自治体クラウド開発実証に係る
標準仕様書（平成 21 年度版）

平成２２年３月

財団法人　地方自治情報センター

変更履歴表

項番	版数	変更理由	変更内容	変更箇所	変更区分 (更新/追加 /削除)	備考
1	1.0	新規	―	―	―	

目次

1. はじめに 1
1.1 本書の位置づけ 1
1.2 検討体制 2
1.3 自治体クラウド標準仕様書に関する説明会 2
1.4 自治体クラウド部会 2
2. 基本方針 3
3. 標準機能 4
3.1 必須要件 4
3.1.1 バックアップ連携 4
3.1.1.1 概要 4
3.1.1.2 要件一覧 7
3.1.1.3 機能 8
3.1.1.4 実装例 13
3.1.2 自治体クラウドコンピューティング（サーバ仮想化） 15
3.1.2.1 概要 15
3.1.2.2 要件一覧 20
3.1.2.3 機能 21
3.2 オプション要件 29
3.2.1 バックアップ連携 29
3.2.1.1 概要 29
3.2.1.2 要件一覧 29
3.2.1.3 機能 30
3.2.2 認証連携 33
3.2.2.1 概要 33
3.2.2.2 要件一覧 35
3.2.2.3 機能 35
3.2.3 業務データ連携 40
3.2.3.1 概要 40
3.2.3.2 要件一覧 43
3.2.3.3 機能 45
4. 拡張機能 51
4.1 バックアップ連携 51
4.1.1 データベースのレプリケーション機能によるリアルタイム同期 51
4.1.1.1 要件一覧 51
4.1.1.2 機能 51
4.1.1.3 実装例 52
4.1.2 専用ストレージによるバックアップデータの遠隔転送 53
4.1.2.1 要件一覧 54
4.1.2.2 機能 54
4.1.2.3 実装例 55
4.2 自治体クラウドコンピューティング 56
4.2.1 概要 56
4.2.2 要件一覧 56
4.2.2.1 静的マイグレーション 56
4.2.2.2 動的マイグレーション（データセンター内） 58
4.2.2.3 動的マイグレーション（データセンター間連携） 58

4.2.2.4 グリッド連携 59
4.3 認証連携 61
4.3.1 概要 61
4.3.2 要件一覧 62
4.3.3 機能 62
4.4 業務データ連携 65
4.4.1 概要 65
4.4.2 要件一覧 67
4.4.3 機能 68
4.4.4 参考（オンサイト/オフサイトの業務データ連携（地方公共団体間）） 70
5. 今後の検討課題 72
6. 付録 用語集

1. はじめに

現在、総務省により進められている「自治体クラウド開発実証事業」は、総合行政ネットワーク（LGWAN）に接続された都道府県域データセンター（以下「都道府県域 DC」という。）と ASP・SaaS 事業者のサービスを組み合わせて共同利用用途の各種業務システム等を構築し、地方公共団体が低廉かつ効率的に利用できる環境である「自治体クラウド」の整備を推進するものである。

自治体クラウド開発実証に係る標準仕様書（以下、「本書」という。）は、「自治体クラウド開発実証事業」に係る標準仕様を定めるものである。

1.1 本書の位置づけ

自治体クラウドは、IT 戦略本部の『デジタル新時代に向けた新たな戦略～三か年緊急プラン～』、『i-Japan 戦略 2015』等に掲げられている施策であり、電子行政クラウドとして国が「霞が関クラウド」を進める中、地方公共団体版の「自治体クラウド」が、平成 21 年度に総務省の開発実証事業として実施された。

「自治体クラウド開発実証事業」は、総合行政ネットワーク(LGWAN)に接続された都道府県域 DC と ASP・SaaS 事業者のサービスを組み合わせて共同利用用途の各種業務システム等を構築し、地方公共団体が低廉かつ効率的に利用できる環境である「自治体クラウド」の整備を推進するものである。開発実証は、北海道、京都府及び佐賀県が LGWAN に接続された都道府県域 DC に自治体クラウドの基盤となる「自治体クラウド連携基盤」、「データバックアップサーバ」等を構築し、北海道(管内 18 市町村)、京都府(同 25)、佐賀県(同 6)、大分県(同 5)、宮崎県(同 4)及び徳島県(同 7)の各実証団体がこの基盤に業務システムを移行等してクラウド化し、「自治体クラウドプロジェクト管理事業者」からの要求事項を踏まえ進められるものである。

地方自治情報センターは、この「自治体クラウド連携基盤」、「データバックアップサーバ」等を構築するための「標準仕様書」を作成し提示することとなっており、実証団体(道府県)に対する説明会や自治体クラウド部会を通じて、実証団体から方向性の確認や情報提供を頂きながら作業を進めてきたところである(自治体クラウド部会は、「共同アウトソーシング推進協議会」が発展改組された「自治体クラウド・共同アウトソーシング推進協議会」に設置された部会である。)。

なお、本書は、開発実証の成果を盛り込んだ作成物ではないことに御留意いただきたい。今後、開発実証の成果を踏まえた改定等を行い、標準仕様書の平成 22 年度版を作成する予定である。

1.2 検討体制

標準仕様書の検討体制と自治体クラウド開発実証事業との関係は次のとおり。

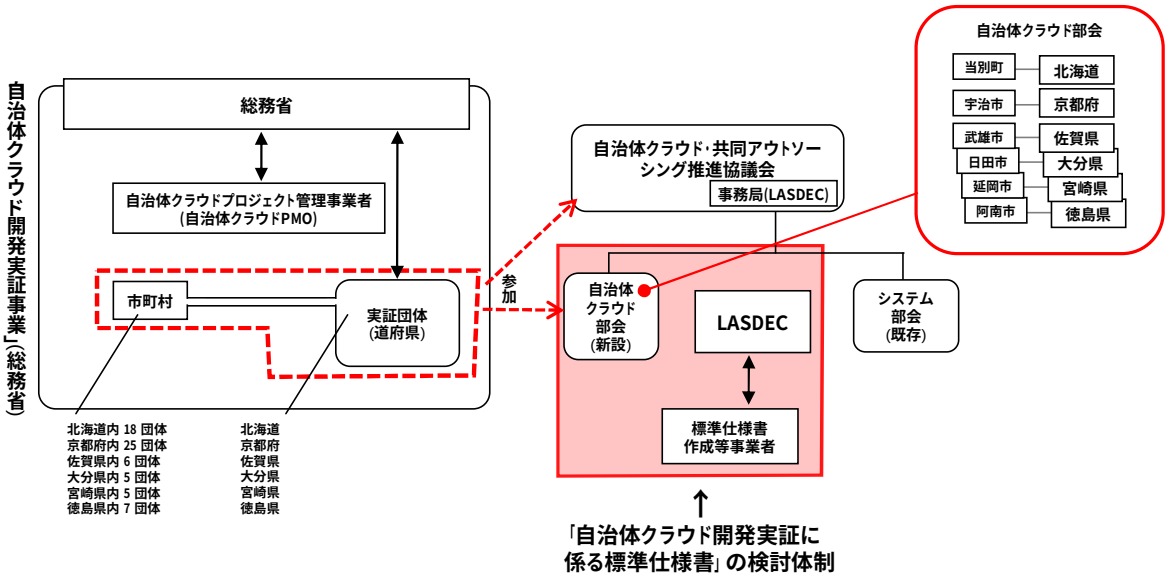


図 1-1　検討体制

1.3 自治体クラウド標準仕様書に関する説明会

本書 1 項から 3 項（「標準仕様書　調達用」）の作成に当たっては、自治体クラウド部会に先立ち、実証団体(道府県)に対する説明会を次のとおり開催した。

・平成２１年　９月３０日(水)　第１回説明会
・平成２１年１０月１５日(木)　第２回説明会
・平成２１年１１月１１日(水)　第３回説明会

1.4 自治体クラウド部会

自治体クラウド部会を次のとおり開催するとともに、自治体クラウド部会メーリングリストを開設し、随時の調整を図った。

・平成２１年１１月２４日(火)　第１回自治体クラウド部会
・平成２２年　３月１５日(月)　第２回自治体クラウド部会

2. 基本方針

本書の作成に当たっては、「自治体クラウド開発実証事業」の標準仕様という位置付け、自治体クラウドを取り巻く環境に配慮し、以下３つのポイントを考慮する。

① 「自治体クラウド開発実証事業」での取組内容
総務省主導による「自治体クラウド開発実証事業」において、平成 21 年度に実証実験として実証団体が取り組む内容と、将来自治体クラウドとして見据えて置くべき内容に分けて標準仕様書の記述を行う。

② 総合行政ネットワーク（LGWAN）
自治体クラウドでは、ネットワークとして LGWAN の利用が前提となっている。この LGWAN は将来の拡張に向けた議論が開始されたところであり、現在に比べ広帯域で柔軟なネットワークとして利用できることも期待されている。標準仕様書の作成に当たっては、現在の LGWAN を前提とする内容と将来の LGWAN を前提とする内容を考慮し記述する。

③ クラウド関連技術の実現可能性
クラウドに関連する技術については、既に多数の実績があり導入の効果がすぐに得られるものと、現時点では十分な実績が無いため導入の効果が期待できず、将来的な導入を視野に入れるべきものが存在する。標準仕様書の作成に当たっては、クラウド関連技術の実現可能性を考慮し、現在導入可能な技術と将来的に有望な技術という観点での記述を行う。

上記を踏まえ、本書では以下のような機能分類を行い、技術方式等について記述している。

【標準機能】
- 平成 21 年度の「自治体クラウド実証事業」にて、実証実験の対象となる要件を記述する。
- 実証団体で実施する必要のある「必須要件」と、任意に選択の上実施する「オプション要件」に分けて記述を行う。
- 現時点で技術的に実現が可能であり、導入によるメリットが得られる要件とする。
- 現在の LGWAN 環境（回線帯域、プロトコル等の導入要件）を利用する前提での記述とする。

【拡張機能】
- 平成 21 年度の実証実験の対象要件ではないが、自治体クラウドを推進するにあたって、業務の効率化、業務継続性の向上が期待できる技術を紹介する。

また、自治体クラウドは、LGWAN に接続された都道府県域 DC で LGWAN-ASP として構築・運用される位置付けとなるため、LGWAN-ASP として遵守すべき要求事項については、「LGWAN-ASP 接続約款」、「LGWAN-ASP 接続技術仕様書」などの LGWAN-ASP 関連ドキュメントに従うものとする。

なお、本書は「自治体クラウド開発実証事業」における、自治体クラウド連携基盤に相当するシステムの技術仕様（バックアップ含む）について定めたものであり、地方公共団体や ASP・SaaS 事業者が提供する業務サービス及び「自治体クラウド開発実証事業」での実証シナリオに関しては、記載対象外とする。

3. 標準機能

3.1 必須要件

3.1.1 バックアップ連携

3.1.1.1 概要

（1）目的

地方公共団体においては大規模な災害・事故が発生した場合、必要な業務を継続できるようにするための環境整備が必要となる。また、財政面、人材面で脆弱な小規模団体も含む各地方公共団体の情報システムの共同化を推進し、それを分散・連携運用する体制を構築することが重要である。

災害、事故等への対策の一環としては、業務情報や住民・企業に関する重要情報のバックアップデータを遠隔地に保管することが重要である。これを LGWAN に接続された都道府県域 DC 等にバックアップデータを分散配置する「バックアップ連携」として行うことで、低廉で運用が容易なサービスを提供する。

（2）適用範囲

バックアップ連携の適用範囲を図 3-1 に示す。

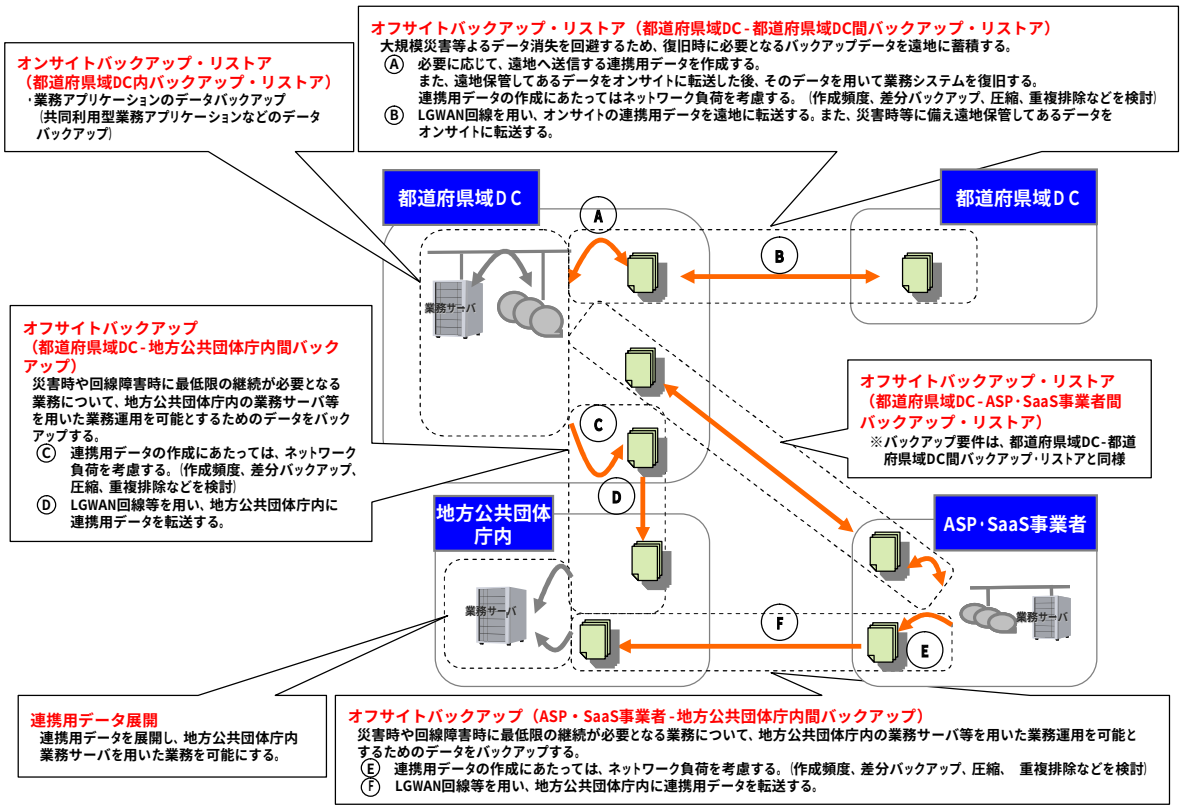


図 3-1　バックアップ連携の適用範囲

バックアップ連携では、バックアップの機能を以下のように分類した。

① データセンター内で通常実施するバックアップ・リストアの機能
- **オンサイトバックアップ・リストア**
  - 都道府県域 DC 内バックアップ・リストア
    都道府県域 DC 内の処理として業務アプリケーションで生成したデータのバックアップ及びリストアを行う。

② 災害発生後復旧時に必要な業務のための連携機能
- **オフサイトバックアップ・リストア**
  - 都道府県域 DC-都道府県域 DC 間バックアップ・リストア
    都道府県域 DC のバックアップデータを他都道府県域 DC へ遠隔バックアップ、他都道府県域 DC からリストアする。

  - 都道府県域 DC-ASP･SaaS 事業者間バックアップ・リストア
    ASP･SaaS 事業者のバックアップデータを都道府県域 DC へ遠隔バックアップ、都道府県域 DC からリストアする。

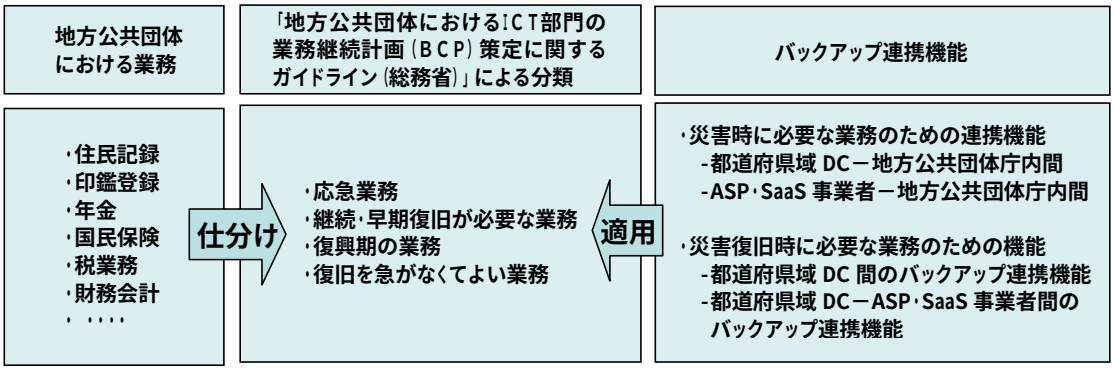
③ 災害発生時に必要な業務のための連携機能：オプション要件
- **オフサイトバックアップ**
  - 都道府県域 DC-地方公共団体庁内間バックアップ
    災害発生時に必要な業務について都道府県域 DC からバックアップデータを取得する。

  - ASP・SaaS 事業者-地方公共団体庁内間バックアップ
    災害発生時に必要な業務について ASP・SaaS 事業者からバックアップデータを取得する。

- 業務の重要度に応じた対応について

自治体クラウドのデータセンターで運用される地方公共団体の業務のうち、災害発生時に業務優先度が高いものについては、災害発生時に必要な業務のための連携機能を用いてバックアップする。

データのバックアップについては業務の重要度などを考慮して実施する必要があるため、これらのバックアップ連携機能とバックアップする業務、データの関係について下図のように整理する。



（A）業務の仕分け

業務の仕分けは「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（総務省）」を参照して実施し、応急業務などに分類する。

（B）業務への連携機能の適用

分類された業務における目標復旧時間、目標復旧レベル、データの目標復旧時点(注)等については各地方公共団体において「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（総務省）」を参照し定め、それぞれに応じて災害発生後復旧時に必要な業務のための連携機能、災害発生時に必要な業務のための連携機能を適用することとする。

（注）

バックアップの頻度は、目標復旧時点（RPO）を基に定める。

1. 情報システムに登録しているデータについて、最大で過去何日間あるいは過去何時間程度データが喪失しても許容できるかを確認する。
2. 過去この時点までのものを災害・事故により失わせない、あるいは　迅速に復旧させるという時点を決定する。
これをデータの「目標復旧時点（RPO）」という。

「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」の様式集では以下のように整理されている。

ア.災害直後のデータが必要不可欠（データの喪失は許容できない）
イ.災害発生前日のデータを喪失しても許容できる
ウ.災害発生前３日間程度の期間のデータを喪失しても許容できる
エ.災害発生前１週間程度の期間のデータを喪失しても許容できる
オ.災害発生前１ヶ月程度の期間のデータを喪失しても許容できる

「目標復旧時間（RTO）」、「目標復旧レベル（RLO）」について、いつまでに復旧する必要があるか、どのレベルで復旧するのかを定め、その要件を満たす運用及びシステムを設計する必要がある。

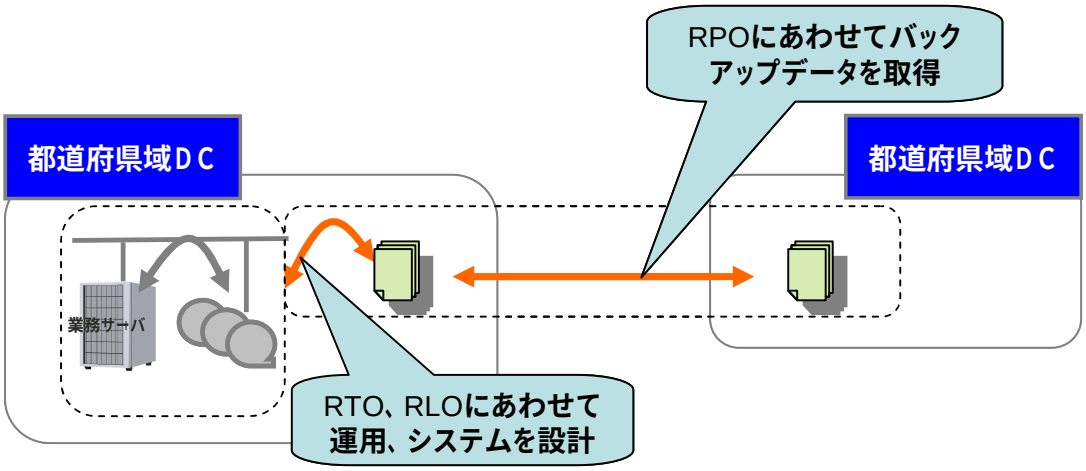


図 3-2　目標復旧時点（RPO）の適用

3.1.1.2 **要件一覧**

バックアップ連携の要件を表 3-1 に示す。

表 3-1　バックアップ連携の要件一覧

項番	要件	内容
1	オンサイトバックアップ・リストア (都道府県域 DC 内バックアップ・リストア)	業務アプリケーションで生成したデータのバックアップ及びリストアできること。
2	オフサイトバックアップ・リストア (都道府県域 DC－都道府県域 DC 間、 都道府県域 DC－ASP・SaaS 事業者間バックアップ・リストア)	連携用データ作成に関する機能 ・ オフサイトバックアップにおける、他都道府県域 DC、ASP・SaaS 事業者とデータ連携するための事前処理(連携用データ作成プロセス)。
		データ連携に関する機能 ・ オフサイトバックアップ・リストアにおける、他都道府県域 DC、ASP・SaaS 事業者とデータ連携するための処理（データ連携プロセス)。
		データ復元に関する機能 ・ オフサイトバックアップにおける、他都道府県域 DC、ASP・SaaS 事業者に保管したデータを復元する処理(データ復元プロセス)。
3	セキュリティ	セキュリティに関する機能 ・ 通信時にセキュリティを確保すること。 ・ 適切にデータを管理すること。

3.1.1.3 機能

（1）オンサイトバックアップ・リストア

都道府県域 DC 内の処理として業務アプリケーションのバックアップ及びリストアができること。なお、この機能については、業務アプリケーション導入時に実装される機能であるため、ここでは詳細な方式については規定しない。

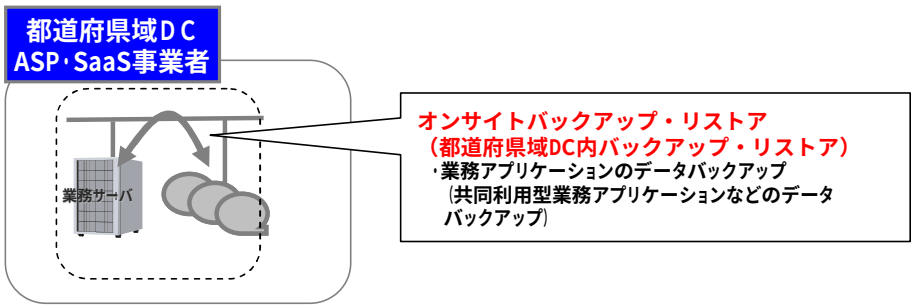


図 3-3　オンサイトバックアップ・リストア（都道府県域 DC 内処理)

（2）オフサイトバックアップ・リストア

（A）連携用データ作成に関する機能

オフサイトバックアップにおける、他都道府県域 DC、ASP・SaaS 事業者とデータ連携するための事前処理(連携用データ作成プロセス)。

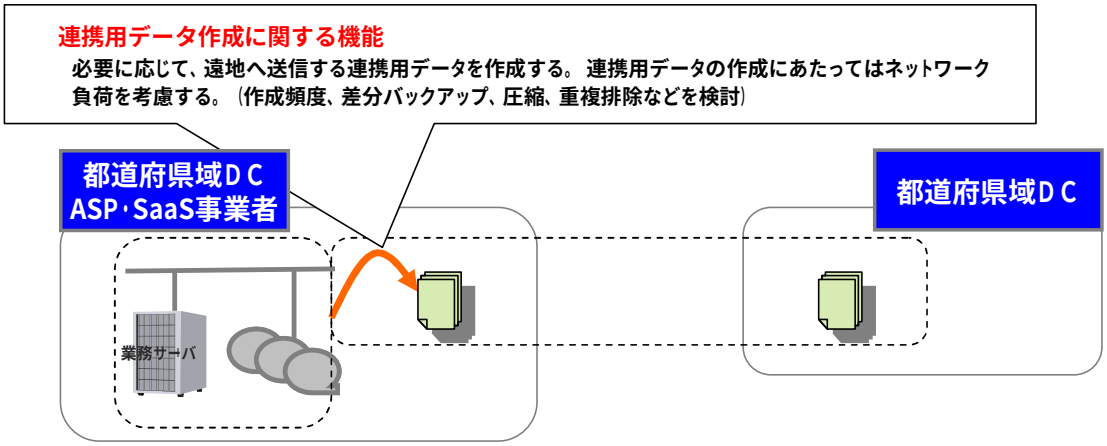


図 3-4　連携用データ作成に関する処理

災害時等に備えオフサイトバックアップ連携するため連携用の送信データを準備する必要がある。この連携用データは、LGWAN を経由して送信されるため、データサイズについて配慮しなければならない。

そのため差分・増分などのデータを抽出し、さらに、圧縮、重複排除などによりデータサイズの縮小を行う。

連携用データ作成処理は、バックアップ対象となる業務システムのバッチ処理に組み込み、実行する。 (オンサイトバックアップ処理にて同様のデータが作成されていれば流用可能)

上記処理において、必要とされる機能は以下となる。

（a）連携用データ作成のための機能

オフサイトバックアップにおける、他都道府県域 DC、ASP・SaaS 事業者とデータ連携するための事前処理

（ア） データ量を低減させるための、差分バックアップや、増分バックアップなどのなどのデータを取得すること。

（イ） 複数データ間に存在する重複部分の排除、データの圧縮等を行うこと。

（b）データの一元管理を行うための機能

（ア） 連携用データの作成日時、保存先などの管理ができる機能

１日１回自動データ連携する仕組みにおいて、回線障害等により数日間、データ連携が正常に行われなかった際は、回線が正常に復帰した後、本来実施されるはずであった「数日間のデータ連携処理」が必要となる。この時、データの一元管理を行うための機能を用い、順次処理が実行される。

（c）データの世代管理を行うための機能

（ア） 保存世代は１世代以上で、必要に応じ長期間保存が可能なこと。

（イ） 保存世代から外れたデータは削除し、領域の再利用が可能なこと。

（d）効率的に連携を行う機能（推奨）

連携用データ作成における一連の作業は、省力化のため、ジョブ管理ソフト等により自動実行させる必要がある。

（ア） 処理を自動で運転できること。

（イ） システムの運転状態をジョブ管理ソフトなどに通報し、状態に応じた連係動作が可能であること。

（ウ） 必要に応じて、バックアップタイミングを「定時起動」、「任意起動」など自由に設定が行えること。

（e）拡張性を高めるための機能（推奨）

（ア） バックアップの運用に影響を与えることなく、容量や性能の拡張ができる機能

バックアップデータ量は、対象業務システム数、データ重要度などにより変化する。拡張が必要になった時、既存システムを長期間運用停止し、システムを再構築することは困難であるため、容易にスケールアウトが可能な機能を事前に備えておくことが重要となる。

（B）データ連携に関する機能

オフサイトバックアップ・リストアにおける、他都道府県域 DC、ASP・SaaS 事業者とデータ連携するための処理(データ連携プロセス)。

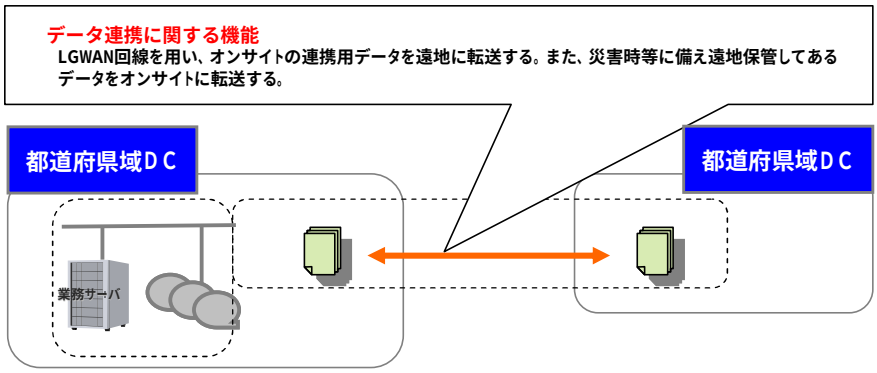


図 3-5　データ連携に関する処理

災害時等においてもバックアップデータが消失しないよう、システムとは別の場所に保管することが重要である。データの遠地保管する場所は、地震、台風など広域にわたって影響をおよぼす場合を考慮し、その範囲を超える地域を選択することが望ましい。

また、安全性、運用性を考慮し、バックアップデータを搬送する方法の選択、バックアップデータを保管する方法、保管場所からの到達時間などを検討する必要がある。この遠地保管に対する手段として可搬媒体での運搬ではなく、デジタルデータとして WAN 回線を用い保管場所に送る方法(データ連携)をとることで、可搬媒体を搬送する場合のセキュリティ上のリスクや到達時間リスクなどを回避することが可能となる。可搬媒体を利用する場合は以下の考慮が必要となる。

- コンピュータ用可搬媒体の搬送・保管を専門にする業者が望ましい。
- 可搬媒体が、磁気テープ等周囲の影響を受け易い媒体の場合、磁気を遮断する金属製の箱などが必要となる。また、気温、湿度、施錠などにも配慮する必要がある。
- 同時に災害の影響を受けることがない地域として保管場所までの到達時間が極端にかかる場所では、有事の際、可搬媒体を取り寄せるのに時間がかかり効率的ではない。また、運送中における事故に遭遇する確率も高くなる。

ネットワーク（LGWAN）を用いたデータ連携において、必要とされる機能は以下となる。

（a）効率的にデータ転送するための機能

（ア） トンネリング機能

データ連携方式を実現するためにトンネリングを行い、連携用データを転送する。

（イ） 重複排除機能（推奨）

LGWAN のネットワーク負荷低減のため、転送するデータの重複部分を自動的に排除し最小限にする機能（推奨）。

転送するデータは事前処理により、差分抽出、圧縮などデータを最小限にする処理が行われているが、この事前処理済みデータを連携先に転送する際、前回のデータ連携までに転送したデータと比較し、変更された部分のみを送付することで大幅にネットワーク帯域を節約できる。

（b）データの一元管理を行うための機能

（ア） 連携用データの作成日時、保存先などの管理ができること。

（イ） 保存世代は１世代以上で、必要に応じ長期間保存が可能なこと。

（ウ） 保存世代から外れたデータは削除し、領域の再利用が可能なこと。

（c）効率的に連携を行う機能（推奨）

連携用データ作成における一連の処理は、省力化のため、ジョブ管理ソフト等により自動実行させることが望ましい。

（ア） 処理を自動で運転できること。

（イ） ネットワーク障害発生時、連携処理動作を変更・設定できること。

（ウ） 必要に応じて、連携タイミングを「定時起動」「任意起動」など自由に設定が行えること。

（C）データ復元に関する機能

オフサイトバックアップにおける、他都道府県域 DC、ASP・SaaS 事業者に保管しているデータを復元する処理(データ復元プロセス)。

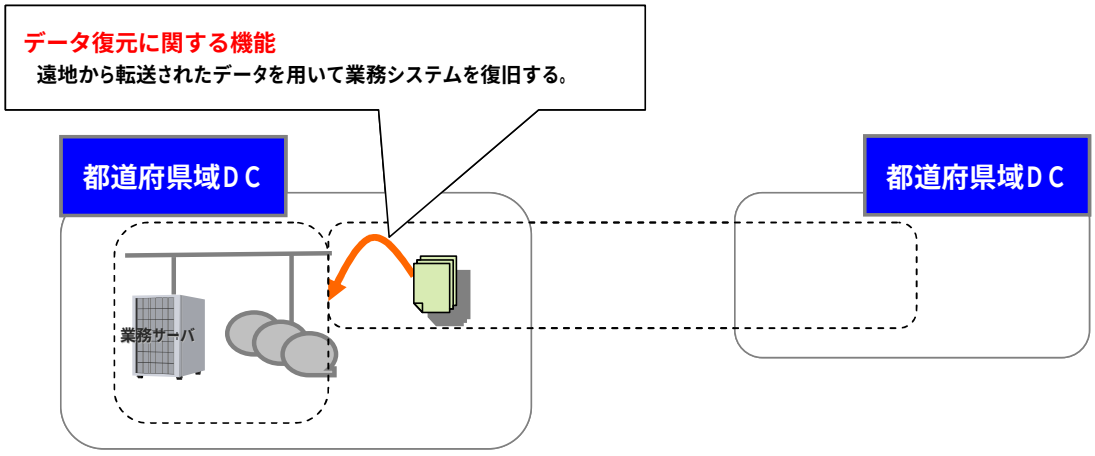


図 3-6　データ復元に関する処理

災害時等に備え遠地保管してあるデータをオンサイトに転送した後、そのデータを用いて業務システムを復旧する。

（a）処理の自動化を行うための機能

（ア） 処理を自動で運転できること。

（D）セキュリティに関する機能

バックアップデータには、個人情報など重要な情報が含まれているため、その送信及び管理には十分なセキュリティが求められる。このデータを他都道府県域 DC、ASP・SaaS 事業者と連携するため、その管理はセキュリティを強く意識した方法を採る必要がある。

また、データ連携するすべてのサイトにおいては、システム運用に関して情報セキュリティマネジメント体系を事前に整備することを強く推奨する。

上記処理において、必要とされる機能は以下となる。

（a）通信時にセキュリティを確保する機能

オフサイトバックアップにおける、他都道府県域 DC、ASP・SaaS 事業者とデータ連携するための事前処理

（ア） 事前に情報を登録することで、特定のアクセス先からのみアクセスできること。

（イ） 秘匿機能
LGWAN **転送中は** IPSec **などで通信内容を秘匿すること。**

（b）データを管理する機能

（ア） データバックアップサーバは、十分なセキュリティを考慮した運用がなされること（LGWAN-ASP **としてのセキュリティ要件を満たすこと。）。**

（イ） データへのアクセス制限を実施し、許可されていないユーザがアクセスした時は、ログに記録することを推奨する。

3.1.1.4 実装例

（1）ファイル転送又はファイル共有を利用するケース

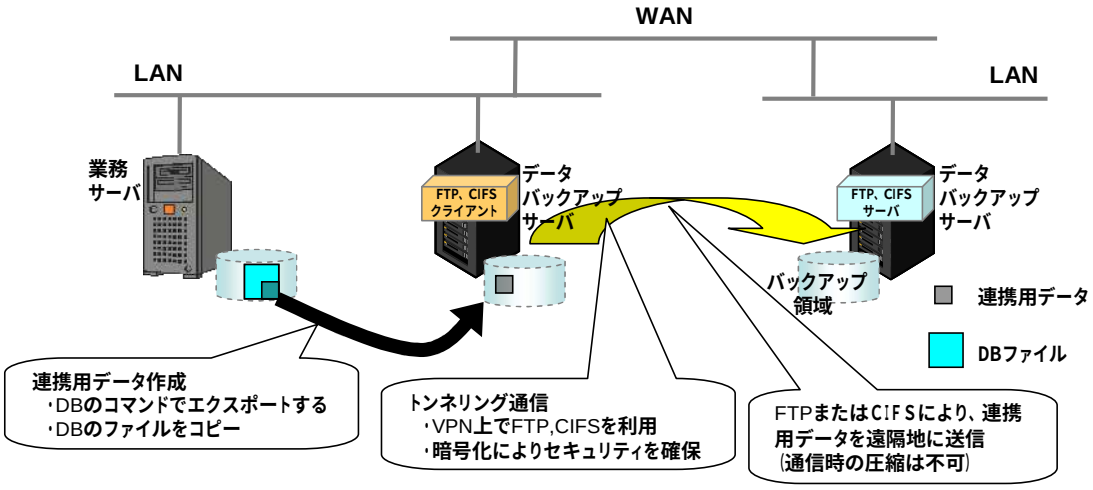


図 3-7　ファイル転送又はファイル共有を利用するケース

（A）連携用データ作成の方法

（a）DB からファイルをエクスポートする場合

DB のソフトウェアに付属しているバックアップコマンドなど(ここでは EXPORT コマンドを例に説明)を利用して連携用データを作成する。EXPORT コマンドをスクリプトで作成し、運用管理ソフトなどと連携することを推奨する。

（ア） 業務ロジックにより増分又は差分バックアップデータを EXPORT コマンドで出力する（ファイルサイズ：小、取得時間：長）

→既存の処理で相当するファイルがあれば流用可能。

（イ） 圧縮ツールを使ってデータ圧縮（バイナリデータのため圧縮率低）（運用作業）

（b）DB ファイルを利用する場合

（ア） OS のコマンドや explorer 等のツールを使ってファイルをコピー（ファイルサイズ：大、 取得時間：短）

→既存の処理で相当するファイルがあれば流用可能。

（イ） 圧縮ツールを使ってデータ圧縮（運用作業）

（B）データ連携の方法

（a）連携用データをファイル転送、ファイル共有などの方法により、トンネリングした経路で連携先データバックアップサーバに転送する。

（2）バックアップソフト固有の通信を利用するケース

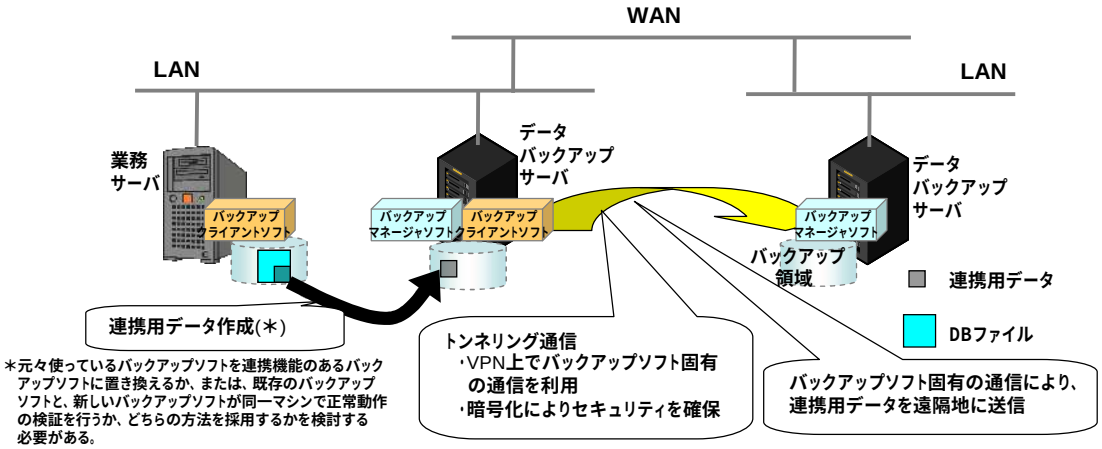


図 3-8　バックアップソフト固有の通信を利用するケース

（A）連携用データ作成の方法

（a）バックアップソフトを使って DB の内部コマンド（EXPORT コマンド）と連携する場合

（ア） 業務ロジックにより増分又は差分バックアップデータをエクスポート（ファイルサイズ：小、取得時間：長）
→既存の処理で相当するファイルがあれば流用可能。

（イ） バックアップソフトの機能を使ってデータ圧縮（既に圧縮されているため、重複排除のみ可能）

（b）バックアップソフトを使って DB ファイルを利用する場合

（ア） バックアップソフトの機能を使ってファイルをコピー（ファイルサイズ：大、 取得時間：短）
→既存の処理で相当するファイルがあれば流用可能。

（イ） バックアップソフトの機能を使ってデータ圧縮（圧縮、重複排除ともに可能）

（B）データ連携の方法

（a）連携用データをバックアップソフトにより、連携先のデータバックアップサーバに保存する。この時、転送データ最適化のため、連携先データバックアップサーバとのデータ重複チェックをバックアップソフトによって実施することが望ましい。

参考

オフサイトバックアップの留意点

DC 間のオフサイトバックアップについては、バックアップデータを送る側と受ける側とで連携する必要がある。連携方法としては、受ける側がどこまで送る側にサービスを提供するかによって次のような分類(選択肢)が考えられる。開発実証としていずれの方法を選択するかは団体間で決定する。

① データセンターの場所やラック等を提供するハウジングサービス(送る側がラック、データバックアップサーバ等を構築。)。
② 受ける側がサーバまで提供するホスティングサービス(バックアップソフト等は送る側が設定。)。
③ 受ける側がバックアップソフト等まで用意する AP サービス(送る側は受け側が提供するバックアップソフト等を利用してバックアップを行う。)。

3.1.2 自治体クラウドコンピューティング（サーバ仮想化）

3.1.2.1 概要

（1）目的

自治体クラウドにおける都道府県域 DC 内システム構築においては、従前の物理サーバをデータセンターに並列に設置する、いわゆる IaaS 型と併せて、昨今の仮想化技術の進展に合わせたクラウド基盤の構築が考えられる。IaaS 型での構築は、既存の「LGWAN-ASP 接続約款」及び「LGWAN-ASP 接続技術仕様」に準拠し実装されるが、仮想化技術を用いて構築する場合は、これら仕様に明確な記載がない。したがって、本仕様にて自治体クラウドコンピューティングとして定義し、この実装方法等について仕様を定めることによりハードウェアの効率利用、運用性の向上を目指す。

なお、図 3-9 に示すとおり、都道府県域 DC 内では、構築するアプリケーションの特性に合わせて、物理サーバ、仮想化サーバの併設も考えられる。

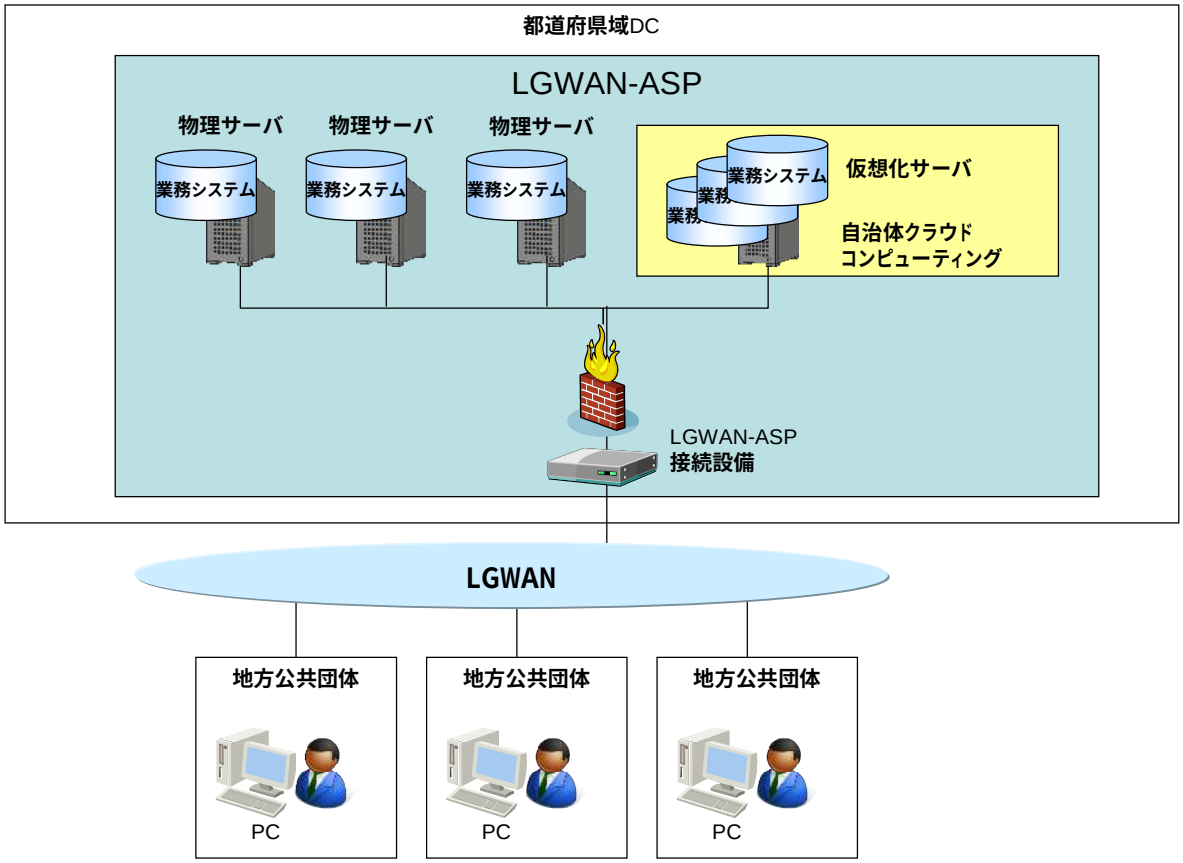


図 3-9　都道府県域 DC の実装イメージ

図 3-9 で示した自治体クラウドコンピューティングについて概要を説明する。

現在、地方公共団体では地方公共団体庁内にサーバを設置し、業務システムごとに独自のハードウェアを利用し運用を行っているケースが多い。

従来のハードウェアの統合対策として 1 つの OS 上に複数の業務アプリケーションをタスクとして稼動（マルチプロセス）させハードウェアの共有化を図る方法がある。この方法では、複数の業務が同一 OS 上で稼動するため、業務が要求する個別のセキュリティレベルを満たせない場合がある（特定業務の都合で OS のセキュリティレベルを下げなければならない場合など）。また、業務間での OS リソースの競合問題及び業務により対応 OS が異なるなどの課題がある。

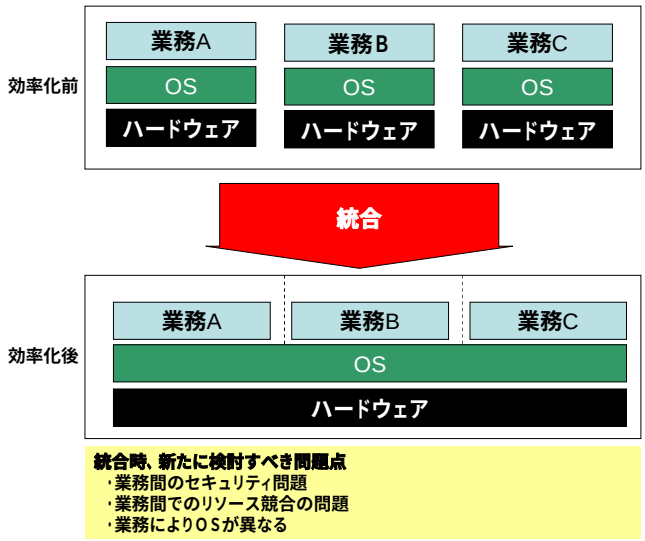


図 3-10　現状のハードウェア統合に対する課題

一方、自治体クラウドコンピューティングを利用したハードウェアの統合では、業務自体が独立した OS 上で動作するため上記課題を解決でき、簡易に業務の統合が可能になる。

これにより、省コスト、省スペース、省電力及び運用負荷の軽減が期待できる。

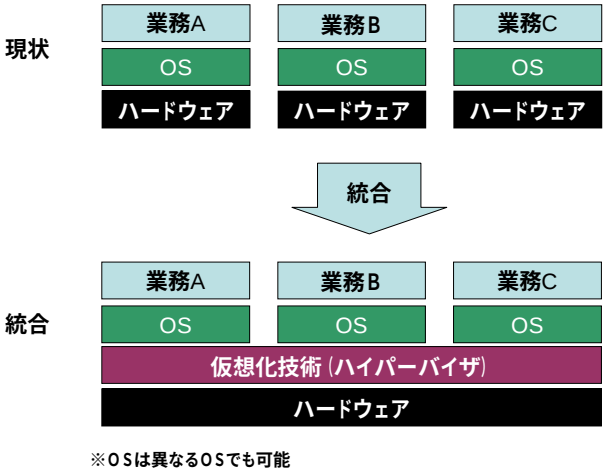


図 3-11　地方公共団体業務システムのハードウェア統合イメージ

業務の統合を考えた場合、統合する全業務の負荷状況や運用状況を考慮する必要がある。たとえば、同じ時間帯に負荷が集中する業務を同じハードウェアに統合した場合などは効率的な利用とはいい難い。また、バックアップタイミングなどが大きく異なる業務を統合させると統合的なバックアップの実施が困難になり効率的な運用とはいい難い。したがって、統合する業務の特性を十分理解した上で組み合わせを考慮する必要がある。

上記を考慮し、最初は地方公共団体内の複数業務統合や、複数地方公共団体による同一業務統合などを試行的展開することにより業務の特性を把握し、最終的には地方公共団体内にとどまらず複数地方公共団体、複数業務でのハードウェア共同利用を目指す。

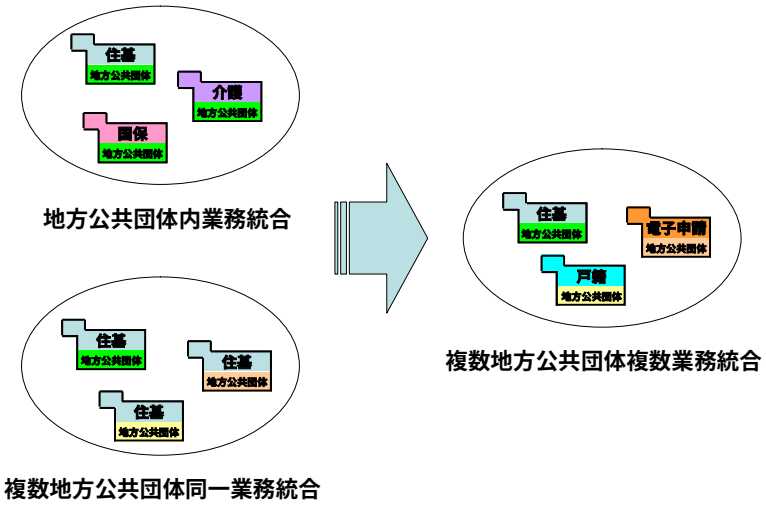


図 3-12　業務の段階的な統合

（2）適用範囲

自治体クラウドコンピューティングにおいても既存の「LGWAN-ASP 接続約款」及び「LGWAN-ASP 接続技術仕様」に準拠する必要があるが、LGWAN-ASP の規約内には仮想化技術に関する記述がされていない。

本節では LGWAN-ASP で利用する仮想化技術について記述する。適用範囲は図 3-13 に示す仮想化サーバ部分とする。

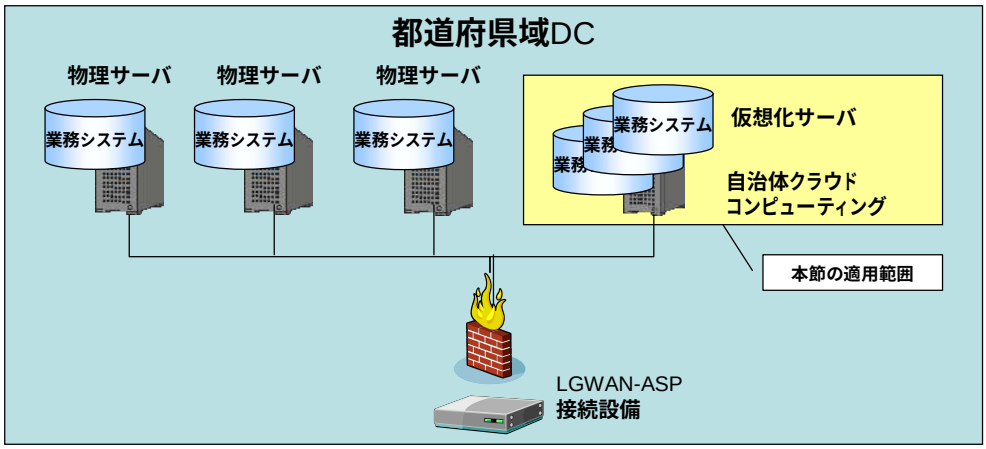


図 3-13　自治体クラウドコンピューティングの適用範囲

地方公共団体業務を自治体クラウドコンピューティングに適用した場合、性能面、運用面等において同一ハードウェア上で稼動する業務システムの組み合わせが重要な要素となる。

組み合わせに関しては、以下の 3 つのパターンが考えられる。

- 同一業務統合型

図 3-14 は複数地方公共団体の同一業務を１つのサーバ上で稼動させる構成で、地方公共団体数にもよるが、単純に業務ごとにハードウェアを準備する必要がある。バックアップタイミング等の統一が図れ、運用面では効率的であるが、業務負荷のタイミングが同一時間帯に集中する恐れがあり、性能面において十分考慮する必要がある。

図 3-14 同一業務統合型

- 地方公共団体内業務統合型

図 3-15 は同一地方公共団体の複数業務を 1 つのサーバ上で稼動させる構成で、地方公共団体ごとにハードウェアを準備する必要がある。負荷のかかる時間帯が異なる業務を稼動させることにより、効率的な利用が可能となるが、業務ごとに運用が異なるため、業務の組み合わせを十分考慮し運用設計する必要がある。

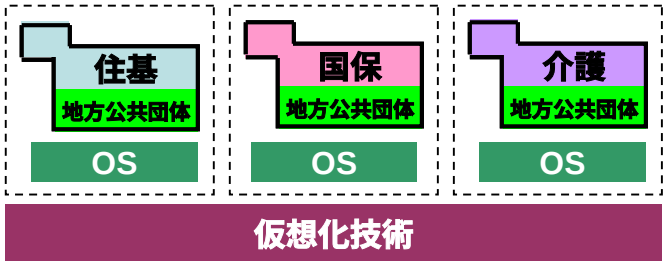


図 3-15 地方公共団体内業務統合型

- 複数地方公共団体／多種業務統合型

図 3-16 は複数地方公共団体が、複数の異なる業務を 1 つのサーバ上で稼動させる構成で、最も効率的な利用が可能である。各地方公共団体の業務毎の負荷状況や運用状況を考慮し組み合わせを設計する必要があり、また、ある業務の運用変更により他業務に影響を与える可能性もあるため、考慮すべき点が多い。

図 3-16 複数地方公共団体／多種業務統合型

（A）制約事項

都道府県域 DC で構築される業務システムは LGWAN を利用して実装されるため、「LGWAN-ASP 接続約款」及び「LGWAN-ASP 接続技術仕様」等に従い構築されなければならない。これら仕様によれば、都道府県域 DC 内のネットワークを、外部ネットワークとの IP リーチャビリティを遮断した独立性を確保するため表 3-2 に示すとおり、「LGWAN 公開セグメント」、「外部ネットワーク公開セグメント」、「ゲートウェイセグメント」及び「運用管理セグメント」の 4 つのセグメントをファイアウォール等により分割して実装する必要がある。

なお、外部ネットワークが存在しない場合は、「外部ネットワーク公開セグメント」を除く 3 つのセグメントより構築実装する。

表 3-2　LGWAN-ASP に係る各セグメントの説明

項番	セグメント名	説明
1	LGWAN 公開セグメント	LGWAN 側へ公開する（地方公共団体が直接アクセスする）Web フロントサーバ等を設置する。
2	外部ネットワーク公開セグメント	LGWAN 以外の外部ネットワークへ公開する Web フロントサーバ等を設置する。
3	ゲートウェイセグメント	「LGWAN 公開セグメント」と「外部ネットワーク公開セグメント」間でデータ連携を行うためのサーバを設置する。
4	運用管理セグメント	「LGWAN 公開セグメント」、「外部ネットワーク公開セグメント」及び「ゲートウェイセグメント」に設置された各種機器を管理するサーバを設置する。

仮想化した場合、複数のセグメントのサーバを 1 つのサーバ上に統合可能であるが、ハイパーバイザーのセキュリティホール等によりサーバ自体が攻撃を受ける危険性がある。この様な場合を考慮し、セグメントごとにサーバを準備する必要がある（図 3-17）。

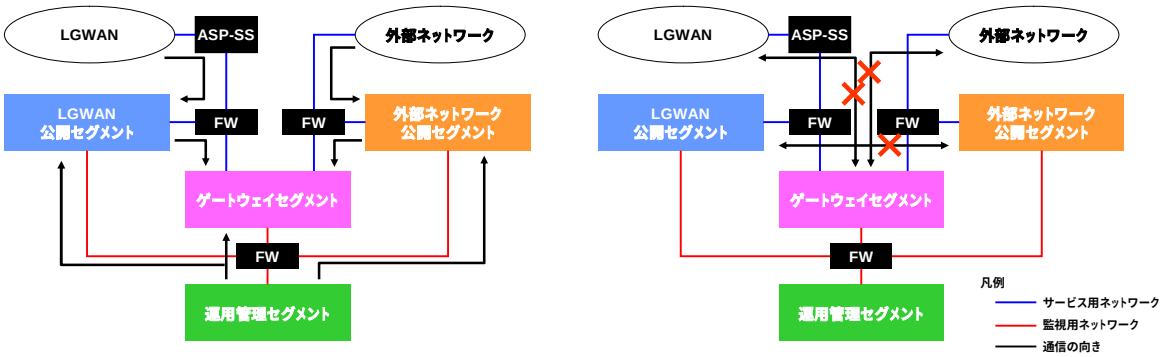


図 3-17　LGWAN-ASP 構築時のネットワーク基本構成

（a）プロトコルの制約

LGWAN 上で利用できるプロトコルは「LGWAN-ASP 接続約款」及び「LGWAN-ASP 接続技術仕様」に定められているため、HTTP 又は HTTPS で通信可能な業務のみ地方公共団体クラウドで実装可能である。

ただし、LGWAN-ASP と地方公共団体間においては、LGWAN 運営協議会の承認により、トンネリング通信を行うことができる。トンネリング通信を行うことで、上記プロトコル以外の業務も統合可能となるが、都道府県域 DC の内部ネットワークと地方公共団体側の庁内ネットワークを意識してネットワーク設計を行う必要がある。

（b）WAN の制約

各地方公共団体内では、比較的広帯域（Ethernet 接続等）なネットワークを介し業務アクセスを行っているが、都道府県域 DC へ業務統合を行った場合、WAN 経由でアクセスすることになる。WAN 経由のアクセスの場合、都道府県 WAN 及び県域アクセス回線を含めた LGWAN 全体の通信速度、仮想サーバの複数稼動による物理サーバへのアクセス集中等がボトルネックとなり、業務にストレスが生じる場合がある。都道府県域 DC へ業務集約を行う場合は、LGWAN 全体の通信速度を考慮する必要がある。

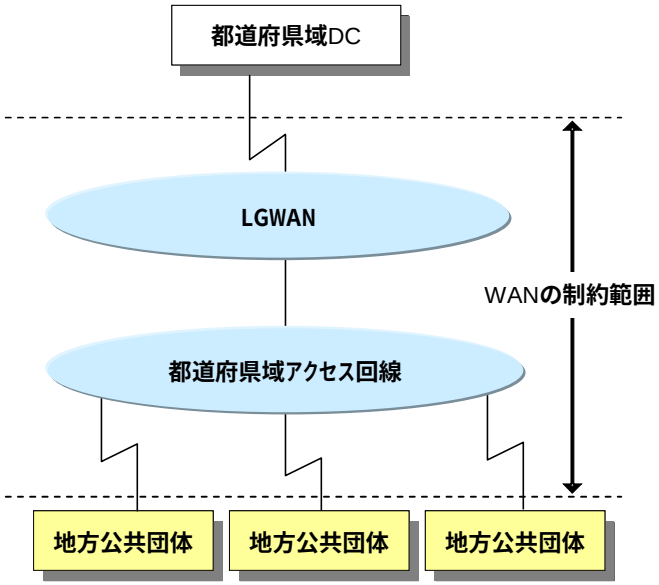


図 3-18　WAN の制約範囲

（c）信頼性・可用性

仮想化を行うと 1 台のハードウェア上で複数地方公共団体の複数業務システムを稼動させることができる。しかし、物理サーバのハードウェア障害が起きた場合、複数業務が停止し多大な被害をこうむることになる。そのため、ハードディスク、NIC 及び電源等の冗長化対策を行い、耐障害性を持たせる必要がある。また、業務毎のクラスタ構成などの検討も推奨する。

3.1.2.2 要件一覧

自治体クラウドコンピューティングの要件を表 3-3 に示す。

表 3-3　自治体クラウドコンピューティングの要件一覧

項番	要件	内容
1	仮想化機能	サーバの仮想化、I/O の仮想化により、サーバ上に複数の環境を提供する機能。
2	セキュリティ	仮想統合することにより、新たに発生するセキュリティリスクを軽減するための対策と要件。

3.1.2.3 機能

（1）仮想化機能

仮想化を行うことで、必要な時に容易にサーバを作成することができるようになる。また、ハードウェア要件により最新機器で動作できないシステム資産も仮想化により延命させることが可能となる。ただし、仮想化できる旧資産の OS が限られる場合がある。

仮想化の特徴は、複数の資源を 1 つに見せることや、1 つの資源を複数の資源に見せること等、下記（A）、（B）、（C）、（D）が考えられる。

サーバの仮想化とは図 3-19 に示すとおり、1 台の物理コンピュータを複数台の仮想的なコンピュータに分割し、それぞれに別の OS やアプリケーションソフトを動作させる技術のことを指す。I/O の仮想化とは 1 台の物理コンピュータに接続されたネットワーク、物理 SCSI 及び Fiber Channel を各仮想サーバ上から占有しているように見せる技術のことを指す。したがって、サーバの仮想化を行うに当たり I/O の仮想化は必須となる。

仮想化技術	ソフトウェア・パーティショニング		ハードウェア・パーティショニング
	ハイパーバイザー型	論理パーティション型	
概要	仮想化ソフトを用い、1台の物理サーバ上に業務統合	OSの論理分割機能を用い、1台の物理サーバ上に業務統合	ハードウェアリソースを物理的に分割し、1台の物理サーバ上に業務統合
イメージ			

図 3-19　仮想化のイメージ

（A）CPU の仮想化

CPU 仮想化機構は、主に OS 移植性の向上、ハイパーバイザー実装の単純化を目的としている。CPU 仮想化機構の実装には、Intel の VT-x、VT-i 及び AMD の AMD-V 等がある。VT-x 及び AMD-V は Intel IA-32 アーキテクチャ向けの仮想化機構であり、VT-i は Intel Itanium アーキテクチャ向けの仮想化機構である。一般的なハイパーバイザーはこれらの仮想化機構を利用し仮想化を行う。

論理パーティション型及びハードウェアパーティショニング型の仮想化については、ハードウェア及び OS に特化した機能になるため本節では定めない。

（B）サーバの仮想化

地方公共団体の業務システムをサーバの仮想化にて統合する場合は、既存の業務システムへの影響を最小限に抑えるため、以下の要件を満たすことを推奨する。

- 複数の異なる OS をサポートすること

  業務システムのクラウド化を促進する場合、その業務システムが動作している OS をサポートすることが必要である。ただし、仮想化製品がサポートしている OS は限定されていることが現状であり、仮想化製品の選定時には留意すること。また、ベンダ固有アーキテクチャにより開発された OS や業務システム等の製品仮想化対応については、別途ベンダ等による検証を行い、対応の可否を検討すること。

- 異なる VM（仮想サーバ）同士は、アクセスを制御する
  都道府県域 DC へ業務統合した場合、複数の VM が同一物理サーバ上で稼動することとなる。VM 同士がアクセスできてしまうと、個人情報等の機密情報の漏えいにつながる恐れがあるため、VM 同士のアクセスを制御する必要がある。

- 物理資源の一元管理ができること
  物理資源を一元的に管理することで、VM に最適なハードウェアリソースの割り当てが可能とし、使用性、効率性を向上させることを推奨する。また、複数業務が同一サーバ上で稼動するため、物理資源の負荷状況把握が困難である。そのため、物理資源の利用状況のモニタリングを行う機能を持つことを推奨する。

- バックアップの取得ができること
  障害時に早急な復旧を行うためバックアップの取得を推奨する。
  バックアップには、VM 自体のバックアップ及びハイパーバイザーのバックアップが存在するので、用途に合わせ、データバックアップサーバ等を構築しバックアップ取得を行うことを推奨する。

- VM 毎のスケジュール運用について
  地方公共団体業務の中には昼間のみ稼動させる業務も少なくない。夜間及び休日はスケジュールにて VM のシャットダウンを行い、サーバ負荷を下げることを推奨する。

- ライセンス体系について
  既存サーバを VM 化する場合において、OS 及びミドルウェアのライセンスが追加で必要となる場合があるので注意すること。

- NTP サーバは仮想化しない
  特定のハイパーバイザー上で業務負荷等により VM の時刻ズレが発生する場合がある。都道府県域 DC 内の機器は LGWAN の時刻に合わせる必要があるため、NTP サーバは仮想化せずに別に設置し、運用する必要がある。

- LGWAN グローバル IP アドレスの申請
  LGWAN グローバル IP アドレスは、都道府県域 DC 内のすべての機器に割り振ることはできないため、プライベート IP アドレスにより構築する必要がある。LGWAN グローバル IP アドレスは、都道府県域 DC に設置する ASP-SS 上で NAT により「LGWAN 公開セグメント」上の公開 VM に割り当てることになる。したがって、「LGWAN-ASP 接続約款」及び「LGWAN-ASP 接続技術仕様」に基づき、公開 VM の数だけ、LGWAN グローバル IP アドレスの申請を行う必要がある。

（C）I/O の仮想化

サーバの仮想化を行うにあたり、セキュリティ・信頼性向上・拡張性を持たせるため、I/O の仮想化を行う必要がある。特に仮想化環境下では、メモリ資源を多量に消費するため、十分なメモリ容量を確保する必要がある。

（a）ネットワークの仮想化

ネットワークの仮想化は、以下の要件を満たすことを推奨する。

- 物理 NIC は共有するため 1Gbps 以上の NIC を持つこと。
  図 3-20 にあるように、複数の VM が同一ハードウェアに統合され NIC を共用することから広帯域の物理 NIC の利用を推奨する。

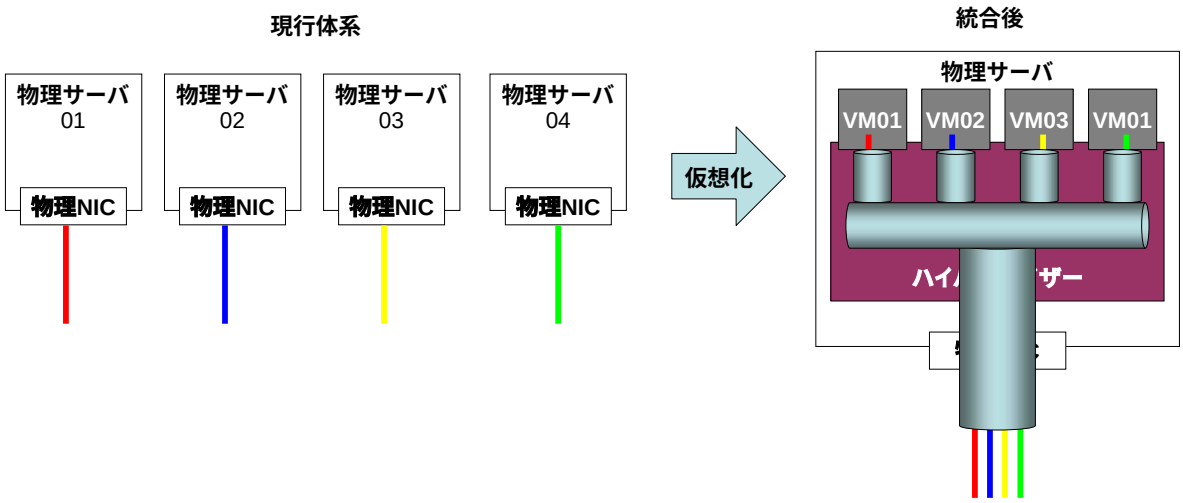


図 3-20　物理サーバへのアクセス集中

- 物理 NIC の二重化ができること
  １つの物理 NIC を複数の VM が利用するため、物理 NIC の障害　により、複数の業務が同時に停止するため、影響が広範囲におよぶことが考えられる。そのため、障害を検知し自動的にインターフェースの引継ぎが可能なバックアップポートの実装を推奨する。

- VM 上で仮想 NIC を複数作成できること
  VM に複数のインターフェースを設ける場合、仮想 NIC を作成す　ることで実現する。そのため、VM 上で仮想 NIC を自由に追加できる機能を持つことを推奨する。また、作成できる仮想 NIC 数に制限がある製品もあるため、業務システムの配置に考慮が必要である。

- ハイパーバイザーに VLAN 機能を有すること
  通常異なるサーバ同士の通信は、ファイアウォールなどによりアクセス制御される必要がある。VM の場合も同様で、同じ物理サーバ上で稼動する VM 同士が自由に通信できる環境は好ましくない。そのためには、仮想 NIC が接続される仮想スイッチが必要となり、VLAN 等によって属するネットワークを制御する必要がある。また、作成できる VLAN 数に制限がある製品もあるため考慮が必要である。

- 各 VM の通信に対し帯域制御ができること
  1 つの VM がネットワーク資源を使い果たしてしまうと、その他の VM 上で動作する地方公共団体業務に遅延などの影響が出るため帯域制御機能が利用できることを推奨する。

- サービス用 NIC と管理用 NIC を物理的に分けること
  サービス用 NIC と管理（運用）用 NIC は物理的に分け、サービス用 NIC 側からハイパーバイザーへのアクセスを低減させることを推奨する。

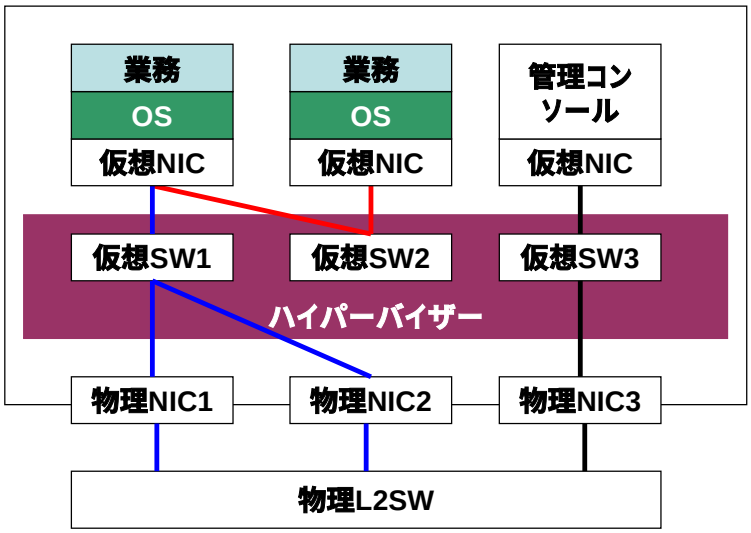


図 3-21　ネットワークの仮想化イメージ

（D）その他の仮想化

上記に加え、製品導入時において考慮すべき点を以下に記述する。

（a）コンソールの仮想化

VM のコンソール機能も仮想化する必要がある。コンソールには、シリアル回線で接続するタイプのシリアルコンソールと、キーボード、ビデオ、マウスを使うグラフィックコンソールがある。コンソールの仮想化により、特別なハードウェアがなくても、VM のコンソールに接続できることを推奨する。

（b）ファームウェアの仮想化

VM 起動時、VM ごとにハードウェアデバイスの起動順序が異なる場合がある。VM ごとにファームウェアの仮想化を行うことで、各々のファームウェアの設定できることを推奨する。

（c）ストレージの仮想化

ストレージ利用率を向上させ、全体的な効率を大幅に引き上げて、コスト削減が可能であるストレージ製品を推奨する。また、ストレージ製品は、仮想化構成に対応できる製品を選択する必要がある。SCSI や Fiber Channel の仮想化により実現される、以下のストレージの仮想化要件を満たすことを推奨する。

- VM のファイルを格納でき、複数の物理サーバからアクセスできること。
- 業務情報の格納されたディスクはアクセス制限を設け、許可された VM 以外からのアクセスを禁止すること。
- VM に公開する仮想ボリュームにアクセス制限ができること。
- 複数の VM からアクセスできること。
- RAID 構成等について考慮すること。
- スナップショット等の容易なバックアップを行うことを推奨する。

次にストレージ仮想化装置等を利用する場合の有効な技術（複数のストレージシステムの統合、仮想プロビジョニング及び ILM）を記述する。

- **複数のストレージシステムの統合**

複数のストレージシステムをサーバからあたかも 1 つのストレージシステムに見せるためのもので、既存のストレージ内にある空き領域を有効利用する場合等に適した技術である。

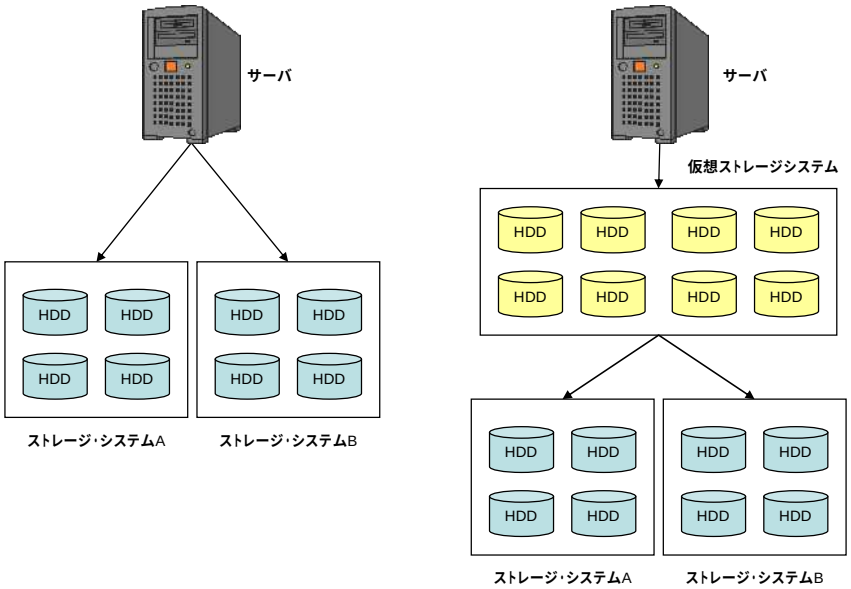


図 3-22　ストレージシステム筐体の境界をまたいだ統合

- **仮想プロビジョニング（シン・プロビジョニング）**

「仮想プロビジョニング」とは「シン・プロビジョニング」とも呼ばれ、ボリュームの容量を仮想化することで複雑な容量設計を不要にし、少ないディスクで運用を開始することができる技術である。サーバは仮想ボリュームで設定された容量を認識するが、物理ディスクの割り当ては、設定容量より少なくても運用可能となる。運用開始後、物理容量が不足した場合、仮想ボリュームに対し新たにディスクの追加を行うことで導入時のコスト削減及び資源の有効活用に貢献できる。

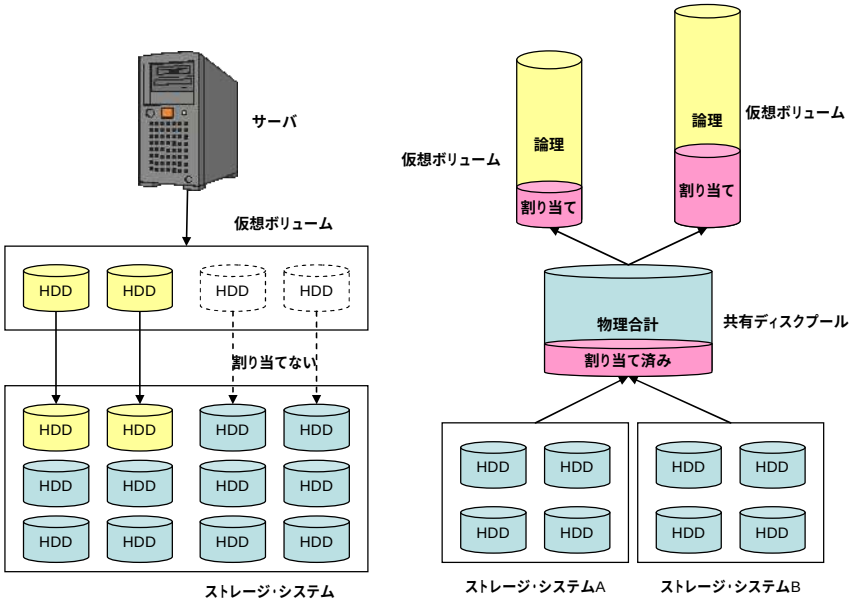


図 3-23　仮想プロビジョニング

• ILM（情報ライフサイクル管理）

「ILM：Information Lifecycle Management=情報ライフサイクル管理」とは、効率的な情報活用を行うため、データの重要度や利用頻度などの変化に応じて、それを格納するのに適したストレージへデータを適宜、移動することである。参照頻度が多い情報は高速ストレージ内に配置し、参照頻度が少ない情報は低速ストレージ内に配置するといった階層型ストレージを実現する。

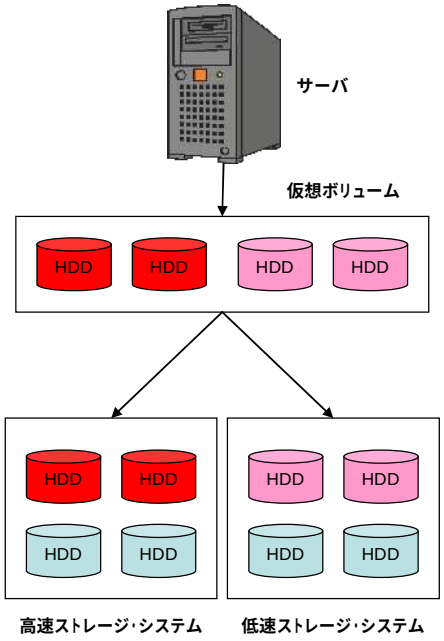


図 3-24　ILM

（2）セキュリティ

仮想化を行わない場合は、OS 等のセキュリティホールを攻撃されても攻撃されたサーバに影響が局所化されていたが、仮想化を行った場合は、他の仮想化された VM への影響を考慮することが重要になる。物理サーバと VM の中間で稼動するハイパーバイザーが攻撃を受けると、この上で動作する VM すべてに影響することが考えられる。そのため、地方公共団体で利用している業務システムを、都道府県域 DC の VM 上に移行するためには、セキュリティについて十分な配慮が必要となる。

併せて、自治体クラウドは LGWAN 上でサービスが展開されるため、「3.1.2.1（2）（A）制約事項」、LGWAN-ASP 接続約款及び LGWAN-ASP 接続仕様に準拠する必要がある。

（A）システム管理に必要となるセキュリティ

自治体クラウドコンピューティングを管理・運用する上で、ハイパーバイザーや VM に最低限必要となるセキュリティ対策を表 3-4 に示す。

表 3-4　システム管理に必要なセキュリティ対策

種類	内容
ユーザ管理とアクセス制御	ハイパーバイザー上で最低限以下のユーザを作成し権限を分割する必要がある。 ・ システム管理者：VM の追加・削除等すべての権限を持つ特権ユーザ ・ VM 管理者：VM の起動と停止など運用管理を行うユーザ。VM ごとにユーザを作成し、他の VM の操作を行えないよう制限する。 上記の他に都道府県域 DC 及び地方公共団体ユーザの運用に必要な権限を割り当てたユーザを作成し、定期的なパスワードの変更など適切なユーザ管理を行う必要がある。
監査ログ	VM 管理者等、ハイパーバイザーを管理するユーザの操作を記録し、定期的な監査を行うことで、不正操作の検知等を実施する。

都道府県域 DC に多数の物理サーバと VM を設置した場合、管理者のユーザ管理を行うための運用負荷が増大するため、ユーザ管理の統合機能を持った製品と連携できるハイパーバイザー製品を導入することを推奨する。

（B）VM のセキュリティ

物理サーバ上で複数の VM が動作するため、VM 間で問題を波及させないため、以下の対策を行うことを推奨する。

- VM ごとに VM 管理者を設定し、他の VM の操作を制限する。
- VM 間のアクセス制御を行い、他の VM のリソースや共用リソースへのアクセス制限を行う。なお、ハイパーバイザーのアクセス制御機能を用いてアクセス制御を行うことを推奨する。
- ハイパーバイザーは定期的なセキュリティパッチを適用し、各 VM 上で動作する OS やアプリケーションの脆弱性に対する攻撃を防ぐため、アンチウイルスソフト等のセキュリティ関連ソフトウェアを VM ごとに導入する。また、LGWAN-ASP 等を利用し、Windows Update やウィルスパターンアップデートを行うことも考慮する。
- テスト用の VM を作成し、本番用 VM へ適用する前に、セキュリティパッチ等のテストを行うことを推奨する。

（C）ネットワークのセキュリティ

都道府県域 DC 内のセキュリティを確保するほか、物理サーバ上の VM 間におけるセキュリティの確保が必要となる。

（a）物理サーバ間通信のセキュリティ

「3.1.2.1（2）（A）制約事項」で記述した LGWAN-ASP での各セグメント分離に合わせて物理サーバを配置し、物理サーバ間の通信をファイアウォールにより制御することで、LGWAN と外部ネットワークのアクセス制御を行う必要がある。

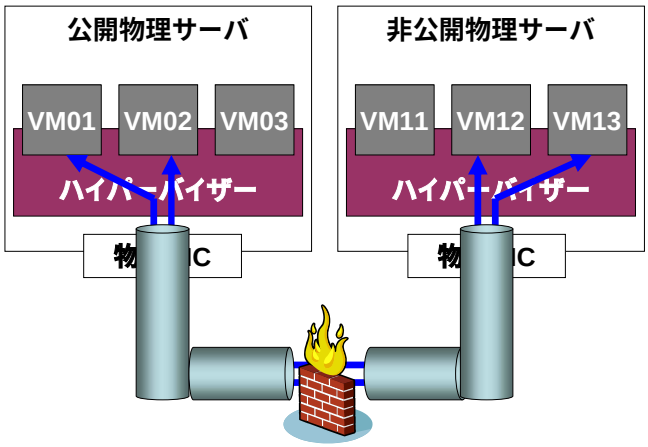


図 3-25　物理サーバ間通信のファイアウォール構成例

（b）VM 間通信のセキュリティ

従来の物理ネットワークであれば、ファイアウォール等でセキュリティ対策を可能としていたが、物理サーバ上の VM 間通信はハイパーバイザー上で行われるため、物理ネットワーク上に配置したこれらの機器による不正アクセスの検知が困難になる。したがって、物理サーバ内で異なる VM 間の通信に制限を行う場合は、図 3-26 に示すような物理ネットワーク上に設置したファイアウォールを経由した通信か、VM 上に構築したファイアウォールを経由した通信を行う必要がある。

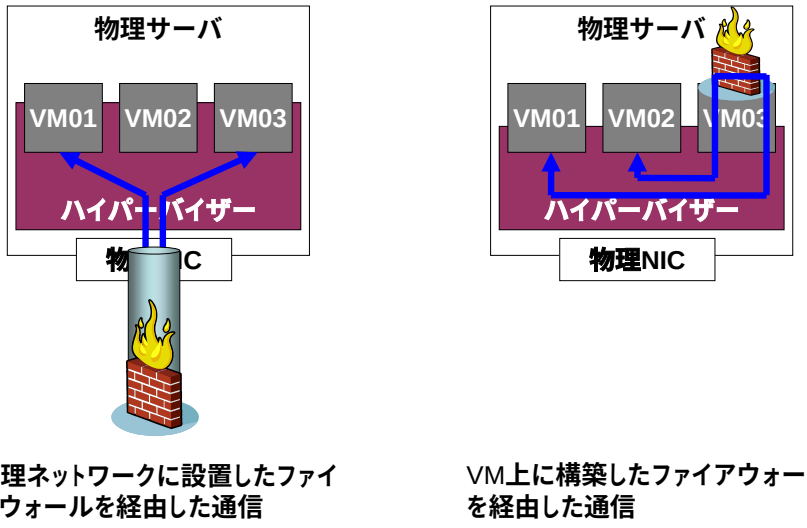


図 3-26　VM 間通信のファイアウォール構成例

（D）ログの運用

ハイパーバイザーのログについては、保存方法、保存期間などの運用規約を定め、セキュリティ事故や監査時に適切な対処ができるよう管理する必要がある。

3.2 オプション要件

3.2.1 バックアップ連携

3.2.1.1 概要

（1）目的

災害時や回線障害時の際にも継続が必要な業務については、地方公共団体庁内のサーバを用いて業務運用を行う必要がある。

そのため、データを都道府県域 DC あるいは ASP・SaaS 事業者から必要なデータを地方公共団体庁内にバックアップ連携を実施することにより、地方公共団体にて応急業務や縮退運転を行いながら、地方公共団体業務を継続するものである。

（2）適用範囲

バックアップ連携(オプション要件)の適用範囲を図 3-27 に示す。

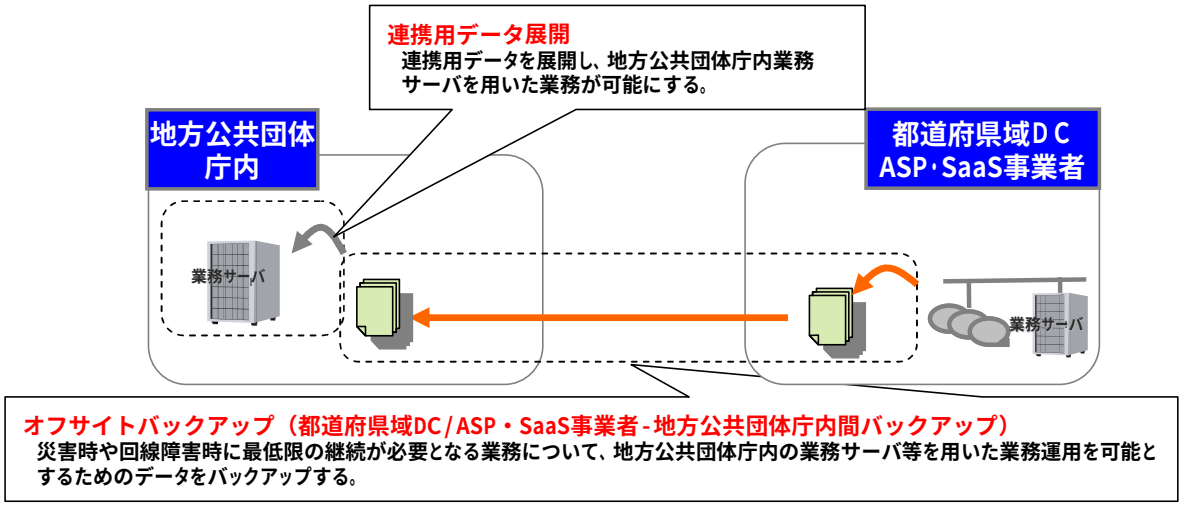


図 3-27　バックアップ連携（オプション要件）の適用範囲

3.2.1.2 要件一覧

バックアップ連携（オプション要件）の要件を表 3-5 に示す。

表 3-5　バックアップ連携（オプション要件）の要件一覧

項番	要件	内容
1	オフサイトバックアップ(都道府県域 DC－地方公共団体庁内間、ASP・SaaS 事業者－地方公共団体庁内間バックアップ)	オフサイトバックアップにおける、他都道府県域 DC、ASP・SaaS 事業者から地方公共団体庁内へのデータ連携するための事前処理(連携用データ作成プロセス)。
		オフサイトバックアップにおける、他都道府県域 DC、ASP・SaaS 事業者から地方公共団体庁内へのデータ連携するための処理(連携用データ作成プロセス)。
2	連携用データ展開	連携用データ展開に関する機能 ・ 都道府県域 DC 又は ASP・SaaS 事業者から受け取った連携用データを地方公共団体庁内に設置された災害時用サーバに展開する処理(データ復元プロセス)。
3	セキュリティ	セキュリティに関する機能 ・ 通信時にセキュリティを確保すること。 ・ 適切にデータを管理すること。

3.2.1.3 機能

（1）オフサイトバックアップ・リストア

（A）連携用データ作成に関する機能

オフサイトバックアップにおける、都道府県域 DC、ASP・SaaS 事業者から地方公共団体庁内へのデータ連携するための事前処理(連携用データ作成プロセス)。

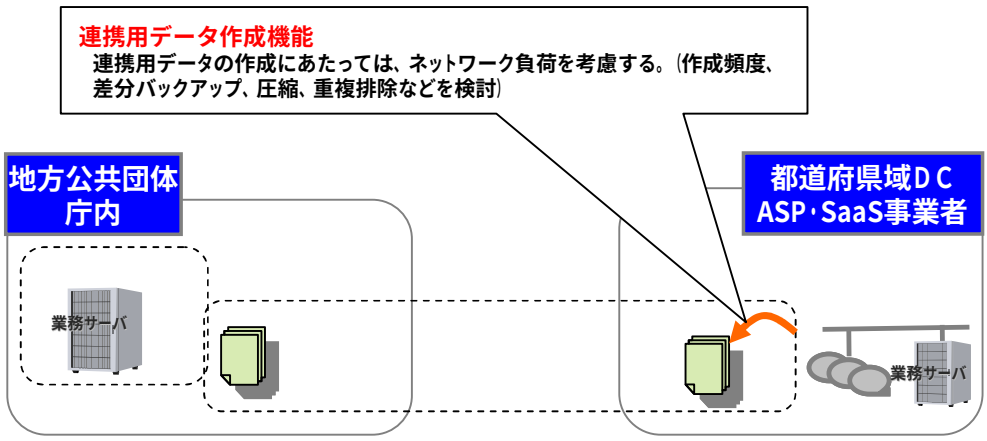


図 3-28　連携用データの作成処理

都道府県域 DC－地方公共団体庁内間、ASP・SaaS 事業者－地方公共団体庁内間オフサイトバックアップ連携では、ネットワーク障害などにより、都道府県域 DC、ASP・SaaS 事業者との回線が切断された場合に備え、地方公共団体庁内で最低限の業務を継続するための最小限のデータを連携する。

上記処理において、必須な機能は以下となる。

（a）最小限のデータを作成するための機能

（ア） 地方公共団体庁内で業務継続を行うために必要最小限のデータ取得できること。

（イ） 複数の地方公共団体のデータを個別に矛盾無くディスクに保存できること。

（ウ） データ量を低減させるための、差分バックアップや、増分バックアップなどを取得できること。

（エ） 複数データ間に存在する重複部分の排除、データの圧縮等を行うこと。

以降の機能は都道府県域 DC 間のオフサイトバックアップと同等である。

（b）データの一元管理を行うための機能

（ア） 連携用データの作成日時、保存先などの管理ができること。

（c）データの世代管理を行うための機能

（ア） 保存世代は１世代以上で、必要に応じ長期間保存が可能なこと。

（イ） 保存世代から外れたデータは削除し、領域の再利用が可能なこと。

（d）効率的に連携を行う機能（推奨）

（ア） 処理を自動で運転できること。

（イ） システムの運転状態をジョブ管理ソフトなどに通報し、連係動作が可能であること。

（ウ） 必要に応じて、バックアップタイミングを「定時起動」、「任意起動」など自由に設定が行えること。

（e）拡張性を高めるための機能（推奨）

（ア） バックアップの運用に影響を与えることなく、容量や性能の拡張ができること。

（B）データ連携に関する機能

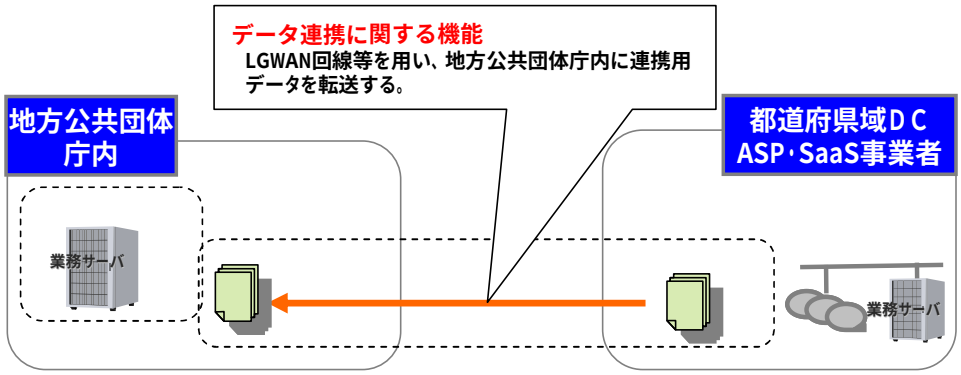


図 3-29　データ連携に関する処理

（a）データ転送時の効率化のための機能（推奨）

（ア） LGWAN のネットワーク負荷低減のため、転送するデータの重複部分を自動的に排除し最小限にすること。

（b）効率的に連携を行う機能（推奨）

システムの運転状態をジョブ管理ソフトなどに通報し状態に応じた連係動作が可能であること。

（ア） 同時に複数連携が可能できること。

（イ） 必要に応じて連携処理の頻度を変更・設定できること。

（ウ） ネットワーク障害発生時、連携処理動作を変更・設定できること。

（2）連携用データ展開

連携用データを地方公共団体庁内に設置された災害時用サーバに展開し、業務を実施可能とする。この機能については、地方公共団体庁内の業務アプリケーションに関連する機能であり、ここでは詳細な方式については規定しない。

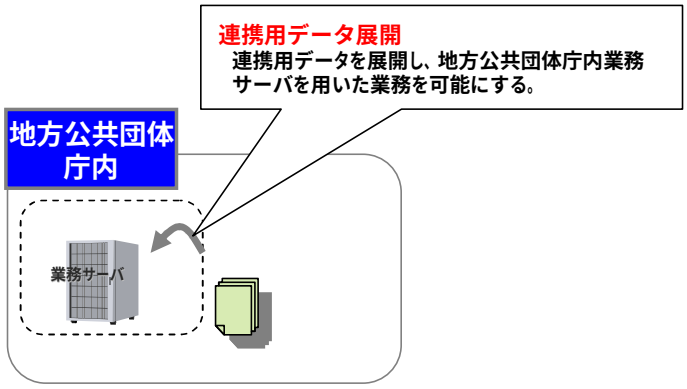


図 3-30　連携用データの展開処理

（3）セキュリティに関する機能

バックアップデータには、個人情報など重要な情報が含まれているため、その送信及び管理には十分なセキュリティが求められる。このデータを他都道府県 DC、ASP・SaaS 事業者と連携するため、その管理はセキュリティを強く意識した方法を採る必要がある。

また、データ連携するすべてのサイトにおいては、システム運用に関して情報セキュリティマネジメント体系を事前に整備することを強く推奨する。

上記処理において、必要とされる機能は以下となる。

（a）通信時にセキュリティを確保する機能

（ア） 事前に情報を登録することで、特定のアクセス先からのみアクセスできる機能。

（イ） 秘匿機能
LGWAN 転送中は IPSec などで通信内容を秘匿すること。

（b）データを管理する機能

（ア） バックアップデータが蓄積されるサーバ（ストレージ）は、十分なセキュリティを考慮した運用がなされること（各地方公共団体のセキュリティポリシーにしたがって運用すること。）。

3.2.2 認証連携

3.2.2.1 概要

（1）目的

自治体クラウドでは、分散配置されたデータセンターに各地方公共団体の業務アプリケーションを効率良く集約し、ユーザがシームレスに利用することができる環境の整備を進めている。一方で、各地方公共団体ユーザは日常業務の中で管理体系の異なる様々な業務アプリケーションを使うことが求められるが、それらのアカウントの ID・パスワード等がシステムごとに独立している場合、適切に使い分け安全管理を行うことは非常に煩雑であり、業務効率にも大きな影響を与える。また、ユーザがパスワードをメモに残す等、安全管理上の問題につながる可能性が懸念される。

そこで、このような問題を解決する機能の 1 つに、異なる業務アプリケーション間でユーザの認証情報を連携・引き継ぎさせるシングルサインオンが挙げられる。シングルサインオンを導入することにより個々のユーザの利便性・生産性が向上するだけでなく、複数の業務アプリケーションごとに独立した認証クレデンシャルを管理する運用コストやセキュリティリスクを軽減することが可能になる（図 3-31）。

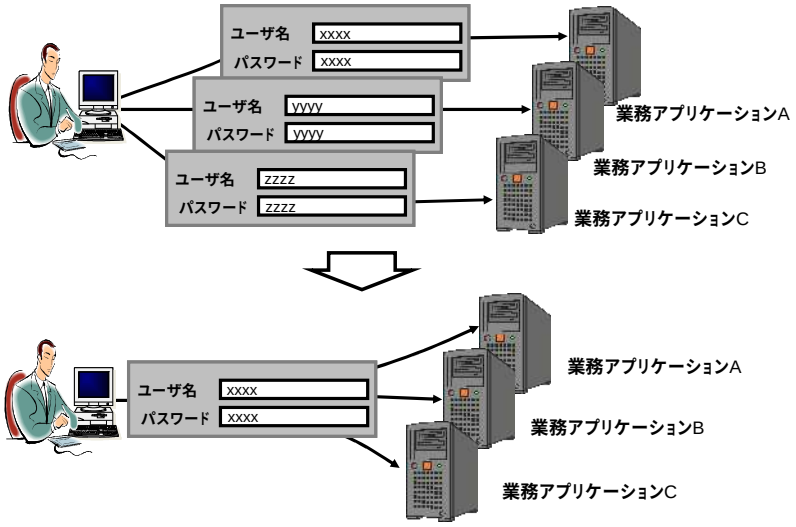


図 3-31　異なる業務アプリケーション間でのシングルサインオンの概念

認証連携機能では、異なる業務アプリケーション間の認証を連携動作させるシングルサインオン機能を実現し、各地方公共団体ユーザに対して簡単かつ安全に自治体クラウド内の複数の業務アプリケーションへログインできる環境を提供する。

（2）適用範囲

認証連携の適用範囲を図 3-32 に示す。

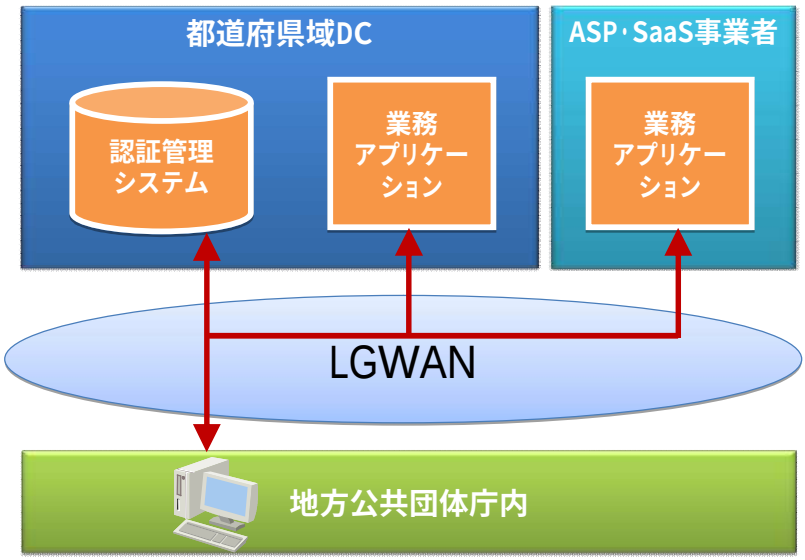


図 3-32　認証連携の適用範囲

本仕様が対象とする範囲は図 3-32 に示すとおり、ユーザ ID やその認証を管理する認証管理システムと、地方公共団体庁内のユーザ端末・業務アプリケーション間で認証を引き継ぐインターフェース部分となる。

なお、複数の業務アプリケーション間でシングルサインオンを導入する際、セキュリティリスクも考慮する必要がある。
例えば、認証のためのパスワードが漏えいしてしまった場合の影響範囲はシングルサインオンが適用されるすべてのシステムに及ぶため、認証方式をパスワードのみで運用するのではなく、例えば IC カードや指紋等の生体認証、ハードウェアトークン等と組み合わせて利用することが望ましい。

また、要求されるセキュリティレベルの異なる業務アプリケーション同士でシングルサインオンを安易に組み込んでしまうと、全体のセキュリティレベルが低い方に引きずられてしまうという懸念点がある。
例えば、個人情報を扱うようなアプリケーションでは厳重な認証手段が要求されるが、一方で秘密情報を扱わないようなアプリケーションでは比較的平易なパスワード認証で運用していることも考えられる。このようなアプリケーション同士をシングルサインオンで結んだ場合、機密レベルの低いアプリケーションを使用しているユーザが認証パスワードの管理を緩慢に行うことも考えられ、その結果、すべてのアプリケーションに影響を及ぼすようなセキュリティリスクが高まる。
上記を踏まえ、シングルサインオンの導入に当たっては以下の点に留意する必要がある。

- 対象となるすべての業務アプリケーションのセキュリティポリシーが同等あるか、シングルサインオンの導入後は同等のセキュリティポリシーで運用することが可能であること。
- すべての業務アプリケーションに統一的にシングルサインオンを導入するのではなく、業務アプリケーションのセキュリティポリシーに応じて導入の可否を検討する。

なお、セキュリティポリシーは業務の内容や重要度、あるいはアプリケーションの管理主体（地方公共団体のデータセンターか ASP か等）に依存して決まるものであり、ここで定義はしない。

3.2.2.2 要件一覧

認証連携の要件を表 3-6 に示す。

表 3-6　認証連携の要件一覧

項番	要件	内容
1	ユーザ認証	業務アプリケーションを使用するに当たって必要となる、ユーザの本人性認証及びアプリケーションの使用許可。
2	通信のセキュリティ	認証連携にかかわるすべてのトランザクションの安全性の担保。
3	シングルサインオン	1 回の認証プロセスで、異なる複数の業務アプリケーションが利用できるようになる機能。

3.2.2.3 機能

本節では 3.2.2.2 で挙げた要件を実現するために考えられる機能を提示する。

（1）ユーザ認証

ユーザ認証は、業務アプリケーションを利用するに当たって、ユーザの本人性認証とアプリケーションの使用許可を受けるものであり、以下の要件を満たすことを推奨する。

- 認証連携を行う際、ユーザは ID とその認証を管理するシステム（認証管理システム）から適切に本人性を認証され、該当する業務アプリケーションの使用許可を受けること。
- ユーザ認証の方式については特定の方式に制限せず、各地方公共団体のポリシーに適するものを採用する。
- 基本的な認証方式として ID・パスワードベースの認証（HTTP Basic 認証や Digest 認証、フォーム認証等、方式は問わない）をサポートしていること。
- より高いセキュリティレベルを確保する場合は、ID・パスワードベースの認証だけに頼らず、IC カード、指紋等の生体認証、ハードウェアトークン等の導入、又はそれらを組み合わせた二要素認証が望ましい。

（2）通信のセキュリティ

認証連携を安全に行うためにはユーザ認証だけでなく、通信の秘匿性・完全性が確保されている必要があり、以下の要件を満たすことを推奨する。

- 認証連携のトランザクションについては HTTPS を使用する。
- 認証連携のためのセキュリティ情報がクライアント端末のブラウザを経由する場合、その情報の正当性を保証するための署名相当のものがシステム側によって付与されていること。

なお、LGWAN-ASP として通信に求められるセキュリティについては、「LGWAN-ASP 契約約款」及び「LGWAN-ASP 接続技術仕様」に準拠するものとする。

（3）シングルサインオン

クライアント端末のブラウザを利用して各種の業務アプリケーションにシングルサインオンを行う方式と特徴を提示する。ただし、ベンダの独自の方式(注)についての記載は対象外とする。

なお、導入に当たっては、方式の特徴と現状のシステム構成を勘案して合理的な方式を選択することが望ましい。

（注）
地方公共団体庁内の ID 管理基盤として Active Directory（Microsoft 社）を導入してシングルサインオンを実現しているケースも多いが、プロトコル制限等により LGWAN での利用は困難であるため、本節では記載対象外とした。

（A）SAML を用いたシングルサインオン

SAML は Cookie を用いたシングルサインオンにおけるセキュリティ上の懸念やドメインの制限を克服するため、標準化団体 OASIS によって策定されたオープンなシングルサインオン方式であり、以下の要件を満たす必要がある。

- 認証管理システムとして IdP（アイデンティティプロバイダ）が定義され、また、各業務アプリケーションが SP（サービスプロバイダ：サービスを提供するシステム）として IdP と信頼関係を構築し、連携すること。
- IdP で払い出される認証情報はアサーションという形式でブラウザの接続先 URL にクエリとして埋め込まれて各業務アプリケーションに引き渡され、シングルサインオンが実現されること。

この方式の概要を以下の図に示す。

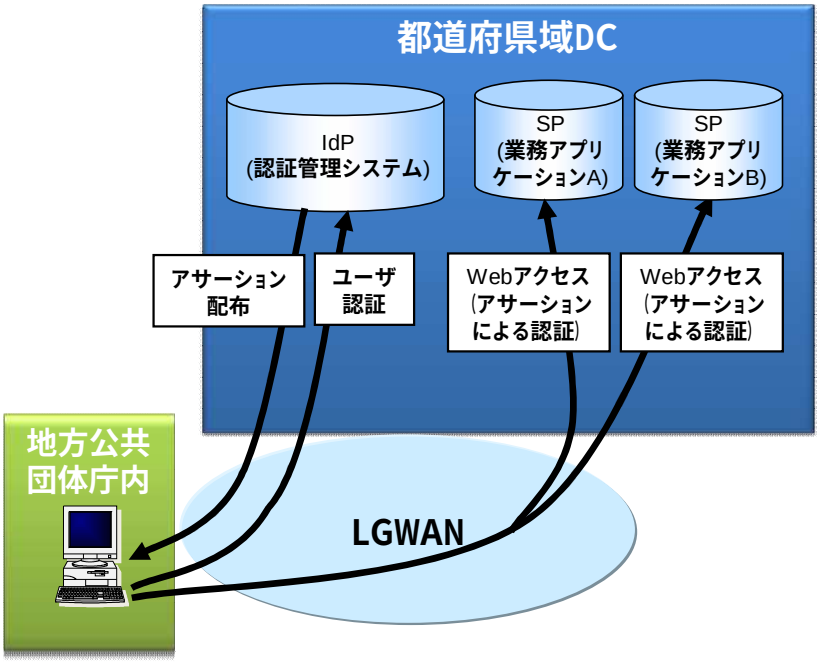


図 3-33　SAML を用いたシングルサインオン

（B）Open ID を用いたシングルサインオン

SAML と並んで注目されるシングルサインオン方式に Open ID がある。OpenID の導入に当たっては、SAML と同様に、以下の要件を満たす必要がある。

- 業務アプリケーションへのログイン時に IdP にアクセスし、認証情報を払い受けることができること。 提供するシステム）として IdP と信頼関
- IdP から払い出された認証情報を利用し、業務アプリケーションサーバへログインできること。

なお、OpenID の特徴は SAML に近いが、SAML がユーザ ID そのものを隠蔽する仮名 ID と呼ばれる仕組みを提供するのに対して Open ID はサーバ間に確立した信頼関係を前提としないオープンなフレームワークであり、グローバルユニークな URL をユーザ ID として利用することから ID のプライバシーに関する仕組みについては劣っている。

（C）リバースプロキシを用いたシングルサインオン

リバースプロキシ方式は、すべての業務アプリケーションサーバへのアクセスの経路上にリバースプロキシが介在してユーザ認証・ポリシー制御を行う方式であり、以下の要件を満たす必要がある。

- 業務アプリケーションへのログインに際してリバースプロキシへアクセスし、ユーザ認証が行われること。
- ユーザ認証をもとにした、リバースプロキシからのリクエストにより業務アプリケーションへログインができること。

この方式の概要を以下の図に示す。

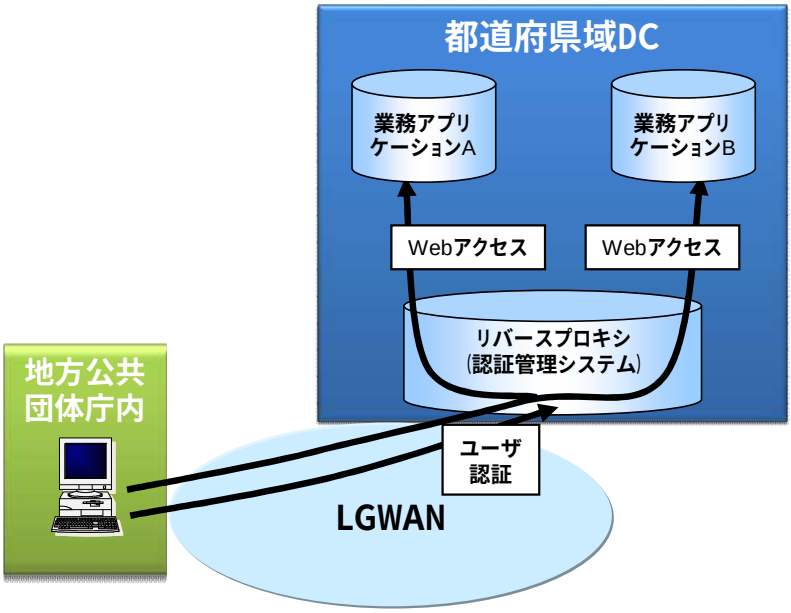


図 3-34 リバースプロキシを用いたシングルサインオン

なお、この方式の特徴は以下のとおりである。

- 個々の業務アプリケーションサーバに特別なプラグインを導入する必要がない。
- クライアント端末からのアクセスが必ずリバースプロキシを通らなければならないため、ネットワーク構成に大きな制限をもたらす。
- 特に地方公共団体をまたぐような異なるドメイン間でのシングルサインオンやユーザ数が大規模になる場合には、この制限が将来的に問題となる可能性がある等の特徴がある。

（D）Cookie を用いたシングルサインオン

OS 依存性を排除した手法としてシングルサインオン Web ブラウザに認証情報としての Cookie を持たせる手法があり、以下の要件を満たす必要がある。る。

- 業務アプリケーションサーバにアクセスしようとするクライアント端末は認証管理システムに接続し、ユーザ認証が実施できること。
- 認証管理システムはブラウザに Cookie を発行し、業務アプリケーションサーバへのリダイレクトを行うこと。
- 業務アプリケーションサーバは Cookie の情報からユーザが正当であることを判断し、以後は認証のプロセスを踏むことなく業務アプリケーションを利用させること。

この方式の概要を以下の図に示す。

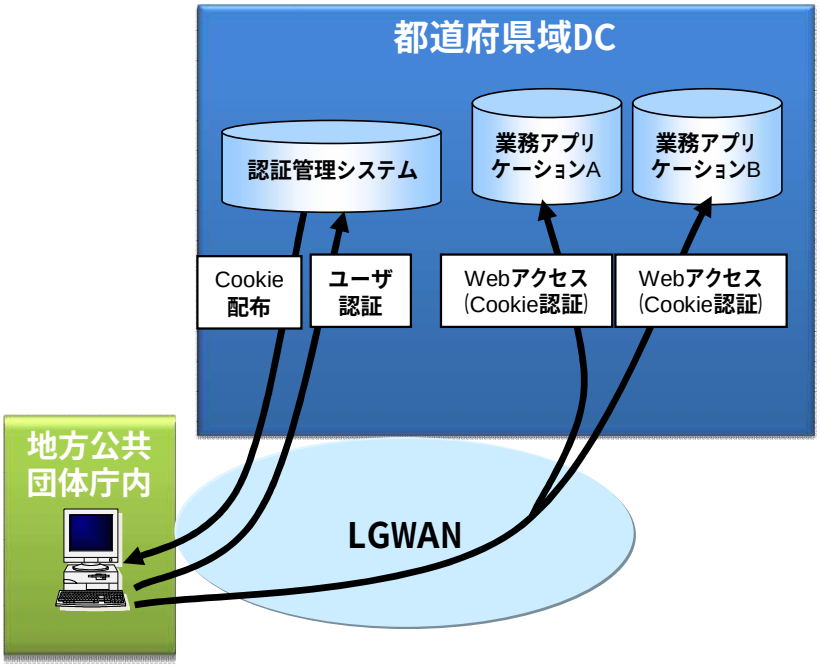


図 3-35　Cookie を用いたシングルサインオン

以上のシングルサインオン方式にはそれぞれ以下のような特長・考慮が必要な点がある。

表 3-7　シングルサインオン方式の比較

#	方式	特長	考慮が必要な点
(A)	SAML	・ OS、ベンダに依存しない ・ ファイアウォールとの親和性が高い ・ 地方公共団体間での連携を想定した構築が可能	・ 普及、実装が成長段階である。 ・ 業務アプリケーションが対応している必要がある。
(B)	Open ID	・ OS、ベンダに依存しない ・ ファイアウォールとの親和性が高い ・ 地方公共団体間での連携を想定した構築が可能	・ 普及、実装が成長段階である。 ・ 業務アプリケーションが対応している必要がある。 ・ SAML と比較すると、ID のプライバシーに関する仕組みが不足している。
(C)	リバースプロキシ	・ サーバにプラグインを導入する必要が無い	・ リバースプロキシが通信のボトルネックとなる。 ・ ネットワーク構成に制限がある。 ・ 地方公共団体間で連携する場合、管理上の懸念がある。 ・ 大規模なユーザ数に対応するのが困難。
(D)	Cookie	・ OS、ベンダに依存しない ・ ファイアウォールとの親和性が高い	・ Cookie そのものにセキュリティリスクがある。 ・ Cookie のドメイン制限により、地方公共団体間で連携ができない恐れがある。 ・ 業務アプリケーションが対応している必要がある。

このように、シングルサインオンを実現する方式には様々なバリエーションがあり、各地方公共団体の現状のシステム構成やセキュリティポリシーを踏まえて方式毎のメリット・デメリットを検討し、実装を進める必要がある。一方で将来的に地方公共団体間の認証連携を実現することを考慮する場合、方式のオープン性、セキュリティの仕組み等から SAML を用いたシングルサインオンへの移行を進めていくことが望ましい。

留意点

上述のシングルサインオン方式の他、複数の業務アプリケーション同士をアプリケーションレイヤで統合することで、個別に実装することも可能である。

この場合、以下の点を留意する必要がある。

- すべてのアプリケーションを統合実装するため手間がかかり、拡張性も低い。
- アクセスが集中した場合にアプリケーションサーバがボトルネックになる。

3.2.3 業務データ連携

3.2.3.1 概要

（1）目的

地方公共団体の業務は、電子申請、電子入札といったフロントオフィス業務や、基幹系業務である住民基本台帳、住民税、介護保険や、内部管理系業務である財務会計、人事給与、文書管理といったバックオフィス業務があり、これらの個々の業務で所管する住民等の基本情報や資格情報等のデータが業務間で連携され運用されている。

自治体クラウド環境においては、これらの業務を実施するために利用する業務アプリケーション（業務 AP）については、一部の業務について、都道府県域 DC 上に構築する。また、一部の業務は ASP・SaaS 事業者が提供する業務 AP を使用する。このように業務 AP がネットワークをまたがった地方公共団体外に配置されるため、業務 AP 間のデータ連携を行う際には、ネットワークを介してサイトをまたがることへの配慮が必要となる。また、地方公共団体外に接続されるネットワークは、地方公共団体間のセキュアなネットワークである LGWAN の利用が求められる（図 3-36 参照）。

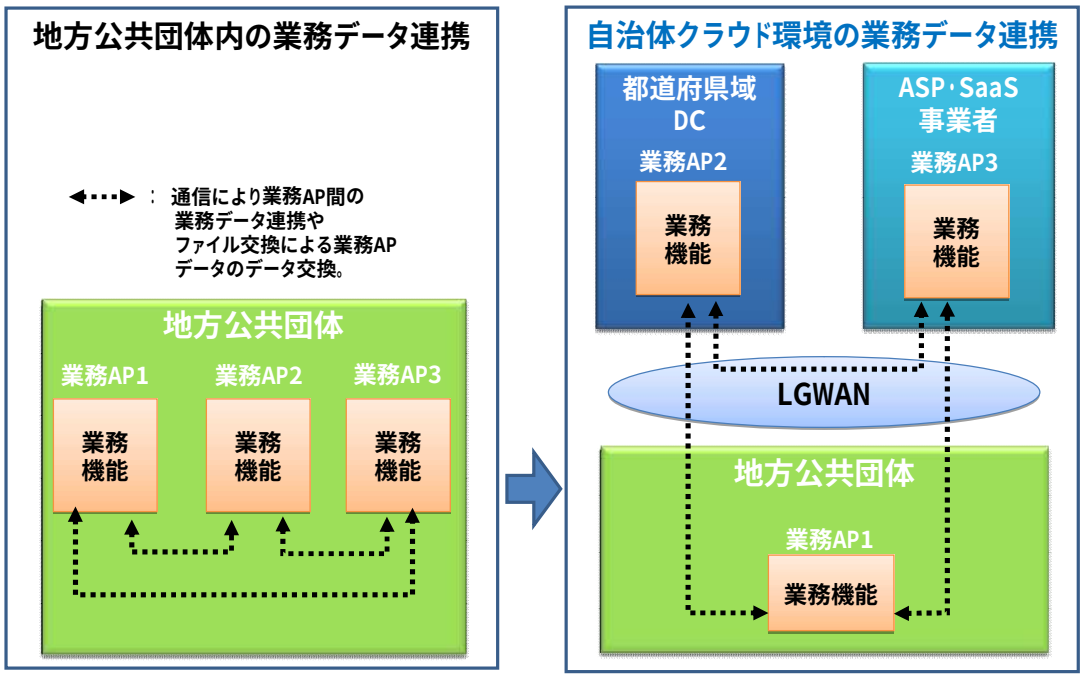


図 3-36　自治体クラウド環境の業務データ連携のイメージ

このような自治体クラウド環境において、業務 AP 間のデータ連携を行うための基本的な要件として以下が考えられる。

- 業務 AP の物理的な配置が変わっても通信に影響を与えない柔軟な連携（メッセージルーティング）
- サイトをまたがって業務データを連携する際の要件（セキュアな SOAP 通信、メッセージ送信、ファイル伝送、送受信ログの記録）
- LGWAN の制約（プロトコル制限、回線帯域）を考慮した運用要件（特に、地方公共団体庁内にセルフ ASP を設置しない場合の、都道府県域 DC からのファイル伝送方法について））

このような要件を業務 AP ごとに装備する必要があるが、重複開発を避け、効率の良い開発を行うため、上記要件の共通部分を集約化した「業務データ連携機能」を都道府県域 DC の機能として装備することを推奨する。

本節では、共通化された機能の集合体である「業務データ連携機能」に求められる要件及び機能について記載する。

なお、「業務データ連携機能」の仕様は、基本的に「地域情報プラットフォーム標準仕様書」及び「LGWAN」の規約に基づいたものとする。

（2）適用範囲

業務データ連携のユースケースと本節の適用範囲を図 3-37、表 3-8 に示す。

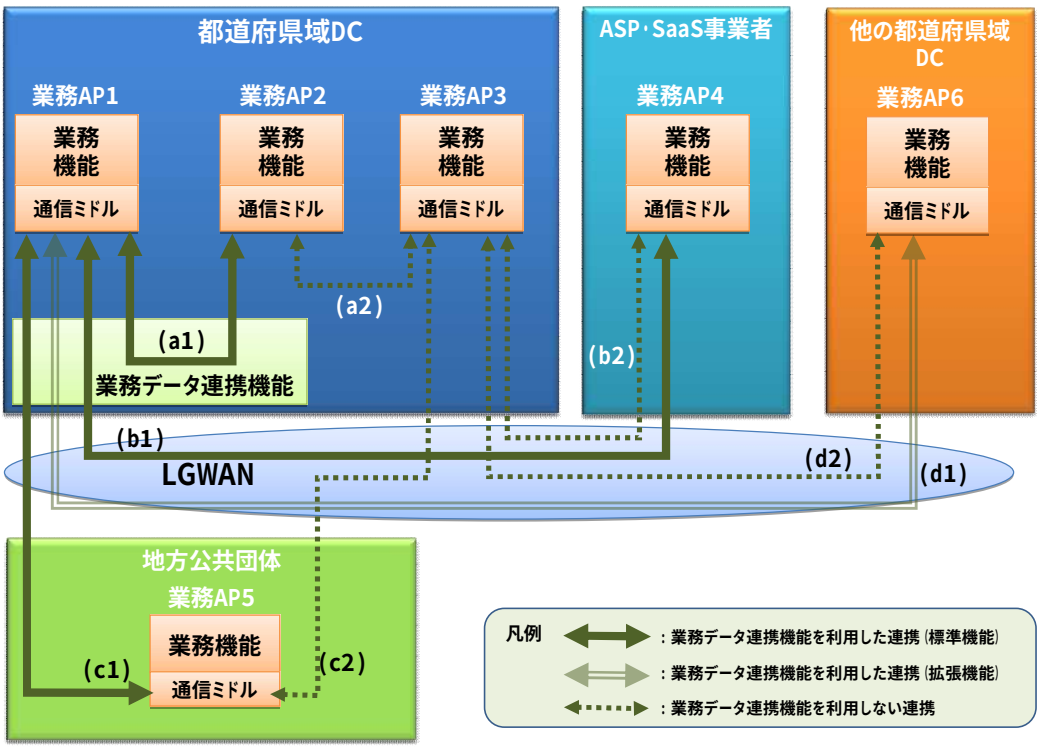


図 3-37　業務データ連携のユースケースと本節の適用範囲の概念図

表 3-8　業務データ連携のユースケースと本節の適用範囲

#	業務データ連携のユースケース		適用範囲	本節での記載
(a)	オンサイトの業務データ連携（同一都道府県域 DC 内）	(a1)業務データ連携機能を利用した連携	適用範囲とする	記載する
		(a2)業務データ連携機能を利用しない連携	適用範囲としない	留意点のみ記載
(b)	オフサイトの業務データ連携（都道府県域 DC－ASP・SaaS 事業者）	(b1)業務データ連携機能を利用した連携	適用範囲とする	記載する
		(b2) 業務データ連携機能を利用しない連携	適用範囲としない	留意点のみ記載
(c)	オフサイトの業務データ連携（都道府県域 DC－地方公共団体庁内）	(c1)業務データ連携機能を利用した連携	適用範囲とする	記載する
		(c2) 業務データ連携機能を利用しない連携	適用範囲としない	留意点のみ記載
(d)	オフサイトの業務データ連携:(都道府県域 DC－他の都道府県域 DC)	(d1)業務データ連携機能を利用した連携	適用範囲とする	記載する（「4.4 業務データ連携」に記載）
		(d2)業務データ連携機能を利用しない連携	適用範囲としない	留意点のみ記載

業務データ連携機能を利用する場合（a1, b1, c1）のユースケースについては、本節で記載する。d1 については、「4.拡張機能」の「4.4 業務データ連携」で記載する。

業務データ連携機能を利用しない場合（a2, b2, c2, d2）のユースケースについては、適用範囲としないため、業務 AP 間の連携仕様は当事者間で個別協議のもと決定する。なお、本節の最後に留意点を記載する。

3.2.3.2 要件一覧

業務データ連携の要件を表 3-9 に示す。

表 3-9　業務データ連携の要件一覧

#	要件	概要	ユースケース（※1）			
			a1	b1	c1-1	c1-2
(A)	基本通信	業務 AP の業務データ連携の基本的な通信として SOAP 通信によるメッセージ交換が行えること。	○	―	―	―
(B)	セキュア通信機能	業務 AP の業務データ連携の通信として通信時の認証と通信内容の秘匿化がある SOAP 通信によるメッセージ交換が行えること。	―	○	○	○
(C)	メッセージルーティング	業務 AP のあて先（エンドポイント）情報を管理し、業務 AP の物理的な配置が変わっても業務 AP 間の通信に影響を与えない柔軟なメッセージルーティングが行えること。	○	○	○	○
(D)	オフサイトのファイル伝送（※2）	オフサイトの業務データ連携を行う際、ファイル伝送（ファイル送信、ファイル受信）が行えること。	―	○	○	○
(E)	地方公共団体庁内にセルフ ASP を設置しない場合のファイル送信（※2）	都道府県域 DC から地方公共団体庁内へのファイル送信が行えること。	―	―	―	○
(F)	地方公共団体庁内にセルフ ASP を設置しない場合のデータ取得（※2）	都道府県域 DC 上の業務 AP から地方公共団体庁内の業務データを取得できること。	―	―	―	○
(G)	送受信ログの記録	業務データ連携機能を中継して連携した送受信のログを記録すること。時刻は LGWAN 基本サービスの時刻同期を使用し同期をとること。	○	○	○	○

【凡例】　○：要件あり、－：該当なし

※1）ユースケースについて
(a1)オンサイトの業務データ連携（同一都道府県域 DC 内）
(b1)オフサイトの業務データ連携（都道府県域 DC－ASP・SaaS 事業者間）
(c1-1)オフサイトの業務データ連携（都道府県域 DC－地方公共団体庁内）で、地方公共団体庁内にセルフ ASP を設置する場合
(c1-2)オフサイトの業務データ連携（都道府県域 DC－地方公共団体庁内）で、地方公共団体庁内にセルフ ASP を設置しない場合

地方公共団体庁内にセルフ ASP を設置する場合と設置しない場合では、LGWAN の通信制約によって要件が異なる。このためユースケース c1 を c1-1 と c1-2 に分解する。地方公共団体庁内にセルフ ASP を設置する場合は、要件は（b1）都道府県域 DC－ASP・SaaS 事業者間の場合と同じである。

※2）メッセージ交換とファイル伝送について

業務 AP 間の業務データ連携方式は、メッセージ交換とファイル伝送があり、それぞれ上り／下りがあるため、以下の 4 パターンの方式がある。

メッセージ交換（問合せ型通信、応答型通信）とファイル伝送（ファイル送信、ファイル受信）について、図 3-38 に、業務 AP1 を都道府県域 DC 上の業務 AP、業務 AP2 を ASP（ASP・SaaS 事業者及び地方公共団体庁内に設置したセルフ ASP）上の業務 AP とした場合の概念図を示す。

オフサイトでの通信方式		主体（都道府県域DC上の業務AP） 連携相手（オフサイトの業務AP（※））	LGWANの通信制約	
			通信プロトコル	地方公共団体内にセルフASPを立てない場合
メッセージ交換	問合せ型通信	業務AP1 →問合せ→ 業務AP2 ←応答← 業務AP1	HTTP(S)が利用可能	都道府県DCから地方公共団体内への通信ができない
	応答型通信	業務AP1 ←問合せ← 業務AP2 →応答→ 業務AP1	HTTP(S)が利用可能	
ファイル伝送	ファイル送信	業務AP1 →ファイル送信→ 業務AP2 ←受信結果(OK/NG)← 業務AP1	HTTP(S)が利用可能。FTPプロトコルは使用できない。	都道府県DCから地方公共団体内への通信ができない
	ファイル受信	業務AP1 ←ファイル受信← 業務AP2 →受信結果(OK/NG)→ 業務AP1	HTTP(S)が利用可能。FTPプロトコルは使用できない。	

（※）地方公共団体内のセルフASPを立てて提供する業務AP及び、ASP・SaaS事業者が提供する業務AP

図 3-38　オフサイトのメッセージ交換とファイル伝送の 4 つのパターン

問合せ型通信とは、個人番号をもとに資格情報や所得情報を取得するような、データを必要とする業務 AP1 が、データ提供元の業務 AP2 に問い合わせて即時にデータを取得するケースである。応答型通信は、逆にデータを必要とする業務 AP2 からの問い合わせに対してデータ提供元の業務 AP 1 が即時にデータを応答するケースである。

ファイル送信とは、住基異動情報を日次や一定間隔（分・秒単位）、あるいはデータ発生時に、介護保険業務や国民年金保険業務へ送付するケースであり、1 月 1 日時点の住基情報を個人住民税業務へ年次で送付するケースのように、データを提供する業務 AP1 が、データを必要とする業務 AP2 に、一定時間ごとにまとめて送付するケースである。逆にファイル受信とは、データを必要とする業務 AP 1 が一定時間ごとにまとまったデータを業務 AP2 より受け取るケースである。

ファイル伝送（ファイル送信、ファイル受信）では、FTP プロトコルが使用されることが多い。しかし、オフサイトのファイル伝送では、LGWAN の通信制約により、FTP プロトコルが使用できないため、代替手段が必要である。これを要件 D に示す。

また、地方公共団体庁内にセルフ ASP を設置しない場合は、都道府県域 DC から地方公共団体庁内への問合せ型通信やファイル送信ができないため、代替手段が必要である。前者を要件 F，後者を要件 E に示す。

3.2.3.3 機能

（1）業務データ連携の構成要素

業務データ連携の概略アーキテクチャを下図に示す。

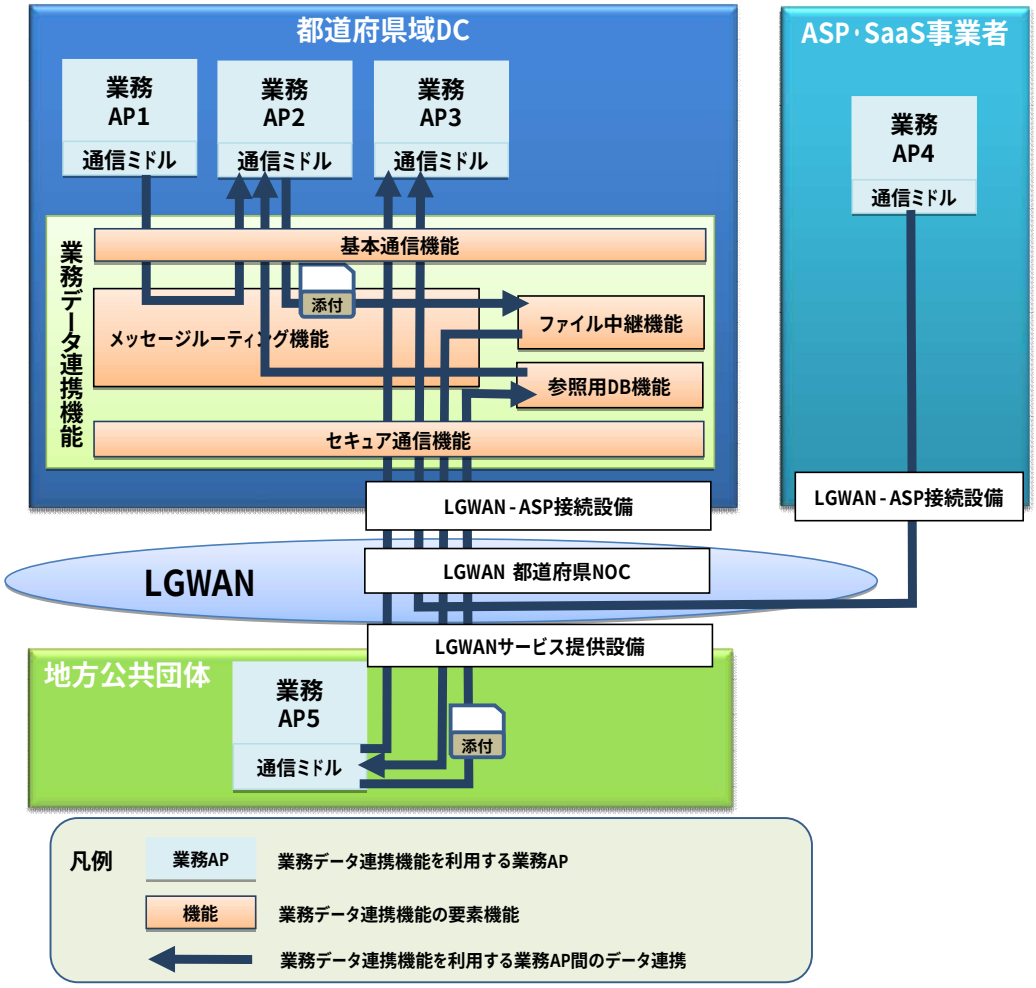


図 3-39　業務データ連携の概略アークテクチャ

（2）業務データ連携の構成要素である機能

業務データ連携の構成要素である機能について、以下に記載する。

表 3-9 の要件一覧で示した業務データ連携のユースケースに応じて、必要となる機能を装備することを推奨する。なお、以下で参照する地域情報プラットフォーム標準仕様書のバージョンは、APPLIC-0008-2009 である。

（A）基本通信

- 基本的な通信機能として SOAP 通信を行う機能である。
- 仕様は、地域情報プラットフォーム標準仕様書の PF 通信機能（プラットフォーム通信標準仕様、2 章）を参照。

（B）セキュア通信機能

- SOAP 通信において、LGKPI に基づく通信時の Web サーバ認証や HTTP ベーシック認証により、通信内容の秘匿化を行う。
- 仕様は、地域情報プラットフォーム標準仕様書の PF 通信機能（プラットフォーム通信標準仕様、2 章）と、PF サイト認証仕様（プラットフォーム通信標準仕様、5.3.1）及び PF 秘匿性確保仕様（プラットフォーム通信標準仕様、5.3.2）を参照。基本的仕様は、地域情報プラットフォーム標準仕様書の PF 通信機能（プラットフォーム通信標準仕様、2 章）と、PF サイト認証仕様（プラットフォーム通信標準仕様、5.3.1）及び PF 秘匿性確保仕様（プラットフォーム通信標準仕様、5.3.2）を参照。

（C）メッセージルーティング

- 宛先情報（業務 AP の名称とエンドポイント（URL）との対応表）を保持する。
- 業務 AP の SOAP メッセージから送信先の業務 AP 名称を取得し、宛先情報からエンドポイントを取得し、SOAP 通信の呼出先を振り分ける機能である。
- 基本通信機能を使って通信する。
- 仕様は、地域情報プラットフォーム標準仕様書の BMR-GW 機能（アーキテクチャ標準仕様、4 章）を参照。

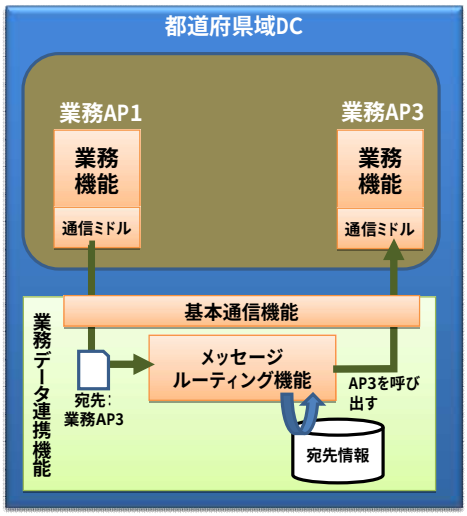


図 3-40　メッセージルーティング機能の例

（D）オフサイトのファイル伝送

- SOAP 通信において、SOAP メッセージにファイルを添付する機能を用いて、ファイル伝送を行う機能である。LGWAN の通信制約を考慮した FTP プロトコルの代替手段である。
- 仕様は、地域情報プラットフォーム標準仕様書の PF 通信機能（プラットフォーム通信標準仕様、2 章）の添付ファイル機能を参照。
- セキュア通信機能を使って通信する。
- LGWAN 回線の帯域を考慮し、大容量のファイルを送受信する場合は、データ圧縮を行う。圧縮機能としては、ZIP 圧縮等のアーカイブ機能の利用が望ましい。さらに、業務データ量や業務要件（伝送タイミング）を考慮の上、ファイル分割や伝送間隔をより細かくし業務データ量を減らすなどの運用設計を行う。

（E）地方公共団体庁内にセルフ ASP を設置しない場合のファイル送信

SOAP 通信において、SOAP メッセージにファイルを添付する機能を用いて、都道府県域 DC から地方公共団体庁内にファイルの送信を行う機能である。LGWAN 通信制約により FTP プロトコルが使用できないことや、地方公共団体庁内にセルフ ASP を設置しないとファイル送信ができなくなることへの代替手段である。

なお、地方公共団体庁内から都道府県域 DC へのファイル送信については、「（D）オフサイトのファイル伝送」にて行う。

- 都道府県域 DC 上の業務 AP から地方公共団体庁内の業務 AP に送信するファイルをファイル中継機能の所定の場所に一時格納する。
- 一定間隔（定刻あるいは、分・秒単位など）で地方公共団体庁内の業務 AP から都道府県域 DC 上の業務 AP に対して問合せ型通信で行われるファイル送信要求を受け、ファイル中継機能は、格納しているファイルを SOAP メッセージに添付し、地方公共団体庁内の業務 AP へ応答する。応答は、SOAP 通信において、SOAP メッセージにファイルを添付する
- セキュア通信機能を使って通信する。
- SOAP メッセージにファイルを添付する仕様は、地域情報プラットフォーム標準仕様書の PF 通信機能（プラットフォーム通信標準仕様、2 章）の添付ファイル機能を参照。
- LGWAN 回線の帯域を考慮し、大容量のファイルを送受信する場合は、データ圧縮を行う。圧縮機能としては、ZIP 圧縮等のアーカイブ機能の利用が望ましい。さらに、業務データ量や、業務的に必要な伝送タイミングを考慮の上、ファイルの分割や、伝送間隔をより細かくし業務データ量を減らすなどの運用設計を行う。
- LGWAN の通信制約を回避するためのファイルのアップロード／ダウンロードや、ファイルの圧縮に関する仕様に関しては、産業・流通系の標準仕様である、流通 BMS 通信プロトコル利用ガイドラインに記載された、「JX 手順仕様」（http://www.dsri.jp/invres/system_standard/19seika.htm）も参照する。

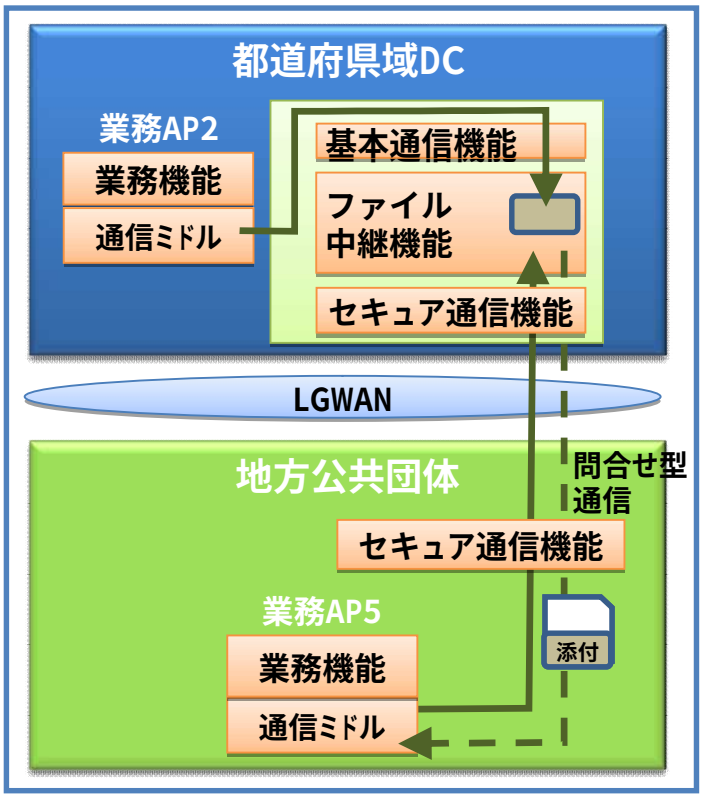


図 3-41　業務 AP2 から業務 AP5 へファイル送信
（地方公共団体庁内にセルフ ASP を設置しない場合）の例

（F）地方公共団体庁内にセルフ ASP を設置しない場合のデータ取得

参照用 DB を用いて、都道府県域 DC の業務 AP が、地方公共団体庁内の業務 AP の業務データを取得する機能である。都道府県域 DC の業務 AP が、地方公共団体庁内の業務 AP に対し業務データ取得要求する場合の代替手段である（メッセージ交換の問合せ型通信の代替手段）。

- 一定間隔（定刻あるいは、分・秒単位など）あるいは、差分データ発生の都度、地方公共団体庁内の業務 AP は業務データ連携機能宛に問合せ型通信用いて業務データを送信する。業務データ連携機能において、参照用 DB 機能は、受取った業務データを参照用 DB に格納する。都道府県域 DC の業務 AP は、参照用 DB を参照することにより、業務データ取得を行う。
- 参照用 DB 機能は、地方公共団体庁内の業務 AP からの業務データを更新するインターフェース及び都道府県域 DC の業務 AP から参照用 DB を参照するためのインターフェース又はビューを提供する。
- セキュア通信機能を使って通信する。
- 参照用 DB 機能の仕様は、地域情報プラットフォーム標準仕様書の公開用 DB 方式の統合 DB 機能（アーキテクチャ標準仕様、4.5.4）を参照。
  なお、公開用 DB に格納するデータ項目や、更新用／参照用インターフェースについては、業務データ連携の当事者間で協議の上決定する。

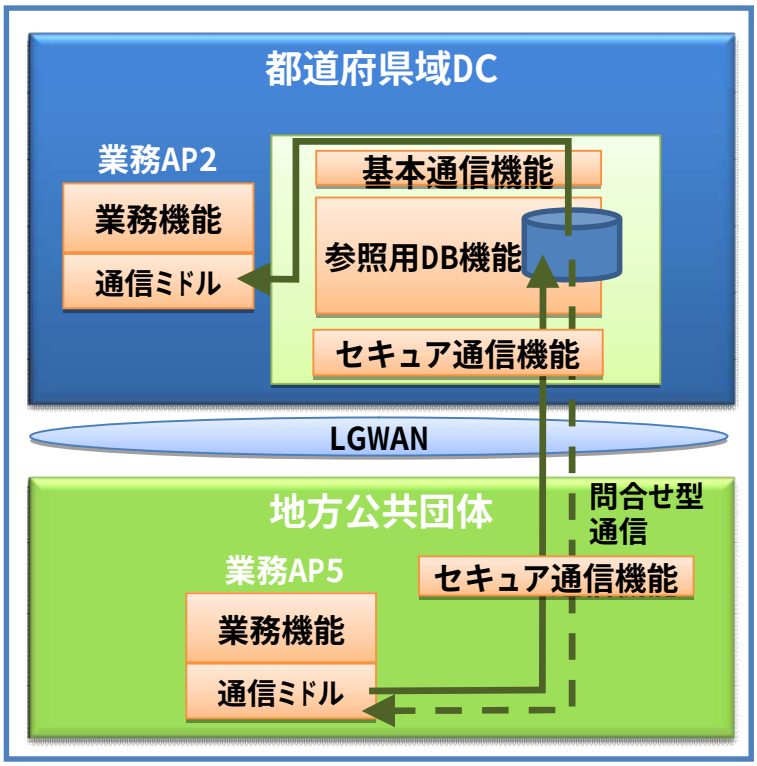


図 3-42　業務 AP2 から業務 AP5 へのデータ取得の例

（G）送受信ログの記録

業務データ連携機能が中継して行うメッセージ交換や、ファイル伝送の送受信の記録をログとして記録する。時刻は、LGWAN 基本サービスである LGWAN　NTP サービスを利用して時刻同期を行うこと。

参考

（1）業務 AP 間の業務データ連携において、業務データ連携機能を利用しない場合の留意点

本節にて、記載した業務データ連携の要件を業務 AP ごとに実装する必要がある。

留意点を以下に示す。

- 基本通信

  業務 AP ごとにそれぞれ基本通信機能を実装し、業務 AP 間で直接通信を行う必要がある。なお、地域情報プラットフォームのアプリケーション標準仕様に準拠している業務 AP は、応答型通信の SOAP インターフェースが既に実装済みである。

- メッセージルーティング

  直接、送付先の業務 AP のエンドポイントを指定して送信する。エンドポイントについは、都道府県域 DC 内で管理しドキュメント化しておくことを推奨する。

- その他の要件

  本節で記載した機能を、業務 AP ごとにそれぞれ実装する。

なお、都道府県域 DC 上の業務 AP が１つの場合、あるいは、オールインワンパッケージで提供され、かつ、都道府県域 DC 内での業務データ連携に限る場合は、従来の地方公共団体庁内でのデータ連携方法と変わりがなく、本節で記載される要件の有効性がなくなるため、業務データ連携機能の導入を推奨するものではない。

（2）地域情報プラットフォーム標準仕様の活用について

交換するメッセージのデータ項目やコード内容を、業務 AP 間で共通化することが望ましい。地域情報プラットフォーム標準仕様書では、業務 AP 間で連携するデータ項目が洗い出されて標準化されているため、データ項目やコード設計のリファレンス（辞書）として活用することが有効である。

地域情報プラットフォーム標準仕様書の「自治体業務アプリケーションユニット標準仕様」の「インターフェース仕様」「項目セット辞書」「コード辞書」などを参照。

4. 拡張機能

4.1 バックアップ連携

4.1.1 データベースのレプリケーション機能によるリアルタイム同期

（1）目的

標準機能におけるバックアップ連携では、バックアップデータの遠隔保管について示してきたが、データベースの規模等によっては復旧まで相当な時間を要してしまう場合や、業務内容によっては許容できる復旧までの作業時間が非常に短い場合がある。

この解決方策の例として、データベースソフトのレプリケーション機能によるリアルタイム同期について示す。このリアルタイム同期を利用することで、、データベースサーバでの障害発生時における業務停止時間を短時間に抑えることが可能となる。

（2）適用範囲

リアルタイム同期は「都道府県域 DC－都道府県域 DC 間」又は「都道府県域 DC－地方公共団体庁内間」を適用範囲とする。

4.1.1.1 要件一覧

「データベースのレプリケーション機能によるリアルタイム同期」の要件を表 4-1 に示す。

表 4-1 「データベースのレプリケーション機能によるリアルタイム同期」の要件一覧

項番	要件	内容
1	障害発生時から復旧までの作業時間の短縮	データベースのレプリケーション機能によるリアルタイム同期。

4.1.1.2 機能

（1）リアルタイム同期機能の概要

リアルタイム同期機能とは、データベースソフトが持つレプリケーション機能を活用し、業務処理によってデータベースが更新等された際に、同期先のデータベースへ更新に関する情報を連携、同じ内容の更新を行うことでデータ同期を図る機能のことである。

「都道府県域 DC－都道府県域 DC 間」又は「都道府県域 DC－地方公共団体庁内間」に同一のデータベース製品を配置し、そのレプリケーション機能を利用することにより障害時の復旧時間を短縮する。

本機能を使用する際の留意点を以下に示す。

- リアルタイム同期を実現するには、遠隔地に同一のデータベース製品を導入する必要がある。
- データベースソフトのレプリケーション機能では、ネットワーク障害等で同期できない場合に同期データをサーバ内に蓄積し、障害回復後に同期処理を実施する機能等も用意されており、同期状態が壊れることは少なくなっている。ただし、あまり同期間隔が開くと、障害回復後に蓄積された大量の同期データが処理されることになるため、ネットワークやサーバに大きな負荷がかかる場合がある。

4.1.1.3 実装例

（1）データベースのレプリケーション機能により遠隔地へリアルタイム同期を行うケース

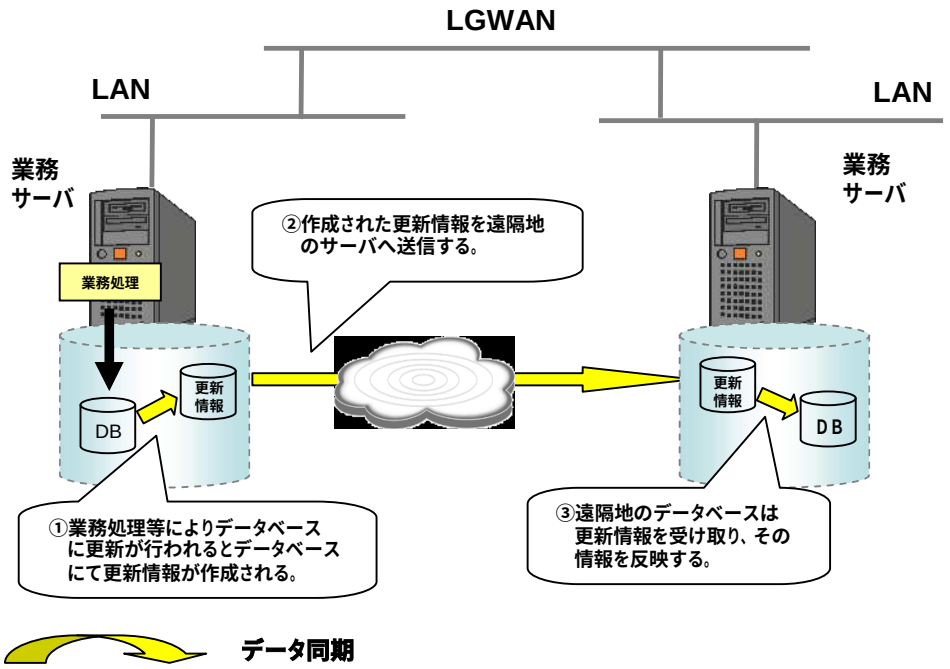


図 4-1　データベースのレプリケーション機能による遠隔地リアルタイム同期

※データベースに更新が行われ、遠隔地のデータベースへ同期が行われる場合の処理フロー。

①：業務処理等により、データベースへの更新が行われる。
②：データベース機能により、更新情報を作成する。
③：遠隔地のデータベースに対して作成された更新情報を送信する。
④：遠隔地のデータベースは受信した更新情報をデータベースに反映する。

4.1.2 専用ストレージによるバックアップデータの遠隔転送

（1）目的

バックアップ連携では、ネットワーク上で大量のデータが通信されるため、ネットワークの効率的な利用、通信コスト削減に向けては、データ通信量の削減が課題となる。

本節では、大幅なデータ通信量の削減が期待でき、また金融機関等でも導入実績がある重複排除技術を有した専用ストレージでのバックアップ連携の実現方式や留意点を記述する。

（2）適用範囲

バックアップデータ量が多い他都道府県域 DC、ASP･SaaS 事業者とのデータ連携を適用範囲とする。

本節にて記載する機能は、必須要件にて示したデータ連携機能の置き換えとなる（図 4-2 の赤破線が置き換え対象）。

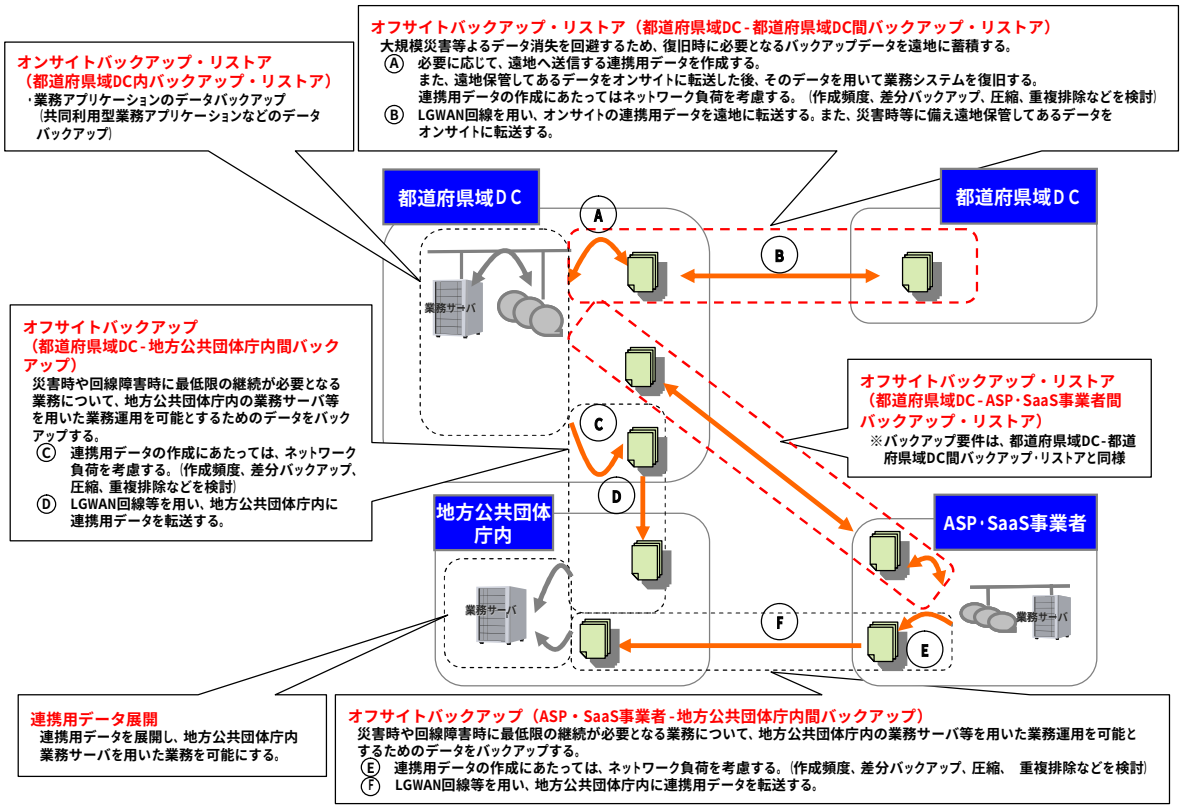


図 4-2 「専用ストレージによるバックアップデータの遠隔転送」の適用範囲

4.1.2.1 要件一覧

「ストレージ機能を用いたオフサイトバックアップ・リストア」の要件を表 4-2 に示す。

表 4-2　「ストレージ機能を用いたオフサイトバックアップ・リストア」の要件一覧

項番	要件	内容
1	オフサイトバックアップ・リストア (都道府県域 DC－都道府県域 DC 間、 都道府県域 DC－ASP・SaaS 事業者間バックアップ・リストア)	データ連携に関する機能 ・ オフサイトバックアップ・リストアにおける、他都道府県域 DC、ASP・SaaS 事業者とデータ連携するための処理（データ連携プロセス）。 ・ 効率的なデータ転送によるネットワーク負荷の軽減。

4.1.2.2 機能

（1）データ連携に関する機能

本機能は適用範囲で記載したとおり、必須要件にて示したデータ連携機能を、ストレージ機能を使用した方式へ置き換えたものである。

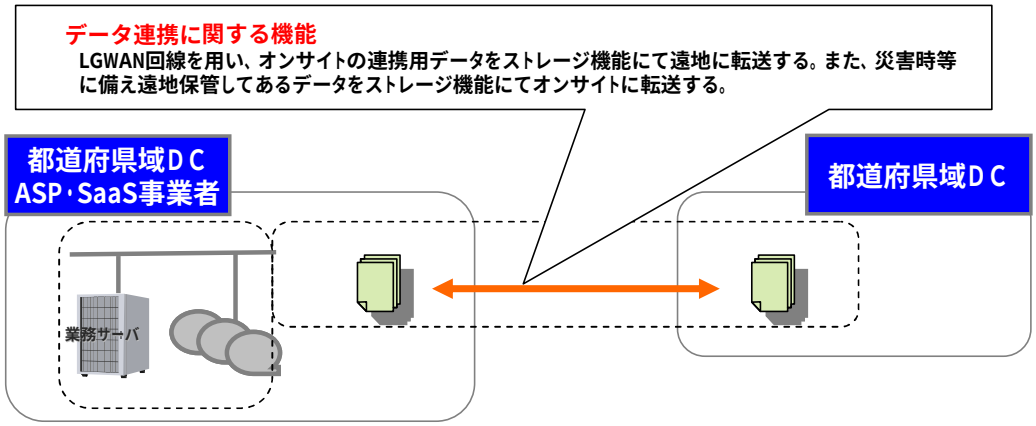


図 4-3　ストレージ機能を使用したデータ連携に関する処理

（A）効率的にデータ転送するための機能

（a）トンネリング機能

データ連携方式を実現するためにトンネリングを行い、連携用データを転送する。

（b）重複排除・圧縮機能

LGWAN のネットワーク負荷低減のため、転送するデータの重複部分を自動的に排除し最小限にする機能。

転送するデータは事前処理により、差分抽出、圧縮などデータを最小限にする処理が行われているが、この事前処理済みデータを連携先に転送する際、重複排除により転送先のデータと比較し、変更された部分を圧縮し送付することで大幅にネットワーク帯域を節約できる。

重複排除はファイル単位での比較でなく、データブロック単位での比較にて行う。

（B）データの一元管理を行うための機能

（a）連携用データの作成日時、保存先などの管理ができること。
（b）保存世代は１世代以上で、必要に応じ長期間保存が可能なこと。
（c）保存世代から外れたデータは削除し、データ領域の再利用が可能なこと。

（C）効率的に連携を行う機能（推奨）

連携用データ作成における一連の処理は、省力化のため、ジョブ管理ソフト等により自動実行させることが望ましい。

（a）処理を自動で運転できること。

（b）保存世代は１世代以上で、必要に応じ長期間保存が可能なこと。

（c）必要に応じて、バックアップタイミングを「定時起動」「任意起動」など自由に設定が行えること。

4.1.2.3 実装例

（1）ストレージ機能を利用するケース

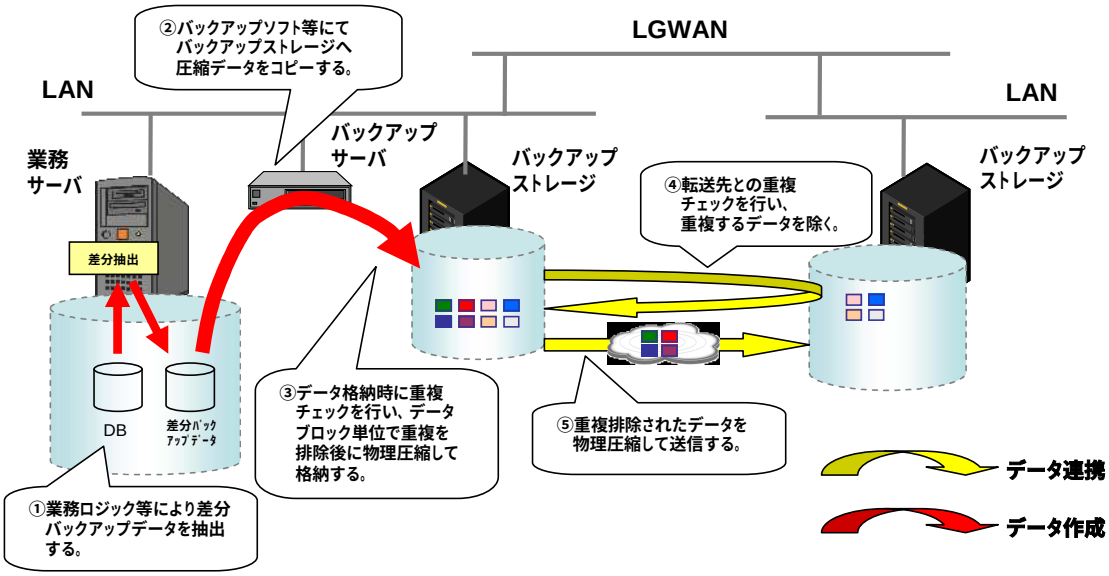


図 4-4　ストレージ機能を利用するケース

（A）データ作成の方法

（a）バックアップデータをバックアップストレージへ保存する方法。

（ア）　業務ロジック等によりバックアップ対象データの差分を抽出する（例えば、前日より増えた DB データ等を抽出する。）。

（イ）　バックアップソフト等を使いバックアップストレージへコピーする。

（ウ）　バックアップストレージへコピーする際にストレージ機能にてバックアップストレージ中のデータとの重複チェックを行い、データブロック単位にて重複するデータブロックを排除する。

（エ）　重複排除されたデータを物理圧縮してバックアップストレージへ格納する。

（B）データ連携の方法

（a）バックアップデータをストレージの機能にて連携先のバックアップストレージへ保存する方法。

（ア）　送信するデータと連携先のデータとの重複チェックを行い、重複するデータブロックを排除する。

（イ）　重複排除されたデータを圧縮し、連携先のバックアップストレージへ送信する。

留意事項

ストレージの機能を利用する場合、転送元と送信先にて同一機種のストレージを実装する必要がある。

4.2 自治体クラウドコンピューティング

4.2.1 概要

（1）目的

既存業務システムを都道府県域 DC の自治体クラウドコンピューティング上に統合するため、静的マイグレーションによる既存システムの移行について記載する。また、可用性及びリソースの柔軟な割り当てによる処理効率向上のための、動的マイグレーション及びグリッド連携について示す。

現状では、マイグレーション及びグリッド連携に関する標準規格が存在しないため、異なる仮想化を実現するソフトウェア間でのマイグレーション及びグリッド連携に制限がある。マイグレーション及びグリッド連携の可否は仮想化を実現するソフトウェアに依存する。そのため、本書では将来考慮すべき拡張要件としてマイグレーション及びグリッド連携を行うために必要となる機能を示す。

4.2.2 要件一覧

自治体クラウドコンピューティング（拡張機能）の機能要件を表 4-3 に示す。

表 4-3　自治体クラウドコンピューティング（拡張機能）の要件一覧

項番	機能要件	内容
1	静的マイグレーション	既存の業務システムを自治体クラウドコンピューティング上で動作するよう変換する機能。
2	動的マイグレーション（データセンター内）	業務を停止することなく、他のサーバで業務を継続する機能。
3	動的マイグレーション（データセンター間連携）	業務を停止することなく、他のデータセンターのサーバで業務を継続する機能。
4	グリッド連携	複数のハードウェアをハイパーバイザーで集約し、大規模なリソースを準備するための機能。

4.2.2.1 静的マイグレーション

（1）静的マイグレーションの概要

静的マイグレーションは、稼働中の業務システムを新しい自治体クラウドコンピューティング上に移行する技法である。静的マイグレーションを行うことで、既存の業務システムを自治体クラウドコンピューティング上で動作するよう変換し、導入、構築作業の大幅な削減を図ることができる。

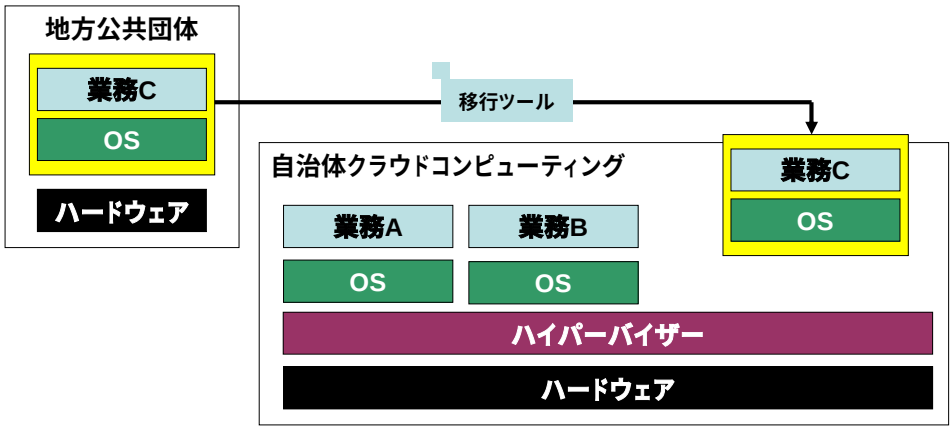


図 4-5　静的マイグレーション（例）

（2）静的マイグレーションの留意事項

地方公共団体の業務システムを、都道府県域 DC に移行する際、以下の留意事項が存在する。

（A）マイグレーションツールの留意事項

ハイパーバイザー製品のマイグレーションツールによって、現行の業務システムが移行可能であるか確認すること。

（B）ソフトウェアのライセンス

現行の業務システムで利用していた、ミドルウェア等のソフトウェアライセンスについて、マイグレーションにより自治体クラウドコンピューティング上に移行する際、新たに購入する必要が生じる場合があるので、利用しているソフトウェアのライセンス条件を確認すること。

（C）LGWAN を用いた業務データの送受信に関する留意事項

地方公共団体の業務システムのサーバ・クライアント端末間の通信は、庁内ネットワークで運用され、外部との接続が行われていないため、通信は暗号化されていないことが多いと考えられる。都道府県域 DC にサーバが統合されることにより、LGWAN を経由した外部との通信が発生する。LGWAN 内の通信はすべて暗号化されているが、都道府県域 DC 内の通信は暗号化されないため、個人情報などの機密情報を取り扱う業務に関しては、都道府県域 DC へ静的マイグレーションを行う際に、HTTPS を利用したサーバとクライアント端末間の暗号化を行う必要がある。

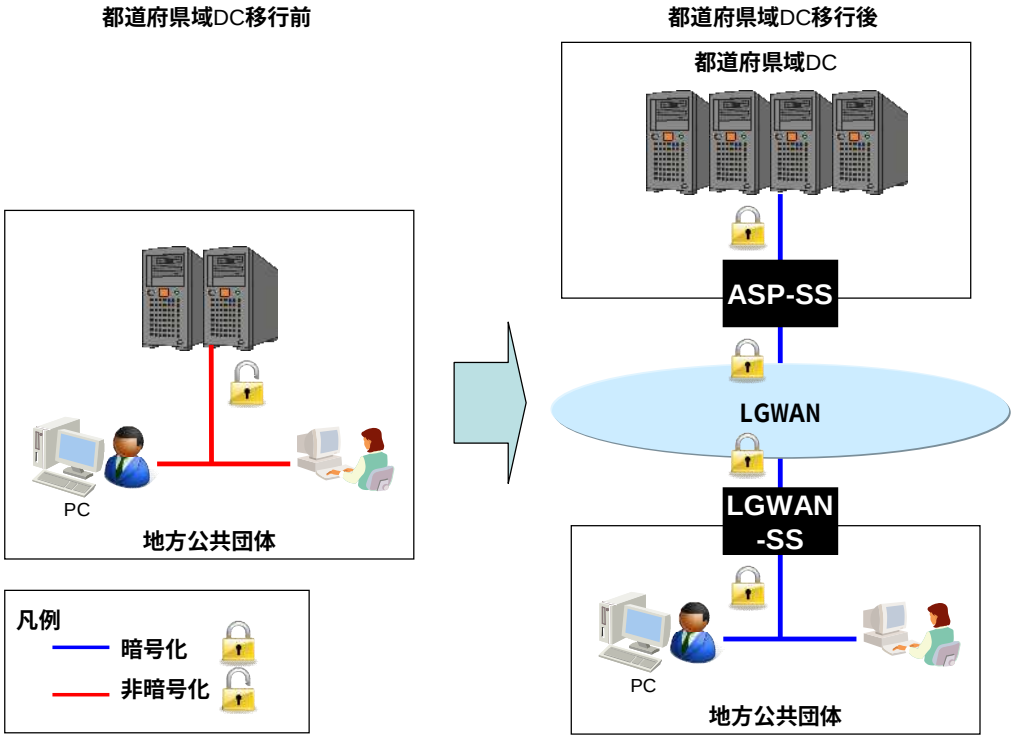


図 4-6　都道府県域 DC 移行前後の通信イメージ

（D）ソフトウェア保守関連の留意事項

自治体の業務システムを都道府県域 DC に移行するタイミングとしてハードウェアの保守期間切れに伴う、システムの入れ替え時が考えられる。ハイパーバイザーの機能により、旧 OS を稼動させて、現行の業務システムを延命させることも可能であるが、利用しているソフトウェアのライセンス条件及び旧 OS のサポート切れに伴うリスクや、最新の業務システムへの移行時期を検討した上で延命を選択すること。

4.2.2.2 動的マイグレーション（データセンター内）

動的マイグレーションは、業務を停止することなく、他のサーバで業務システムを稼動させることができる技術である。稼働中の環境を他のサーバに引継ぎ、業務をそのまま継続させることが可能になる。これにより、ハードウェアリソースを効率的に利用した補完運用が可能になる。

本機能を実装するには、ハイパーバイザー間で動的マイグレーションが可能な環境であることと、業務システムのデータ同期が行われていることが必要となる。同一データセンター内であれば同じ仮想化製品を 2 台のハードウェアに導入することにより実現可能である。

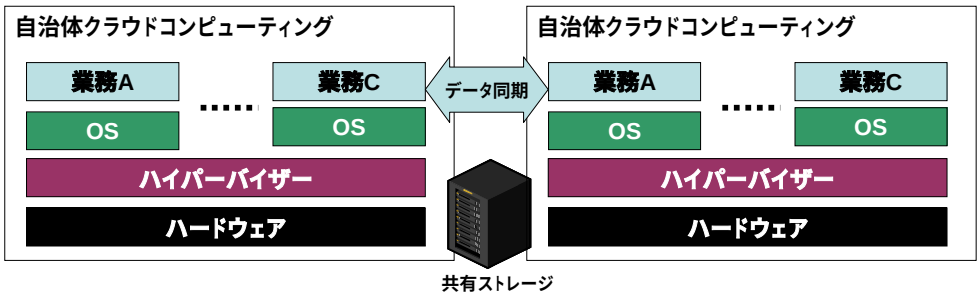


図 4-7　動的マイグレーション

4.2.2.3 動的マイグレーション（データセンター間連携）

（1）動的マイグレーション（データセンター間連携）の概要

図 4-8 に示すとおり、異なる都道府県域 DC 間で、業務システムをマイグレーションにより移行し、補完運用を行う。業務システムの補完運用を行う場合、対象業務で利用している業務データの同期を行う必要がある。都道府県域 DC 間で業務システムのマイグレーションと業務データの同期を行うため、マイグレーションとデータの同期が行える仕様の製品を採用することが必要となる。

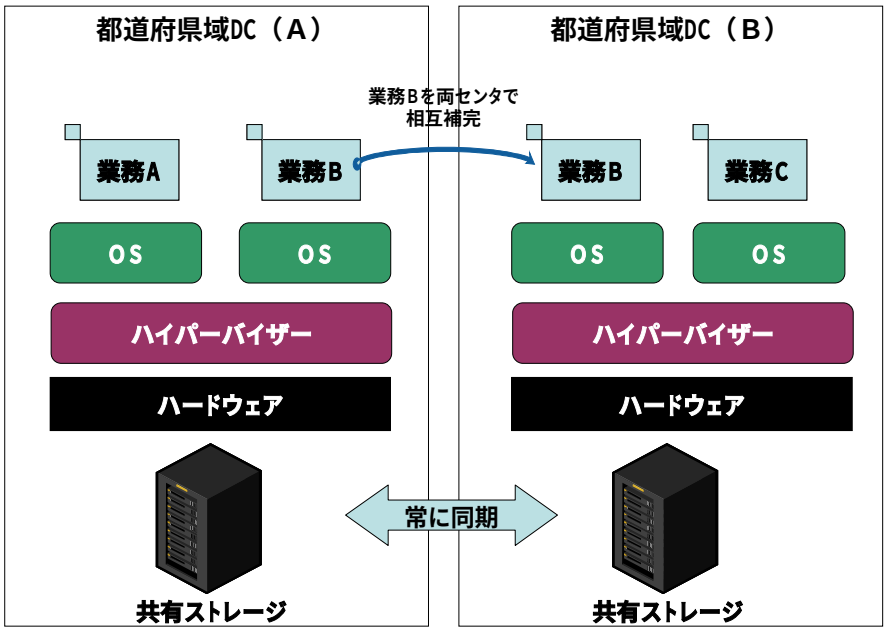


図 4-8　業務システム補完運用のイメージ

（2）動的マイグレーション（データセンター間連携）の留意事項

（A）業務データ同期の標準化

現状、ハイパーバイザー間及び業務データを同期するためのストレージ間の同期を行う標準仕様が定められていないため、異なるハイパーバイザー製品間やストレージ間での同期が困難である。データセンター間での動的マイグレーションを実現するには、同一の製品を利用するか、相互接続が確認されている製品を採用する必要がある。

（B）回線負荷の増大

データセンター間での動的マイグレーションを行うためには、常に業務データの同期が行われている必要がある。LGWAN を介したデータ同期による回線負荷の増大が懸念されるため、回線速度の増速や、帯域制御により他の通信に影響を与えないように考慮する。

4.2.2.4 グリッド連携

（1）グリッド連携の概要

グリッドとは、一般的には、グリッドコンピューティングに代表される、ネットワークを介して複数のコンピュータを接続し、一つのコンピュータとして動作させる技術である。

本書で示すグリッド連携とは、図 4-9 に示すとおり、複数のハードウェアをハイパーバイザーで集約することで、単独のハードウェアでは実現できないリソースを準備することが可能となる技術を指す。グリッド連携により大規模なリソースを準備することができるため、人口規模の大きい自治体の業務処理や複数の業務を、自治体クラウドコンピューティング上に展開することが可能となる。また、プロビジョニングが容易となり処理能力の向上及び可用性の向上や、業務システムの負荷に応じたリソースの再割り当てが容易となる。

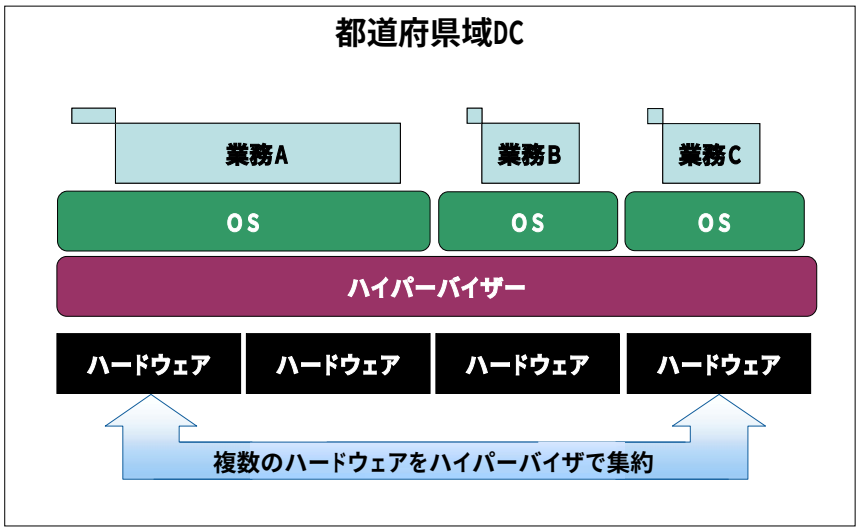


図 4-9　グリッド連携イメージ

（2）グリッド連携の留意事項

（A）LGWAN-ASP の制約

グリッド連携を実現する場合においても、「3.1.2.1（2）（A）制約事項」に示す LGWAN-ASP の各セグメントは物理的に独立したものとし、各セグメント内でグリッド連携を行う必要がある。

（B）グリッド連携の標準化

現状、グリッド連携を実現するための標準仕様が定められていないため、異なるハイパーバイザー製品間でのグリッド連携は困難である。グリッド連携を行う場合は、同一の製品を利用する必要がある。ハードウェアの追加など、拡張を行う場合は、同一のハイパーバイザー製品を導入する必要がある。

4.3 認証連携

4.3.1 概要

（1）目的

標準機能では業務システムの属性を考慮した上で適切な適用範囲のもとでシングルサインオンを導入し、情報の重要度に応じた認証レベル（ID/パスワード、PKI 等）を考慮することを記載した。本節では、拡張機能として今後各地方公共団体が幅広く認証連携機能を活用してさらなる業務効率化を推進していくための発展的な基盤整備としてクラウドサービス間でのシングルサインオン、属性情報の連携の 2 つの仕様を想定し記載する。

（2）適用範囲

クラウドサービス間での認証連携の適用範囲を図 4-10 に示す。

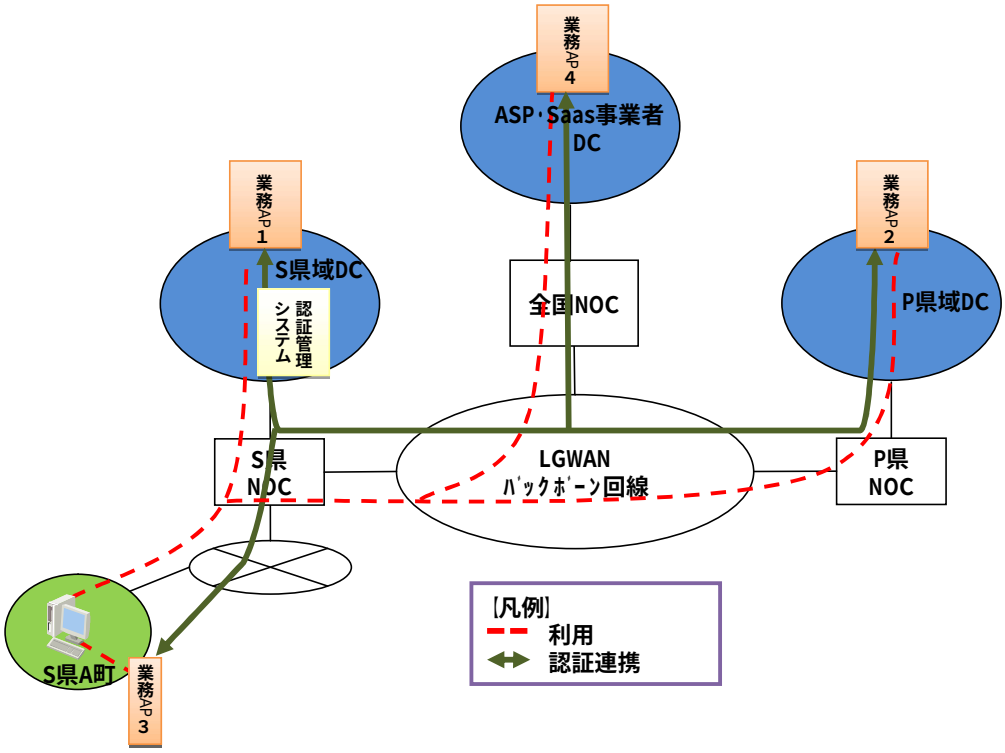


図 4-10　異なるサービス提供者を横断した認証連携

複数の ASP 事業者等、異なるサービス提供者を横断した認証連携の実現が、ユーザの業務効率向上に寄与するケースが考えられる。例えば、ある市町村の課がその業務に応じて異なる ASP 事業者から業務アプリケーションの提供を受ける場合にも、それらのアプリケーション間で透過的に認証を連携させることが可能になり、ユーザに ASP 事業者の存在を全く意識させないで済む。

ここでは複数のクラウドサービスをまたいだシングルサインオンを実現するための認証連携方式として OS やベンダに依存しないオープンな仕様かつユーザ ID そのものを隠蔽する等高度なプライバシー機能を提供する SAML を想定し、その実現方式についてセキュリティ等を踏まえて記述する。また、その際、異なる ID 管理者体系をまたいだ ID の統合管理が必要になるため、運用面での留意事項も考慮する。

一方で、業務システム間での認証連携が実現した環境下では、認証・認可を前提としてユーザの属性情報（例えばメールアドレスや所属部課等）も業務システムをまたいで流通させることが可能になる。これにより属性情報の一括管理が可能になり、情報の一意性の保証や最新化が容易になるとともに、特定のサービスに他サービスの属性データを連携することが可能になる。本項では、属性情報を安全にクラウドサービス間で流通させるための機能に関する代表的な技術仕様として、SAML2.0 の周辺仕様である ID-WSF を想定し留意点を記述する。

4.3.2 要件一覧

クラウドサービス間での認証連携の要件を表 4-4 に示す。

表 4-4　クラウドサービス間での認証連携の要件一覧

項番.	要件	内容
1	ユーザ ID の連携	複数のクラウドサービスをまたいでユーザ ID が連携できるように、IdP と SP がサービス提供者を越えて信頼関係を構築・維持する機能。
2	ユーザ ID の隠蔽	ユーザのプロファイル情報が収集されることを防ぐための、ユーザ ID を隠蔽する機能。
3	属性情報の連携	自治体クラウド内の業務アプリケーションがユーザの属性情報を利用したサービスを提供する場合に必要となる属性情報連携機能。

4.3.3 機能

本節では 4.3.2 で挙げた要件を実現するために考えられる機能を提示する。

（1）ユーザ ID の連携

図 4-11 に示すとおり、SAML を用いて複数クラウドサービスをまたぐシングルサインオンを考えた場合、サインオンの対象となる業務アプリケーション（SP）は複数のサービス提供者やサービス調達者をまたいで存在すると想定される。このような場合でも安全にユーザの認証情報を連携させるために必要な条件は、以下のとおりである。

- IdP と各 SP が互いに信頼関係を保っていること。
  （信頼関係を構築するためには、事前に IdP の運用者と SP の運用者の間で IdP-SP 間の信頼関係を構築することが合意され、IdP、SP の信頼相手のリストに正しく追加されている必要がある）
- IdP にアサーション（ユーザの認証情報）をどこに提供すべきかが設定されていること。
- 各 SP にアサーションをどこから取得すべきかが設定されていること。

また、ユーザ ID の管理（発行や削除など）はサービス調達者ごとの ID 管理者において行われるのが通常であるが、複数のサービス提供者をまたいで ID を連携させる場合、既存の ID 体系を崩すことなく ID 同士の結びつけを行う統括的な ID 管理者が必要になる。

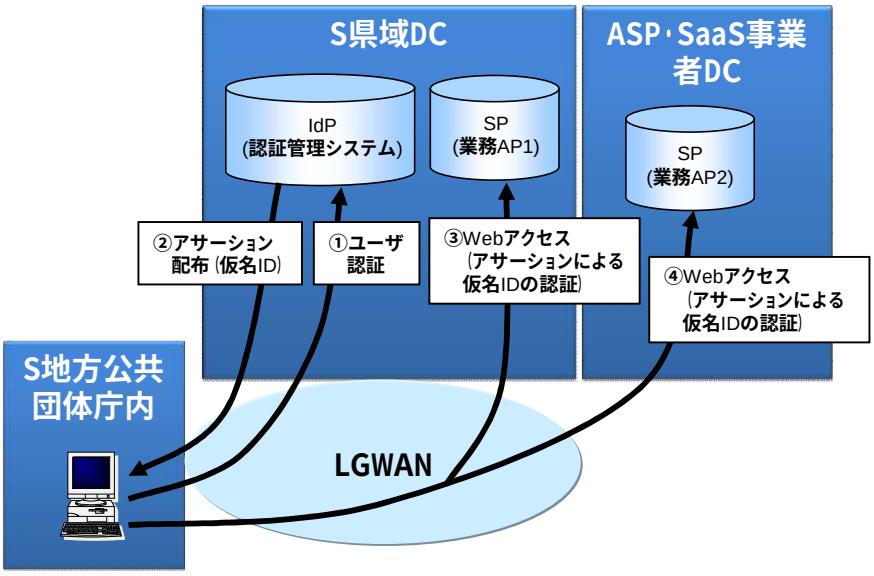


図 4-11　SAML を用いたクラウドサービス間でのシングルサインオン

（2）ユーザ ID の隠蔽

複数のサービス提供者をまたいでユーザ ID を連携する場合、通常はユーザ ID 情報が各サービス提供者間で共有されるが、その結果、各業務アプリケーションで保持しているユーザ毎の操作履歴やプロファイル情報と簡単に割付けされて、別の用途に利用されるプライバシーの問題（名寄せ）をはらんでいる。

SAML では名寄せを防ぐ方法として IdP と SP の間でユーザ ID を一意に識別するための別の ID（Name ID）を共有し、それをランダムな文字列による仮名 ID とすることで実際のユーザ ID を隠蔽する。このとき、各 SP は Name ID を実際のユーザ ID に紐付けて管理する。

（3）属性情報の連携

自治体クラウド内の業務アプリケーションがユーザの属性情報を利用したサービスを提供する場合、その属性情報を安全に取得する必要がある。ID-WSF においてユーザの属性情報は、属性情報を提供するプロバイダによって管理され、各業務アプリケーションからの要求に対して都度提供される。

なお、ID-WSF（2.0）では主に以下のエンティティを利用することでユーザの属性情報流通を実現する。

- WSC（Web Service Consumer）：ユーザの属性情報の利用者であるサービスプロバイダ（SP）
- WSP（Web Service Provider）：ユーザの属性情報を提供するプロバイダ
- DS（Discovery Service）：WSP の場所を管理するプロバイダ

これらのエンティティは図 4-12 のように互いに連携動作を行う。

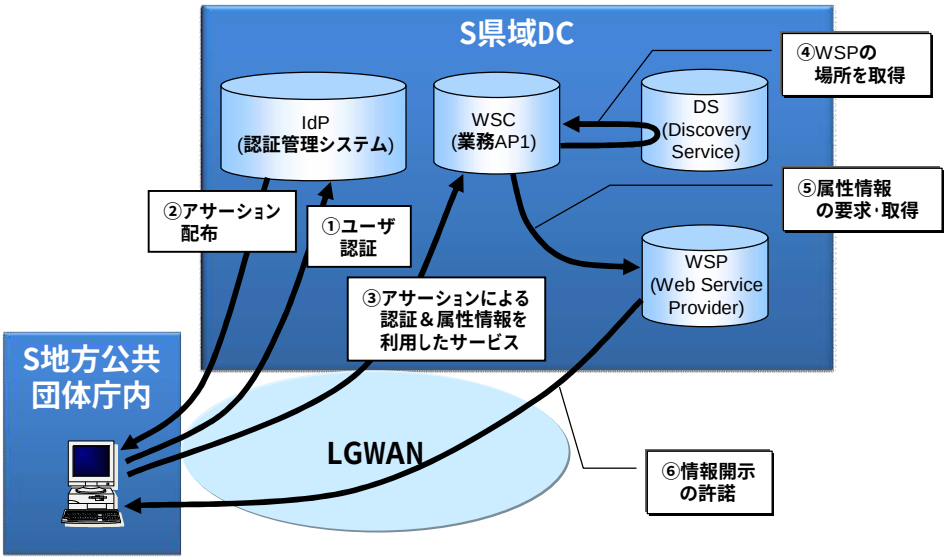


図 4-12　ID-WSF による属性情報の連携

①②：通常の SAML の動作に従い、ユーザ認証・アサーションの取得を行う。
③　：各業務アプリケーションへログオンし、属性情報を利用したサービスを要求する。
この時、WSC は属性情報を取得するため、WSP へ接続する必要がある。
④　：ユーザの所属するドメインによって WSP が異なるロケーションに分散していることが考えられるため、DS に対して WSP の場所を問い合わせする。DS は WSP の場所を WSC に回答する。
⑤　：WSC は WSP に属性情報を要求する。
⑥　：WSP はユーザから情報開示を行ってよいか許諾を得た上でその属性情報を提供する。

これらの手続きにより、業務アプリケーションはユーザの属性情報に応じた柔軟なサービスを提供することが可能になる。ただし、この仕組みが正しく安全に動作するためには以下の前提条件を満たしていることが求められる。

- ID-WSF に基づいて属性情報の連携を行うユーザは、あらかじめ自分の属性情報を自治体クラウド内の WSP に登録しておくこと。
- その WSP の情報はあらかじめ DS に登録されていること。
- DS のロケーション情報そのものは、ユーザがシングルサインオンをする際に発行されるアサーションに記述され、WSC によって利用されること。

4.4 業務データ連携

4.4.1 概要

(1) 目的

「3.標準機能」では、都道府県の主導による都道府県域内の都道府県域 DC-ASP・SaaS 事業者-地方公共団体内の業務 AP を利用することを想定した業務データ連携機能を記載した。本節では、拡張機能として今後、希望するすべての地方公共団体が自治体クラウドに参加するための仕組みをめざした環境整備に向け、以下の事項を想定した業務データ連携機能を記載する。

(a) 同一地方公共団体内の業務効率化のための選択肢の拡大

地方公共団体は、自団体が所属する都道府県域内の業務 AP の利用にとどまらず、自団体が属さない他都道府県域が提供する業務 AP の利用も可能とする。仮に、S 県 A 町は、S 県域 DC が提供する業務 AP1 と、P 県域 DC が提供する業務 AP2 を利用した場合、業務 AP1 と業務 AP2 間での業務データ連携を行う形態である。本節では、本形態である、「**オフサイトの業務データ連携（都道府県域 DC-他の都道府県域 DC）**」の要件と、機能を記載する。

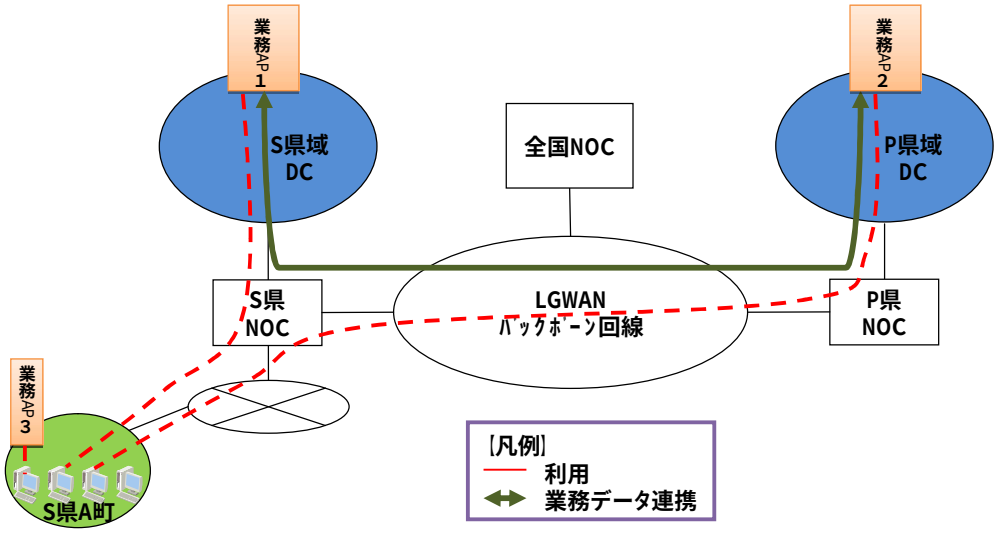


図 4-13　拡張機能：業務データ連携（都道府県域 DC-他の都道府県域 DC）

(b) 業務範囲の拡張としての地方公共団体間での連携

地方公共団体は、他地方公共団体が発行した証明書等を住民手続きに添付書類として求めている場合がある。仮に、他地方公共団体等が保有しているデータを業務データ連携により共有が可能になると、ワンストップ型の行政サービスや地方公共団体間も含めたバックオフィスの効率化等につながる。

本節では、「**オンサイト/オフサイトの業務データ連携（地方公共団体間）**」としての方向性を示す。

ただし、現時点では業務データ連携機能の定義に使用している「地域情報プラットフォーム標準仕様書」において、地方公共団体間データ連携の要件、機能定義が検討中であることから本書においても要件、機能は記載せず、地域情報プラットフォーム等の最新動向を「参考」として列挙する。

（2）適用範囲

拡張機能としての業務データ連携のユースケースは、下図に示す都道府県域 DC-他都道府県域 DC の業務データ連携の部分である。ただし、バックアップ連携機能で他都道府県域 DC に退避したバックアップデータを活用して他都道府県域 DC の業務 AP を利用するといった業務データ連携は対象外である。また、地方公共団体からの業務 AP の利用は、Web ブラウザ等のクライアントから LGWAN 経由でアクセスして利用する方法を想定している。

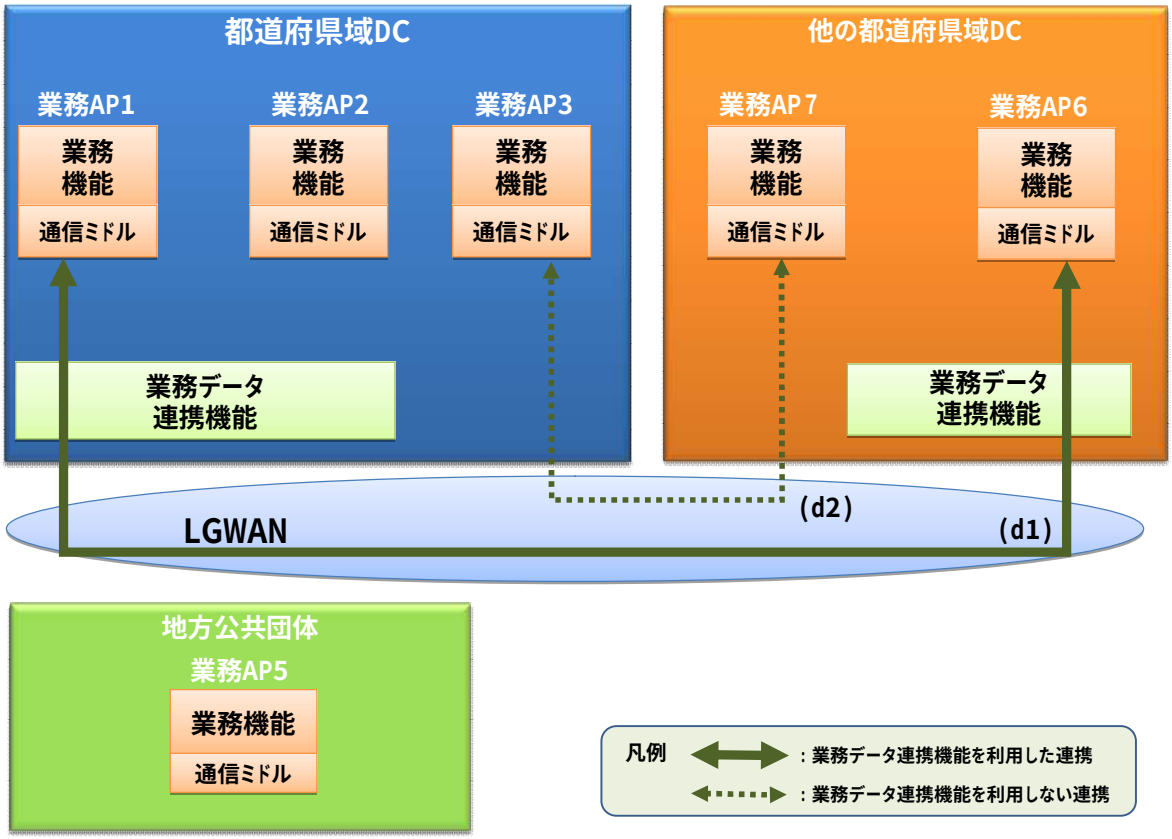


図 4-14　業務データ連携（拡張機能）の本節の適用範囲の概念図

表 4-5　業務データ連携（拡張機能）のユースケースと本節の適用範囲

#	業務データ連携のユースケース		適用範囲	本節での記載
(d)	オフサイトの業務データ連携:(都道府県域 DC－他の都道府県域 DC)	(d1)業務データ連携機能を利用した連携	適用範囲とする	本項で記載する
		(d2)業務データ連携機能を利用しない連携	適用範囲としない	留意点のみ記載

なお、業務データ連携機能を利用しない場合（d2）のユースケースについては、業務 AP 間の連携仕様を当事者間で個別協議のもと決定する。

4.4.2 要件一覧

業務データ連携（拡張機能）の要件を表 4-6 に示す（「表 3-9」に「(d1)オフサイトの業務データ連携（都道府県域 DC－他の都道府県域 DC 間）」のユースケースで要件がある事項の該当有無を追記している（赤枠）。）。

表 4-6　業務データ連携（拡張機能）の要件一覧

#	要件	概要	ユースケース（※1）				
			a1	b1	c1-2	c1-2	d1
(A)	基本通信	業務 AP の業務データ連携の基本的な通信として SOAP 通信によるメッセージ交換が行えること。	○	―	―	―	―
(B)	セキュア通信機能	業務 AP の業務データ連携の通信として通信時の認証と通信内容の秘匿化がある SOAP 通信によるメッセージ交換が行えること。	―	○	○	○	○
(C)	メッセージルーティング	業務 AP のあて先(エンドポイント) 情報を管理し、業務 AP の物理的な配置が変わっても業務 AP 間の通信に影響を与えない柔軟なメッセージルーティングが行えること。	○	○	○	○	○
(D)	オフサイトのファイル伝送（※2）	オフサイトの業務データ連携を行う際、ファイル伝送（ファイル送信、ファイル受信）が行えること。	―	○	○	○	○
(E)	地方公共団体庁内にセルフ ASP を設置しない場合のファイル送信（※2）	都道府県域 DC から地方公共団体庁内へのファイル送信が行えること。	―	―	―	○	―
(F)	地方公共団体庁内にセルフ ASP を設置しない場合のデータ取得（※2）	都道府県域 DC 上の業務 AP から地方公共団体庁内の業務データを取得できること。	―	―	―	○	―
(G)	送受信ログの記録	業務データ連携機能を中継して連携した送受信のログを記録すること。時刻は LGWAN 基本サービスの時刻同期を使用し同期をとること。	○	○	○	○	○

【凡例】　○：要件あり、－：該当なし

※1）ユースケースについて
(a1)オンサイトの業務データ連携（同一都道府県域 DC 内）
(b1)オフサイトの業務データ連携（都道府県域 DC－ASP・SaaS 事業者間）
(c1-1)オフサイトの業務データ連携（都道府県域 DC－地方公共団体庁内）で、地方公共団体庁内にセルフ ASP を設置する場合
(c1-2)オフサイトの業務データ連携（都道府県域 DC－地方公共団体庁内）で、地方公共団体庁内にセルフ ASP を設置しない場合
(d1)オフサイトの業務データ連携（都道府県域 DC－他の都道府県域 DC 間）
※2）3 項 P44「メッセージ交換とファイル伝送について」を参照

4.4.3 機能

（1）業務データ連携の構成要素

オフサイトの業務データ連携(都道府県域 DC-他都道府県域 DC)の構成要素を示す。

業務データ連携の概略アーキテクチャを下図に示す。

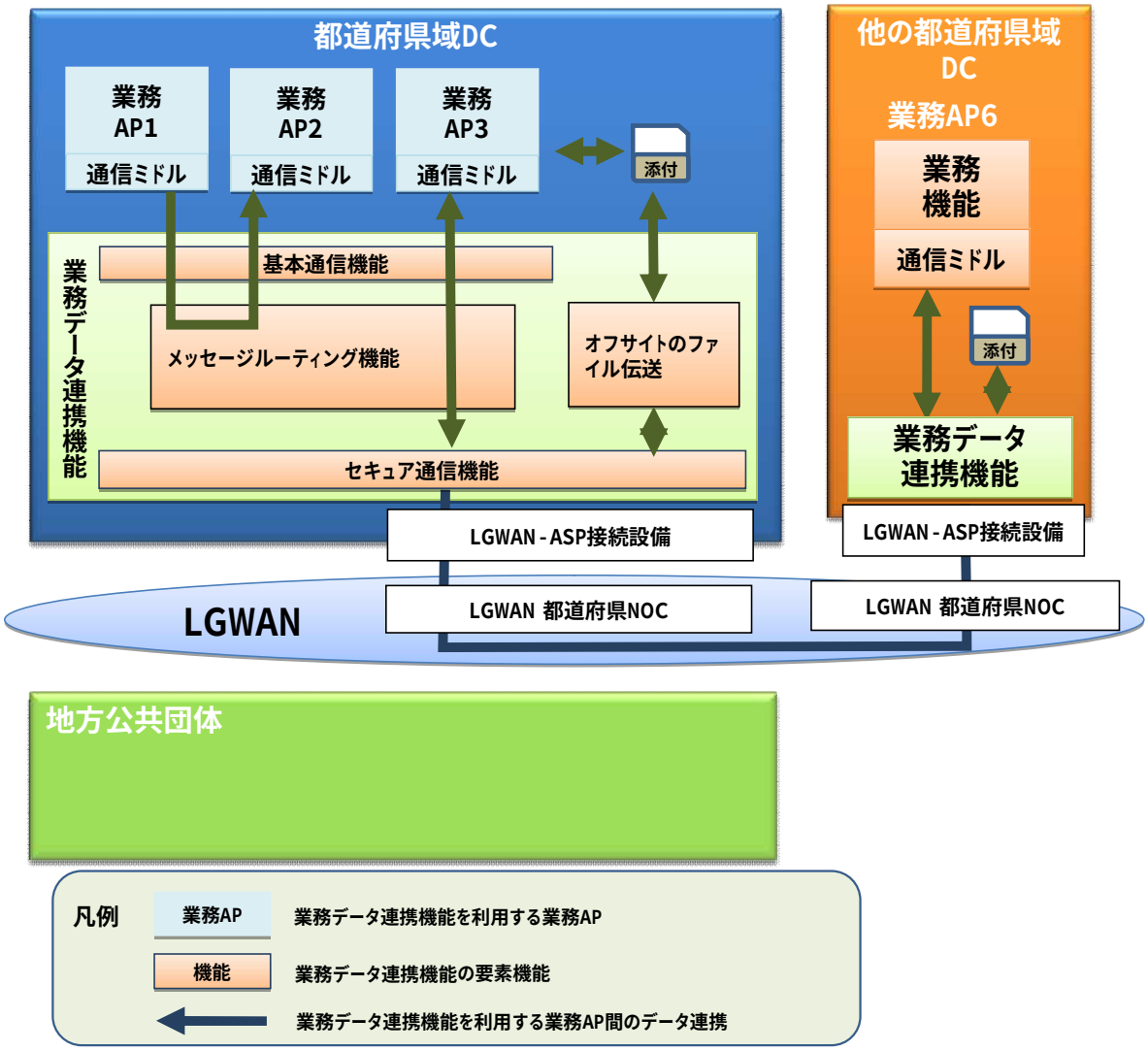


図 4-15　他の都道府県 DC 間の業務データ連携の概略アーキテクチャ

（2）業務データ連携の構成要素である機能

オフサイトの業務データ連携(都道府県域 DC-他都道府県域 DC)の機能の説明を以下に記載する。なお、以下で参照する地域情報プラットフォーム標準仕様書のバージョンは、APPLIC-0008-2009 である。

（A）セキュア通信機能

- 標準機能と同様である。
- なお、都道府県域 DC と他の都道府県域 DC 間の双方で業務データ連携機能を有している場合は、各都道府県域 DC の業務データ連携機能がセキュア通信機能を実現する。

（B）メッセージルーティング

- 標準機能と同様である。
- なお、他の都道府県域 DC 上に業務 AP を呼び出す場合のルーティングにおいて、他の都道府県域 DC が業務データ連携機能を導入しているか否かで、ルーティング先のエンドポイントが異なる。未導入の場合は、他の都道府県域 DC 上に業務 AP のサービスのエンドポイントにルーティングするが、他の都道府県域 DC が業務データ連携機能を導入している場合は、他の都道府県域 DC 上の業務データ連携機能のエンドポイントへルーティングし、他の都道府県域 DC 内の業務 AP へ業務データ連携機能が更にルーティングする方法となる。逆に、他の都道府県域 DC 内の業務 AP から自都道府県域 DC 内の業務 AP が呼び出された場合も同様の処理を実現する。

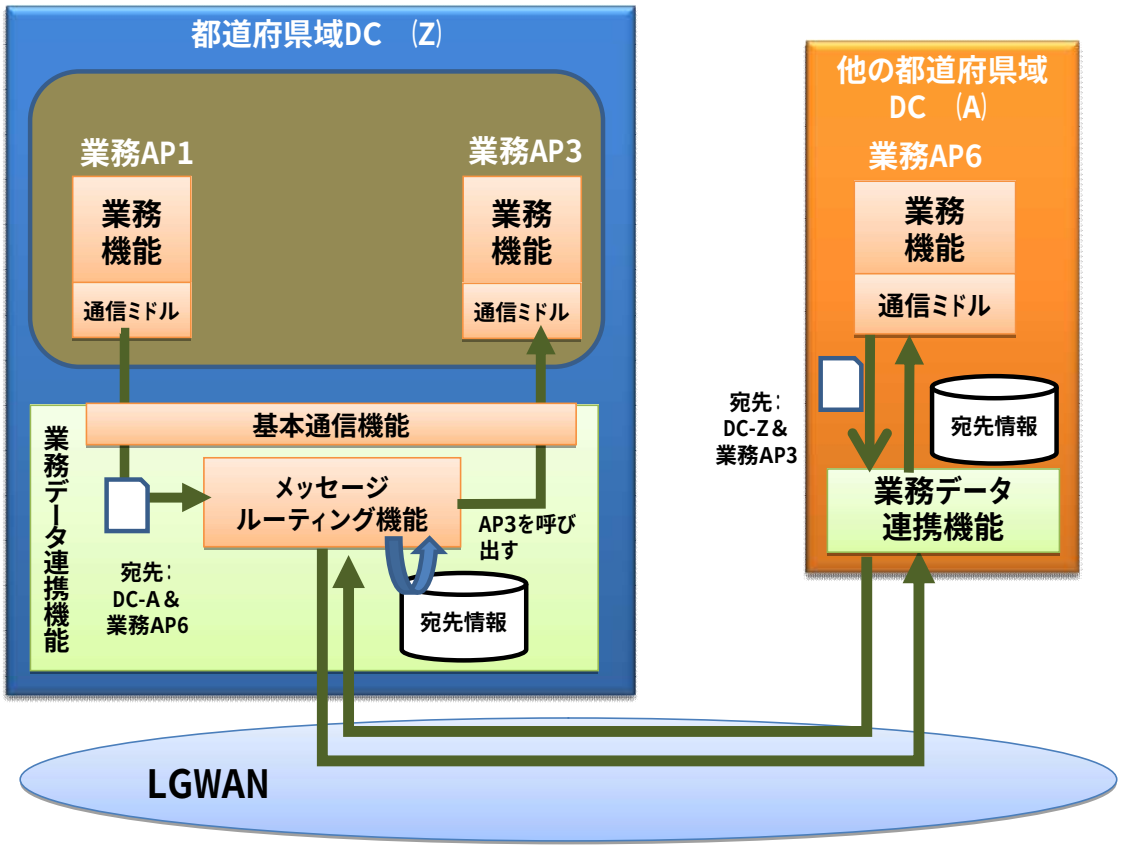


図 4-16　他の都道府県 DC 間のメッセージルーティング機能の例

（C）オフサイトのファイル伝送

- 標準機能と同様である。

（D）送受信ログの記録

- 標準機能と同様である。

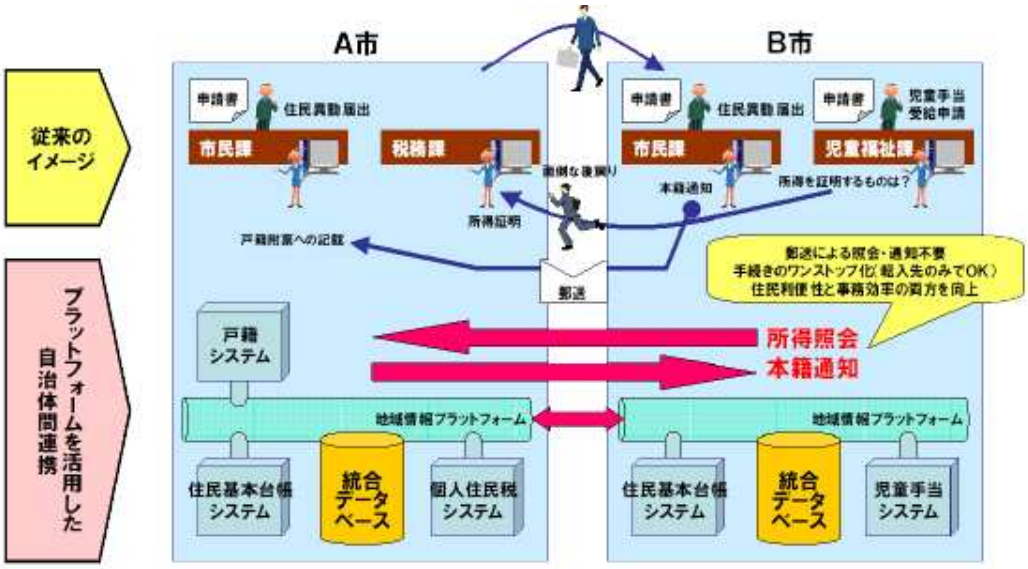
4.4.4 参考（オンサイト/オフサイトの業務データ連携（地方公共団体間））

前節までの標準機能及び拡張機能では、自治体クラウド環境において、論理的な地方公共団体内部の業務 AP 間の業務データ連携を対象としており、地方公共団体内の業務の効率化、情報システムの改革を推進し、さらに、希望するすべての地方公共団体が自治体クラウドに参加するための仕組みをめざした環境整備が可能となる。

本節では、ワンストップ型の行政サービスや他地方公共団体も含めたバックオフィスの効率化ということも視野にいれ、業務データ連携の連携範囲を拡張（地方公共団体内部から国との連携、他地方公共団体との連携、民間との連携）することが想定される最新動向を記載する。

（1）地域情報プラットフォーム標準仕様（APPLIC）

当該仕様書の業務データ連携機能で採用している地域情報プラットフォーム標準仕様書である。地域情報プラットフォームは、地方公共団体内部の業務 AP の業務データ連携のみならず、地方公共団体間連携や官民連携といった業務データ連携に必要な標準化を進めている。

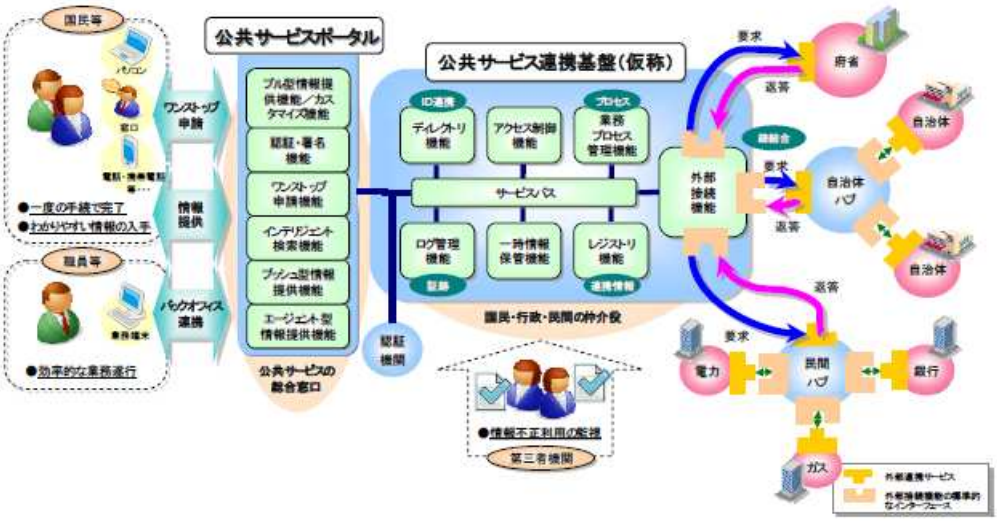


出典：地域情報プラットフォーム基本説明書 V4.0(P17)より

参考 URL：http://www.applic.or.jp

（2）次世代電子行政サービス基盤等検討プロジェクトチーム（内閣官房）

国・地方の枠を超えた電子行政窓口サービスの展開を念頭に置き、フロントオフィスとバックオフィス及びバックオフィス相互の連携や民間手続との連携等を図ることにより、様々な行政手続を基本的にワンストップで簡便に行える次世代の電子行政サービス基盤の標準モデルの構築に向けた検討がされている。また、平成 21 年 12 月には、次世代電子行政の技術的方策について、バックオフィス連携を進める観点からできるだけ具体的に示す中間報告が公開されている。この中間報告書の中では、地域情報プラットフォーム標準仕様書を活用することも記載されている。



出典：次世代電子行政サービス基盤等検討プロジェクトチーム中間報告書（P21）より

参考 URL：http://www.kantei.go.jp/jp/singi/it2/nextg/index.html

（3）原口ビジョン（総務省）

地域の絆の再生として２０２０年時点ですべての世帯（１００%）でブロードバンドサービスを利用する施策として下記の施策例が掲げられている。

- **電子行政の実現による行政刷新**
  - ✔ **国民本位の電子行政を実現（すべての申請処理を電子化）（２０１４年）**
  - ✔ **２４時間３６５日オンライン行政サービスを利用可能化（２０１４年）**

参考 URL：http://www.soumu.go.jp/main_content/000048728.pdf

（4）スマート・クラウド研究会（総務省）

総務省は、総務副大臣が主宰する「スマート・クラウド研究会」における検討の「中間取りまとめ（案）－スマート・クラウド戦略－」についての意見公募を行っている（平成 22 年 2 月 10 日）。電子政府の実現に向けては、「行政サービスの「見える化」」「国民に開かれた「オープンガバメント」の推進」「無駄を排除した「行政刷新」」が目的に集約され、政府の電子行政クラウド「霞が関クラウド」や、地方自治体の電子行政クラウド「自治体クラウド」を推進することが必要である。とされている。

参考 URL：http://www.soumu.go.jp/menu_news/s-news/02ryutsu02_000023.html

5. 今後の検討課題

本項では、6 つの実証団体（北海道、京都府、佐賀県、大分県、宮崎県、徳島県）から自治体クラウド開発実証の取組過程で新たに認識した課題のヒアリングを行い、標準仕様書の検討過程で認識した課題と併せて記述する。

なお、本書 1 項から 4 項では技術的な仕様を示しているが、本項では技術的な事項に制限せず、自治体クラウドの推進に向けて検討が必要となるであろう事項について 4 つの分野に分けて記述する。

（1）制度

（A） バックアップ連携時の責任分担、免責条件

- 他地方公共団体のデータを保管する際の責任分担、紛失・消失時の保管側 DC の免責条件等の整理（自治体クラウド利用規約等の検討）
- 他地方公共団体のデータを保管する際の個人情報保護のあり方や戸籍データを庁外に出せない等の個別条例の取り扱いに関する検討

（B） 管理体制

- セキュリティに関する問題が発生しないよう、自治体クラウドを利用する地方公共団体のセキュリティ水準を一定にするため、地方公共団体におけるネットワークや機器等の管理基準の検討

（2）標準化

（A）文字コード・外字

- 文字コード、外字に関する取り決めに関する検討（データ移行性に関連）

（B）業務プロセス

- 地方公共団体が行う組織見直しや業務アプリケーションのカスタマイズ削減等の業務プロセス改善(BPR)を実施する手順の整備と地方公共団体間での情報の共有

（C）データ移行

- 庁内業務アプリケーションや ASP・SaaS サービスが地域情報プラットフォームに準拠している場合でも、移行作業時は業者間の調整（データ加工、移行作業等）が発生する状況であり、地方公共団体毎の事情に応じた柔軟なサービス利用を図るためには、データ移行に関する標準仕様、業務フロー、データベース構造の共通化の検討が必要
- クラウド事業者の乗り換え等を想定し、地域情報プラットフォームに準拠していることで業務データ連携が簡易にできる範囲と個別に調整等が必要となる範囲についての明確化が必要

（3）LGWAN

（A） 審査基準・制度

- IaaS(Infrastructure as a Service)や PaaS(Platform as a Service)を LGWAN 上で提供する場合の審査基準の定義(明確化）が必要
- LGWAN でのシステム構成変更・IP アドレス割り当て等は事前の申請手続きが必要であり、、仮想化技術を利用した動的リソース割り当てには対応が難しいため、手続き変更等の検討が必要

（B） 帯域、通信プロトコル

- DC へのデータ集約及びバックアップ連携によるネットワーク負荷増大に対応した LGWAN 及び県域ネットワークのあり方の検討
- 「LGWAN-ASP 接続約款」及び「LGWAN-ASP 接続技術仕様」等で許可されていないプロトコルの利用に関する検討（当面はバックアップ連携のみが該当）

（C）普及促進施策

- サービス事業者を容易に乗り換えできるようにして普及促進を図るため、サービス事業者に対して、データ及び設定情報を出力できる機能の提供や求めに応じて詳細設計レベルの資料提供及び解説を LGWAN-ASP として義務化することの検討
- LGWAN-ASP サービス事業者の参入を容易にするため、初期から一定額の利用料を請求するのではなく、サービス利用団体の増加に伴って利用料が増加するなどの価格体系の検討

（4）運営

（A）費用、事業形態

- リソースの占有度合い（使用量、処理量）による費用負担等も含めた、自治体クラウドサービス料金に関する考え方の整理
- 自治体クラウドの構築・運用を行う場合の事業形態（第 3 セクター、事務組合、都道府県など）の整理
- 地方公共団体でのクラウドサービス利用料の予算化において、サービスの提供を受けるという性質から、委託費ではなく役務費での予算化などの検討が必要

（B）支援体制

- 自治体クラウドによる地方公共団体の支援と地域 IT 産業の振興を両立させるため、制度改正対応等で情報収集体制が弱い地域ベンダが不利にならないよう、システム改修期間を見込んだ制度改正内容の公表リミットを定めるなどの取組に関する検討

6. 付録 用語集

本書で用いられる主な用語の説明を以下に示す。

No.	用語	説明
1	ASP・SaaS 事業者	アプリケーションを、ネットワークを経由したサービスとして提供する事業者。
2	Basic 認証	HTTP で定義される認証方式の 1 つ。ユーザ名とパスワードを暗号化することなく Base64 エンコードして送信するという特徴を持つ。
3	BMR-GW 機能	地域情報プラットフォーム通信におけるサービス呼び出しの宛先を動的に調整可能とするルーティング機能を提供する。
4	Cookie	Web サイトの提供者が、Web ブラウザを通じて訪問者のコンピュータに一時的にデータを書き込んで保存させる仕組みのこと。
5	Digest 認証	HTTP の認証方法の 1 つでユーザ名とパスワードを、サーバが生成した乱数と組み合わせてハッシュ化することで盗聴に対する耐性を持つ。
6	DS	Discovery Service の略称。ID-WSF のフレームワークにおける、WSP の場所を管理するプロバイダのこと。
7	ID-WSF	Liberty Alliance が定めた仕様 Identity Web Services Framework の略称で、ユーザの属性情報の安全な流通方法を規定している。
8	IdP	Identity Provider の略称。SAML のフレームワークの中で認証を管理するプロバイダのこと。
9	IPSec	IP パケットを暗号化して通信内容の盗聴や改ざんを防止するための技術。
10	NIC	ネットワークインターフェースカードを示す。
11	Open ID	URL 形式の ID を用いて様々な Web サービスの認証を実現する仕組み。シングルサインオンに利用される。
12	PF 通信	地域情報プラットフォーム標準仕様に規定されているプラットフォーム通信標準仕様に従った通信のこと。
13	SaaS	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。サービス型ソフトウェアとも呼ばれる。
14	SAML	Security Assertion Markup Language の略称で、標準化団体 OASIS（Organization for the Advancement of Structured Information Standards）において策定された、認証情報を安全に交換するための XML 仕様。
15	SP	Service Provider の略称。SAML のフレームワークにおけるサービス提供者のこと。
16	VM(Virtual Machine)	仮想マシン。ソフトウェアにより仮想的なハードウェアを作成し、その上で既存の OS やアプリケーションを動作させることができる機能を示す。
17	WSC	Web Service Consumer の略称。ID-WSF のフレームワークにおける、ユーザの属性情報の利用者であるサービス提供者（SP）のこと。
18	WSP	Web Service Provider の略称。ID-WSF のフレームワークにおける、ユーザの属性情報を提供するプロバイダのこと。
19	アーキテクチャ標準仕様	地域情報プラットフォーム標準仕様書のドキュメントのうち、サービス連携を支える基盤アプリの諸要件・プロトコル等を取り決めた仕様（アーキテクチャが中心）。
20	アクティブディレクトリ（AD）	マイクロソフトによって開発され、Windows 2000 Server から導入されたディレクトリサービス。

No.	用語	説明
21	アサーション	SAML のフレームワークで用いられるユーザの認証を証明する情報であり、IdP によって発行される。
22	エンドポイント	ネットワークに接続されたサーバ等のネットワーク端末のこと。
23	クレデンシャル	ユーザの認証に使用されるセキュリティ情報。パスワードや公開鍵証明書、Kerberos チケット等が該当する。
24	コード辞書	自治体業務アプリケーションユニット標準仕様で規定されているデータ項目において、共通的なリファレンスとなるデータ項目のコード値及びコード値に対応する内容を定義した辞書のこと。
25	シングルサインオン	ユーザが一度認証を受けることにより、利用可能な業務アプリケーションすべてにログイン可能となる機能。
26	セキュア通信機能	SOAP 通信において、通信時のサーバ・クライアント認証と通信内容の秘匿化を行う機能。
27	セキュリティポリシー	組織における情報資産のセキュリティを確保する上での考え方や必要な体制・組織・運用を含めた規定のこと。
28	データ連携	業務アプリケーション間で、業務に必要なデータを交換すること。通信を利用する場合やファイルを利用する場合がある。
29	ハードウェアトークン	ユーザがシステムを利用する際の認証のために使う物理デバイスのこと。
30	ハイパーバイザー	仮想化を実現するための専用 OS。ハイパーバイザーを利用し VM を作成する。本書ではホスト OS も含む場合がある。
31	ファイル中継機能	業務データ連携機能の要素機能であり、地域情報プラットフォーム標準仕様に規定される公開用 DB 方式を採用した統合 DB 機能を提供する。具体的には、データを参照する側の業務アプリケーション向けに公開するための業務インターフェースの提供と、データを提供する側の業務アプリケーションが、公開するデータを登録するためのインターフェースを提供する。
32	フォーム認証	Web での認証方式の 1 つで、HTML のフォームを用いてユーザ名・パスワードを送る方式。
33	プラットフォーム通信標準仕様	地域情報プラットフォーム標準仕様書のドキュメントのうち、サービス連携を支える基盤アプリケーションの諸要件・プロトコル等を取り決めた仕様（通信規約が中心）
34	プロビジョニング	ハードウェア等のリソースを事前に準備しておき、利用者の要求に応じてリソースを割り当て、サービスを提供する。
35	マイグレーション	既存の OS や業務システムを VM 上に移行する機能を示す。また、VM から他の VM へ移行する機能も含む。
36	ユーザ	業務アプリケーションを実際に利用するユーザ。各自治体の職員等が該当する。
37	リバースプロキシ	特定のサーバへのリクエストが必ず経由するように設置されたプロキシサーバのこと。
38	ルーティング機能	SOAP 通信において、サービス呼び出しの宛先となる業務 AP の位置情報を突き合わせ、呼出し先を振り分ける機能。
39	基本通信機能	基本的な通信機能として SOAP 通信を行う機能。
40	業務データ連携機能	業務データ連携機能は、都道府県域 DC 内に設置された業務アプリケーションと、都道府県域 DC 内の他の業務アプリケーション又は自治体内あるいは ASP・SaaS 事業者内の業務アプリケーションとの間で、PF 通信にてデータ連携を行う手段を提供する。

No.	用語	説明
41	項目セット辞書	自治体業務アプリケーションユニット標準仕様で規定されているデータ項目において、共通的なリファレンスとなるデータ項目の集合体の型を定義した辞書のこと。
42	参照用 DB 機能	LGWAN 制約により、他サイトとの問合せ型通信を行えない場合に、他サイトとの通信の中継を行う機能。
43	自治体業務アプリケーションユニット標準仕様	地域情報プラットフォーム標準仕様書のドキュメントのうち、自治体内で業務データ連携に必要な業務アプリケーションユニットのインターフェース仕様を規定（26 業務を規定）。
44	重複排除	あるデータセットを細分化し、重複しているデータを除外する技術。
45	地域情報プラットフォーム標準仕様書	財団法人 全国地域情報化推進協会が策定・公開している標準仕様書。
46	認証管理システム	認証連携を実現する上で中核となるシステム。ユーザ ID やその認証を管理する。