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。

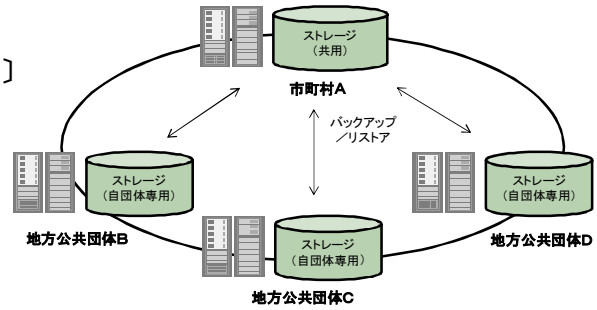
■複数の地方公共団体でバックアップサイトを共同利用する。
（コスト軽減に係るスケールメリット：共同利用＞単独利用）

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。

---

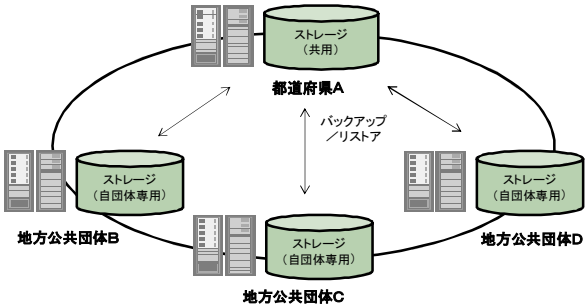
[50] バックアップサイトの実例としては、次のような事例がある。
・釜石市では、基幹系システムのバックアップサイトとして北九州市のクラウド基盤を利用している。また、被災時に最低限の業務ができるよう、データセンターからネットワーク経由で一部のバックアップデータを転送し、庁舎内に保管している。詳細は「第１章　第１節－３－（２）オ（イ）自治体クラウドの仕様」を参照のこと。
・岩手県では、県内の希望市町村に対して「行政情報データバックアップサービス」を提供するためのシステム構築を進めており、平成 25 年 4 月からサービスを開始する予定である。本サービスは、県内のデータセンターにシステムを設置し、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〕



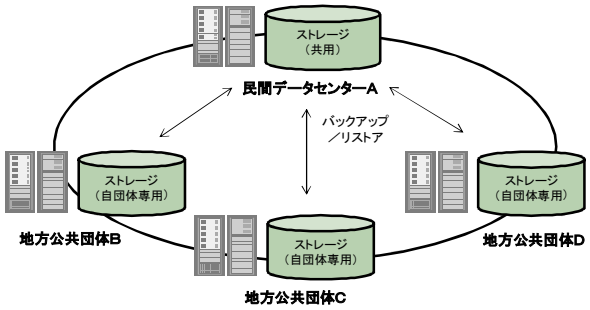
図－３９　市町村が自庁舎施設内に設置するシステムを、他の団体が
バックアップサイトとして共同利用するイメージ

〔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

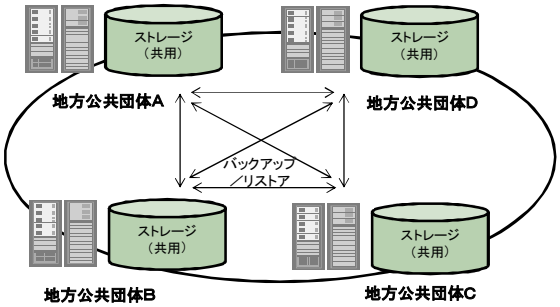
〔ケース３〕



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

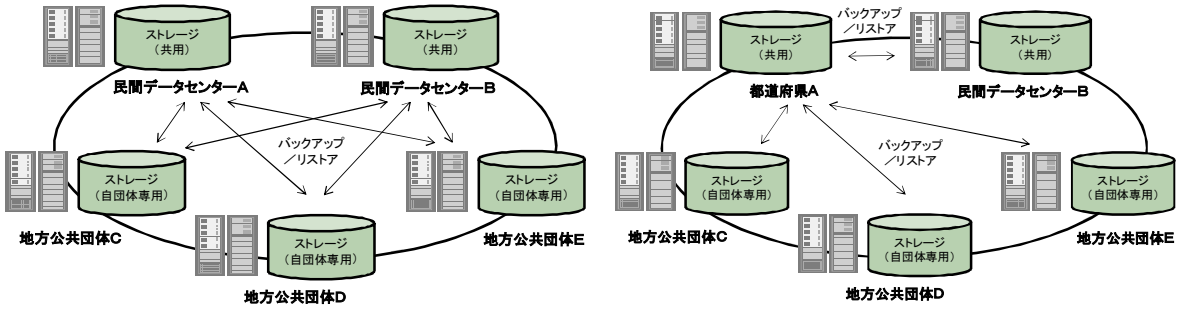
[51] 地方公共団体（都道府県あるいは市町村）が民間データセンターを利用して、バックアップサイトとして使用する場合は、データの所在の明確化、初期・運用コスト及びセキュリティレベルが自庁舎施設内に設置するシステムを利用する場合と異なることから、〔ケース３〕民間データセンターの共同利用に区分する。

〔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

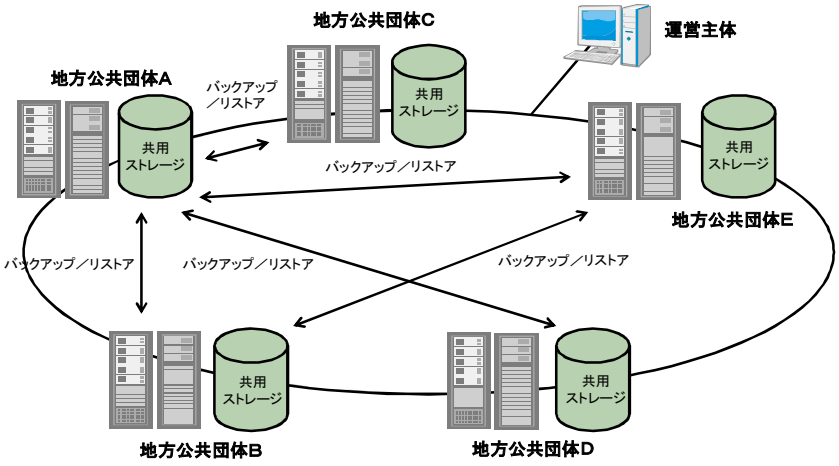
バックアップサイトの構築及び運用に係る考慮点を踏まえて、具体的な枠組みを以下のように考えた。

・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

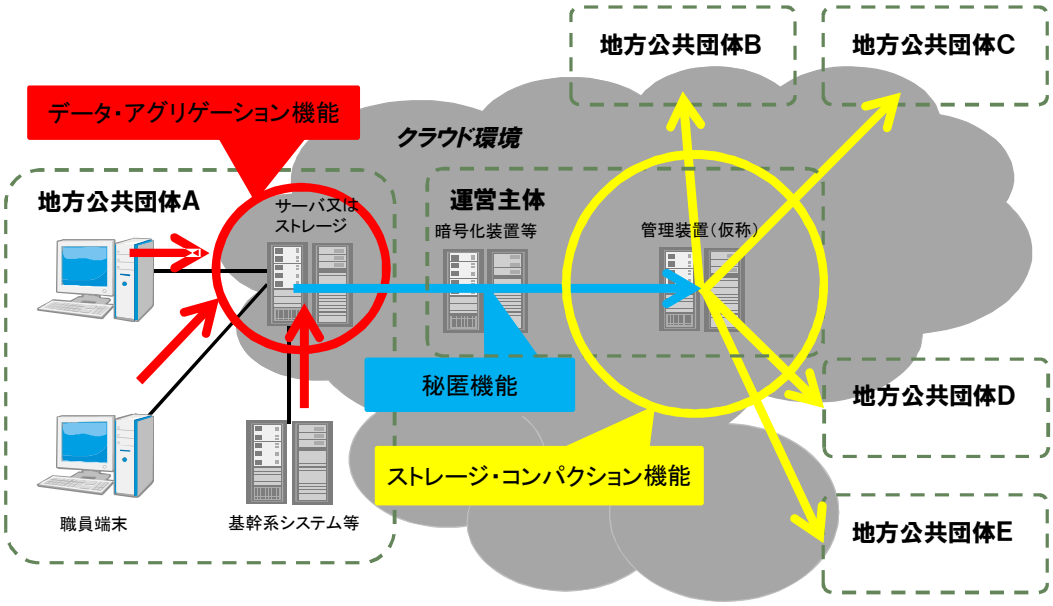
２　バックアップサイトを構成する機能

（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。

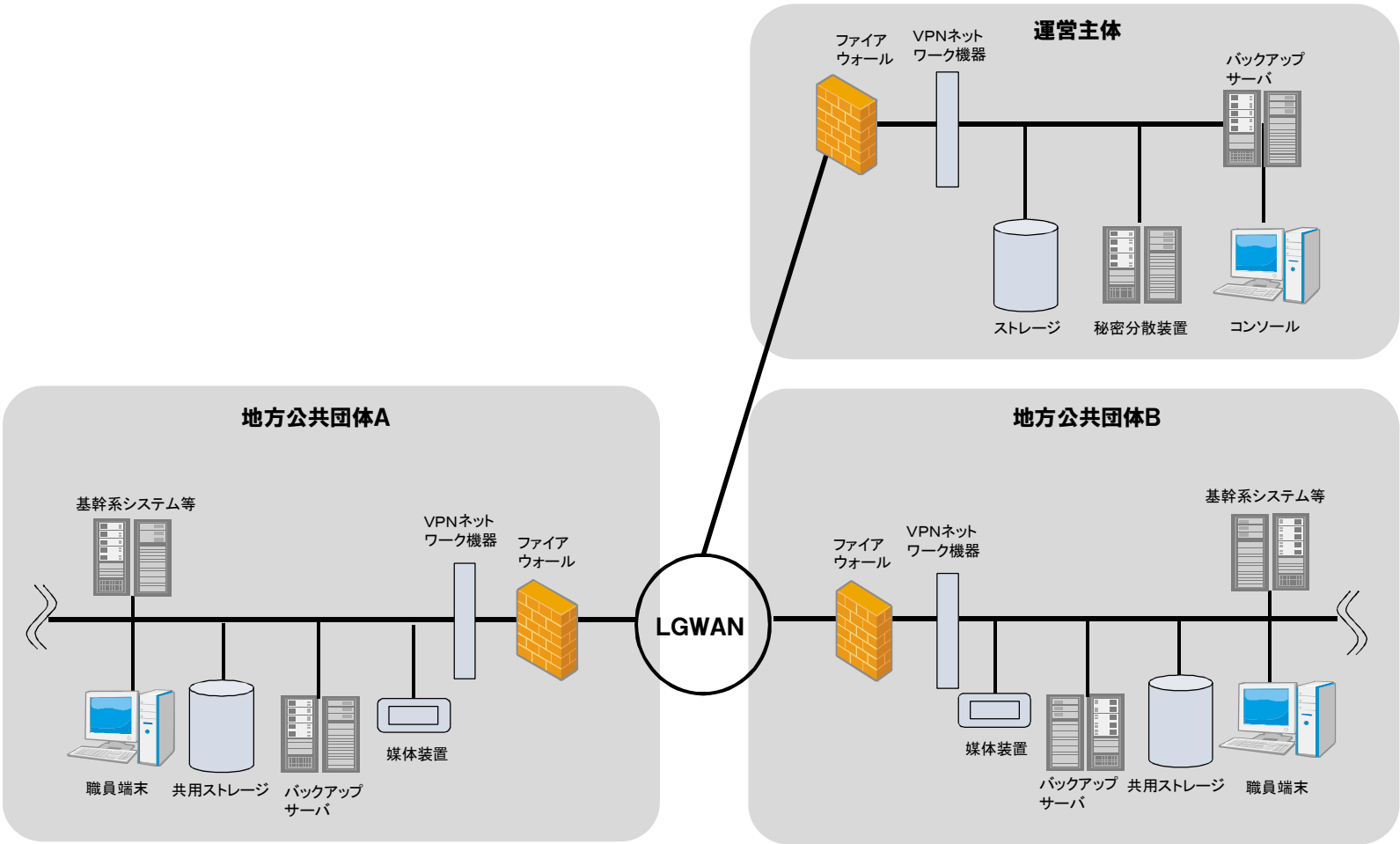
（ウ）機能の実現方法

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。

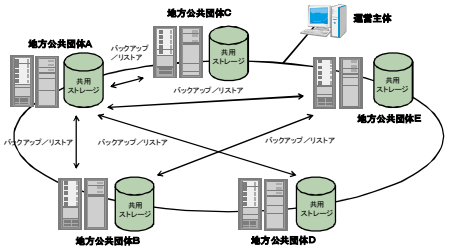
[58] ストレージ・コンパクション機能 No.5～8 に相当。「第２節－２－（２）機能概要」を参照のこと。

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。

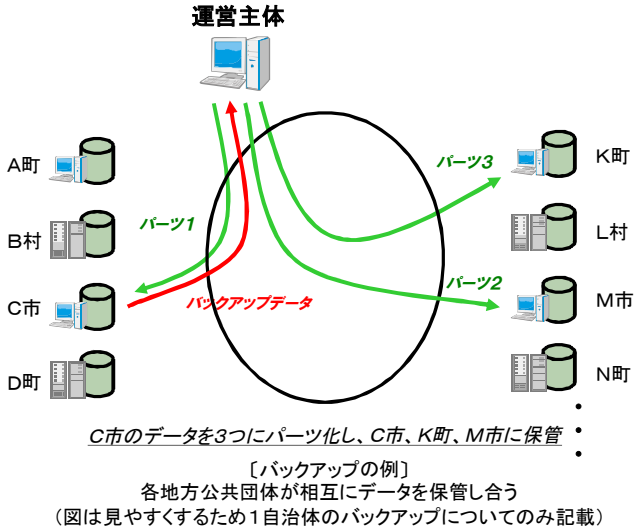
イ　バックアップ・リストア方式[60]

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）。

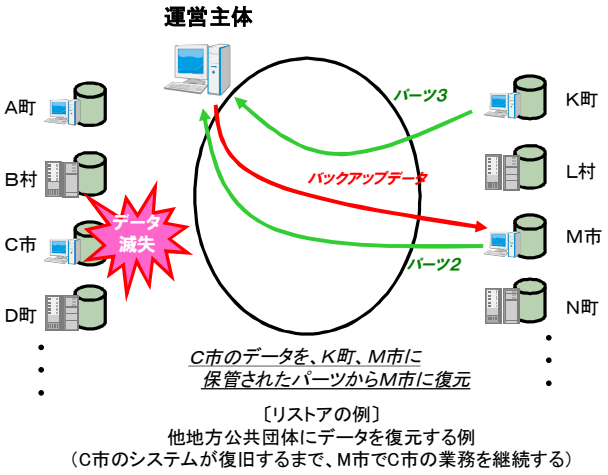


図－４８　バックアップのイメージ

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

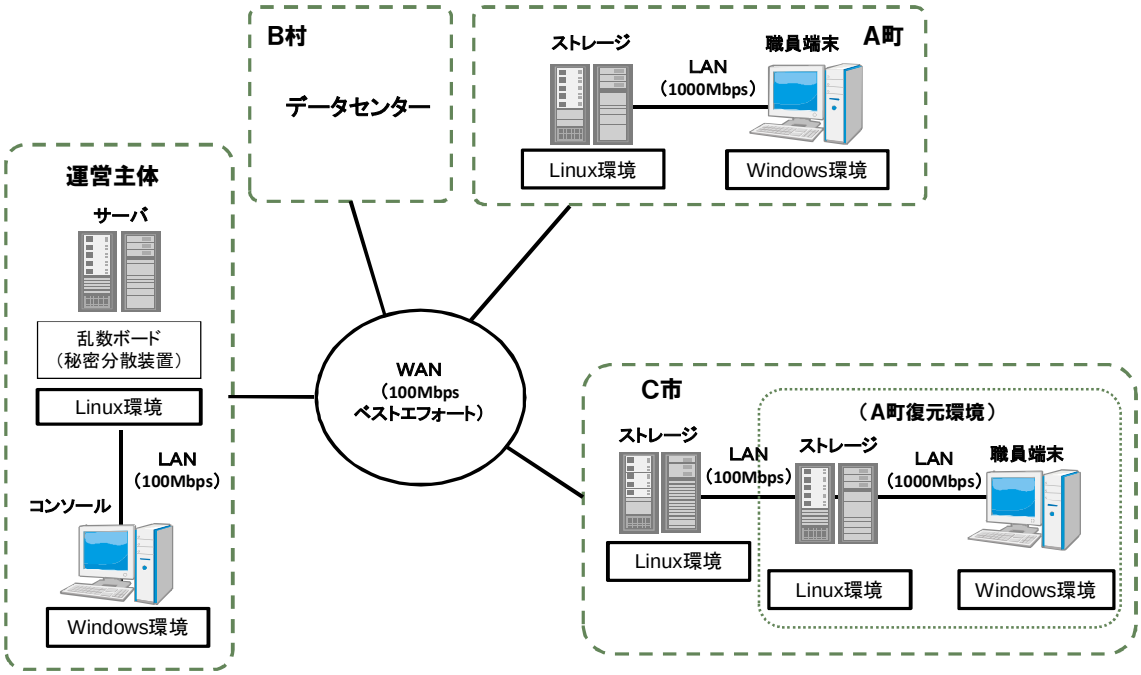
ア　基本的な考え方

・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。

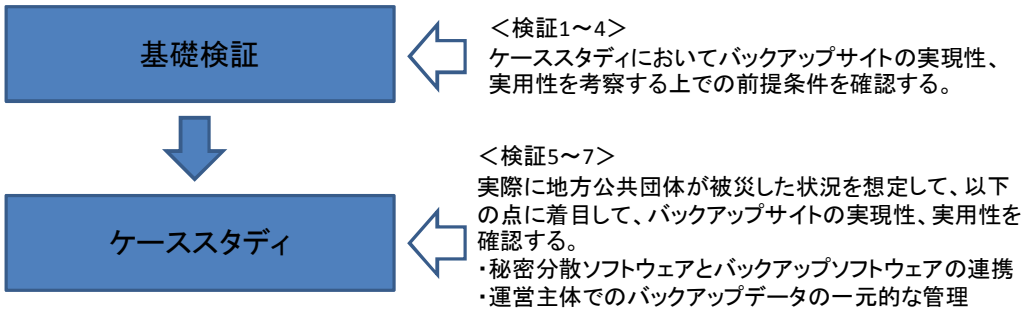


図－５０　実証実験の機器構成

表－４３　実証実験の機器構成仕様

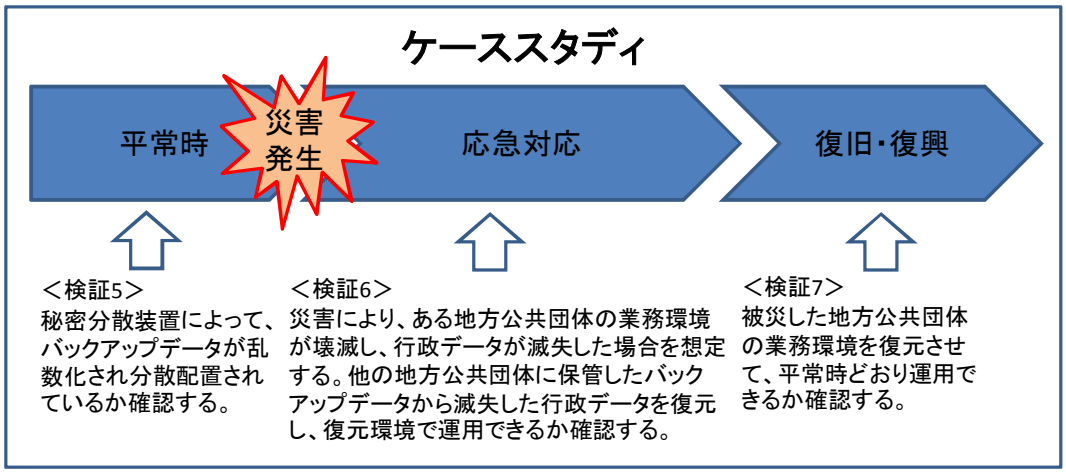
区分	種別	メーカ名及び品番	CPU	メモリ	ディスク容量	真性乱数ボード	アプリケーション	OS
A町	ストレージ	ニューテック SmartNAS	ATOM Dual Core 1.86GHz	4GB	8TB			CentOS 5.8
	職員端末（PC）	DELL VOSTRO	Core i3 3.3Ghz	4GB	1TB		True Image2013 (Acronis)	Windows7（64）
B村	クラウド	NTT コム BHE クラウド	3GHz	5GB	1TB			RedHat 5.7
C市	ストレージ	ニューテック SmartNAS	ATOM Dual Core 1.86GHz	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。

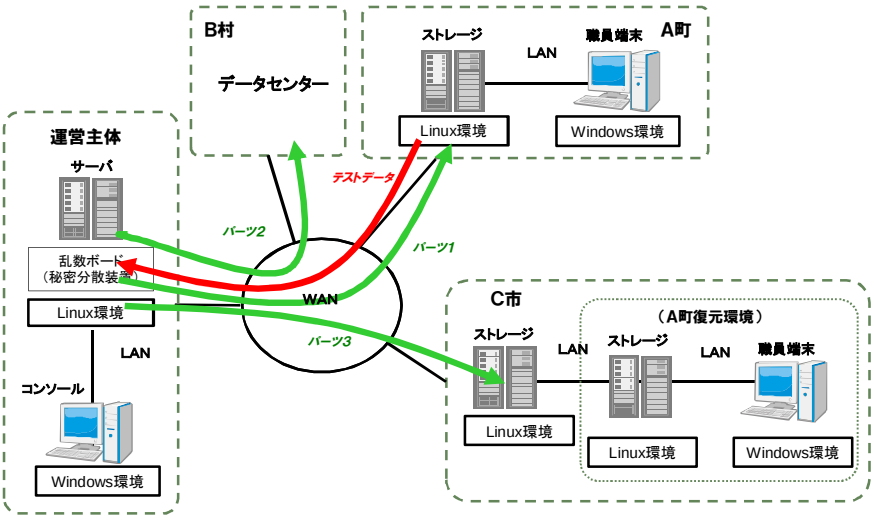
①A 町→運営主体（データ転送／テストデータ）

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。

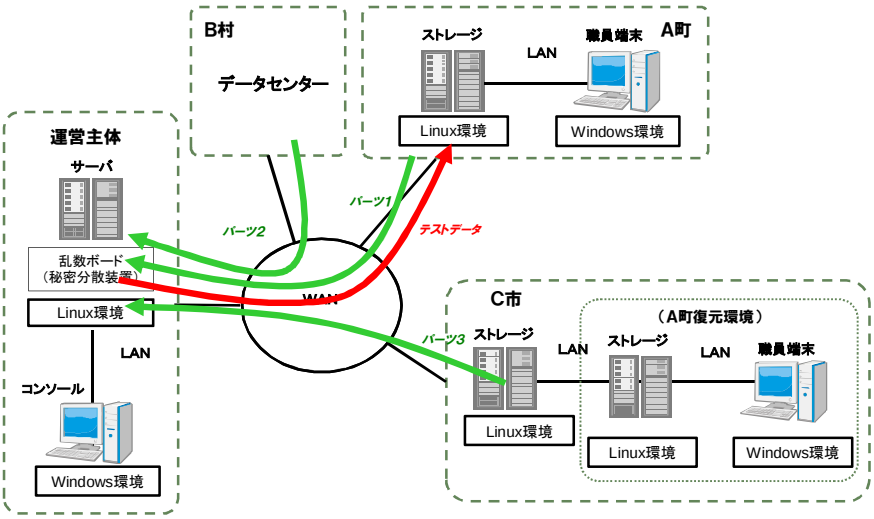
①A 町→運営主体（データ転送／パーツ 1）

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）

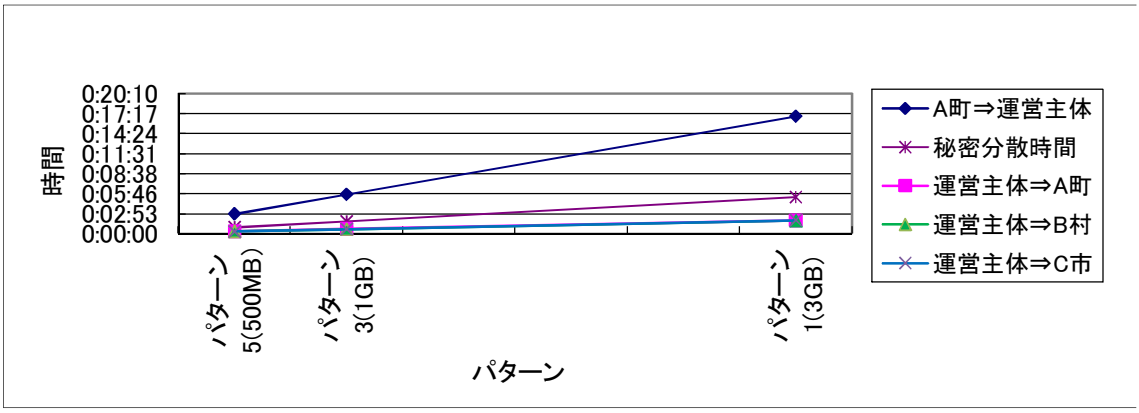
イ　結果

（ア）検証項目 1-1：バックアップ

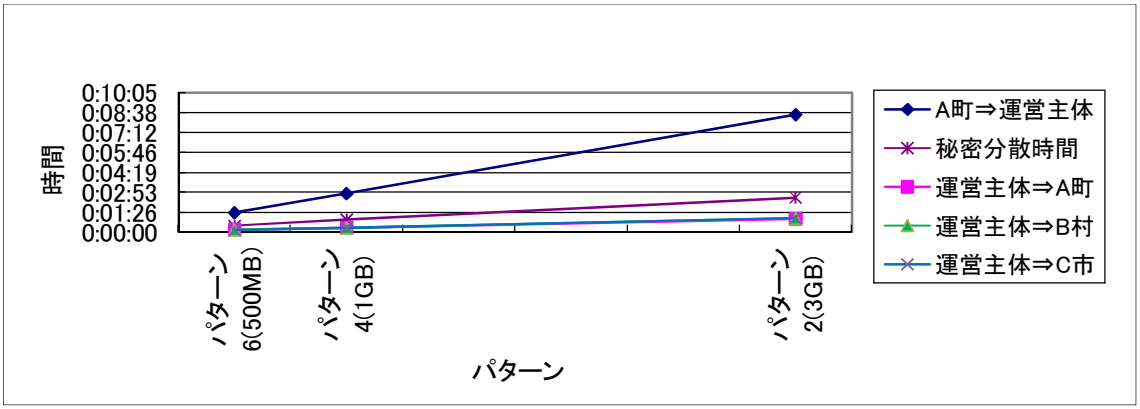
表－４６　バックアップ処理時間（検証内容 1-1）

（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）



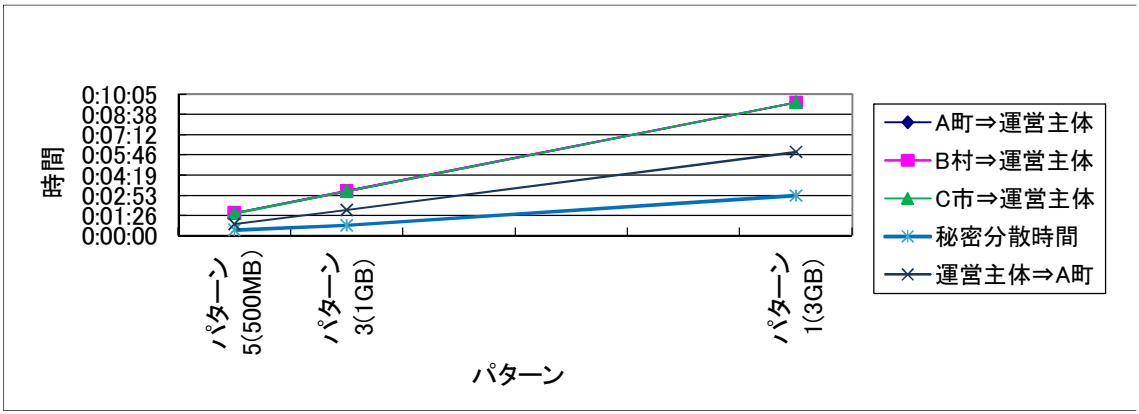
図－５６　検証１（パターン 2、4、6）の結果比較（バックアップ処理）

（イ）検証項目 1-2：リストア

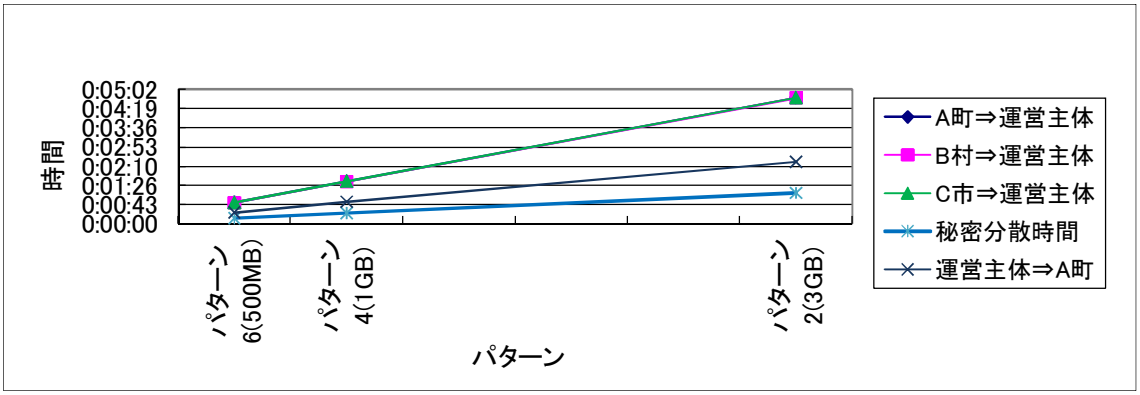
表－４７　リストア処理時間（検証内容 1-2）

（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）

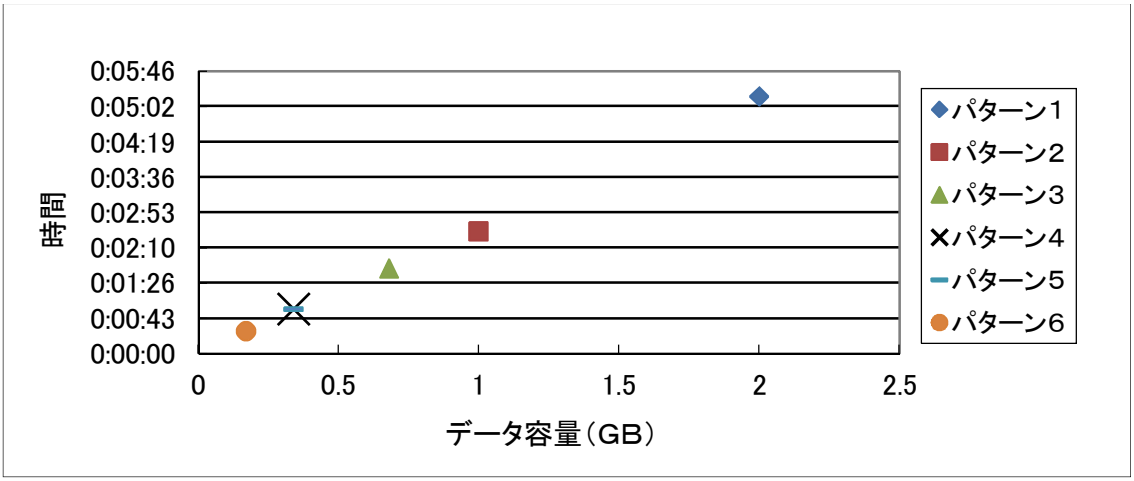


図－５８　検証１（パターン２、４、６）の結果比較（リストア処理）

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

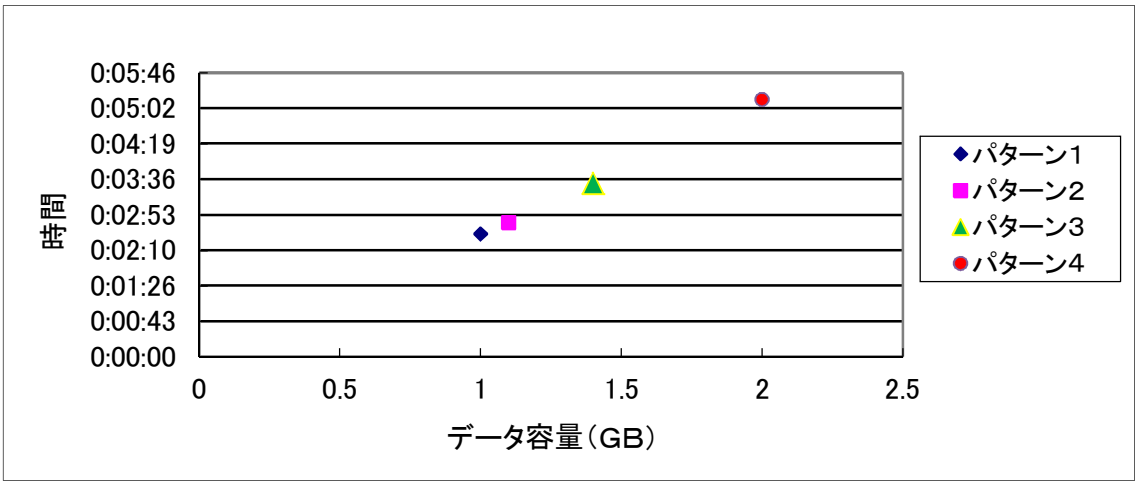
表－５１　リストア処理時間（検証項目 2-2）

（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）

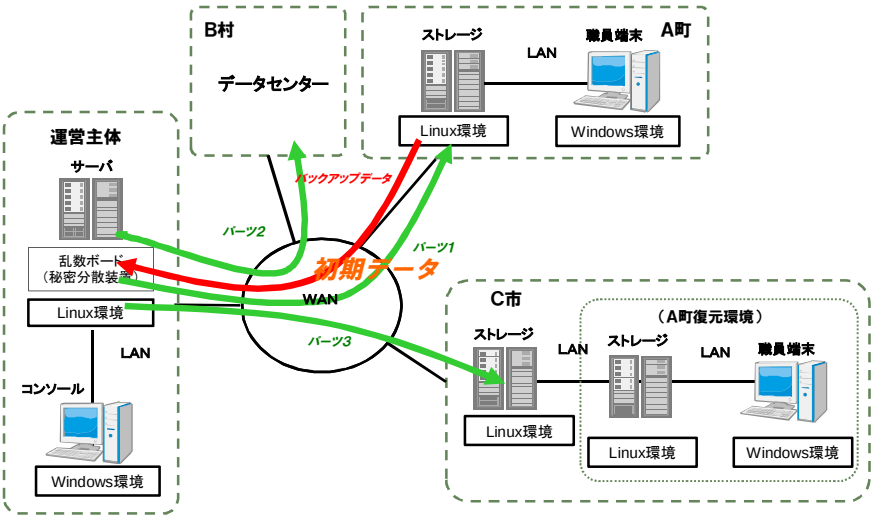
データ量		ファイル構成			フォルダ構成
総データ量	１ファイルあたりのデータ量	ファイル形式の多様性	データ全体の圧縮	ファイル作成元 OS 環境の多様性	
3GB	ファイルあたりのデータ量が概ね 1,000KB～5,000KB のファイルで構成	Word、Excel、PowerPoint、Access、Visio、PDF、テキスト、EXE などのファイル形式が混在（圧縮形式のファイルを含む）しているファイルで構成	データ全体を圧縮した構成	様々な OS（Windows、Mac、Linux など）環境で作成されたファイルが入り混じったファイルで構成	複数の階層構造、空フォルダを含むフォルダ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

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）

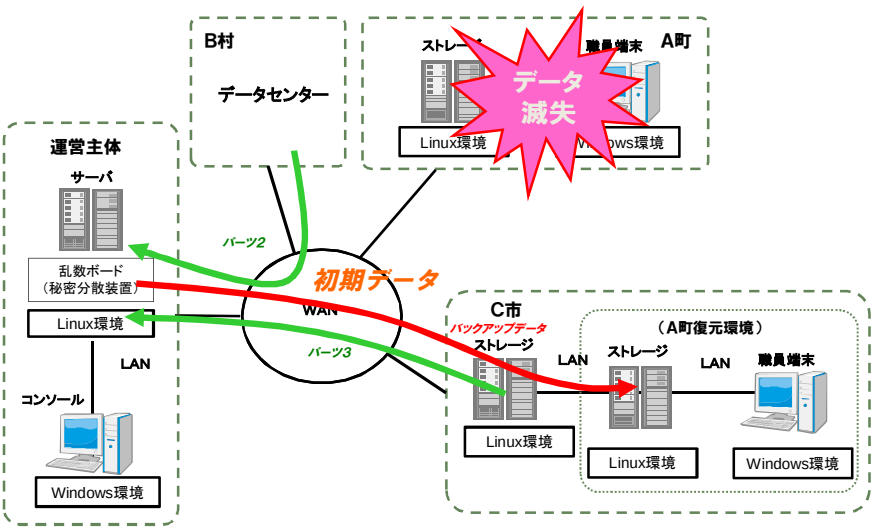
②C 市→運営主体（データ転送／パーツ 3）

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）

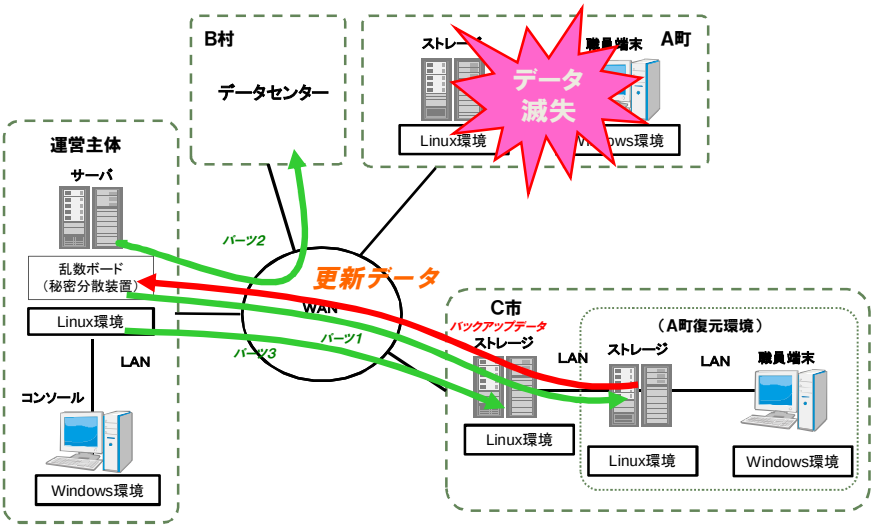
③A 町（復元環境）→運営主体（データ転送／バックアップデータ）

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）

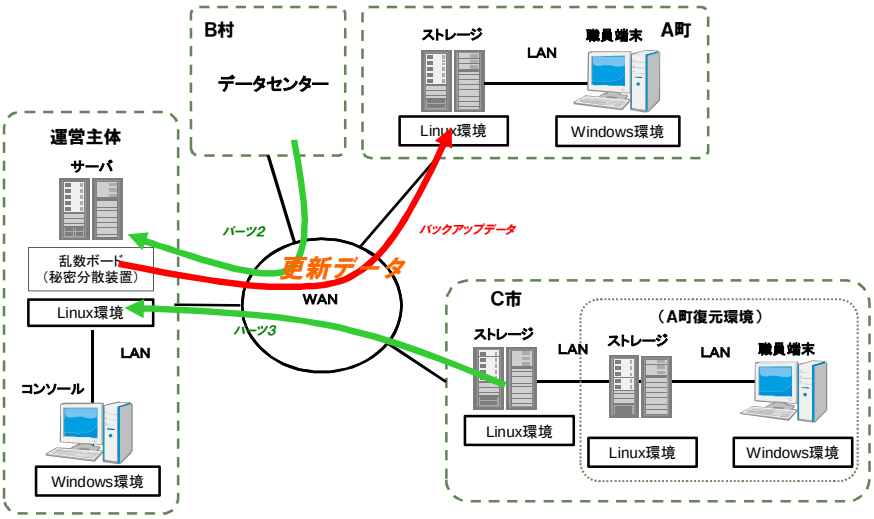
②C 市→運営主体（データ転送／パーツ 3）

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。

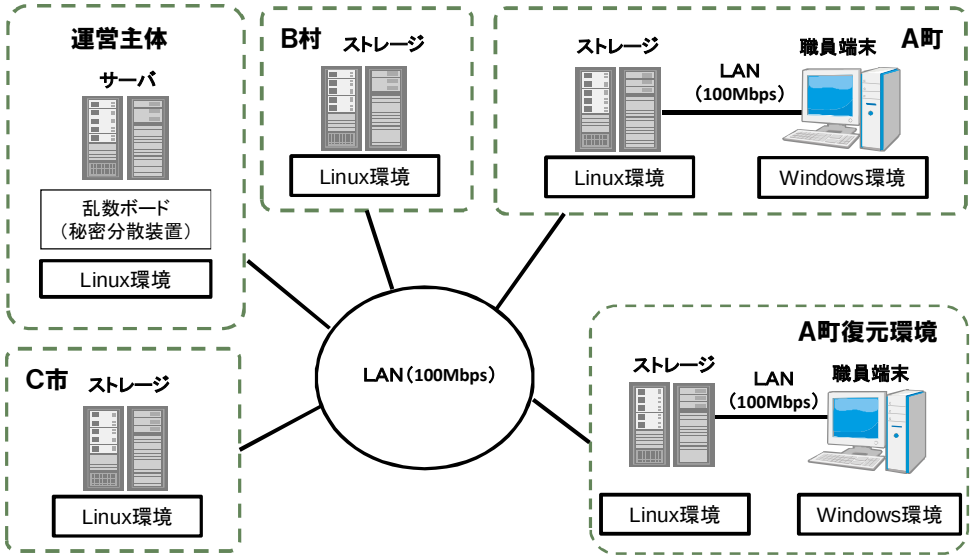
イ　実施環境

（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）

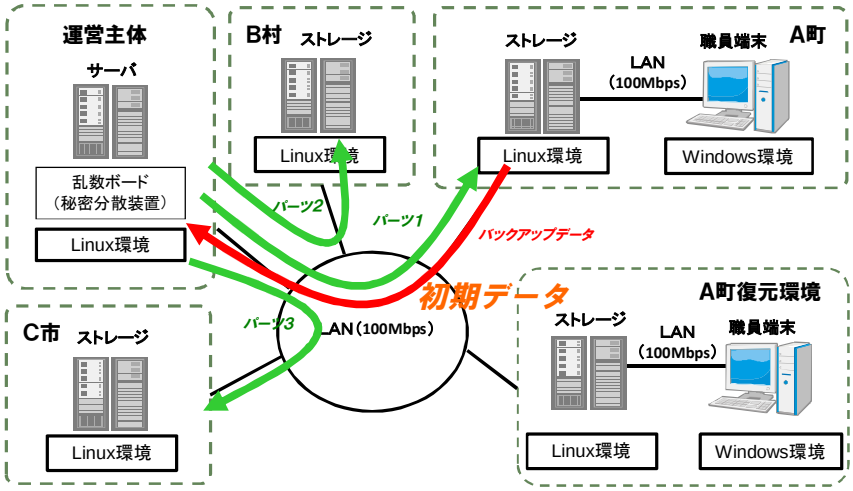
③A 町（業務環境）→運営主体（データ転送／バックアップデータ）

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）

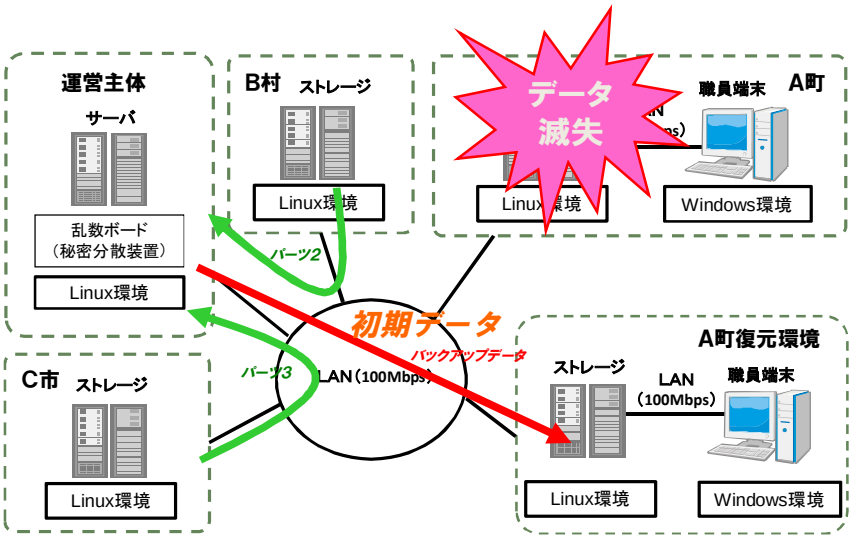
c　検証項目 8-3：復元環境へのリストア

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）

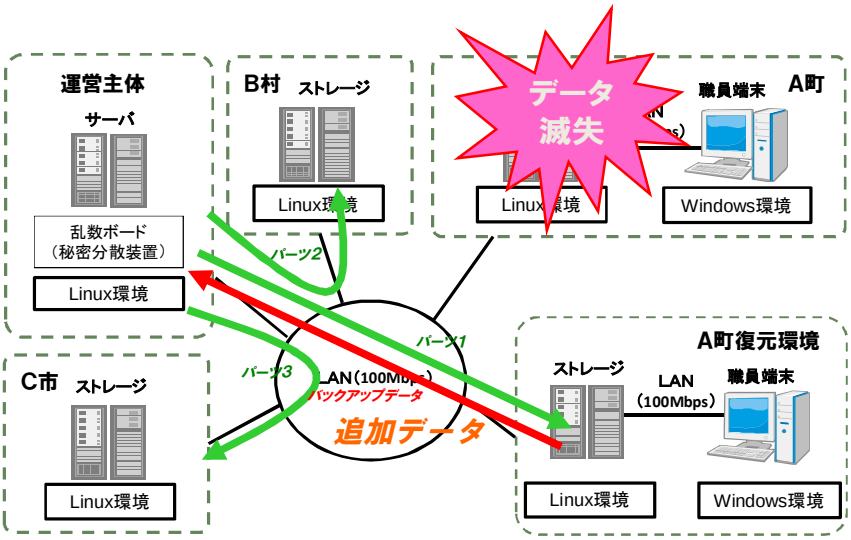
③A 町（復元環境）→運営主体（データ転送／バックアップデータ）

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）

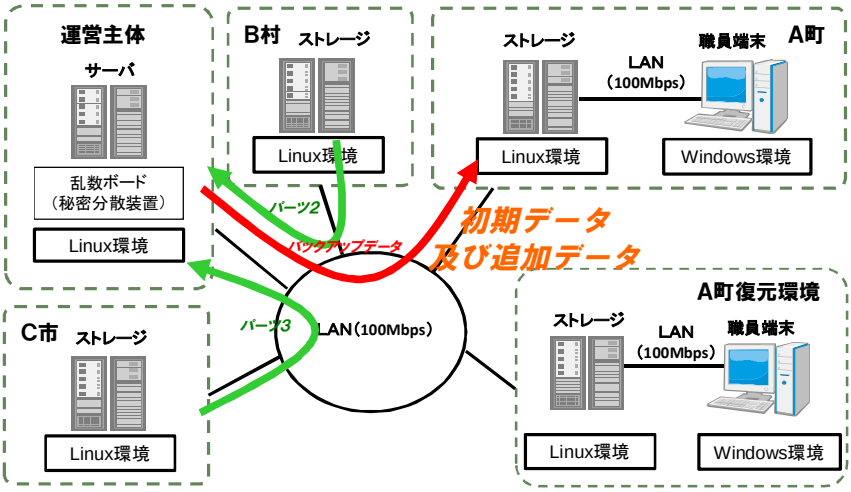
②C 市→運営主体（データ転送／パーツ 3）

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。

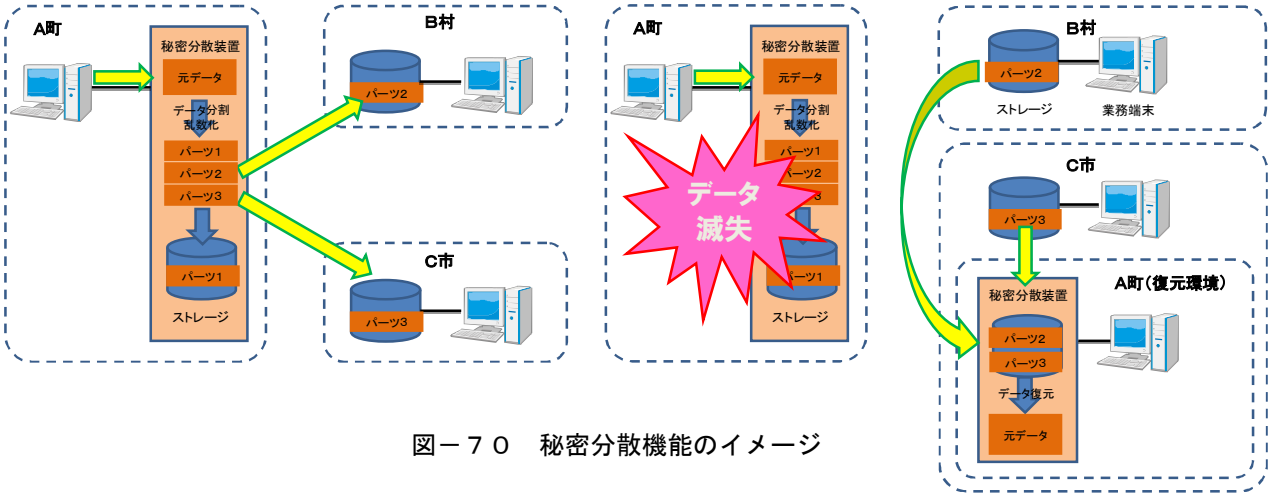
そのため、本調査研究では、以下に示す秘密分散方式（機能）を用い、関係法令等を遵守したデータの取扱いを実現し、かつ災害等によるデータ滅失に備えた信頼性の高いデータバックアップ方式の実効性等を検証する。

〔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

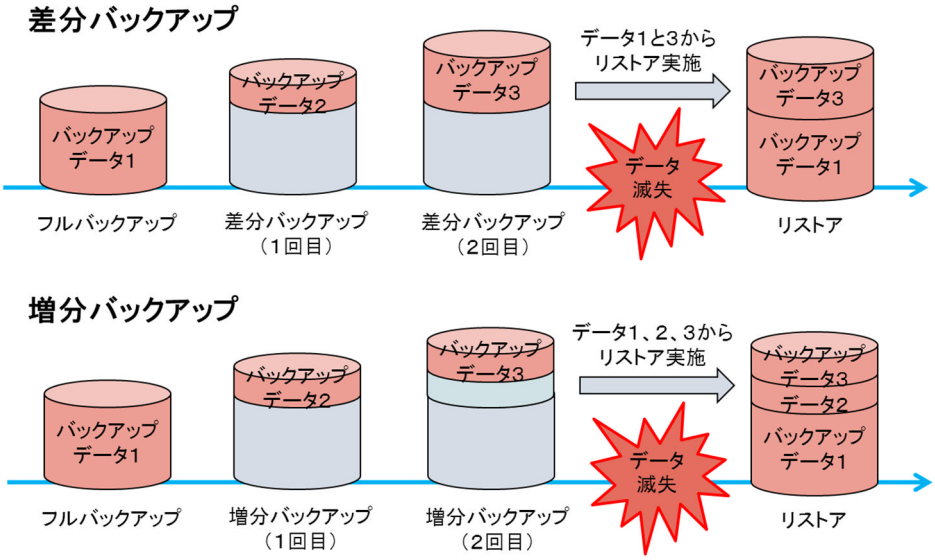
参考資料　バックアップ・リストア方法

〔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。