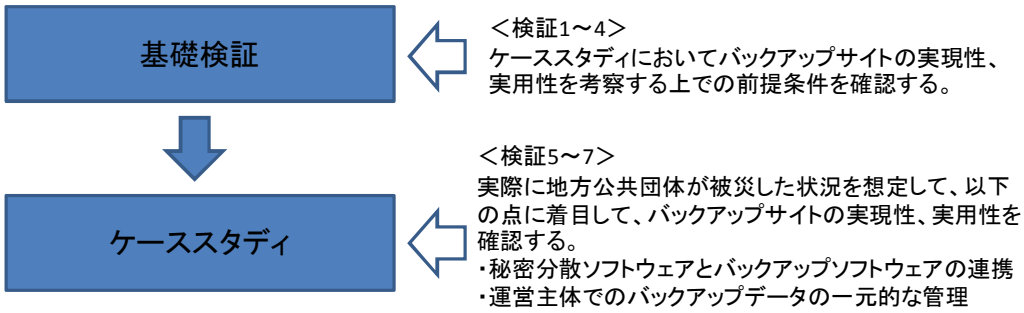


図－５０　実証実験の機器構成

表－４３　実証実験の機器構成仕様

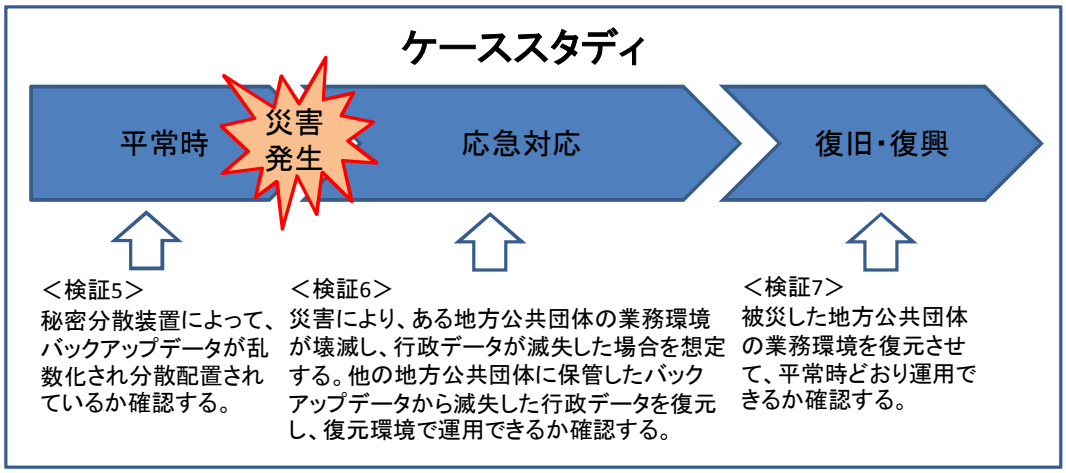
区分	種別	メーカ名及び品番	CPU	メモリ	ディスク容量	真性乱数ボード	アプリケーション	OS
A町	ストレージ	ニューテック SmartNAS	ATOM Dual Core 1.86GHz	4GB	8TB			CentOS 5.8
	職員端末（PC）	DELL VOSTRO	Core i3 3.3Ghz	4GB	1TB		True Image2013 (Acronis)	Windows7（64）
B村	クラウド	NTT コム BHE クラウド	3GHz	5GB	1TB			RedHat 5.7
C市	ストレージ	ニューテック SmartNAS	ATOM Dual Core 1.86GHz	4GB	8TB			CentOS 5.8
運営主体	サーバ	ニューテック NAP-6100	Xeon 2.4GHz	6GB	1TB	GRANG-PC IC-8CH (LE Tech)	SECLANCER（ケイレックス）	CentOS 5.8
A町復元環境	ストレージ	ニューテック NAP-6100	Xeon 2.4GHz	6GB	1TB			CentOS 5.8
	職員端末（PC）	DELL VOSTRO	Core i3 3.3GHz	4GB	1TB		True Image2013 (Acronis)	Windows7（64）

（３）実施概要



図－５１　検証項目

＜検証 1＞基礎検証:データ量がバックアップ及びリストアに与える影響の検証
＜検証 2＞基礎検証:ファイル構成がバックアップ及びリストアに与える影響の検証
＜検証 3＞基礎検証:フォルダ構成がバックアップ及びリストアに与える影響の検証
＜検証 4＞基礎検証:アプリケーションソフトウェアの業務継続性の検証



図－５２　ケーススタディのシナリオ

＜検証 5＞ケーススタディ:平常時を想定した検証
＜検証 6＞ケーススタディ:被災時(応急対応)を想定した検証
＜検証 7＞ケーススタディ:被災時(復旧・復興)を想定した検証

3　実証内容及び結果

（１）＜検証 1＞基礎検証:データ量がバックアップ及びリストアに与える影響の検証

表－４４　検証内容（検証内容 1-1、1-2）

検証項目	検証内容	検証パターン
1-1：バックアップ	データ量（総データ量及び 1 ファイルあたりのデータ量）がバックアップに必要な（データ投入、データ転送、データ格納に係る）時間に与える影響を確認する。	（次表参照）
1-2：リストア	データ量（総データ量及び 1 ファイルあたりのデータ量）がリストアに必要な（データ投入、データ転送、データ格納に係る）時間に与える影響を確認する。	

表－４５　検証パターン（検証内容 1-1、1-2）

	データ量		ファイル構成			フォルダ構成	（参考）データ全体圧縮後のデータ量
	総データ量	１ファイルあたりのデータ量	ファイル形式の多様性	データ全体の圧縮	ファイル作成元 OS 環境の多様性		
パターン 1	3GB	ファイルあたりのデータ量が概ね 1,000KB～5,000KB のファイルで構成	Word、Excel、Power Point、Access、Visio、PDF、テキスト、EXE などのファイル形式が混在（圧縮形式のファイルを含む）しているファイルで構成	データ全体を圧縮した構成	様々な OS（Windows、Mac、Linux など）環境で作成されたファイルが入り混じったファイルで構成	複数の階層構造、空フォルダを含むフォルダ構成	2GB
パターン 2		ファイルあたりのデータ量が概ね 100KB～500KB のファイルで構成					1GB
パターン 3	1GB	ファイルあたりのデータ量が概ね 1,000KB～5,000KB のファイルで構成					680MB
パターン 4		ファイルあたりのデータ量が概ね 100KB～500KB のファイルで構成					340MB
パターン 5	500MB	ファイルあたりのデータ量が概ね 1,000KB～5,000KB のファイルで構成					340MB
パターン 6		ファイルあたりのデータ量が概ね 100KB～500KB のファイルで構成					170MB

ア　実施手順

（ア）検証項目 1-1：バックアップ

A 町のストレージに登録したテストデータを運営主体にデータ転送し、運営主体において秘密分散機能で暗号化・分割した上で、A 町、B 村及び C 市に分散配置する。

本検証で計測する時間は以下のとおり。

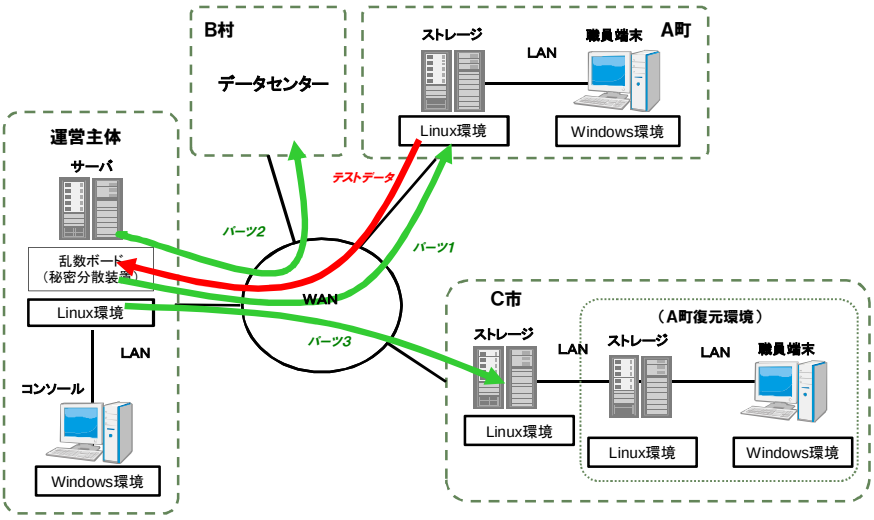
①A 町→運営主体（データ転送／テストデータ）

②運営主体での秘密分散処理

③運営主体→A 町（データ転送／パーツ 1）

④運営主体→B 村（データ転送／パーツ 2）

⑤運営主体→C 市（データ転送／パーツ 3）



図－５３　バックアップ時のデータの流れ（検証項目 1-1：バックアップ）

（イ）検証項目 1-2：リストア

A 町、B 村及び C 市に分散配置しているテストデータから、運営主体において秘密分散機能でリストアを行い、A 町のストレージにテストデータをデータ転送する。

本検証で計測する時間は以下のとおり。

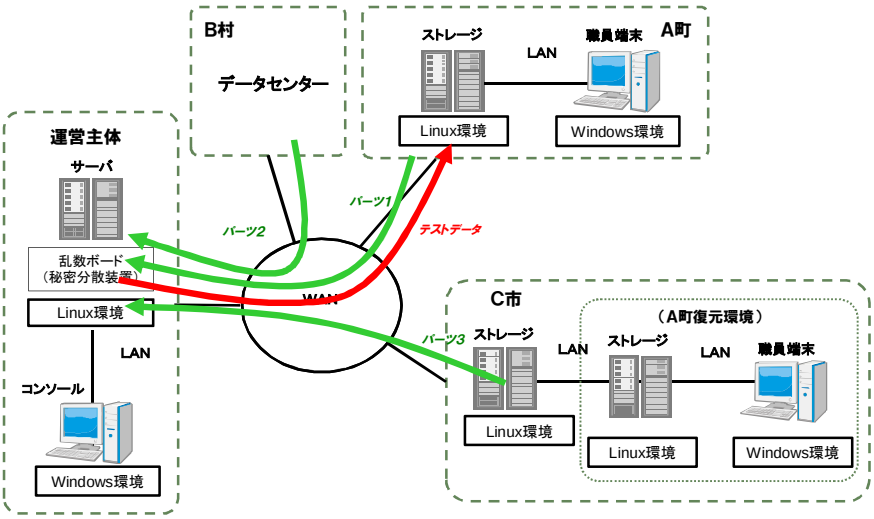
①A 町→運営主体（データ転送／パーツ 1）

②B 村→運営主体（データ転送／パーツ 2）

③C 市→運営主体（データ転送／パーツ 3）

④運営主体での秘密分散処理

⑤運営主体→A 町（データ転送／テストデータ）



図－５４　リストア時のデータの流れ（検証項目 1-2：リストア）

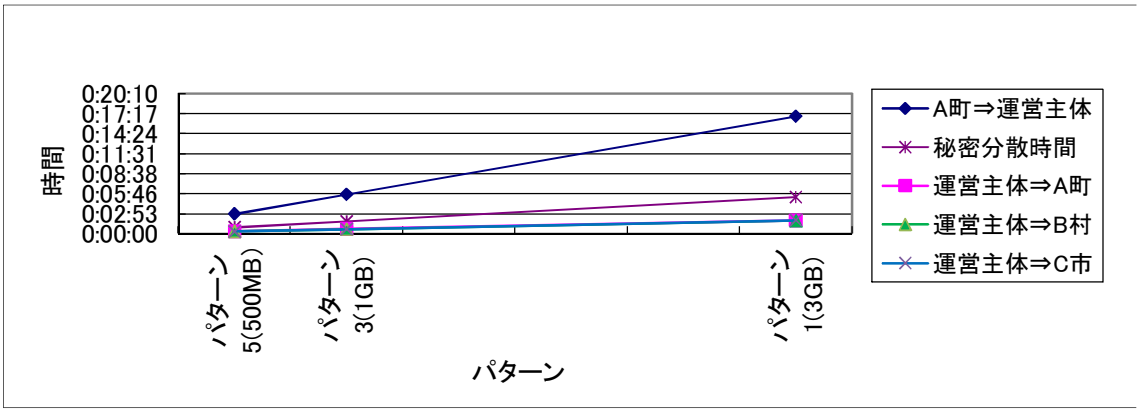
イ　結果

（ア）検証項目 1-1：バックアップ

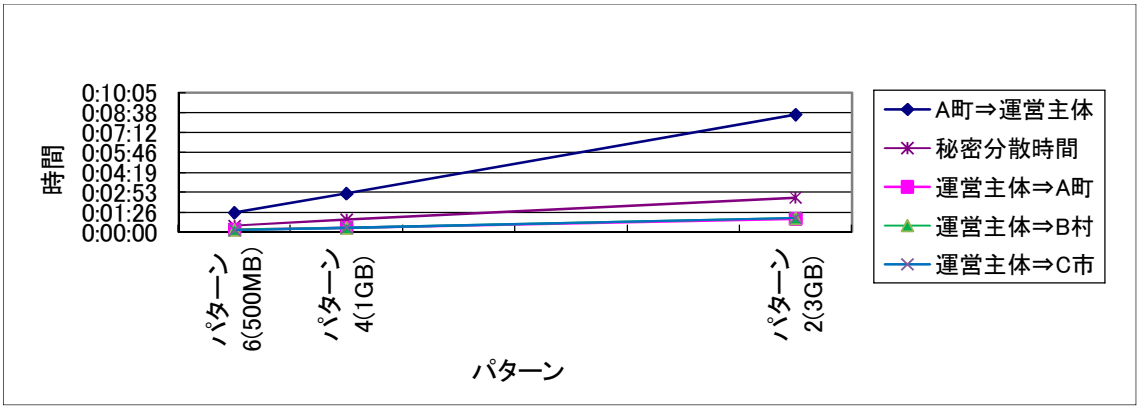
表－４６　バックアップ処理時間（検証内容 1-1）

（単位）時間：分：秒

	①A町→運営主体（データ転送）	②運営主体での秘密分散処理	③運営主体→A町（データ転送）	④運営主体→B村（データ転送）	⑤運営主体→C市（データ転送）	合計
パターン 1	0:16:51	0:05:14	0:01:54	0:01:49	0:01:55	0:27:43
パターン 2	0:08:29	0:02:29	0:00:56	0:01:00	0:01:01	0:13:55
パターン 3	0:05:37	0:01:44	0:00:40	0:00:36	0:00:36	0:09:13
パターン 4	0:02:47	0:00:54	0:00:19	0:00:18	0:00:19	0:04:37
パターン 5	0:02:49	0:00:54	0:00:20	0:00:20	0:00:18	0:04:41
パターン 6	0:01:24	0:00:27	0:00:10	0:00:10	0:00:09	0:02:20



図－５５　検証１（パターン 1、3、5）の結果比較（バックアップ処理）



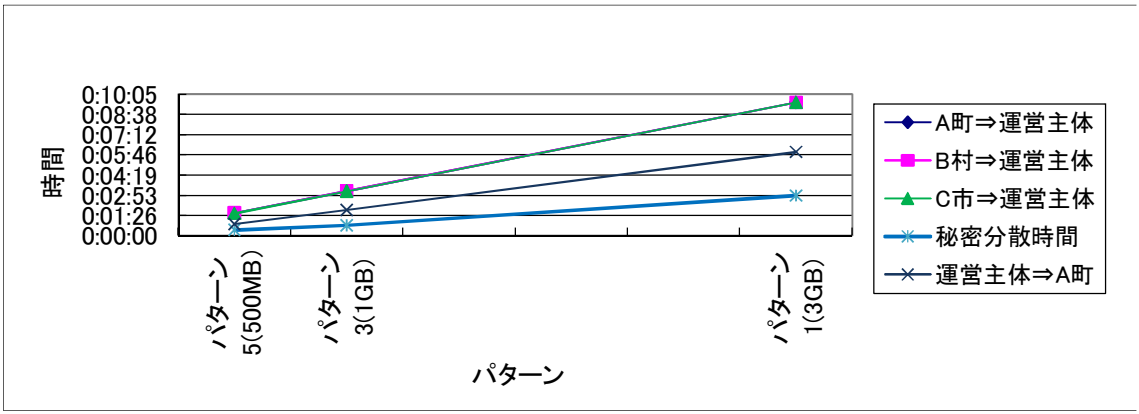
図－５６　検証１（パターン 2、4、6）の結果比較（バックアップ処理）

（イ）検証項目 1-2：リストア

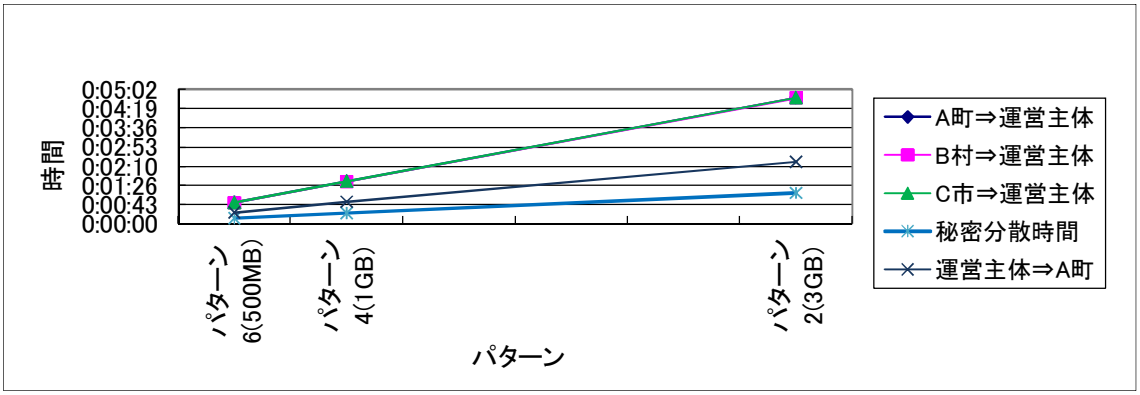
表－４７　リストア処理時間（検証内容 1-2）

（単位）時間：分：秒

	①Ａ町→運営主体（データ転送）	②Ｂ村→運営主体（データ転送）	③Ｃ市→運営主体（データ転送）	④運営主体での秘密分散処理	⑤運営主体→Ａ町（データ転送）	合計
パターン 1	0:09:29	0:09:28	0:09:28	0:02:50	0:05:57	0:37:12
パターン 2	0:04:43	0:04:42	0:04:43	0:01:09	0:02:19	0:17:36
パターン 3	0:03:10	0:03:10	0:03:09	0:00:43	0:01:49	0:12:01
パターン 4	0:01:35	0:01:34	0:01:35	0:00:24	0:00:49	0:05:57
パターン 5	0:01:35	0:01:36	0:01:34	0:00:23	0:00:48	0:05:56
パターン 6	0:00:48	0:00:47	0:00:47	0:00:12	0:00:25	0:02:59



図－５７　検証１（パターン１、３、５）の結果比較（リストア処理）

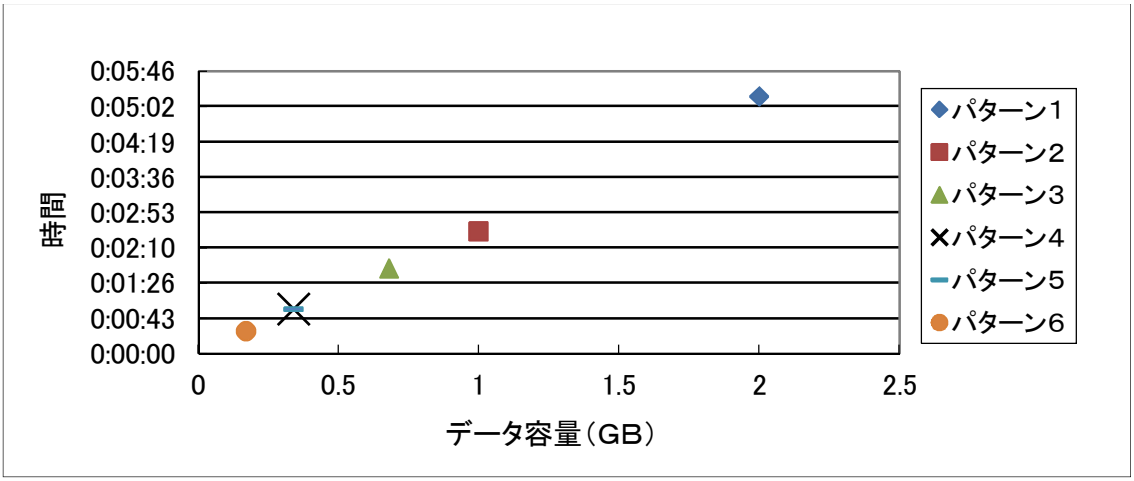


図－５８　検証１（パターン２、４、６）の結果比較（リストア処理）

ウ　まとめ

検証パターン１、３、５及び検証パターン２、４、６の場合を比較した結果、秘密分散に要する時間はテストデータのデータ量に比例して増加することが示された。

また、検証パターン 1～6 のそれぞれの場合において、各テストデータの全体を圧縮した後のデータ量と秘密分散に要する時間の関係を以下に示す。



図－５９　検証１におけるテストデータのデータ量と秘密分散時間の関係

上記の結果から、秘密分散に要する時間はテストデータのデータ量（圧縮後のデータ量[65]）に比例して増加することが示された。

なお、検証パターン 1～6 においては各拠点間のデータ転送時間もテストデータのデータ量に対して増加傾向を示した。

各検証において、機器構成上の同じ区間（例えば、A 町⇔運営主体）においても、A 町から運営主体に対してデータ転送する場合と、逆に運営主体から A 町に対してデータ転送する場合の転送時間が異なっている。本検証においては、すべての検証において､A 町から運営主体に対してデータ転送する場合の転送時間が、運営主体からA町に対してデータ転送する場合の転送時間よりも長くなっている。主な原因としては、運営主体の秘密分散システムにおいて、A 町から運営主体にデータ転送すると同時に、運営主体において秘密分散用のデータをコピーしている為、ディスクの入出力が増加し、データ転送に係る時間が増加したものと考えられる。

[65] テストデータの圧縮後のデータ量については「第 3 節－3－(1)　検証パターン（検証内容 1-1、1-2)」を参照のこと。

（２）＜検証 2＞基礎検証:ファイル構成がバックアップ及びリストアに与える影響の検証

表－４８　検証内容（検証内容 2-1、2-2）

検証項目	検証内容	検証パターン
2-1 : バックアップ	ファイル構成（ファイル形式及びファイル作成元の OS 環境）がバックアップに必要な（データ投入、データ転送、データ格納に係る）時間に与える影響を確認する	（次表参照）
2-2 : リストア	ファイル構成（ファイル形式及びファイル作成元の OS 環境）がリストアに必要な（データ投入、データ転送、データ格納に係る）時間に与える影響を確認する	

表－４９　検証パターン（検証内容 2-1、2-2）

	データ量		ファイル構成			フォルダ構成	（参考）データ全体圧縮後のデータ量
	総データ量[66]	1 ファイルあたりのデータ量	ファイル形式の多様性	データ全体の圧縮	ファイル作成元 OS 環境の多様性		
パターン 1	3GB	ファイルあたりのデータ量が概ね 100KB～500KB のファイルで構成	○	データ全体を圧縮した構成	○	複数の階層構造、空フォルダを含むフォルダ構成	1GB
パターン 2					×		1.1GB
パターン 3			×		○		1.4GB
パターン 4					×		2GB

【凡例】- ファイル形式の多様性

○：Word、Excel、PowerPoint、Access、Visio、PDF、テキスト、EXE などのファイル形式（圧縮形式のファイルを含む）が混在しているファイルで構成。

×：特定のファイル形式（Word、Excel、PowerPoint 等）で構成されるファイルで構成。

- ファイル作成元 OS 環境の多様性

○：様々な OS（Windows、Mac、Linux など）環境で作成されたファイルで構成。

×：特定の OS 環境で作成されたファイルで構成。

ア　実施手順

検証項目 2-1 及び 2-2 の実施手順は検証項目 1-1 及び 1-2 と同様とする。

[66] 総データ量は、データ全体を圧縮する前のデータ量。

イ　結果

（ア）検証項目 2-1：バックアップ

表－５０　バックアップ処理時間（検証項目 2-1）

（単位）時間：分：秒

	①Ａ町→運営主体（データ転送）	②運営主体での秘密分散処理	③運営主体→Ａ町（データ転送）	④運営主体→Ｂ村（データ転送）	⑤運営主体→Ｃ市（データ転送）	合計
パターン 1	0:08:29	0:02:29	0:00:56	0:01:00	0:01:01	0:13:55
パターン 2	0:09:04	0:02:43	0:01:02	0:01:00	0:01:04	0:14:53
パターン 3	0:11:27	0:03:31	0:04:59	0:01:15	0:05:22	0:26:34
パターン 4	0:16:45	0:05:13	0:04:02	0:01:53	0:02:01	0:29:54

（イ）検証項目 2-2：リストア

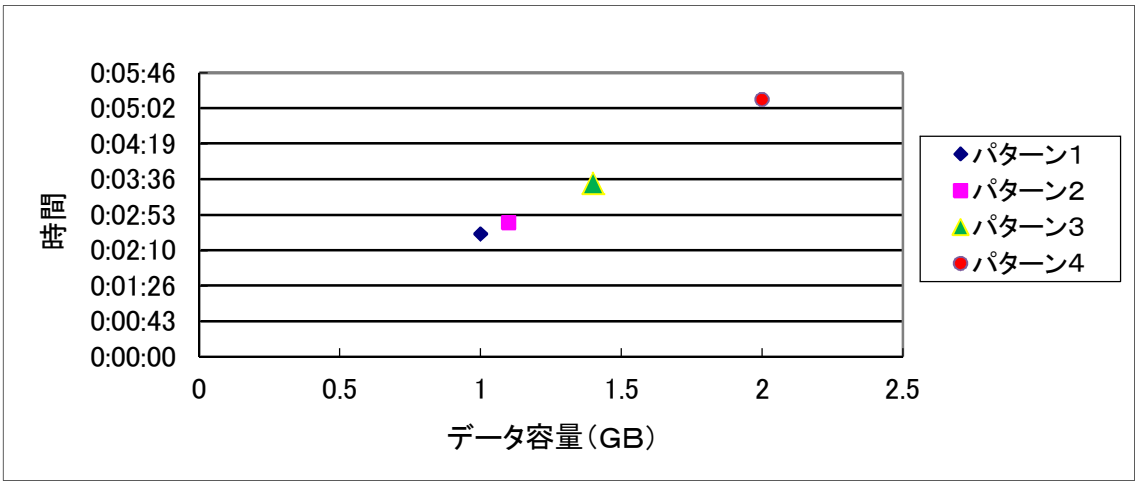
表－５１　リストア処理時間（検証項目 2-2）

（単位）時間：分：秒

	①Ａ町→運営主体（データ転送）	②Ｂ村→運営主体（データ転送）	③Ｃ市→運営主体（データ転送）	④運営主体での秘密分散処理	⑤運営主体→Ａ町（データ転送）	合計
パターン 1	0:04:43	0:04:42	0:04:43	0:01:09	0:02:19	0:17:36
パターン 2	0:05:06	0:05:06	0:05:06	0:01:05	0:03:28	0:19:51
パターン 3	0:06:23	0:06:24	0:06:24	0:01:37	0:03:38	0:24:26
パターン 4	0:09:25	0:09:25	0:09:25	0:02:08	0:12:01	0:42:24

ウ　まとめ

検証パターン 1～4 の場合において、各テストデータの全体を圧縮した後のデータ量と秘密分散に要する時間の関係を以下に示す。



図－６０　検証２におけるテストデータのデータ量と秘密分散時間の関係

上記の結果から、秘密分散に要する時間はテストデータのデータ量（圧縮後のデータ量[67]）に比例して増加することが示された。

なお、バックアップ実施時において各拠点間のデータ転送時間に差異があるのは、それぞれのネットワークにおけるスループットが時間と共に変化したためと考えられる。

[67] テストデータの圧縮後のデータ量については「第 3 節－3－(2)　検証パターン（検証内容 2-1、2-2）」を参照のこと。

（３）＜検証 3＞基礎検証：フォルダ構成がバックアップ及びリストアに与える影響の検証

表－５２　検証内容（検証項目 3-1、3-2）

検証項目	検証内容	検証パターン
3-1：バックアップ	フォルダ構成がバックアップに必要な（データ投入、データ転送、データ格納に係る）時間に与える影響を確認する	（次表参照）
3-2：リストア	フォルダ構成がリストアに必要な（データ投入、データ転送、データ格納に係る）時間に与える影響を確認する	

表－５３　検証パターン（検証項目 3-1、3-2）

	データ量		ファイル構成			フォルダ構成
	総データ量	１ファイルあたりのデータ量	ファイル形式の多様性	データ全体の圧縮	ファイル作成元 OS 環境の多様性	
パターン 1	3GB	ファイルあたりのデータ量が概ね 1,000KB～5,000KB のファイルで構成	Word、Excel、Power Point、Access、Visio、PDF、テキスト、EXE などのファイル形式が混在（圧縮形式のファイルを含む）しているファイルで構成	データ全体を圧縮した構成	様々な OS（Windows、Mac、Linux など）環境で作成されたファイルが入り混じったファイルで構成	複数の階層構造、空フォルダを含むフォルダ構成
パターン 2						複数の階層構造を持たない、空フォルダを含まないフォルダ構成

ア　実施手順

検証項目 3-1 及び 3-2 の実施手順は検証項目 1-1 及び 1-2 と同様とする。

イ　結果

（ア）検証項目 3-1：バックアップ

表－５４　バックアップ処理時間（検証項目 3-1）

（単位）時間：分：秒

	①Ａ町→運営主体（データ転送）	②運営主体での秘密分散処理	③運営主体→Ａ町（データ転送）	④運営主体→Ｂ村（データ転送）	⑤運営主体→Ｃ市（データ転送）	合計
パターン 1	0:16:55	0:05:15	0:02:19	0:01:50	0:02:15	0:28:34
パターン 2	0:16:58	0:05:14	0:01:52	0:01:52	0:02:04	0:28:00

（イ）検証項目 3-2：リストア

表－５５　リストア処理時間（検証項目 3-2）

（単位）時間：分：秒

	①Ａ町→運営主体（データ転送）	②Ｂ村→運営主体（データ転送）	③Ｃ市→運営主体（データ転送）	④運営主体での秘密分散処理	⑤運営主体→Ａ町（データ転送）	合計
パターン 1	0:09:28	0:09:28	0:09:28	0:02:25	0:04:46	0:35:35
パターン 2	0:09:29	0:09:31	0:09:28	0:02:30	0:04:49	0:35:47

ウ　まとめ

検証パターン 1、2 の場合を比較した結果、秘密分散に要する時間には殆ど変化がなかった。また、検証 2 の結果から、秘密分散に要する時間は圧縮後のテストデータのデータ量に比例することが示されている。よって、今回の検証において比較検証したフォルダ構成は、圧縮後のデータ量には殆ど影響しなかったと考えられる。

なお、バックアップ実施時において各拠点間のデータ転送時間に差異があるのは、それぞれのネットワークにおけるスループットが時間と共に変化したためと考えられる。

（４）＜検証 4＞基礎検証:アプリケーションソフトウェアの業務継続性の検証

表－５６　検証内容（検証項目 4）

検証項目	検証内容	検証パターン
4：業務再開	復元環境において業務アプリケーションソフトウェアをリストアして業務を再開できるか確認する	（次表参照）

表－５７　検証パターン（検証項目 4）

データ量		ファイル構成			フォルダ構成
総データ量	１ファイルあたりのデータ量	ファイル形式の多様性	データ全体の圧縮	ファイル作成元 OS 環境の多様性	
3GB	ファイルあたりのデータ量が概ね 100KB～500KB のファイルで構成	Word、Excel、PowerPoint、Access、Visio、PDF、テキスト、EXE などのファイル形式が混在（圧縮形式のファイルを含む）しているファイルで構成	データ全体を圧縮した構成	様々な OS（Windows、Mac、Linux など）環境で作成されたファイルが入り混じったファイルで構成	複数の階層構造、空フォルダを含むフォルダ構成

ア　実施手順

検証項目 2-2 のパターン 1 を実施した後に、A 町にリストアした業務アプリケーションソフトウェアを用いて業務を再開する。

イ　結果

業務環境において業務アプリケーションソフトウェアをリストアし、正常に作動することを確認した（業務を継続して実施できることを確認した)。

（５）基礎検証のまとめ(検証項目 1～4)

検証 1～4 の結果、秘密分散に要する時間は、テストデータのデータ量、テストデータのファイル構成等に影響を受けるものの、最終的には、圧縮後のデータ量に比例して増加することが示された。

また、秘密分散処理でバックアップ及びリストアした業務アプリケーションソフトウェアが正常に作動することを確認した。

（６）＜検証 5＞ケーススタディ:平常時を想定した検証

表－５８　検証内容（検証項目 5）

検証項目	検証内容	検証パターン
5:業務環境からのバックアップ	平常時運用を想定して、業務環境からバックアップサイトへのバックアップが実施できるか確認する	（次表参照）

表－５９　検証パターン（検証項目 5）

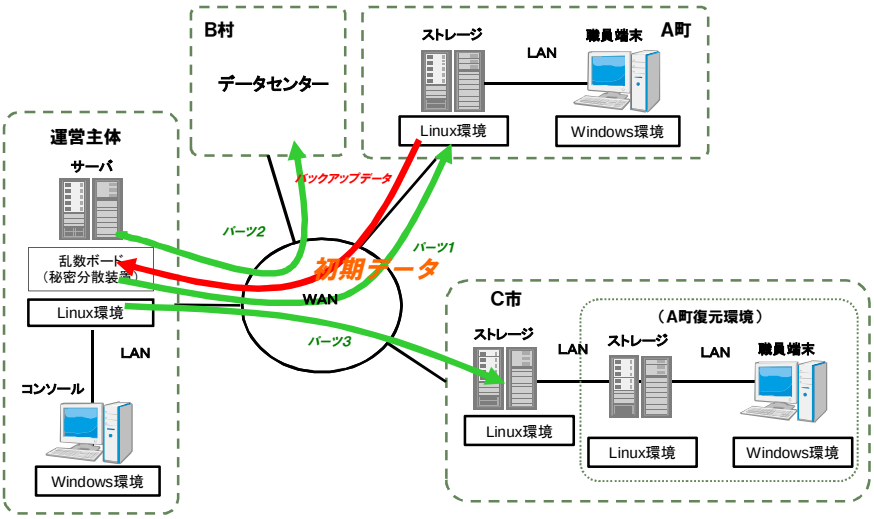
データ量		ファイル構成			フォルダ構成
総データ量	１ファイルあたりのデータ量	ファイル形式の多様性	データ全体の圧縮	ファイル作成元 OS 環境の多様性	
3GB	ファイルあたりのデータ量が概ね 1,000KB～5,000KB のファイルで構成	Word、Excel、PowerPoint、Access、Visio、PDF、テキスト、EXE などのファイル形式が混在（圧縮形式のファイルを含む）しているファイルで構成	データ全体を圧縮した構成	様々な OS（Windows、Mac、Linux など）環境で作成されたファイルが入り混じったファイルで構成	複数の階層構造、空フォルダを含むフォルダ構成

ア　実施手順

A 町（業務環境）の職員端末に登録したテストデータ（初期データ）を、バックアップソフトウェアを用いて暗号化・圧縮してバックアップデータを作成し、これを A 町（業務環境）のストレージに保管する。A 町（業務環境）のストレージからバックアップデータを運営主体にデータ転送する。運営主体において秘密分散機能で暗号化・分割した上で、A 町（業務環境）、B 村及び C 市に分散配置する。

本検証で計測する時間は以下のとおり。

①A 町（業務環境／職員端末）におけるテストデータのバックアップ処理
②A 町（業務環境／職員端末）→A 町（業務環境／ストレージ）（データ転送）
③A 町（業務環境）→運営主体（データ転送／バックアップデータ）
④運営主体での秘密分散処理
⑤運営主体→A 町（業務環境）（データ転送／パーツ 1）
⑥運営主体→B 村（データ転送／パーツ 2）
⑦運営主体→C 市（データ転送／パーツ 3）



図－６１　バックアップ時のデータの流れ（検証項目５：業務環境からのバックアップ）

イ　結果

表－６０　業務環境からのバックアップ処理時間

（単位）時間：分：秒

	①A町（業務環境／職員端末）における暗号化（バックアップ）	②A町（業務環境／職員端末）→A町（ストレージ）（データ転送）	③A町→運営主体（データ転送）	④運営主体での秘密分散処理	⑤運営主体→A町（データ転送）	⑥運営主体→B村（データ転送）	⑦運営主体→C市（データ転送）	合計
パターン１	0:05:53	0:02:02	0:16:58	0:05:43	0:01:53	0:01:51	0:02:02	0:36:22

検証の結果、バックアップソフトウェアと秘密分散ソフトウェアを組み合わせて、平常時のバックアップを実施することができた。

また、A 町（業務環境）のストレージからバックアップデータを運営主体にデータ転送、運営主体において秘密分散機能で暗号化・分割を実施、A 町（業務環境）、B 村及び C 市に分散配置するまでの一連の操作を運営主体のコンソールから実施することができた。

今回のテストデータのデータ量（3GB）において、業務環境からのバックアップ処理が完了するまでの所要時間は 30 分程度であった。

（７）＜検証 6＞ケーススタディ:被災時(応急対応)を想定した検証

表－６１　検証内容（検証項目 6-1、6-2）

検証項目	検証内容	検証パターン
6-1：復元環境へのリストア	被災時（応急対応）運用を想定して、バックアップサイトから復元環境へのリストアが実施できるか確認する	（次表参照）
6-2：業務再開	被災時（応急対応）運用を想定して、復元環境において業務アプリケーションソフトウェアをリストアして業務を再開できるか確認する	

表－６２　検証パターン（検証項目 6-1、6-2）

データ量		ファイル構成			フォルダ構成
総データ量	１ファイルあたりのデータ量	ファイル形式の多様性	データ全体の圧縮	ファイル作成元 OS 環境の多様性	
3GB	ファイルあたりのデータ量が概ね 1,000KB～5,000KB のファイルで構成	Word、Excel、PowerPoint、Access、Visio、PDF、テキスト、EXE などのファイル形式が混在（圧縮形式のファイルを含む）しているファイルで構成	データ全体を圧縮した構成	様々な OS（Windows、Mac、Linux など）環境で作成されたファイルが入り混じったファイルで構成	複数の階層構造、空フォルダを含むフォルダ構成

ア　実施手順

（ア）検証項目 6-1：復元環境へのリストア

検証項目 5 実施後に災害が発生し、A 町（業務環境）が壊滅してテストデータ（初期データ）が滅失した場合を想定し、B 村及び C 市に分散配置しているバックアップデータから、運営主体において秘密分散機能でリストアを行い、A 町（復元環境）のストレージにバックアップデータをデータ転送する。これを A 町（復元環境）の職員端末に保管し、バックアップソフトウェアを用いて元のテストデータ（初期データ）を復元する。

本検証で計測する時間は以下のとおり。

①B 村→運営主体（データ転送／パーツ 2）

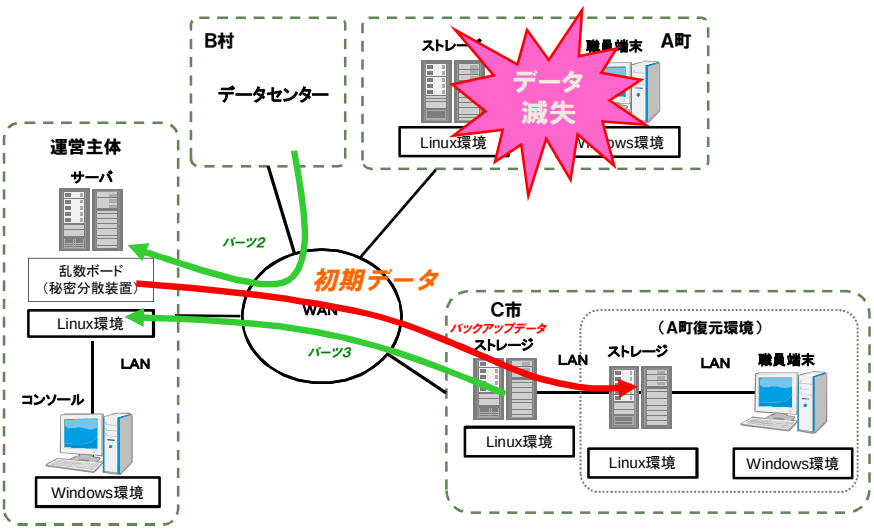
②C 市→運営主体（データ転送／パーツ 3）

③運営主体での秘密分散処理

④運営主体→A 町（復元環境）（データ転送／バックアップデータ）

⑤A 町（復元環境／サーバ）→A 町（復元環境／職員端末）（データ転送）

⑥A 町（復元環境／職員端末）におけるテストデータのリストア処理



図－６２　リストア時のデータの流れ（検証項目 6-1：復元環境へのリストア）

（イ）検証項目 6-2：業務再開

リストアした業務アプリケーションソフトウェアを用いて業務を再開する。

イ　結果

（ア）検証項目 6-1：復元環境へのリストア

表－６３　復元環境へのリストア処理時間（検証項目 6-1）

（単位）時間：分：秒

	①B村→運営主体（データ転送）	②C市→運営主体（データ転送）	③運営主体での秘密分散処理	④運営主体→A町（復元環境）（データ転送）	⑤A町（復元環境／ストレージ）→A町（復元環境／職員端末）（データ転送）	⑥A町（復元環境／職員端末）におけるリストア処理	合計
パターン 1	0:09:35	0:09:28	0:02:14	0:04:54	0:02:12	0:04:18	0:32:41

（イ）検証項目 6-2：業務再開

復元環境において業務アプリケーションソフトウェアをリストアし、正常に作動する[68]ことを確認した（業務を継続して実施できることを確認した）。

ウ　まとめ

検証の結果、バックアップソフトウェアと秘密分散ソフトウェアを組み合わせて、復元環境へテストデータの復元し、業務を継続すること（被災時の応急対応）ができた。

また、B 村及び C 市に分散配置しているバックアップデータを運営主体にデー

68 実際の被災時においては、ハードウェア設置、ネットワーク敷設及びソフトウェアのインストール等のリストア環境整備に係る作業が必要となる。

タ転送、運営主体において秘密分散機能でリストアを実施、A 町（復元環境）のストレージにデータ転送するまでの一連の操作を運営主体のコンソールから実施することができた。

今回のテストデータのデータ量（3GB）において、復元環境へのリストア処理が完了するまでの所要時間は 30 分程度であった。

（８）＜検証 7＞ケーススタディ:被災時(復旧・復興)を想定した検証

表－６４　検証内容（検証項目 7-1、7-2、7-3）

検証項目	検証内容	検証パターン
7-1：復元環境からのバックアップ	被災時（復旧・復興）運用を想定して、復元環境からバックアップサイトへのバックアップが実施できるか確認する	（次表参照）
7-2：業務環境へのリストア	被災時（復旧・復興）運用を想定して、バックアップサイトから業務環境へのリストアが実施できるか確認する	
7-3：業務再開	被災時（復旧・復興）運用を想定して、業務環境において業務アプリケーションソフトウェアをリストアして業務を再開できるか確認する	

表－６５　検証パターン（検証項目 7-1、7-2、7-3）

データ量		ファイル構成			フォルダ構成
総データ量	1 ファイルあたりのデータ量	ファイル形式の多様性	データ全体の圧縮	ファイル作成元 OS 環境の多様性	
6GB	ファイルあたりのデータ量が概ね 1,000KB～5,000KB のファイルで構成	Word、Excel、PowerPoint、Access、Visio、PDF、テキスト、EXE などのファイル形式が混在（圧縮形式のファイルを含む）しているファイルで構成	データ全体を圧縮した構成	様々な OS（Windows、Mac、Linux など）環境で作成されたファイルが入り混じったファイルで構成	複数の階層構造、空フォルダを含むフォルダ構成

ア　実施手順

（ア）検証項目 7-1：復元環境からのバックアップ

A 町（復元環境）の職員端末に登録したテストデータ（更新データ）を、バックアップソフトウェアを用いて暗号化・圧縮してバックアップデータを作成し、これを A 町（復元環境）のストレージに保管する。A 町（復元環境）のストレージからバックアップデータを運営主体にデータ転送する。運営主体において秘密分散機能で暗号化・分割した上で、A 町（復元環境）、B 村及び C 市に分散配置する。

本検証で計測する時間は以下のとおり。

①A 町（復元環境／職員端末）におけるテストデータのバックアップ処理

②A 町（復元環境／職員端末）→A 町（復元環境／ストレージ）（データ転送）

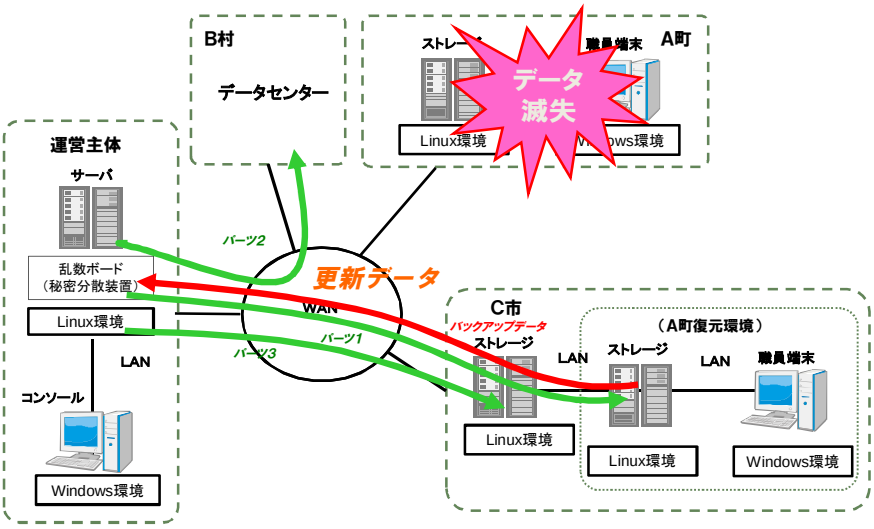
③A 町（復元環境）→運営主体（データ転送／バックアップデータ）

④運営主体での秘密分散処理

⑤運営主体→A 町（復元環境）（データ転送／パーツ 1）

⑥運営主体→B 村（データ転送／パーツ 2）

⑦運営主体→C 市（データ転送／パーツ 3）



図－６３　バックアップ時のデータの流れ（検証項目 7-1：復元環境からのバックアップ）

（イ）検証項目 7-2：業務環境へのリストア

検証項目 7-1 実施後に、A 町（業務環境）が復元・復旧したと想定して、B 村及び C 市に分散配置しているバックアップデータから、運営主体において秘密分散機能でリストアを行い、A 町（業務環境）のストレージにバックアップデータをデータ転送する。これを A 町（業務環境）の職員端末に保管し、バックアップソフトウェアを用いて元のテストデータ（更新データ）を復元する。

本検証で計測する時間は以下のとおり。

①B 村→運営主体（データ転送／パーツ 2）

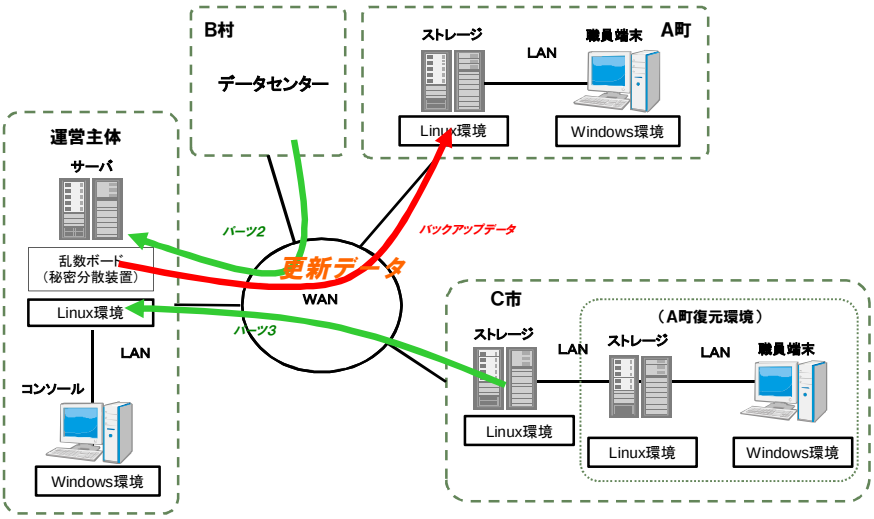
②C 市→運営主体（データ転送／パーツ 3）

③運営主体での秘密分散処理

④運営主体→A 町（業務環境）（データ転送／バックアップデータ）

⑤A 町（業務環境／ストレージ）→A 町（業務環境／職員端末）（データ転送）

⑥A 町（業務環境／職員端末）におけるテストデータのリストア処理



図－６４　リストア時のデータの流れ（検証項目 7-2：業務環境へのリストア）

（ウ）検証項目 7-3：業務再開

リストアした業務アプリケーションソフトウェアを用いて業務を再開する。

イ　結果

（ア）検証項目 7-1：復元環境からのバックアップ

表－６６　復元環境からのバックアップ処理時間（検証項目 7-1）

（単位）時間：分：秒

	①A町（復元環境／職員端末）におけるテストデータのバックアップ処理	②A町（復元環境／職員端末）→A町（復元環境／ストレージ）（データ転送）	③A町（復元環境）→運営主体（データ転送）	④運営主体での秘密分散処理	⑤運営主体→A町（復元環境）（データ転送）	⑥運営主体→B村（データ転送）	⑦運営主体→C市（データ転送）	合計
パターン 1	0:10:30	0:04:10	0:33:43	0:11:35	0:03:42	0:03:38	0:04:55	1:12:13

（イ）検証項目 7-2：業務環境へのリストア

表－６７　業務環境へのリストア処理時間（検証項目 7-2）

（単位）時間：分：秒

	①B村→運営主体（データ転送）	②C市→運営主体（データ転送）	③運営主体での秘密分散処理	④運営主体→A町（データ転送）	⑤A町（業務環境／ストレージ）→A町（業務環境／職員端末）（データ転送）	⑥A町（業務環境／職員端末）におけるテストデータのリストア処理	合計
パターン 1	0:18:58	0:18:57	0:04:55	0:10:13	0:04:12	0:05:31	1:02:46

（ウ）検証項目 7-3：業務再開

業務環境において業務アプリケーションソフトウェアをリストアし、正常に作動する[69]ことを確認した（業務を継続して実施できることを確認した）。

ウ　まとめ

検証の結果、バックアップソフトウェアと秘密分散ソフトウェアを組み合わせて、復元環境からのバックアップしたテストデータを業務環境に復元し、業務を継続すること（被災時の復旧・復興対応）ができた。

また、A 町（復元環境）のストレージからバックアップデータを運営主体にデータ転送、運営主体において秘密分散機能で暗号化・分割を実施、A 町（復元環境）、B 村及び C 市に分散配置するまでの操作、B 村及び C 市に分散配置しているバックアップデータを運営主体にデータ転送、運営主体において秘密分散機能でリストアを実施、及び、A 町（業務環境）のストレージにデータ転送するまでの操作を、運営主体のコンソールから実施することができた。

今回のテストデータのデータ量（6GB）において、復元環境からのバックアップ処理及び業務環境へのリストア処理が完了するまでの所要時間はそれぞれ 1 時間程度であった。

（９）ケーススタディのまとめ（検証項目 5～7）

検証 5～7 の結果、バックアップソフトウェアと秘密分散ソフトウェアを組み合わせて、平常時、被災時の応急対応及び復旧・復興対応が可能であることが示された。

また、運営主体から各団体のディレクトリへのデータ格納、データの取得及び削除等が運営主体のコンソールから実施可能であったことから、運営主体がバックアップサイトを集中管理できることが示された。履歴管理の面においては、運営主体の秘密分散ログにて転送時間、分散時間等を取得可能であり、運用ログにより過去分の履歴管理の活用が可能であることが示された。なお、今回の検証範囲外であったが、各団体のストレージ容量、サーバ運用等を、ネットワーク経由で監視することにより、運営主体においてバックアップサイト上のすべてのサーバ、ストレージ、ネットワーク等の統合監視運用が可能となる。

バックアップ処理及びリストア処理に要した所要時間については、データ量（3GB）においてそれぞれ 30 分程度、データ量（6GB）においてそれぞれ 1 時間程度であることから、実際の運用にも耐えられると推察される。

---

[69] 実際の被災時においては、ハードウェア設置、ネットワーク敷設及びソフトウェアのインストール等のリストア環境整備に係る作業が必要となる。

4　補足 増分バックアップを含めたケーススタディ

前項までは、地方公共団体のクラウド型バックアップサイトを実現する上で必要となる基本的な機能の実現性について検証した。

実際の運用においては、バックアップ処理の効率化を目的として増分バックアップ[70]を実施することが想定される。そのため、増分バックアップを実施した場合にも、バックアップサイトが支障なく運用できることを確認する。

（１）実証範囲

バックアップソフトウェアと秘密分散ソフトウェアの組合せにおいて、増分バックアップが正常に機能するか検証する。

（２）実証仕様

ア　前提条件[71]

（ア）ネットワーク[72]

・ネットワークは LAN 環境（100Mbps）を用いる。

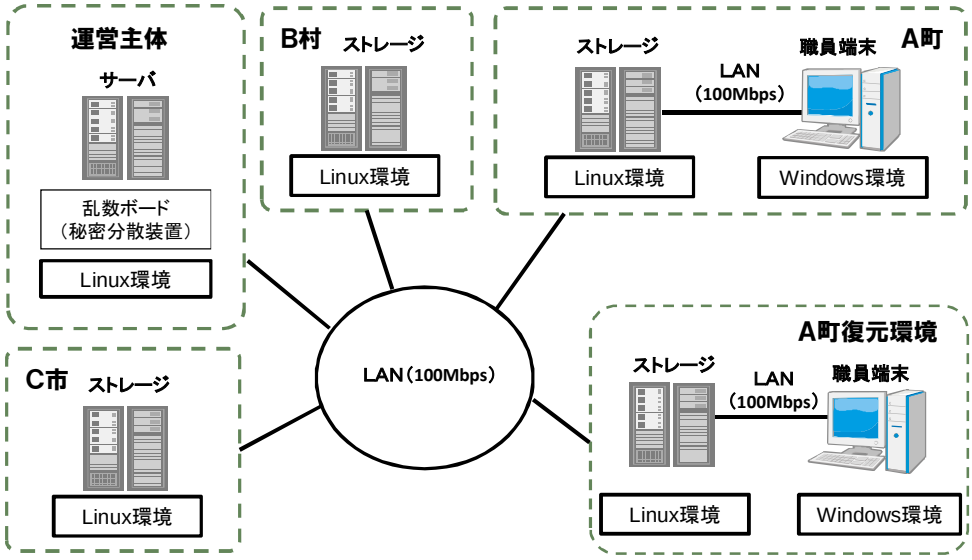
イ　実施環境

（ア）基本的な考え方

・本追加検証においては、LAN 環境において実施環境を構成する。

（イ）機器構成

実証実験の機器構成を以下に示す。



図－６５　実証実験の機器構成（増分バックアップを含めたケーススタディ）

---

[70] 増分バックアップは、「（章末）参考資料　バックアップ・リストア方法」を参照のこと。
[71] ネットワーク以外の前提条件は、「第３節－2－(1)　前提条件」を参照のこと。
[72] データ転送に要する所要時間は、スループット等の影響を受けて前後する可能性がある。本調査研究において、各検証項目は１回ずつ検証を実施するため、より厳密に所要時間を計測するには、複数回検証を実施して平均値を算出する必要等がある。

表－６８　実証実験の機器構成仕様（増分バックアップを含めたケーススタディ）

区分	種別	メーカ名及び品番	CPU	メモリ	ディスク容量	真性乱数ボード	アプリケーション	OS
A町	ストレージ	ニューテックSmartNAS	ATOM Dual Core 1.86GHz	4GB	8TB			CentOS 5.8
	職員端末（PC）	DELL VOSTRO	Core i3 3.3Ghz	4GB	1TB		True Image2013 (Acronis)	Windows 7（64）
B村	ストレージ	ニューテックSmartNAS	ATOM Dual Core 1.86GHz	4GB	8TB			CentOS 5.8
C市	ストレージ	ニューテックSmartNAS	ATOM Dual Core 1.86GHz	4GB	8TB			CentOS 5.8
運営主体	サーバ	ニューテックNAP-6100	Xeon 2.4GHz	6GB	1TB	GRANG-PC IC-8CH (LE Tech)	SECLANCER（ケイレックス）	CentOS 5.8
A町復元環境	ストレージ	ニューテックSmartNAS	ATOM Dual Core 1.86GHz	4GB	8TB			CentOS 5.8
	職員端末（PC）	DELL VOSTRO	Core i3 3.3Ghz	4GB	1TB		True Image2013 (Acronis)	Windows 7（64）

ウ　実施概要

検証項目[73]を以下に示す。

＜検証 8＞ケーススタディ：平常時及び被災時（応急対応）を想定した検証（増分バックアップを含む）

＜検証 9＞ケーススタディ：被災時（復旧・復興）を想定した検証（増分バックアップを含む）

[73] 検証 1～7 の内容及びケーススタディのシナリオは、「第 3 節－2－（3）実施概要」を参照のこと。

（３）実証内容及び結果

ア　＜検証 8＞ケーススタディ：平常時及び被災時（応急対応）を想定した検証（増分バックアップを含む）

表－６９　検証内容（検証項目 8-1、8-2、8-3、8-4）

検証項目	検証内容	検証パターン
8-1 : 業務環境からのバックアップ	平常時運用を想定して、業務環境からバックアップサイトへのバックアップが実施できるか確認する	（次表参照）
8-2 : 業務環境からの増分バックアップ	平常時運用を想定して、業務環境からバックアップサイトへの増分バックアップが実施できるか確認する	
8-3 : 復元環境へのリストア	被災時（応急対応）運用を想定して、（検証項目 8-1 実施後に）バックアップサイトから復元環境へのリストアが実施できるか確認する	
8-4 : 業務再開	被災時（応急対応）運用を想定して、復元環境において業務アプリケーションソフトウェアをリストアして業務を再開できるか確認する	

表－７０　検証パターン（検証項目 8-1）

検証パターン	データ量		ファイル構成			フォルダ構成
	総データ量	1 ファイルあたりのデータ量	ファイル形式の多様性	データ全体の圧縮	ファイル作成元 OS 環境の多様性	
パターン 1	3GB	ファイルあたりのデータ量が概ね 1,000KB～5,000KB のファイルで構成	Word、Excel、PowerPoint、Access、Visio、PDF、テキスト、EXE などのファイル形式が混在（圧縮形式のファイルを含む）しているファイルで構成	データ全体を圧縮した構成	様々な OS（Windows、Mac、Linux など）環境で作成されたファイルが入り混じったファイルで構成	複数の階層構造、空フォルダを含むフォルダ構成

表－７１　検証パターン（検証項目 8-2）

検証パターン	データ量		ファイル構成			フォルダ構成
	総データ量	1 ファイルあたりのデータ量	ファイル形式の多様性	データ全体の圧縮	ファイル作成元 OS 環境の多様性	
パターン 1	3GB	ファイルあたりのデータ量が概ね 1,000KB～5,000KB のファイルで構成	Word、Excel、PowerPoint、Access、Visio、PDF、テキスト、EXE などのファイル形式が混在（圧縮形式のファイルを含む）しているファイルで構成	データ全体を圧縮した構成	様々な OS（Windows、Mac、Linux など）環境で作成されたファイルが入り混じったファイルで構成	複数の階層構造、空フォルダを含むフォルダ構成
パターン 2	1GB					
パターン 3	500MB					

表－７２　検証パターン（検証項目 8-3、8-4）

データ量		ファイル構成			フォルダ構成
総データ量	1 ファイルあたりのデータ量	ファイル形式の多様性	データ全体の圧縮	ファイル作成元 OS 環境の多様性	
3GB	ファイルあたりのデータ量が概ね 1,000KB～5,000KB のファイルで構成	Word、Excel、PowerPoint、Access、Visio、PDF、テキスト、EXE などのファイル形式が混在（圧縮形式のファイルを含む）しているファイルで構成	データ全体を圧縮した構成	様々な OS（Windows、Mac、Linux など）環境で作成されたファイルが入り混じったファイルで構成	複数の階層構造、空フォルダを含むフォルダ構成

（ア）実施手順

ａ　検証項目 8-1：業務環境からのバックアップ

A 町（業務環境）の職員端末に登録したテストデータ（初期データ）を、バックアップソフトウェアを用いて暗号化・圧縮してバックアップデータを作成し、これをA町（業務環境）のストレージに保管する。A 町（業務環境）のストレージからバックアップデータを運営主体にデータ転送する。運営主体において秘密分散機能で暗号化・分割した上で、A 町（業務環境）、B 村及び C 市に分散配置する。

本検証で計測する時間は以下のとおり。

①A 町（業務環境／職員端末）におけるテストデータのバックアップ処理

②A 町（業務環境／職員端末）→A 町（業務環境／ストレージ）（データ転送）

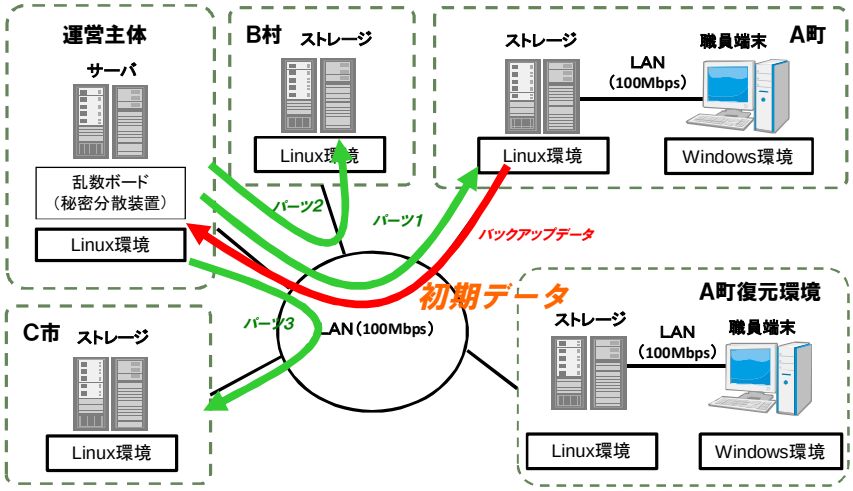
③A 町（業務環境）→運営主体（データ転送／バックアップデータ）

④運営主体での秘密分散処理

⑤運営主体→A 町（業務環境）（データ転送／パーツ 1）

⑥運営主体→B 村（データ転送／パーツ 2）

⑦運営主体→C 市（データ転送／パーツ 3）



図－６６　バックアップ時のデータの流れ[74]（検証項目 8-1：業務環境からのバックアップ）

b　検証項目 8-2：業務環境からの増分バックアップ

A 町（業務環境）の職員端末に登録したテストデータ（追加データ）を、バックアップソフトウェアを用いて暗号化・圧縮してバックアップデータを作成し、これを A 町（業務環境）のストレージに保管する。A 町（業務環境）のストレージからバックアップデータを運営主体にデータ転送する。運営主体において秘密分散機能で暗号化・分割した上で、A 町（業務環境）、B 村及び C 市に分散配置する。

本検証で計測する時間は以下のとおり。

①A 町（業務環境／職員端末）におけるテストデータのバックアップ処理
②A 町（業務環境／職員端末）→A 町（業務環境／ストレージ）（データ転送）
③A 町（業務環境）→運営主体（データ転送）
④運営主体での秘密分散処理
⑤運営主体→A 町（業務環境）（データ転送）
⑥運営主体→B 村（データ転送）
⑦運営主体→C 市（データ転送）

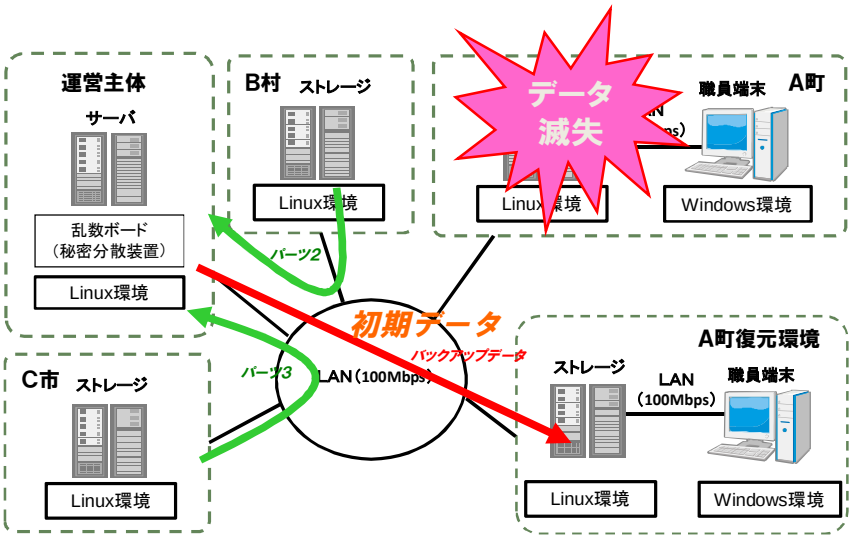
c　検証項目 8-3：復元環境へのリストア

検証項目 8-1 実施後に災害が発生し、A 町（業務環境）が壊滅してテストデータ（初期データ）が滅失した場合を想定し、B 村及び C 市に分散配置しているバックアップデータから、運営主体において秘密分散機能でリストアを行い、A 町（復元環境）のストレージにバックアップデータをデータ転送する。これを A 町（復元環境）の職員端末に保管し、バックアップソフトウェアを用いて元のテストデータ（初期データ）を復元する。

本検証で計測する時間は以下のとおり。

[74] 検証項目 8-2 についても同様の流れである。

①B 村→運営主体（データ転送／パーツ 2）
②C 市→運営主体（データ転送／パーツ 3）
③運営主体での秘密分散処理
④運営主体→A 町（復元環境）（データ転送／バックアップデータ）
⑤A 町（復元環境／サーバ）→A 町（復元環境／職員端末）（データ転送）
⑥A 町（復元環境／職員端末）におけるテストデータのリストア処理



図－６７　リストア時のデータの流れ（検証項目 8-3：復元環境へのリストア）

d　検証項目 8-4：業務再開

リストアした業務アプリケーションソフトウェアを用いて業務を再開する。

（イ）結果

a　検証項目 8-1：業務環境からのバックアップ

表－７３　業務環境からのバックアップ処理時間（検証項目 8-1）

（単位）時間：分：秒

	①A 町（業務環境／職員端末）における暗号化（バックアップ）	②A 町（業務環境／職員端末）→A 町（ストレージ）（データ転送）	③A 町→運営主体（データ転送）	④運営主体での秘密分散処理	⑤運営主体→A 町（データ転送）	⑥運営主体→B 村（データ転送）	⑦運営主体→C 市（データ転送）	合計
パターン 1	0:05:52	0:03:00	0:14:07	0:05:21	0:01:41	0:01:40	0:01:40	0:33:21

b　検証項目 8-2：業務環境からの増分バックアップ

表－７４　業務環境からの増分バックアップ処理時間（検証項目 8-2）

（単位）時間：分：秒

	①A町（業務環境／職員端末）における暗号化（バックアップ）	②A町（業務環境／職員端末）→A町（ストレージ）（データ転送）	③A町→運営主体（データ転送）	④運営主体での秘密分散処理	⑤運営主体→A町（データ転送）	⑥運営主体→B村（データ転送）	⑦運営主体→C市（データ転送）	合計
パターン 1	0:05:36	0:03:02	0:13:12	0:05:15	0:01:40	0:01:40	0:01:41	0:32:06
パターン 2	0:02:27	0:01:04	0:04:42	0:01:48	0:00:34	0:00:34	0:00:33	0:11:42
パターン 3	0:01:40	0:00:34	0:02:17	0:00:55	0:00:17	0:00:17	0:00:17	0:06:17

c　検証項目 8-3：復元環境へのリストア

表－７５　復元環境へのリストア処理時間（検証項目 8-3）

（単位）時間：分：秒

	①B村→運営主体（データ転送）	②C市→運営主体（データ転送）	③運営主体での秘密分散処理	④運営主体→A町（復元環境）（データ転送）	⑤A町の復元環境（ストレージ）→A町の復元環境（職員端末）（データ転送）	⑥A町の復元環境（職員端末）におけるリストア処理	合計
パターン 1	0:01:40	0:01:40	0:02:08	0:02:58	0:03:00	0:04:18	0:15:44

d　検証項目 8-4：業務再開

復元環境において業務アプリケーションソフトウェアをリストアし、正常に作動する[75]ことを確認した（業務を継続して実施できることを確認した）。

（ウ）まとめ

検証 8-1 については、検証 5 とほぼ同じ結果が得られた。秘密分散に係る時間は、検証 5 が「0:05:43」、検証 8-1 が「0:05:21」である。

なお、検証 5 と検証 8-1 の検証結果において、A 町（職員端末）→A 町（サーバ）に係る時間、各拠点間のデータ転送に係る時間のそれぞれに差異が生じている理由は、実証実験を実施したネットワーク環境が異なるためである。

また検証 8-2 の結果から、バックアップソフトウェアと秘密分散ソフトウェアを組み合わせて、増分バックアップを実施できることを確認した。

検証 8-3 については、検証 6-1 とほぼ同じ結果が得られた。秘密分散に係る時間は、検証 6-1 が「0:02:14」、検証 8-3 が「0:02:08」である。なお、検証 6-1

[75] 実際の被災時においては、ハードウェア設置、ネットワーク敷設及びソフトウェアのインストール等のリストア環境整備に係る作業が必要となる。

と検証 8-3 の検証結果において、各拠点間のデータ転送に係る時間、A 町の復元環境（サーバ）→A 町の復元環境（職員端末）に係る時間のそれぞれに差異が生じている理由は、実証実験を実施したネットワーク環境が異なるためである。

イ　<検証 9>ケーススタディ：被災時（復旧・復興）を想定した検証（増分バックアップを含む）

表－７６　検証内容（検証項目 9-1、9-2、9-3）

検証項目	検証内容	検証パターン
9-1：復元環境からの増分バックアップ	被災時（復旧・復興）運用を想定して、復元環境からバックアップサイトへの増分バックアップが実施できるか確認する	（次表参照）
9-2：業務環境へのリストア	被災時（復旧・復興）運用を想定して、バックアップサイトから業務環境へのリストアが実施できるか確認する	
9-3：業務再開	被災時（復旧・復興）運用を想定して、業務環境において業務アプリケーションソフトウェアをリストアして業務を再開できるか確認する	

表－７７　検証パターン（検証項目 9-1）

検証パターン	データ量		ファイル構成			フォルダ構成
	総データ量	1 ファイルあたりのデータ量	ファイル形式の多様性	データ全体の圧縮	ファイル作成元 OS 環境の多様性	
パターン 1	3GB	ファイルあたりのデータ量が概ね 1,000KB～5,000KB のファイルで構成	Word、Excel、PowerPoint、Access、Visio、PDF、テキスト、EXE などのファイル形式が混在（圧縮形式のファイルを含む）しているファイルで構成	データ全体を圧縮した構成	様々な OS（Windows、Mac、Linux など）環境で作成されたファイルが入り混じったファイルで構成	複数の階層構造、空フォルダを含むフォルダ構成
パターン 2	1GB					
パターン 3	500MB					

表－７８　検証パターン（検証項目 9-2、9-3）

検証パターン	データ量		ファイル構成			フォルダ構成
	総データ量	1ファイルあたりのデータ量	ファイル形式の多様性	データ全体の圧縮	ファイル作成元 OS 環境の多様性	
パターン 1	3GB+3GB	ファイルあたりのデータ量が概ね 1,000KB～5,000KB のファイルで構成	Word、Excel、PowerPoint、Access、Visio、PDF、テキスト、EXE などのファイル形式が混在（圧縮形式のファイルを含む）しているファイルで構成	データ全体を圧縮した構成	様々な OS（Windows、Mac、Linux など）環境で作成されたファイルが入り混じったファイルで構成	複数の階層構造、空フォルダを含むフォルダ構成
パターン 2	3GB+1GB					
パターン 3	3GB+500MB					

（ア）実施手順

a　検証項目 9-1：復元環境からの増分バックアップ

A 町（復元環境）の職員端末に登録したテストデータ（追加データ）からバックアップソフトウェアを用いて暗号化・圧縮してバックアップデータを作成し、これを A 町（復元環境）のストレージに保管する。A 町の復元環境のストレージからバックアップデータを運営主体にデータ転送する。運営主体において秘密分散機能で暗号化・分割した上で、A 町（復元環境）、B 村及び C 市に分散配置する。

本検証で計測する時間は以下のとおり。

①A 町（復元環境／職員端末）におけるテストデータのバックアップ処理

②A 町（復元環境／職員端末）→A 町（復元環境／ストレージ）（データ転送）

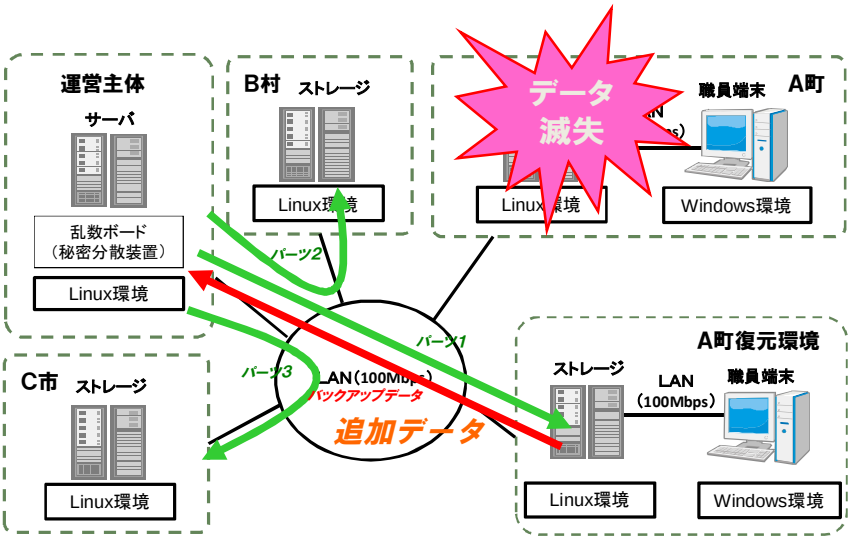
③A 町（復元環境）→運営主体（データ転送／バックアップデータ）

④運営主体での秘密分散処理

⑤運営主体→A 町（復元環境）（データ転送／パーツ 1）

⑥運営主体→B 村（データ転送／パーツ 2）

⑦運営主体→C 市（データ転送／パーツ 3）



図－６８バックアップ時のデータの流れ（検証項目 9-1：復元環境からの増分バックアップ）

b　検証項目 9-2：業務環境へのリストア

検証項目 9-1 実施後に、A 町（業務環境）が復元・復旧したと想定して、B 村及び C 市に分散配置しているバックアップデータから、運営主体において秘密分散機能でリストアを行い、A 町（業務環境）のストレージにバックアップデータをデータ転送する。これを A 町（業務環境）の職員端末に保管し、バックアップソフトウェアを用いて元のテストデータ（初期データ及び追加データ）を復元する。

本検証で計測する時間は以下のとおり。

①B 村→運営主体（データ転送／パーツ 2）

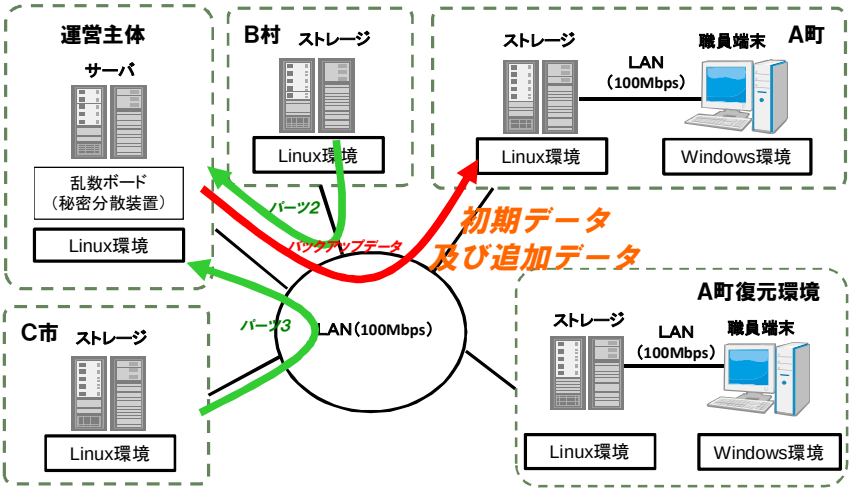
②C 市→運営主体（データ転送／パーツ 3）

③運営主体での秘密分散処理

④運営主体→A 町（業務環境）（データ転送／バックアップデータ）

⑤A 町（業務環境／ストレージ）→A 町（業務環境／職員端末）（データ転送）

⑥A 町（業務環境／職員端末）におけるテストデータのリストア処理



図－６９　リストア時のデータの流れ（検証項目 9-2：業務環境へのリストア）

c　検証項目 9-3：業務再開

リストアした業務アプリケーションソフトウェアを用いて業務を再開する。

（イ）結果

a　検証項目 9-1：復元環境からの増分バックアップ

表－７９　復元環境からのバックアップ処理時間（検証項目 9-1）

（単位）時間：分：秒

	①A 町（復元環境／職員端末）におけるテストデータのバックアップ処理	②A 町（復元環境／職員端末）→A 町（復元環境／ストレージ）（データ転送）	③A 町（復元環境）→運営主体（データ転送）	④運営主体での秘密分散処理	⑤運営主体→A 町（復元環境）（データ転送）	⑥運営主体→B 村（データ転送）	⑦運営主体→C 市（データ転送）	合計
パターン 1	0:05:36	0:03:00	0:13:16	0:05:17	0:01:39	0:01:40	0:01:40	0:32:08
パターン 2	0:02:28	0:01:06	0:04:39	0:01:48	0:00:35	0:00:34	0:00:35	0:11:45
パターン 3	0:01:39	0:00:36	0:02:20	0:00:59	0:00:18	0:00:18	0:00:18	0:06:28

ｂ　検証項目 9-2：業務環境へのリストア

表－８０　業務環境へのリストア処理時間（検証項目 9-2、9-3）

（単位）時間：分：秒

	①Ｂ村→運営主体（データ転送）	②Ｃ市→運営主体（データ転送）	③運営主体での秘密分散処理	④運営主体→Ａ町（データ転送）	⑤Ａ町（業務環境／ストレージ）→Ａ町（業務環境／職員端末）（データ転送）	⑥Ａ町（業務環境／職員端末）におけるテストデータのリストア処理	合計
パターン 1	0:03:22	0:03:21	0:04:50	0:05:56	0:06:00	0:05:30	0:28:59
パターン 2	0:02:04	0:02:04	0:03:42	0:03:59	0:04:02	0:04:31	0:20:22
パターン 3	0:01:58	0:01:58	0:03:04	0:03:26	0:03:32	0:04:26	0:18:24

ｃ　検証項目 9-3：業務再開

業務環境において業務アプリケーションソフトウェアをリストアし、正常に作動する[76]ことを確認した（業務を継続して実施できることを確認した）。

（ウ）まとめ

検証の結果、バックアップソフトウェアと秘密分散ソフトウェアを組み合わせて、復元環境からの増分バックアップを実施できることを確認した。

検証 9-2 については、検証 7-2 とほぼ同じ結果が得られた。秘密分散に係る時間は、パターン 1(3GB)において、検証 7-2 が「0:04:55」、検証 9-2 が「0:04:50」である。なお、検証 7-2 と検証 9-2 の検証結果において、各拠点間のデータ転送に係る時間、A 町（サーバ）→A 町（職員端末）に係る時間のそれぞれに差異が生じている理由は、実証実験を実施したネットワーク環境が異なるためである。

ウ　増分バックアップを含めたケーススタディのまとめ（検証項目 8～9）

検証 8～9 の結果、バックアップソフトウェアと秘密分散ソフトウェアを組み合わせて、増分バックアップが可能なこと、バックアップ（フルバックアップ）及び増分バックアップを組み合わせて、平常時、被災時の応急対応及び復旧・復興対応が可能であることが示された。

[76] 実際の被災時においては、ハードウェア設置、ネットワーク敷設及びソフトウェアのインストール等のリストア環境整備に係る作業が必要となる。

５　実証実験を経て

以上のように、一般に利用可能な既存技術を用いて、複数の団体間で相互に情報を保管しあうクラウド型バックアップサイトが具備すべき主な基本機能は実現可能であることが明らかになった。

特に、本実験で検証した秘密分散技術を用いることで、各団体が相互に保管する情報は、分散暗号化（断片化）されたものとなり、その断片一つからでは決して元の情報を復元することはできない。そのため、その断片一つ一つは、個人情報等の保護対象の情報には該当せず、単なる記号の羅列に過ぎないものとなる。

なお、クラウドコンピューティングの技術の利用に際しては、ネットワークの性能やコスト等が問題視されるが、インターネットや多様なモバイル端末の急激な普及拡大、今後想定される大規模災害に向けた ICT-BCP の実現等のために、ネットワークそのものや効率的なバックアップ等に関する技術開発が加速する傾向にある。以下においては、そのような技術のなかで、クラウド型バックアップサイトにも活用可能な事例を紹介する。

現時点では、今回のようなクラウド型バックアップサイトの事例は未だないが、本検討及び実験の結果等が、第 2 章において示したバックアップ・リストア基準に則した行政データ管理を支えるインフラ及びツールとしての当該サイトの普及を推進し、災害に強い地方公共団体の情報システムを実現する上での一助となることを願って止まない。

〔Open Flow 技術の活用〕

近年ネットワークに関する基盤技術なかで、Open Flow という技術が注目を集めている。この技術を用いることにより、「ネットワーク構成の動的な変更」が可能となり、ネットワーク全体の冗長性、信頼性の向上を図ることができる。また、時間帯やサイト間（例：A 市と運営主体間等）を特定し、その間の通信経路を制御する等が可能になり、通信コストを抑えつつ一定の品質や信頼性を確保することが可能となる。

〔重複排除機能等の活用〕

バックアップ処理時間の短縮やバックアップデータ量を削減することは、システムの保守・管理の効率化やコスト削減に資するだけでなく、ネットワークを介してデータをバックアップするクラウド型バックアップサイトを利用する上でも非常に有益である。近年は、重複排除機能を高度化したバックアップソフトや、そのような機能を備えたデータストレージが開発されている。これらを活用し、バックアップするデータ量を適正化することで、ネットワーク上の輻輳軽減による信頼性向上、通信時間の縮減によるコストの削減等が期待される。

参考資料　秘密分散機能

地方公共団体が管理・運用を行うデータには、個人情報をはじめ機密性が高く、取扱い等について法令により規定されているものが少なくない。ICT を活用した機密保護や関係法令等への対応を検討することが必要であり有用である。

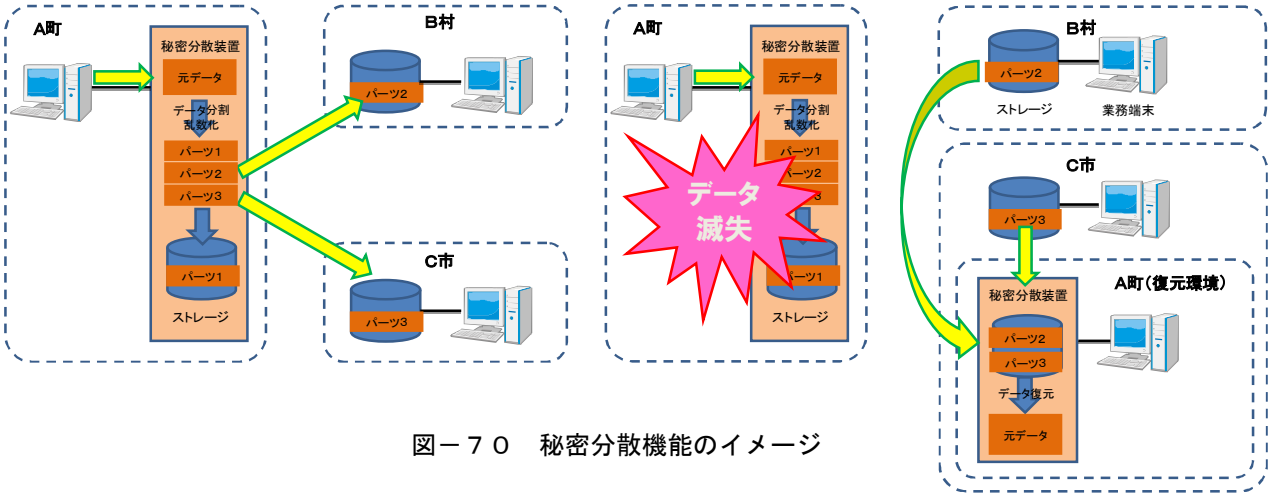
そのため、本調査研究では、以下に示す秘密分散方式（機能）を用い、関係法令等を遵守したデータの取扱いを実現し、かつ災害等によるデータ滅失に備えた信頼性の高いデータバックアップ方式の実効性等を検証する。

〔機能のポイント〕

・元データが機密情報（例：個人情報等）であっても、秘密分散され異なる場所に保管されたパーツ（1～3）それぞれは、機密情報に該当するものではなくなる。
　→　複数の保管場所が必要
・元データは、2 つのパーツが揃わないと復元することができない。

〔バックアップの例〕　　〔リストアの例〕

他自治体に復元環境を構築しデータを復元、業務継続する例



図－７０　秘密分散機能のイメージ

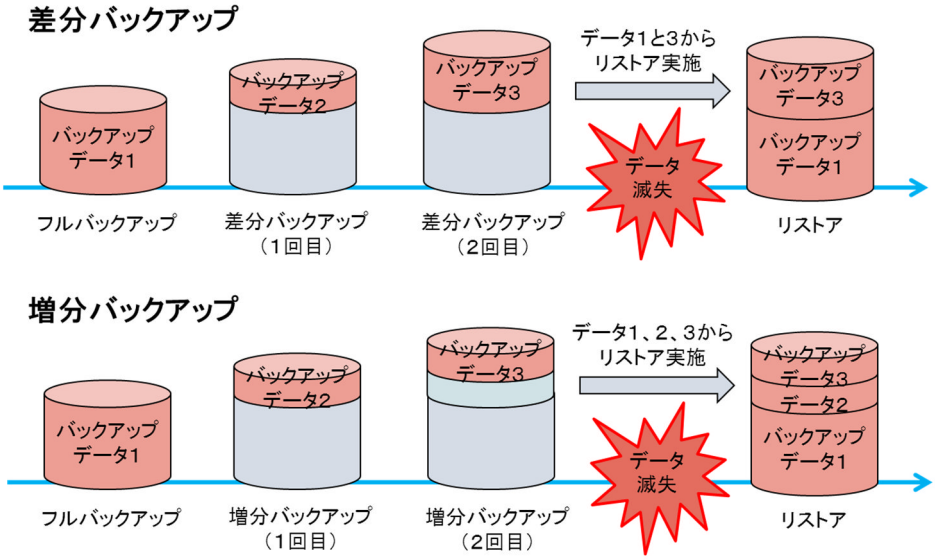
参考資料　バックアップ・リストア方法

〔バックアップ方法〕

差分バックアップは、フルバックアップを実施した時点から更新（追加、変更及び削除）されたデータのバックアップを実施する。リストアするためには、最新の差分バックアップとフルバックアップのバックアップデータが必要になる。

増分バックアップは、前回バックアップを実施した時点から更新（追加、変更及び削除）されたデータのバックアップを実施する。バックアップ時間は差分バックアップよりも短くなるが、リストアするためには、すべてのバックアップのバックアップデータが必要になる。

本実証実験においては、実際にバックアップサイトを運用した際のバックアップ処理の効率化を目的として、増分バックアップについて検証を実施する。



図－７１　リストア処理に必要になるバックアップデータ

〔リストア方法〕

データの滅失が発生した際には、バックアップサイトに保管しているバックアップデータからデータをリストアする。バックアップされているデータ量が非常に大きい場合には、ネットワーク経由でリストアするのに非常に長い時間を要するため、外部媒体を利用してバックアップデータを回収してリストアする方法も想定される。

おわりに ～災害に強い地方公共団体の情報システムの実現に向けて～

本調査研究では、**「行政データ管理のあり方とバックアップサイト」**に焦点を当てて、下記のとおり取りまとめた。

１　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

本調査研究において、東日本大震災の被災団体における行政データの管理の実態やその滅失等による住民サービスへの影響等を調査した結果、次のことが明らかになった。

・今回の震災により電子データや紙データの滅失があった。
・データ滅失の被害があった地方公共団体では、行政事務や住民サービスの復旧に要した期間が長期化し、調査段階において復旧できていない事例もある。

上記のような事態に備えるためには、地方公共団体における行政データの適切な管理の一環として、行政データのバックアップ及びリストアが重要になることから、全庁的な統一ルールの策定が必要になると考える。

地方公共団体における行政データの適切な管理は、主に公文書管理規程、情報セキュリティポリシー並びに ICT-BCP の策定・実施が鍵になる。そのため、行政データのバックアップ及びリストアについては、それらの中で相互に関連づけされながら、位置づけられることが必要になる。

その上で、データのバックアップという観点及び地方公共団体における前述の 3 つの策定状況[77]から鑑みるに、本調査研究では、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する解決方策について検討し、既存のデータ管理に関わる規則・規程等を収集、分析、参考としながら、バックアップ・リストア基準を策定し、情報セキュリティポリシーの実施手順の一つとして位置づけることとした。

情報セキュリティポリシーでは、主に情報システム及び電子データを対象範囲としているため、システムとして管理されている電子データのみならず、ローカル PC 等に保存されている電子データについてもバックアップの対象となる。

また、情報セキュリティポリシーの対象範囲に含まれていない情報システムで取り扱うデータを印刷した文書やシステム関連文書以外の文書についても、今回のヒアリング調査において「重要な情報」であることが確認できたため、可能な限り紙データについても重要度の分類を実施し、電子化を推進することが重要と考える。

具体的には、バックアップ・リストア基準は、①基礎となるデータの整備、②データのバックアップ方法構築のポイント、③バックアップ媒体の保管方法構築のポイント、

---

77 情報セキュリティポリシーと ICT-BCP の策定状況については、「地方自治情報管理概要～電子自治体の推進状況（平成２３年４月１日現在）～」P33 と P41 を参照のこと。
http://www.soumu.go.jp/denshijiti/pdf/120327_1.pdf
なお、特定被災地方公共団体における ICT-BCP 等の策定状況については、「第１章　第１節―２　アンケート調査」を参照のこと。

④バックアップ手順書策定におけるポイント、⑤リストア手順書策定におけるポイントについて検証している。

上記の①では、前述の対象範囲を明確にした上で、日々の運用においては、情報システムはシステム更改等による改編があり、電子データは日々増減するため、定期的な情報システムの棚卸や電子データの重要度の分類の見直しを実施することを推奨している。

②では、行政データの更新頻度や参照頻度に応じてバックアップ頻度を見直すことで、被災時における行政データの滅失を最小限に抑えることができると考えている。

③では、バックアップデータを保管するに当たり、今回の震災における被災の広範囲さ及び庁舎の壊滅等を踏まえ、バックアップデータはできるだけ遠隔地に保管することが望ましいと考える。

そして、④～⑤では、被災時に遠隔地保管したバックアップデータをリストアするに当たり、職員（最悪の場合は他部署の職員）が混乱の中で手順書どおりに作業ができるよう、各機能別の手順書ではなく、実際の作業の流れに沿ったバックアップ・リストア手順書を整備することが望ましいと考えられる。また、その後、バックアップ・リストア手順書に基づき、リストアに係る訓練を行うことで、被災時の対応がスムーズになると考えられる。

上記のとおり、各地方公共団体においては、各々の実情に応じたバックアップ・リストア基準の策定を行って頂きたい。運用においては、P（Plan 計画）、D（Do 実行）、C（Check 評価）、A（Act 改善）を着実に実施し、状況変化に対応したバックアップ・リストア基準の維持・管理に努めて頂きたいと願うところである。

2　ICT 部門におけるバックアップサイトの利活用方策

本調査研究では、前述のバックアップ・リストア基準に基づき取得したバックアップデータをどのような方法（バックアップサイト）で管理・保管するかについて、行政データのバックアップサイトの利活用形態及びその有効性、運用性等を検証し、取りまとめた。

バックアップサイトの実際の組合せパターンは数多く存在するが、本調査研究においては、想定事例として次の 5 つの事例を挙げている。

- 〔想定事例 1〕本庁舎内にバックアップデータを媒体で保管する。
- 〔想定事例 2〕自地方公共団体内の支所等（本庁舎外）にバックアップデータを媒体又はネットワーク経由で保管する。
- 〔想定事例 3〕他地方公共団体にバックアップデータを媒体又はネットワーク経由で保管する。
- 〔想定事例 4〕民間事業者にバックアップデータを媒体で保管する。
- 〔想定事例 5〕民間事業者にバックアップデータをネットワーク経由で保管する。

各地方公共団体におけるバックアップサイトの選択においては、団体規模、予算、業務の内容、バックアップの頻度等、各地方公共団体の抱える事情に応じて検討してほしいと考えている。

その上で、地方公共団体におけるバックアップサイトの構成要素を踏まえて、より災害に強いバックアップサイトの条件として、遠隔地への保管、地方公共団体と同等以上のセキュリティレベルの確保、ネットワーク経由のデータ転送による柔軟なバックアップ・リストア処理の実現、共同利用によるコストメリットを考慮して、次の 4 つのケースを想定し検討を行った。

- [ケース 1]市町村が自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。
- [ケース 2]都道府県が自庁舎施設内に設置するシステムを、当該都道府県内の団体（市町村）がバックアップサイトとして共同利用する。
- [ケース 3]民間データセンターを、地方公共団体がバックアップサイトとして共同利用する。
- [ケース 4]複数の地方公共団体が自庁舎施設内に設置するシステムを、バックアップサイトとして相互に利用する（クラウド型バックアップサイト）。

上記の 4 つのケースについて、バックアップサイトのセキュリティ、保守・運用に係る作業負荷、構築・運用に係る費用、個人情報の保管先としての承認の容易さの観点から評価したところ、[ケース 4]が相対的に高い評価結果となった。このため、複数の地方公共団体が一つのシステムを共同利用せずに、地方公共団体のシステムを相互に共同利用する[ケース 4]を対象とした実証実験を実施し、その実現性、実用性及び運用性に関する検討を行った。

実証実験の対象としたクラウド型バックアップサイトは、バックアップ対象のデータを設定したディレクトリに集合させてバックアップデータを作成する機能（データ・アグリゲーション（Data Aggregation）機能）と、バックアップデータの秘匿性を担保する機能（秘匿機能）、各地方公共団体のバックアップサイトの状態監視とバックアップデータの保管先を管理する機能（ストレージ・コンパクション（Storage Compaction）機能）によって構成される。

このクラウド型バックアップサイトは、現時点では本事例は存在していないため、選択肢の一つとして提案するものであるが、バックアップデータはできるだけ遠隔地に保管すべきこと、安全性の観点から分散保管することが望ましいこと、民間のデータセンターの利用は経費的に負荷が大きいことから、全国の地方公共団体が相互協力し、各々が記録保存領域（ストレージ等）を提供して相互利用することにより、民間のデータセンターを複数利用するよりも安価で、広域災害による行政データ滅失のリスクを最小限にできるのではないかと考えた。加えて、分散保管の際に秘密分散技術を用いることで、分散保管のデメリットである情報の漏えいリスクの解消も期待することができる。

上記の構想に基づき実証実験を行った結果、クラウド型バックアップサイトは、具備すべき主な基本機能は技術的に実現可能であることが検証された。

現在、全国の地方公共団体で相互応援協定等の締結が進んでいるが、物資や職員等による応援が主であり、情報システムでの応援の例はまだ少ない。クラウド型バックアップサイトの実現により、地方公共団体における相互応援協定等に情報システムに係る応援を含めれば、当該サイトではバックアップデータのリカバリ先を指定できるので、自庁舎が被災した際に締結先の地方公共団体において業務の運用が可能となり、地方公共団体間の広域連携、すなわち地方公共団体間の協働がさらに進むことになる。

上記のとおり、本調査研究において提言したバックアップ・リストア基準を地方公共団体が策定し、それを支えるバックアップサイトの方策が充実されることで、災害に強い地方公共団体の情報システムの実現に資することになれば幸いである。

付録

アンケート調査票

災害に強い地方公共団体の情報システムのあり方に関する調査研究

アンケート調査票（情報システム部門用）

財団法人 地方自治情報センター

本アンケートは、地方公共団体が行政事務や住民サービス等に使用している以下のデータ

基幹系データ　：

住民情報や戸籍、税などのデータ。担当部署または全庁で組織的に一元管理しているデータ。

注：専用のソフトウェアで作成や処理等が行われます。

個別管理データ：

各職員が、担当する行政事務や住民サービス等を実施するために、個人で作成・管理している文書やデータ。保管場所や媒体は問いません（各職員が使用しているパソコン、部署や全庁的に設けている共有フォルダ、紙等）。

注：汎用的なワープロソフト、表計算ソフト等で作成されます。

について、それぞれのバックアップ状況や東日本大震災によるデータ滅失等の被災状況、住民に密接に関係する行政事務や住民サービスにおけるデータ滅失の影響（個別管理データのみ）及びデータ管理ポリシーの策定状況等を調査することを目的としています。

〔注１〕本調査における個別管理データとは、住民に密接に関係する行政事務や住民サービスに用いられる文書やデータをさす。具体的には、住民が申請や届出等を行う事務や老人介護サービスなどの各種サービスにおいて、作成・保管される文書やデータをいう。

■ご記入頂いたアンケート調査票の返却は、以下によりお願い申し上げます。

返却の際には本紙（表紙）を外し、次頁（1 頁）以降を提出してください。

＿＿＿＿月＿＿＿＿日までに

（部署）＿＿＿＿＿＿＿＿＿＿＿＿（ご担当者）＿＿＿＿＿＿様までにご提出ください。

Ⅰ 貴部署について

Q1. 貴部署についてお伺いします。

団体名

市・町・村

部署名

＊できるだけ正確・詳細にご記入ください。

主な所管業務・事業

部署に所属している職員の人数（含む臨時雇用、嘱託等）

人

Ⅱ 基幹系データ及び基幹系システム等について

Q２. 基幹系データのバックアップについてお伺いします。

ｑ１．基幹系データのバックアップを業務担当部署ではなく、貴情報システム部門で行っていますか。
該当するもの１つに〇を付けてください。

１．行っている
２．行っていない ***→Ｑ６にお進みください***

ｑ２．現在の基幹系データのバックアップの方法及びその保管場所等についてお伺いします。いずれも該当するもの全てに〇を付けてください。

1．基幹系システムのバックアップ装置を用いて媒体にバックアップしている（ネットワークは経由せず）

→ **保管場所**〔a．自庁内、b．自市町村内（自庁外）、c．他市町村〕

→ **媒体**〔a．ハードディスク、b．磁気媒体、c.その他（　　）〕

2．基幹系システムの設置場所とは異なるデータセンターに、ネットワークを経由してバックアップしている（含むオンラインストレージ）

→ **データセンターの場所**〔a．自市町村内（自庁外）、b．他市町村、c．不明〕

3．その他のバックアップの方法（具体的に＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

→ **保管場所等**〔a．自庁内、b．自市町村内（自庁外）、c．他市町村、d．不明〕

q３．前問 Q2-q２で回答したバックアップ方法を選択した理由についてお伺いします。選択する際の最も大きな要因（理由）１つに○を付けてください。

1．導入費用の安さ
2．運用費用の安さ
3．運用の容易性や省力化
4．システムやネットワークの構成や機能の制約
5．バックアップやリストアの信頼性の高さ
6．過去からの方法を踏襲
7．その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

＊具体的に記入してください

q４．前出Q2-q２でバックアップ・データを保管している場所を、「他市町村」と回答した団体のうち、地方公共団体に保管している場合にお答えください。

保管先の団体は、貴団体と災害協定や姉妹都市など何らかの連携を約束している団体ですか。該当するもの全てに○を付けてください。

1．災害協定を締結している団体である
2．姉妹都市（含む友好都市、親善都市等）の関係を締結している団体である
3．「＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿」の関係を締結している団体である

＊具体的に記入してください

4．何ら締結していない団体である

Q3. 現時点（東日本大震災の発生後）における、バックアップ方法の見直しの状況ついてお伺いします。

q1．前問Q2-q２でお答え頂いたバックアップ方法について、該当するものに○を付けてください。

1．今後、見直す予定である　→ *次のｑ２にお進みください*

2．東日本大震災後に見直した方法である
3．見直す予定はない
4．わからない
→ *Ｑ４にお進みください*

q2．上記Q3-q１で「１」を選択された方にお伺いします。見直す予定のバックアップ方法について、いずれも該当するもの全てに○を付けてください。

1．基幹系システムのバックアップ装置を用いて媒体にバックアップする（ネットワークは経由せず）
→ **保管場所**〔a．自庁内、b．自市町村内（自庁外）、c．他市町村〕
→ **媒体**〔a．ハードディスク、b．磁気媒体、c.その他（　　）〕

2．基幹系システムの設置場所とは異なるデータセンターに、ネットワークを経由してバックアップする（含むオンラインストレージ）
→ **データセンターの場所**〔a．自市町村内（自庁外）、b．他市町村、c．不明〕

3．その他のバックアップの方法（具体的に＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
→ **保管場所等**〔a．自庁内、b．自市町村内（自庁外）、c．他市町村、d．不明〕

4．現時点ではバックアップ方法は決まっていない　→ *Ｑ４にお進みください*

q3．前問Q3-q２で回答したバックアップ方法を選択する理由についてお伺いします。選択する際の最も大きな要因（理由）１つに○を付けてください。

1．導入費用の安さ
2．運用費用の安さ
3．運用の容易性や省力化
4．システムやネットワークの構成や機能の制約
5．バックアップやリストアの信頼性の高さ
6．その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
＊具体的に記入してください

ｑ４．前出Ｑ３-ｑ２でバックアップ・データを保管する場所を、「他市町村」と回答した団体のうち、地方公共団体に保管する場合にお答えください。
保管先の団体は、貴団体と災害協定や姉妹都市など何らかの連携を約束している団体ですか。該当するもの全てに○を付けてください。

１．災害協定を締結している（または締結予定の）団体である
２．姉妹都市（含む友好都市、親善都市等）の関係を締結している（または締結予定の）団体である
３．「＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿」の関係を締結している（または締結予定の）団体である　＊具体的に記入してください
４．何ら締結していない（または締結する予定のない）団体である

Ｑ４．東日本大震災による貴団体の基幹系情報システムへの影響についてお伺いします。該当するもの１つに○を付けてください。

１．業務に支障がでるような被害はなかった
２．被害（含む一部）を受けたが、業務は継続できた
３．被害（含む一部）を受け、業務は継続できなくなった

Ｑ５．東日本大震災による基幹系データのバックアップ・データへの影響についてお伺いします。該当するもの１つに○を付けてください。

１．まったく滅失しなかった
２．数%～30%程度滅失した
３．30%～70%程度滅失した
４．70%～100%近く滅失した
５．すべて滅失した

Ⅲ 個別管理データについて

Ｑ６．貴団体における全庁的な個別管理データの所在や利用状況等についてお伺いします。該当するもの１つに○を付けてください。

１．所在や利用状況を把握している
２．現在把握していないが、今後把握する予定がある
３．現在把握しておらず、今後も把握する予定はない
４．現在把握しておらず、今後把握するか否かわからない

Q7. 貴団体における全庁的な個別管理データの利用や管理（含むバックアップ等）に関する規定（含む使用または作成の禁止等）についてお伺いします。該当するもの1つに○を付けてください。

1．規定がある
2．現在規定はないが、今後策定する予定がある
3．現在規定はなく、今後も策定する予定はない
4．現在規定はなく、今後策定するか否かわからない

Q8. 個別管理データについてお伺いします。
貴部署では、住民に密接に関係する行政事務や住民サービスに用いている個別管理データを使用して業務や事業を行っていますか。
該当するもの1つに○を付けてください。

1．使用している
2．使用していない ***→Q10 にお進みください***

Q9-1. **住民に密接に関係する行政事務や住民サービスに用いている**個別管理データについてお伺いします。

〔注1〕個別管理データが複数ある場合には、住民に**より密接に関係し、滅失による影響が大きい**行政事務や住民サービスに用いられているものについてご回答ください。

〔注2〕上記のような個別管理データが書ききれない場合は、必要に応じてコピー（7頁～10頁）してご記入ください。

整理番号	q1. 個別管理データの名称 できるだけ正確に記載してください。	q2. 主な情報項目（内容） データに記載・記録されている主な情報項目	q3. 使用している業務や事業・住民サービス等の名称と内容	q4. 日常使用しているデータの記録媒体 1つに○を付けてください。 （バックアップの目的で記録しているものとは異なります）	q5. データの容量 〔例〕2G（HDやUSBメモリー等の場合）、A4用紙100枚程度（紙媒体の場合）、CD-RW2枚（CD-RWの場合）	q6. データのバックアップの状況 該当するものに○を付けてください。	q7. データへのアクセス頻度 ここでいう“アクセス”とは、データの閲覧・新規登録・修正・削除・再利用（例：名簿の作成等）等を意味しています。該当するもの1つに○を付けてください。
記入例	**老人介護サービス提供事業者リスト**	**・事業者名 ・住所 ・電話番号 ・代表者氏名 ・主な事業内容 ・施設規模 ・職員数 ・登録年月日 ・備考**	・名称: **すこやかシルバー支援事業** ・内容: **高齢者の健康・福祉向上に資する各種情報の収集・提供（含む講演会・セミナーの開催等）**	1. 紙媒体 2. PCの内部HDまたは外付けHD 3. CD-RW, DVD-RW等 4. USBメモリー、SDメモリー等 5. 共有フォルダ 6. その他（具体的に記入してください） ＿＿＿＿＿＿	**約５０MB（メガバイト）**	1. バックアップしていない 2. バックアップしている （バックアップに使用している媒体に○を付けてください） 2-1. 紙媒体（印刷やコピーによるバックアップ） 2-2. PCの外付けHD 2-3. CD-R、-RW, DVD-R、-RW 2-4. USBメモリー、SDメモリー等 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿ 2-6. 媒体がわからない	1. 概ね毎日 2. 1週間に数回程度 3. 1ヶ月に数回程度 4. 1年に数回程度 5. その他（具体的に記入してください） ＿＿＿＿＿＿
1			・名称: ・内容:	1. 紙媒体 2. PCの内部HDまたは外付けHD 3. CD-RW, DVD-RW 4. USBメモリー、SDメモリー等 5. 共有フォルダ 6. その他（具体的に記入してください） ＿＿＿＿＿＿		1. バックアップしていない 2. バックアップしている （バックアップに使用している媒体に○を付けてください） 2-1. 紙媒体（印刷やコピーによるバックアップ） 2-2. PCの外付けHD 2-3. CD-R、-RW, DVD-R、-RW 2-4. USBメモリー、SDメモリー等 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿ 2-6. 媒体がわからない	1. 概ね毎日 2. 1週間に数回程度 3. 1ヶ月に数回程度 4. 1年に数回程度 5. その他（具体的に記入してください） ＿＿＿＿＿＿
2			・名称: ・内容:	1. 紙媒体 2. PCの内部HDまたは外付けHD 3. CD-RW, DVD-RW 4. USBメモリー、SDメモリー等 5. 共有フォルダ 6. その他（具体的に記入してください） ＿＿＿＿＿＿		1. バックアップしていない 2. バックアップしている （バックアップに使用している媒体に○を付けてください） 2-1. 紙媒体（印刷やコピーによるバックアップ） 2-2. PCの外付けHD 2-3. CD-R、-RW, DVD-R、-RW 2-4. USBメモリー、SDメモリー等 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿ 2-6. 媒体がわからない	1. 概ね毎日 2. 1週間に数回程度 3. 1ヶ月に数回程度 4. 1年に数回程度 5. その他（具体的に記入してください） ＿＿＿＿＿＿

整理番号	q1. 個別管理データの名称 できるだけ正確に記載してください。	q2. 主な情報項目（内容） データに記載・記録されている主な情報項目	q3. 使用している業務や事業・住民サービス等の名称と内容	q4. 日常使用しているデータの記録媒体 1つに○を付けてください。 （バックアップの目的で記録しているものとは異なります）	q5. データの容量 〔例〕2G（HDやUSBメモリー等の場合）、A4用紙100枚程度（紙媒体の場合）、CD-RW２枚（CD-RWの場合）	q6. データのバックアップの状況 該当するものに○を付けてください。	q7. データへのアクセス頻度 ここでいう“アクセス”とは、データの閲覧・新規登録・修正・削除・再利用（例：名簿の作成等）等を意味しています。該当するもの１つに○を付けてください。
3			・名称： ・内容：	1. 紙媒体 2. PCの内部HDまたは外付けHD 3. CD-RW, DVD-RW 4. USBメモリー、SDメモリー等 5. 共有フォルダ 6. その他（具体的に記入してください） ＿＿＿＿＿＿		1. バックアップしていない 2. バックアップしている （バックアップに使用している媒体に○を付けてください） 2-1. 紙媒体（印刷やコピーによるバックアップ） 2-2. PCの外付けHD 2-3. CD-R、-RW, DVD-R、-RW 2-4. USBメモリー、SDメモリー等 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿ 2-6. 媒体がわからない	1. 概ね毎日 2. 1週間に数回程度 3. 1ヶ月に数回程度 4. 1年に数回程度 5. その他（具体的に記入してください） ＿＿＿＿＿＿
4			・名称： ・内容：	1. 紙媒体 2. PCの内部HDまたは外付けHD 3. CD-RW, DVD-RW 4. USBメモリー、SDメモリー等 5. 共有フォルダ 6. その他（具体的に記入してください） ＿＿＿＿＿＿		1. バックアップしていない 2. バックアップしている （バックアップに使用している媒体に○を付けてください） 2-1. 紙媒体（印刷やコピーによるバックアップ） 2-2. PCの外付けHD 2-3. CD-R、-RW, DVD-R、-RW 2-4. USBメモリー、SDメモリー等 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿ 2-6. 媒体がわからない	1. 概ね毎日 2. 1週間に数回程度 3. 1ヶ月に数回程度 4. 1年に数回程度 5. その他（具体的に記入してください） ＿＿＿＿＿＿
5			・名称： ・内容：	1. 紙媒体 2. PCの内部HDまたは外付けHD 3. CD-RW, DVD-RW 4. USBメモリー、SDメモリー等 5. 共有フォルダ 6. その他（具体的に記入してください） ＿＿＿＿＿＿		1. バックアップしていない 2. バックアップしている （バックアップに使用している媒体に○を付けてください） 2-1. 紙媒体（印刷やコピーによるバックアップ） 2-2. PCの外付けHD 2-3. CD-R、-RW, DVD-R、-RW 2-4. USBメモリー、SDメモリー等 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿ 2-6. 媒体がわからない	1. 概ね毎日 2. 1週間に数回程度 3. 1ヶ月に数回程度 4. 1年に数回程度 5. その他（具体的に記入してください） ＿＿＿＿＿＿

Q9-2. 東日本大震災による個別管理データや、行政事務や住民サービスへの影響についてお伺いします（前問Q9-1と同じ整理番号のデータについてご回答ください）。

整理番号	q8. 日常使用しているデータの滅失状況 1つに○を付けてください。 （バックアップ・データではありません）。	q9. バックアップ・データの滅失状況 1つに○を付けてください。 （日常使用しているデータではありません）。	q10. 震災前のような事務や住民サービス等が行えるまでに要した時間 1つに○を付けてください。	q11. 滅失したデータの回復方法 1つに○を付けてください。	q11. 滅失したデータの回復に要した人数、費用 おおよその人数、金額をお答えください。	q12. データの滅失による影響 発災直後から概ね数週間の間 ○を付けてください	q12. データの滅失による影響 発災から概ね約半年後 ○を付けてください	震災前の状況に回復するまでに、データ滅失による影響を受けたと考えられる住民の延べ人数 例えば震災前の１日当たりの平均的な利用者数等により推計してください
記入例	1. まったく滅失しなかった 2. 数%～30%程度滅失した 3. 30%～70%程度滅失した 4. 70%～100%近く滅失した 5. すべて滅失した	1. バックアップしていないため該当しない 2. まったく滅失しなかった 3. 数%～30%程度滅失した 4. 30%～70%程度滅失した 5. 70%～100%近く滅失した 6. すべて滅失した	1. 1週間以内 2. 数週間程度 3. 数ヶ月程度 4. 半年程度 5. 約1年程度 6. 約1年6ヶ月程度 7. 未だ回復していない	1. CD,DVD,USB等の媒体に記録したバックアップ・データを使用 2. バックアップのために印刷やコピーしていた紙媒体を使用 3. 他のシステム等で使用していたデータ(電子媒体で管理)を使用 4. 滅失した情報が記載されている資料等(紙媒体)を使用 5. その他(具体的に記入してください) ＿＿＿＿＿＿＿＿	・延べ人数 約 １０ 人日 (回復に要した日数×従事した一日当たりの平均人数) ・人件費 約 １５０ 千円 (延べ員数(上記)×貴職標準額(日割り)) ・PC購入費・修繕費 約 ２６０ 千円 (おおその合計金額をご記入ください)	1. まったく事務や住民サービスが実施できなくなった 2. ある程度は実施することができた (以下該当するものすべてに○を付けてください) 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他(具体的に記入してください) ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができた	1. まったく事務や住民サービスが実施できなかった 2. ある程度は実施することができた (以下該当するものすべてに○を付けてください) 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他(具体的に記入してください) ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができるようになった	・延べ人数 約 ８０ 人日 (一日当たりの平均的な利用者数等×回復に要した日数)
1	1. まったく滅失しなかった 2. 数%～30%程度滅失した 3. 30%～70%程度滅失した 4. 70%～100%近く滅失した 5. すべて滅失した	1. バックアップしていないため該当しない 2. まったく滅失しなかった 3. 数%～30%程度滅失した 4. 30%～70%程度滅失した 5. 70%～100%近く滅失した 6. すべて滅失した	1. 1週間以内 2. 数週間程度 3. 数ヶ月程度 4. 半年程度 5. 約1年程度 6. 約1年6ヶ月程度 7. 未だ回復していない	1. CD,DVD,USB等の媒体に記録したバックアップ・データを使用 2. バックアップのために印刷やコピーしていた紙媒体を使用 3. 他のシステム等で使用していたデータ(電子媒体で管理)を使用 4. 滅失した情報が記載されている資料等(紙媒体)を使用 5. その他(具体的に記入してください) ＿＿＿＿＿＿＿＿	・延べ人数 約 人日 (回復に要した日数×従事した一日当たりの平均人数) ・人件費 約 千円 (延べ員数(上記)×貴職標準額(日割り)) ・PC購入費・修繕費 約 千円 (おおその合計金額をご記入ください)	1. まったく事務や住民サービスが実施できなくなった 2. ある程度は実施することができた (以下該当するものすべてに○を付けてください) 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他(具体的に記入してください) ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができた	1. まったく事務や住民サービスが実施できなかった 2. ある程度は実施することができた (以下該当するものすべてに○を付けてください) 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他(具体的に記入してください) ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができるようになった	・延べ人数 約 人日 (一日当たりの平均的な利用者数等×回復に要した日数)
2	1. まったく滅失しなかった 2. 数%～30%程度滅失した 3. 30%～70%程度滅失した 4. 70%～100%近く滅失した 5. すべて滅失した	1. バックアップしていないため該当しない 2. まったく滅失しなかった 3. 数%～30%程度滅失した 4. 30%～70%程度滅失した 5. 70%～100%近く滅失した 6. すべて滅失した	1. 1週間以内 2. 数週間程度 3. 数ヶ月程度 4. 半年程度 5. 約1年程度 6. 約1年6ヶ月程度 7. 未だ回復していない	1. CD,DVD,USB等の媒体に記録したバックアップ・データを使用 2. バックアップのために印刷やコピーしていた紙媒体を使用 3. 他のシステム等で使用していたデータ(電子媒体で管理)を使用 4. 滅失した情報が記載されている資料等(紙媒体)を使用 5. その他(具体的に記入してください) ＿＿＿＿＿＿＿＿	・延べ人数 約 人日 (回復に要した日数×従事した一日当たりの平均人数) ・人件費 約 千円 (延べ員数(上記)×貴職標準額(日割り)) ・PC購入費・修繕費 約 千円 (おおその合計金額をご記入ください)	1. まったく事務や住民サービスが実施できなくなった 2. ある程度は実施することができた (以下該当するものすべてに○を付けてください) 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他(具体的に記入してください) ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができた	1. まったく事務や住民サービスが実施できなかった 2. ある程度は実施することができた (以下該当するものすべてに○を付けてください) 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他(具体的に記入してください) ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができるようになった	・延べ人数 約 人日 (一日当たりの平均的な利用者数等×回復に要した日数)

整理番号	q8. 日常使用しているデータの滅失状況 1つに○を付けてください。 （バックアップ・データではありません）。	q9. バックアップ・データの滅失状況 1つに○を付けてください。 （日常使用しているデータではありません）。	q10. 震災前のような事務や住民サービス等が行えるまでに要した時間 1つに○を付けてください。	q11. 滅失したデータの回復方法 1つに○を付けてください。	q11. 滅失したデータの回復に要した人数、費用 おおよその人数、金額をお答えください。	q12. データの滅失による影響		
						発災直後から概ね数週間の間 ○を付けてください	発災から概ね約半年後 ○を付けてください	震災前の状況に回復するまでに、データ滅失による影響を受けたと考えられる住民の延べ人数 例えば震災前の１日当たりの平均的な利用者数等により推計してください
3	1. まったく滅失しなかった 2. 数%～30%程度滅失した 3. 30%～70%程度滅失した 4. 70%～100%近く滅失した 5. すべて滅失した	1. バックアップしていないため該当しない 2. まったく滅失しなかった 3. 数%～30%程度滅失した 4. 30%～70%程度滅失した 5. 70%～100%近く滅失した 6. すべて滅失した	1. 1週間以内 2. 数週間程度 3. 数ヶ月程度 4. 半年程度 5. 約1年程度 6. 約1年6ヶ月程度 7. 未だ回復していない	1. CD,DVD,USB等の媒体に記録したバックアップ・データを使用 2. バックアップのために印刷やコピーしていた紙媒体を使用 3. 他のシステム等で使用していたデータ（電子媒体で管理）を使用 4. 滅失した情報が記載されている資料等（紙媒体）を使用 5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿	・延べ人数 約＿＿＿人日 （回復に要した日数×従事した一日当たりの平均人数） ・人件費 約＿＿＿千円 （延べ員数（上記）×貴職標準額（日割り）） ・PC購入費・修繕費 約＿＿＿千円 （おおよその合計金額をご記入ください）	1. まったく事務や住民サービスが実施できなくなった 2. ある程度は実施することができた （以下該当するものすべてに○を付けてください） 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができた	1. まったく事務や住民サービスが実施できなかった 2. ある程度は実施することができた （以下該当するものすべてに○を付けてください） 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができるようになった	・延べ人数 約＿＿＿人日 （一日当たりの平均的な利用者数等×回復に要した日数）
4	1. まったく滅失しなかった 2. 数%～30%程度滅失した 3. 30%～70%程度滅失した 4. 70%～100%近く滅失した 5. すべて滅失した	1. バックアップしていないため該当しない 2. まったく滅失しなかった 3. 数%～30%程度滅失した 4. 30%～70%程度滅失した 5. 70%～100%近く滅失した 6. すべて滅失した	1. 1週間以内 2. 数週間程度 3. 数ヶ月程度 4. 半年程度 5. 約1年程度 6. 約1年6ヶ月程度 7. 未だ回復していない	1. CD,DVD,USB等の媒体に記録したバックアップ・データを使用 2. バックアップのために印刷やコピーしていた紙媒体を使用 3. 他のシステム等で使用していたデータ（電子媒体で管理）を使用 4. 滅失した情報が記載されている資料等（紙媒体）を使用 5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿	・延べ人数 約＿＿＿人日 （回復に要した日数×従事した一日当たりの平均人数） ・人件費 約＿＿＿千円 （延べ員数（上記）×貴職標準額（日割り）） ・PC購入費・修繕費 約＿＿＿千円 （おおよその合計金額をご記入ください）	1. まったく事務や住民サービスが実施できなくなった 2. ある程度は実施することができた （以下該当するものすべてに○を付けてください） 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができた	1. まったく事務や住民サービスが実施できなかった 2. ある程度は実施することができた （以下該当するものすべてに○を付けてください） 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができるようになった	・延べ人数 約＿＿＿人日 （一日当たりの平均的な利用者数等×回復に要した日数）
5	1. まったく滅失しなかった 2. 数%～30%程度滅失した 3. 30%～70%程度滅失した 4. 70%～100%近く滅失した 5. すべて滅失した	1. バックアップしていないため該当しない 2. まったく滅失しなかった 3. 数%～30%程度滅失した 4. 30%～70%程度滅失した 5. 70%～100%近く滅失した 6. すべて滅失した	1. 1週間以内 2. 数週間程度 3. 数ヶ月程度 4. 半年程度 5. 約1年程度 6. 約1年6ヶ月程度 7. 未だ回復していない	1. CD,DVD,USB等の媒体に記録したバックアップ・データを使用 2. バックアップのために印刷やコピーしていた紙媒体を使用 3. 他のシステム等で使用していたデータ（電子媒体で管理）を使用 4. 滅失した情報が記載されている資料等（紙媒体）を使用 5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿	・延べ人数 約＿＿＿人日 （回復に要した日数×従事した一日当たりの平均人数） ・人件費 約＿＿＿千円 （延べ員数（上記）×貴職標準額（日割り）） ・PC購入費・修繕費 約＿＿＿千円 （おおよその合計金額をご記入ください）	1. まったく事務や住民サービスが実施できなくなった 2. ある程度は実施することができた （以下該当するものすべてに○を付けてください） 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができた	1. まったく事務や住民サービスが実施できなかった 2. ある程度は実施することができた （以下該当するものすべてに○を付けてください） 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができるようになった	・延べ人数 約＿＿＿人日 （一日当たりの平均的な利用者数等×回復に要した日数）

Ⅳ データ管理等について

Q１０. 貴団体の文書管理規定において、電子データに関する規定についてお伺いします。該当するもの１つに○を付けてください。

１．規定を設けている
２．規定を設けていないが、今後設ける予定である
３．規定を設けておらず、今後も設ける予定がない
4．規定を設けておらず、今後設けるか否かわからない

Q11. 貴団体における BCP（business continuity plan：業務継続計画）及び ICT-BCP についてお伺いします。該当するものそれぞれ１つに○を付けてください。

〔注１〕ICT-BCP とは、情報システムや情報システム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す。

q1. BCP について

１．策定している
２．現在策定していないが、今後策定する予定がある
３．現在策定しておらず、今後も策定する予定はない
４．現在策定しておらず、今後策定するか否かわからない

q2. ICT-BCP について

１．策定している
２．現在策定していないが、今後策定する予定がある
３．現在策定しておらず、今後も策定する予定はない
４．現在策定しておらず、今後策定するか否かわからない

Q12. 貴団体におけるデータ管理ポリシー及びデータバックアップ・リストア基準についてお伺いします。該当するものそれぞれ１つに○を付けてください。

〔注２〕データ管理ポリシーとは、組織におけるデータの管理について、基本的な方針や方法・体制等を総合的・体系的にとりまとめたものです。

〔注３〕データバックアップ・リストア基準とは、データ管理ポリシーに基づき、データの種類や重要度等に応じてバックアップやリストアする単位や方法、頻度（またはタイミング）等をとりまとめたものです。

q1．データ管理ポリシーについて

1．策定している
2．現在策定していないが、今後策定する予定がある
3．現在策定しておらず、今後も策定する予定はない
4．現在策定しておらず、今後策定するか否かわからない

q2．データバックアップ・リストア基準について

1．策定している
2．現在策定していないが、今後策定する予定がある
3．現在策定しておらず、今後も策定する予定はない
4．現在策定しておらず、今後策定するか否かわからない

Q13．貴団体における**共有ストレージ（含む共有フォルダ等）**についてお伺いします。
該当するもの1つに○を付けてください。

1．現在導入（利用）している
2．現在導入（利用）していないが、今後導入（利用）する予定がある
3．現在導入（利用）しておらず、今後も導入（利用）する予定はない
4．現在導入（利用）しておらず、今後導入（利用）するか否かわからない

Q14．貴団体における**文書管理システム**についてお伺いします。
該当するもの1つに○を付けてください。

1．現在導入（利用）している
2．現在導入（利用）していないが、今後導入（利用）する予定がある
3．現在導入（利用）しておらず、今後も導入（利用）する予定はない
4．現在導入（利用）しておらず、今後導入（利用）するか否かわからない

Q15．貴団体における**シンクライアント**についてお伺いします。
該当するもの1つに○を付けてください。

1．現在導入（利用）している
2．現在導入（利用）していないが、今後導入（利用）する予定がある
3．現在導入（利用）しておらず、今後も導入（利用）する予定はない
4．現在導入（利用）しておらず、今後導入（利用）するか否かわからない

Q16. データ管理等について、以下にお答えください。

q1. 個別管理データの管理やバックアップ方法などについて、貴団体の方針や考え方、ご意見等があればご記入ください。

q2. 本アンケート調査等の結果を踏まえて、地方公共団体が使用するデータ（含む基幹系データ、個別管理データ）に関するデータ管理ポリシー、バックアップ・リストア基準を作成する予定です。
ポリシーや基準について、ご意見やご希望等があればご記入ください。

質問は以上です。
ご協力頂きありがとうございました。

災害に強い地方公共団体の情報システムのあり方に関する調査研究

アンケート調査票（業務担当部署用）

財団法人 地方自治情報センター

本アンケートは、地方公共団体が行政事務や住民サービス等に使用している以下のデータ

基幹系データ　：

住民情報や戸籍、税などのデータ。担当部署または全庁で組織的に一元管理しているデータ。

注：専用のソフトウェアで作成や処理等が行われます。

個別管理データ：

各職員が、担当する行政事務や住民サービス等を実施するために、個人で作成・管理している文書やデータ。保管場所や媒体は問いません（各職員が使用しているパソコン、部署や全庁的に設けている共有フォルダ、紙等）。

注：汎用的なワープロソフト、表計算ソフト等で作成されます。

について、それぞれのバックアップ状況や東日本大震災によるデータ滅失等の被災状況、住民に密接に関係する行政事務や住民サービスにおけるデータ滅失の影響（個別管理データのみ）及びデータ管理ポリシーの策定状況等を調査することを目的としています。

〔注１〕本調査における個別管理データとは、住民に密接に関係する行政事務や住民サービスに用いられる文書やデータをさす。具体的には、住民が申請や届出等を行う事務や老人介護サービスなどの各種サービスにおいて、作成・保管される文書やデータをいう。

■ご記入頂いたアンケート調査票の返却は、以下によりお願い申し上げます。

返却の際には本紙（表紙）を外し、次頁（1 頁）以降を提出してください。

＿＿＿＿月＿＿＿＿日までに

（部署）＿＿＿＿＿＿＿＿＿＿＿＿（ご担当者）＿＿＿＿＿＿様までにご提出ください。

Ⅰ　貴部署について

Q1. 貴部署についてお伺いします。

団体名

部署名

＊できるだけ正確・詳細にご記入ください。

主な所管業務・事業

部署に所属している職員の人数（含む臨時雇用、嘱託等）

Q２. 貴部署が使用している**部屋またはスペース**に対する、東日本大震災の影響をお伺いします。該当するもの１つに○を付けてください。

１．業務に支障がでるような被害はなかった
２．被害（含む一部）を受けたが、業務は継続できた
３．被害（含む一部）を受け、業務は継続できなくなった

Q３. 貴部署が使用している**紙媒体の文献、資料等**に対する、東日本大震災の影響をお伺いします。該当するもの１つに○を付けてください。

１．業務に支障がでるような被害はなかった
２．被害（含む一部）を受けたが、業務は継続できた
３．被害（含む一部）を受け、業務は継続できなくなった

Ⅱ　基幹系データ及び基幹系システム等について

Q４. 基幹系データのバックアップについてお伺いします。

ｑ１．基幹系データのバックアップを情報システム部門ではなく、貴部署で行っていますか。
該当するもの１つに○を付けてください。

1．行っている
2．行っていない ***→Q8 にお進みください***

ｑ２．現在の基幹系データのバックアップの方法及びその保管場所等についてお伺いします。いずれも該当するもの全てに○を付けてください。

1．基幹系システムのバックアップ装置を用いて媒体にバックアップしている（ネットワークは経由せず）
　→ **保管場所**〔ａ．自庁内、ｂ．自市町村内（自庁外）、ｃ．他市町村〕
　→ **媒体**〔ａ．ハードディスク、ｂ．磁気媒体、c.その他（　　）〕
2．基幹系システムの設置場所とは異なるデータセンターに、ネットワークを経由してバックアップしている（含むオンラインストレージ）
　→ **データセンターの場所**〔ａ．自市町村内（自庁外）、ｂ．他市町村、ｃ．不明〕
3．その他のバックアップの方法（具体的に＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
　→ **保管場所等**〔ａ．自庁内、ｂ．自市町村内（自庁外）、ｃ．他市町村、ｄ．不明〕

ｑ３. 前問Ｑ４-ｑ２で回答したバックアップ方法を選択した理由についてお伺いします。選択する際の最も大きな要因（理由）１つに○を付けてください。

1．導入費用の安さ
2．運用費用の安さ
3．運用の容易性や省力化
4．システムやネットワークの構成や機能の制約
5．バックアップやリストアの信頼性の高さ
6．過去からの方法を踏襲
7．その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
＊具体的に記入してください

ｑ４．前出Ｑ４-ｑ２でバックアップ・データを保管している場所を、「他市町村」と回答した団体のうち、地方公共団体に保管している場合にお答えください。
保管先の団体は、貴団体と災害協定や姉妹都市など何らかの連携を約束している団体ですか。該当するもの全てに○を付けてください。

１．災害協定を締結している団体である
２．姉妹都市（含む友好都市、親善都市等）の関係を締結している団体である
３．「＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿」の関係を締結している団体である
＊具体的に記入してください
４．何ら締結していない団体である
５．わからない

Ｑ５．現時点（東日本大震災の発生後）における、バックアップ方法の見直しの状況ついてお伺いします。

ｑ１．前問Ｑ４-ｑ２でお答え頂いたバックアップ方法について、該当するものに○を付けてください。

１．今後、見直す予定である　→　次のｑ２にお進みください
２．東日本大震災後に見直した方法である
３．見直す予定はない　→　Ｑ６にお進みください
４．わからない

ｑ２．上記Ｑ５-ｑ１で「１」を選択された方にお伺いします。見直す予定のバックアップ方法について、いずれも該当するもの全てに○を付けてください。

１．基幹系システムのバックアップ装置を用いて媒体にバックアップする（ネットワークは経由せず）
→ **保管場所**〔ａ．自庁内、ｂ．自市町村内（自庁外）、ｃ．他市町村〕
→ **媒体**〔ａ．ハードディスク、ｂ．磁気媒体、c.その他（　　）〕
２．基幹系システムの設置場所とは異なるデータセンターに、ネットワークを経由してバックアップする（含むオンラインストレージ）
→ **データセンターの場所**〔ａ．自市町村内（自庁外）、ｂ．他市町村、ｃ．不明〕
３．その他のバックアップの方法（具体的に＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
→ **保管場所等**〔ａ．自庁内、ｂ．自市町村内（自庁外）、ｃ．他市町村、ｄ．不明〕
４．現時点ではバックアップ方法は決まっていない　→　Ｑ６にお進みください

ｑ３．前問Ｑ５-ｑ２で回答したバックアップ方法を選択する理由についてお伺いします。選択する際の最も大きな要因（理由）１つに○を付けてください。

１．導入費用の安さ
２．運用費用の安さ
３．運用の容易性や省力化
４．システムやネットワークの構成や機能の制約
５．バックアップやリストアの信頼性の高さ
６．その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
＊具体的に記入してください

ｑ４．前出Ｑ５-ｑ２でバックアップ・データを保管する場所を、「他市町村」と回答した団体のうち、地方公共団体に保管する場合にお答えください。
保管先の団体は、貴団体と災害協定や姉妹都市など何らかの連携を約束している団体ですか。該当するもの全てに○を付けてください。

１．災害協定を締結している（または締結予定の）団体である
２．姉妹都市（含む友好都市、親善都市等）の関係を締結している（または締結予定の）団体である
３．「＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿」の関係を締結している（または締結予定の）団体である　＊具体的に記入してください
４．何ら締結していない（または締結する予定のない）団体である
５．わからない

Ｑ６．東日本大震災による貴団体の基幹系情報システムへの影響についてお伺いします。該当するもの１つに○を付けてください。

１．業務に支障がでるような被害はなかった
２．被害（含む一部）を受けたが、業務は継続できた
３．被害（含む一部）を受け、業務は継続できなくなった

Ｑ７．東日本大震災による基幹系データのバックアップ・データへの影響についてお伺いします。該当するもの１つに○を付けてください。

１．まったく滅失しなかった
２．数%～30%程度滅失した
３．30%～70%程度滅失した
４．70%～100%近く滅失した
５．すべて滅失した

Ⅲ　個別管理データについて

Q8. 個別管理データについてお伺いします。
貴部署では、個別管理データを用いて業務や事業を行っていますか。
該当するもの１つに○を付けてください。

１．使用している
２．使用していない　***→Q10 にお進みください***

Q9-1. **住民に密接に関係する行政事務や住民サービスに用いている**個別管理データについてお伺いします。

〔注1〕個別管理データが複数ある場合には、住民に**より密接に関係し、滅失による影響が大きい**行政事務や住民サービスに用いられているものについてご回答ください。

〔注2〕上記のような個別管理データが書ききれない場合は、必要に応じてコピー（7頁～10頁）してご記入ください。

整理番号	q1. 個別管理データの名称 できるだけ正確に記載してください。	q2. 主な情報項目（内容） データに記載・記録されている主な情報項目	q3. 使用している業務や事業・住民サービス等の名称と内容	q4. 日常使用しているデータの記録媒体 1つに○を付けてください。 （バックアップの目的で記録しているものとは異なります）	q5. データの容量 〔例〕2G（HDやUSBメモリー等の場合）、A4用紙100枚程度（紙媒体の場合）、CD-RW2枚（CD-RWの場合）	q6. データのバックアップの状況 該当するものに○を付けてください。	q7. データへのアクセス頻度 ここでいう“アクセス”とは、データの閲覧・新規登録・修正・削除・再利用（例：名簿の作成等）等を意味しています。該当するもの1つに○を付けてください。
記入例	**老人介護サービス提供事業者リスト**	**・事業者名 ・住所 ・電話番号 ・代表者氏名 ・主な事業内容 ・施設規模 ・職員数 ・登録年月日 ・備考**	・名称: **すこやかシルバー支援事業** ・内容: **高齢者の健康・福祉向上に資する各種情報の収集・提供（含む講演会・セミナーの開催等）**	1. 紙媒体 2. PCの内部HDまたは外付けHD 3. CD-RW, DVD-RW等 4. USBメモリー、SDメモリー等 5. 共有フォルダ 6. その他（具体的に記入してください） ＿＿＿＿＿＿	**約５０MB（メガバイト）**	1. バックアップしていない 2. バックアップしている （バックアップに使用している媒体に○を付けてください） 2-1. 紙媒体（印刷やコピーによるバックアップ） 2-2. PCの外付けHD 2-3. CD-R、-RW, DVD-R、-RW 2-4. USBメモリー、SDメモリー等 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿ 2-6. 媒体がわからない	1. 概ね毎日 2. 1週間に数回程度 3. 1ヶ月に数回程度 4. 1年に数回程度 5. その他（具体的に記入してください） ＿＿＿＿＿＿
1			・名称: ・内容:	1. 紙媒体 2. PCの内部HDまたは外付けHD 3. CD-RW, DVD-RW 4. USBメモリー、SDメモリー等 5. 共有フォルダ 6. その他（具体的に記入してください） ＿＿＿＿＿＿		1. バックアップしていない 2. バックアップしている （バックアップに使用している媒体に○を付けてください） 2-1. 紙媒体（印刷やコピーによるバックアップ） 2-2. PCの外付けHD 2-3. CD-R、-RW, DVD-R、-RW 2-4. USBメモリー、SDメモリー等 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿ 2-6. 媒体がわからない	1. 概ね毎日 2. 1週間に数回程度 3. 1ヶ月に数回程度 4. 1年に数回程度 5. その他（具体的に記入してください） ＿＿＿＿＿＿
2			・名称: ・内容:	1. 紙媒体 2. PCの内部HDまたは外付けHD 3. CD-RW, DVD-RW 4. USBメモリー、SDメモリー等 5. 共有フォルダ 6. その他（具体的に記入してください） ＿＿＿＿＿＿		1. バックアップしていない 2. バックアップしている （バックアップに使用している媒体に○を付けてください） 2-1. 紙媒体（印刷やコピーによるバックアップ） 2-2. PCの外付けHD 2-3. CD-R、-RW, DVD-R、-RW 2-4. USBメモリー、SDメモリー等 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿ 2-6. 媒体がわからない	1. 概ね毎日 2. 1週間に数回程度 3. 1ヶ月に数回程度 4. 1年に数回程度 5. その他（具体的に記入してください） ＿＿＿＿＿＿

整理番号	q1. 個別管理データの名称 できるだけ正確に記載してください。	q2. 主な情報項目（内容） データに記載・記録されている主な情報項目	q3. 使用している業務や事業・住民サービス等の名称と内容	q4. 日常使用しているデータの記録媒体 1つに○を付けてください。 （バックアップの目的で記録しているものとは異なります）	q5. データの容量 〔例〕2G（HDやUSBメモリー等の場合）、A4用紙100枚程度（紙媒体の場合）、CD-RW２枚（CD-RWの場合）	q6. データのバックアップの状況 該当するものに○を付けてください。	q7. データへのアクセス頻度 ここでいう“アクセス”とは、データの閲覧・新規登録・修正・削除・再利用（例：名簿の作成等）等を意味しています。該当するもの１つに○を付けてください。
3			・名称： ・内容：	1. 紙媒体 2. PCの内部HDまたは外付けHD 3. CD-RW, DVD-RW 4. USBメモリー、SDメモリー等 5. 共有フォルダ 6. その他（具体的に記入してください） ＿＿＿＿＿＿		1. バックアップしていない 2. バックアップしている （バックアップに使用している媒体に○を付けてください） 2-1. 紙媒体（印刷やコピーによるバックアップ） 2-2. PCの外付けHD 2-3. CD-R、-RW, DVD-R、-RW 2-4. USBメモリー、SDメモリー等 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿ 2-6. 媒体がわからない	1. 概ね毎日 2. 1週間に数回程度 3. 1ヶ月に数回程度 4. 1年に数回程度 5. その他（具体的に記入してください） ＿＿＿＿＿＿
4			・名称： ・内容：	1. 紙媒体 2. PCの内部HDまたは外付けHD 3. CD-RW, DVD-RW 4. USBメモリー、SDメモリー等 5. 共有フォルダ 6. その他（具体的に記入してください） ＿＿＿＿＿＿		1. バックアップしていない 2. バックアップしている （バックアップに使用している媒体に○を付けてください） 2-1. 紙媒体（印刷やコピーによるバックアップ） 2-2. PCの外付けHD 2-3. CD-R、-RW, DVD-R、-RW 2-4. USBメモリー、SDメモリー等 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿ 2-6. 媒体がわからない	1. 概ね毎日 2. 1週間に数回程度 3. 1ヶ月に数回程度 4. 1年に数回程度 5. その他（具体的に記入してください） ＿＿＿＿＿＿
5			・名称： ・内容：	1. 紙媒体 2. PCの内部HDまたは外付けHD 3. CD-RW, DVD-RW 4. USBメモリー、SDメモリー等 5. 共有フォルダ 6. その他（具体的に記入してください） ＿＿＿＿＿＿		1. バックアップしていない 2. バックアップしている （バックアップに使用している媒体に○を付けてください） 2-1. 紙媒体（印刷やコピーによるバックアップ） 2-2. PCの外付けHD 2-3. CD-R、-RW, DVD-R、-RW 2-4. USBメモリー、SDメモリー等 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿ 2-6. 媒体がわからない	1. 概ね毎日 2. 1週間に数回程度 3. 1ヶ月に数回程度 4. 1年に数回程度 5. その他（具体的に記入してください） ＿＿＿＿＿＿

Q9-2. 東日本大震災による個別管理データや、行政事務や住民サービスへの影響についてお伺いします（前問Q9-1と同じ整理番号のデータについてご回答ください）。

整理番号	q8. 日常使用しているデータの滅失状況 1つに○を付けてください。 （バックアップ・データではありません）。	q9. バックアップ・データの滅失状況 1つに○を付けてください。 （日常使用しているデータではありません）。	q10. 震災前のような事務や住民サービス等が行えるまでに要した時間 1つに○を付けてください。	q11. 滅失したデータの回復方法 1つに○を付けてください。	q11. 滅失したデータの回復に要した人数、費用 おおよその人数、金額をお答えください。	q12. データの滅失による影響 発災直後から概ね数週間の間 ○を付けてください	q12. データの滅失による影響 発災から概ね約半年後 ○を付けてください	震災前の状況に回復するまでに、データ滅失による影響を受けたと考えられる住民の延べ人数 例えば震災前の１日当たりの平均的な利用者数等により推計してください
記入例	1. まったく滅失しなかった 2. 数%～30%程度滅失した 3. 30%～70%程度滅失した 4. 70%～100%近く滅失した 5. すべて滅失した	1. バックアップしていないため該当しない 2. まったく滅失しなかった 3. 数%～30%程度滅失した 4. 30%～70%程度滅失した 5. 70%～100%近く滅失した 6. すべて滅失した	1. 1週間以内 2. 数週間程度 3. 数ヶ月程度 4. 半年程度 5. 約1年程度 6. 約1年6ヶ月程度 7. 未だ回復していない	1. CD,DVD,USB等の媒体に記録したバックアップ・データを使用 2. バックアップのために印刷やコピーしていた紙媒体を使用 3. 他のシステム等で使用していたデータ(電子媒体で管理)を使用 4. 滅失した情報が記載されている資料等(紙媒体)を使用 5. その他(具体的に記入してください) ＿＿＿＿＿＿	・延べ人数 約 １０ 人日 (回復に要した日数×従事した一日当たりの平均人数) ・人件費 約 １５０ 千円 (延べ員数(上記)×貴職標準額(日割り)) ・PC購入費・修繕費 約 ２６０ 千円 (およその合計金額をご記入ください)	1. まったく事務や住民サービスが実施できなくなった 2. ある程度は実施することができた (以下該当するものすべてに○を付けてください) 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他(具体的に記入してください) ＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができた	1. まったく事務や住民サービスが実施できなかった 2. ある程度は実施することができた (以下該当するものすべてに○を付けてください) 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他(具体的に記入してください) ＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができるようになった	・延べ人数 約 ８０ 人日 (一日当たりの平均的な利用者数等×回復に要した日数)
1	1. まったく滅失しなかった 2. 数%～30%程度滅失した 3. 30%～70%程度滅失した 4. 70%～100%近く滅失した 5. すべて滅失した	1. バックアップしていないため該当しない 2. まったく滅失しなかった 3. 数%～30%程度滅失した 4. 30%～70%程度滅失した 5. 70%～100%近く滅失した 6. すべて滅失した	1. 1週間以内 2. 数週間程度 3. 数ヶ月程度 4. 半年程度 5. 約1年程度 6. 約1年6ヶ月程度 7. 未だ回復していない	1. CD,DVD,USB等の媒体に記録したバックアップ・データを使用 2. バックアップのために印刷やコピーしていた紙媒体を使用 3. 他のシステム等で使用していたデータ(電子媒体で管理)を使用 4. 滅失した情報が記載されている資料等(紙媒体)を使用 5. その他(具体的に記入してください) ＿＿＿＿＿＿	・延べ人数 約 人日 (回復に要した日数×従事した一日当たりの平均人数) ・人件費 約 千円 (延べ員数(上記)×貴職標準額(日割り)) ・PC購入費・修繕費 約 千円 (およその合計金額をご記入ください)	1. まったく事務や住民サービスが実施できなくなった 2. ある程度は実施することができた (以下該当するものすべてに○を付けてください) 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他(具体的に記入してください) ＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができた	1. まったく事務や住民サービスが実施できなかった 2. ある程度は実施することができた (以下該当するものすべてに○を付けてください) 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他(具体的に記入してください) ＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができるようになった	・延べ人数 約 人日 (一日当たりの平均的な利用者数等×回復に要した日数)
2	1. まったく滅失しなかった 2. 数%～30%程度滅失した 3. 30%～70%程度滅失した 4. 70%～100%近く滅失した 5. すべて滅失した	1. バックアップしていないため該当しない 2. まったく滅失しなかった 3. 数%～30%程度滅失した 4. 30%～70%程度滅失した 5. 70%～100%近く滅失した 6. すべて滅失した	1. 1週間以内 2. 数週間程度 3. 数ヶ月程度 4. 半年程度 5. 約1年程度 6. 約1年6ヶ月程度 7. 未だ回復していない	1. CD,DVD,USB等の媒体に記録したバックアップ・データを使用 2. バックアップのために印刷やコピーしていた紙媒体を使用 3. 他のシステム等で使用していたデータ(電子媒体で管理)を使用 4. 滅失した情報が記載されている資料等(紙媒体)を使用 5. その他(具体的に記入してください) ＿＿＿＿＿＿	・延べ人数 約 人日 (回復に要した日数×従事した一日当たりの平均人数) ・人件費 約 千円 (延べ員数(上記)×貴職標準額(日割り)) ・PC購入費・修繕費 約 千円 (およその合計金額をご記入ください)	1. まったく事務や住民サービスが実施できなくなった 2. ある程度は実施することができた (以下該当するものすべてに○を付けてください) 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他(具体的に記入してください) ＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができた	1. まったく事務や住民サービスが実施できなかった 2. ある程度は実施することができた (以下該当するものすべてに○を付けてください) 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他(具体的に記入してください) ＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができるようになった	・延べ人数 約 人日 (一日当たりの平均的な利用者数等×回復に要した日数)

整理番号	q8. 日常使用しているデータの滅失状況 1つに○を付けてください。 （バックアップ・データではありません）。	q9. バックアップ・データの滅失状況 1つに○を付けてください。 （日常使用しているデータではありません）。	q10. 震災前のような事務や住民サービス等が行えるまでに要した時間 1つに○を付けてください。	q11. 滅失したデータの回復方法 1つに○を付けてください。	q11. 滅失したデータの回復に要した人数、費用 おおよその人数、金額をお答えください。	q12. データの滅失による影響		
						発災直後から概ね数週間の間 ○を付けてください	発災から概ね約半年後 ○を付けてください	震災前の状況に回復するまでに、データ滅失による影響を受けたと考えられる住民の延べ人数 例えば震災前の１日当たりの平均的な利用者数等により推計してください
3	1. まったく滅失しなかった 2. 数%～30%程度滅失した 3. 30%～70%程度滅失した 4. 70%～100%近く滅失した 5. すべて滅失した	1. バックアップしていないため該当しない 2. まったく滅失しなかった 3. 数%～30%程度滅失した 4. 30%～70%程度滅失した 5. 70%～100%近く滅失した 6. すべて滅失した	1. 1週間以内 2. 数週間程度 3. 数ヶ月程度 4. 半年程度 5. 約1年程度 6. 約1年6ヶ月程度 7. 未だ回復していない	1. CD,DVD,USB等の媒体に記録したバックアップ・データを使用 2. バックアップのために印刷やコピーしていた紙媒体を使用 3. 他のシステム等で使用していたデータ（電子媒体で管理）を使用 4. 滅失した情報が記載されている資料等（紙媒体）を使用 5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿	・延べ人数 約＿＿＿人日 （回復に要した日数×従事した一日当たりの平均人数） ・人件費 約＿＿＿千円 （延べ員数（上記）×貴職標準額（日割り）） ・PC購入費・修繕費 約＿＿＿千円 （およその合計金額をご記入ください）	1. まったく事務や住民サービスが実施できなくなった 2. ある程度は実施することができた （以下該当するものすべてに○を付けてください） 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができた	1. まったく事務や住民サービスが実施できなかった 2. ある程度は実施することができた （以下該当するものすべてに○を付けてください） 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができるようになった	・延べ人数 約＿＿＿人日 （一日当たりの平均的な利用者数等×回復に要した日数）
4	1. まったく滅失しなかった 2. 数%～30%程度滅失した 3. 30%～70%程度滅失した 4. 70%～100%近く滅失した 5. すべて滅失した	1. バックアップしていないため該当しない 2. まったく滅失しなかった 3. 数%～30%程度滅失した 4. 30%～70%程度滅失した 5. 70%～100%近く滅失した 6. すべて滅失した	1. 1週間以内 2. 数週間程度 3. 数ヶ月程度 4. 半年程度 5. 約1年程度 6. 約1年6ヶ月程度 7. 未だ回復していない	1. CD,DVD,USB等の媒体に記録したバックアップ・データを使用 2. バックアップのために印刷やコピーしていた紙媒体を使用 3. 他のシステム等で使用していたデータ（電子媒体で管理）を使用 4. 滅失した情報が記載されている資料等（紙媒体）を使用 5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿	・延べ人数 約＿＿＿人日 （回復に要した日数×従事した一日当たりの平均人数） ・人件費 約＿＿＿千円 （延べ員数（上記）×貴職標準額（日割り）） ・PC購入費・修繕費 約＿＿＿千円 （およその合計金額をご記入ください）	1. まったく事務や住民サービスが実施できなくなった 2. ある程度は実施することができた （以下該当するものすべてに○を付けてください） 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができた	1. まったく事務や住民サービスが実施できなかった 2. ある程度は実施することができた （以下該当するものすべてに○を付けてください） 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができるようになった	・延べ人数 約＿＿＿人日 （一日当たりの平均的な利用者数等×回復に要した日数）
5	1. まったく滅失しなかった 2. 数%～30%程度滅失した 3. 30%～70%程度滅失した 4. 70%～100%近く滅失した 5. すべて滅失した	1. バックアップしていないため該当しない 2. まったく滅失しなかった 3. 数%～30%程度滅失した 4. 30%～70%程度滅失した 5. 70%～100%近く滅失した 6. すべて滅失した	1. 1週間以内 2. 数週間程度 3. 数ヶ月程度 4. 半年程度 5. 約1年程度 6. 約1年6ヶ月程度 7. 未だ回復していない	1. CD,DVD,USB等の媒体に記録したバックアップ・データを使用 2. バックアップのために印刷やコピーしていた紙媒体を使用 3. 他のシステム等で使用していたデータ（電子媒体で管理）を使用 4. 滅失した情報が記載されている資料等（紙媒体）を使用 5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿	・延べ人数 約＿＿＿人日 （回復に要した日数×従事した一日当たりの平均人数） ・人件費 約＿＿＿千円 （延べ員数（上記）×貴職標準額（日割り）） ・PC購入費・修繕費 約＿＿＿千円 （およその合計金額をご記入ください）	1. まったく事務や住民サービスが実施できなくなった 2. ある程度は実施することができた （以下該当するものすべてに○を付けてください） 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができた	1. まったく事務や住民サービスが実施できなかった 2. ある程度は実施することができた （以下該当するものすべてに○を付けてください） 2-1. 実施に要する時間が増えた 2-2. 実施に要する人手が増えた 2-3. 事務や住民サービスの内容が限定された 2-4. 事務や住民サービスの質が低下した 2-5. その他（具体的に記入してください） ＿＿＿＿＿＿＿＿ 3. 発災前と変わりなく実施することができるようになった	・延べ人数 約＿＿＿人日 （一日当たりの平均的な利用者数等×回復に要した日数）

Ⅳデータ管理等について

Q10. 貴団体におけるデータ管理ポリシー及びデータバックアップ・リストア基準についてお伺いします。該当するものそれぞれ１つに○を付けてください。

〔注１〕データ管理ポリシーとは、組織におけるデータの管理について、基本的な方針や方法・体制等を総合的・体系的にとりまとめたものです。

〔注2〕データバックアップ・リストア基準とは、データ管理ポリシーに基づき、データの種類や重要度等に応じてバックアップやリストアする単位や方法、頻度（またはタイミング）等をとりまとめたものです。

q1. データ管理ポリシーについて

１．策定している

２．現在策定していないが、今後策定する予定がある

３．現在策定しておらず、今後も策定する予定はない

４．現在策定しておらず、今後策定するか否かわからない

q2. データバックアップ・リストア基準について

１．策定している

２．現在策定していないが、今後策定する予定がある

３．現在策定しておらず、今後も策定する予定はない

４．現在策定しておらず、今後策定するか否かわからない

Q11. 貴部署の職員が作成・管理している個別管理データについて、その管理やバックアップの方法・実施主体（部署）、ルール等について、ご意見やご希望等があればご記入ください。

Q１２．今後、震災等が発生しても、貴部署で実施している行政事務や住民サービスを継続するために、実施している（あるいは今後実施する予定の）取組みや計画等があれば以下にご記入ください。

質問は以上です。
ご協力頂きありがとうございました。

災害に強い地方公共団体の情報システムのあり方に関する調査研究
－行政データ管理とバックアップサイトについて－

平成２５年３月発行
発行　財団法人　地方自治情報センター
〒102-8419 東京都千代田区一番町２５番地（全国町村議員会館内）
電話０３（５２１４）８００２～３

LASDEC（ラスデック）、当センターの組織名の英語表記（Local Authorities Systems Development Center）を略したものです。


LASDEC