自治体クラウド開発実証に係る
標準仕様書（平成 22 年度版）

第 1.0 版

平成 23 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

総務省事業として平成 21 年度から進められた「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且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。

本「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として定めるものであるとともに、開発実証事業での取組成果を踏まえて、今後地方公共団地が自治体クラウドの導入を検討する際に参考となる内容についても併せて記述する。

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、現在は総務省が自治体クラウドの導入促進を進めるために設立した自治体クラウド推進本部でもその推進が図られている。

「自治体クラウド開発実証事業」は、総務省により平成 21 年度から進められている施策であり、北海道、京都府及び佐賀県の 3 県は、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データバックアップサーバ、仮想化されたサーバ空間等を新たに構築し、大分県、宮崎県及び徳島県は ASP・SaaS 事業者からのサービス提供の形態で業務システム等を移行してクラウド化し、総務省が選定した「自治体クラウドプロジェクト管理事業者」からの指示等を踏まえ実証実験を進めてきた。

なお、実証団体は、北海道管内 29 市町村、京都府 25 市町村、佐賀県 6 市町村、大分県 5 市町村、宮崎県 5 市町村及び徳島県 8 市町村の計 78 団体である。

一方、財団法人地方自治情報センターは、自治体クラウド開発実証事業における「データバックアップサーバ」等の基盤を構築するための指針となる「標準仕様書」を作成して実証団体へ提示することとなっており、平成 21 年度から継続して事業を行ってきた。

平成 21 年度は、実証団体に対する説明会や自治体クラウド部会[1]を通して各実証団体の取組の情報提供を受け、「自治体クラウド開発実証事業に係る標準仕様書(平成 21 年度版)」として取りまとめを行った。

また、平成 22 年度は、昨年度作成した「自治体クラウド開発実証事業に係る標準仕様書 平成 21 年度版」について、実証団体からの実証実験での取組結果や標準仕様書への要望等をヒアリングし、その結果を本書「自治体クラウド開発実証事業に係る標準仕様書(平成 22 年度版)」として改訂を実施した。

なお、財団法人地方自治情報センターは、平成２２年度自治体クラウド・共同アウトソーシング移行促進事業において、「自治体クラウド開発実証事業に係る標準仕様書　平成 21 年度版」に準拠した自治体クラウドの構築及び業務システムの共同化を実施する団体を公募し、３グループ（留萌地域電算共同化推進協議会、福井坂井地区広域市町村圏事務組合、奈良県基幹系システム共同化検討会）に市町村の取組に係る経費を助成した。(参考資料参照)

[1] 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。

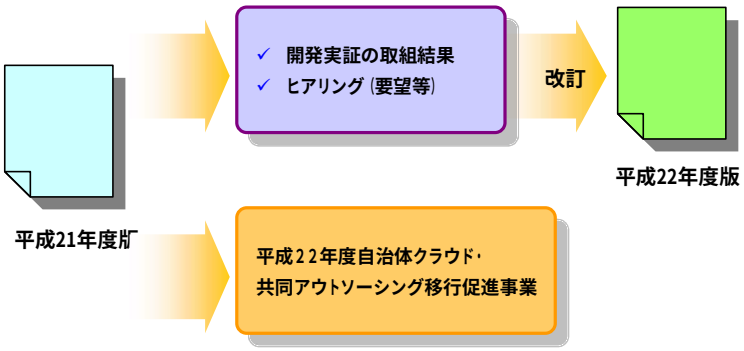


図 1-1　標準仕様書の改訂と移行促進事業

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図 1-2 のとおり。

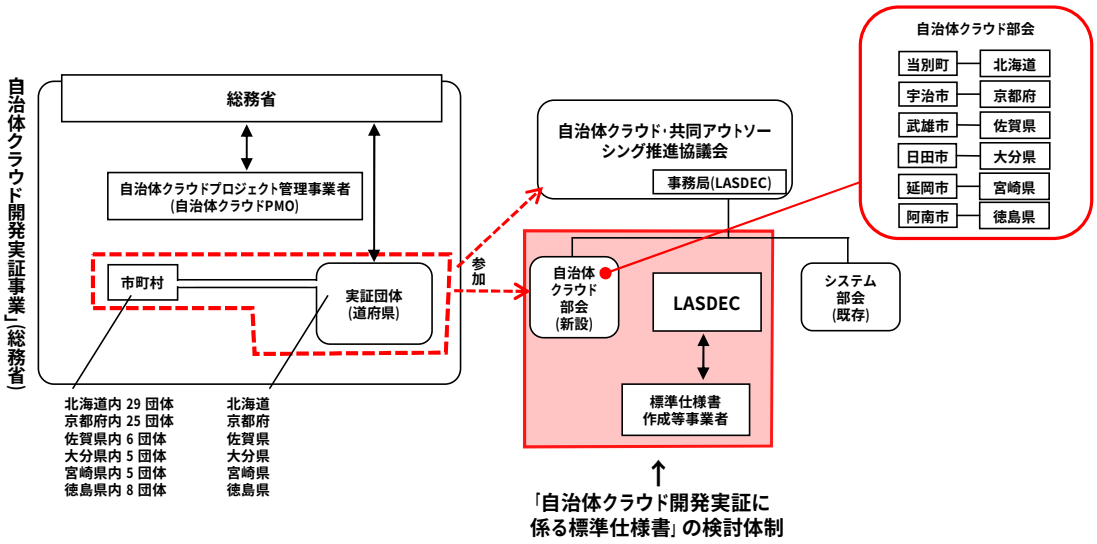


図 1-2　検討体制

1.3 自治体クラウド標準仕様書に関する説明会

平成２１年度の標準仕様書の作成に当たっては、自治体クラウド部会の開催に先立ち、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、標準仕様書の内容について随時の調整を図った。

【平成２１年度】
- 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

1.5 実証団体ヒアリング

平成２２年度版の作成に当たっては、以下の期間で実証団体（宮崎県、北海道、大分県、佐賀県、京都府、徳島県）を訪問し、実証実験の取組結果を踏まえた標準仕様書の改訂要望等についてヒアリングを実施した。

【ヒアリング実施期間】
平成２２年１２月６日(月) ～　平成２２年１２月２０日(月)

2. 基本方針

本書は、「自治体クラウド開発実証事業」の標準仕様として記述すべき内容に加え、自治体クラウドを取り巻く環境、さらに開発実証事業での取組成果を踏まえ、以下３つのポイントを考慮して記述する。

(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 年度から実証団体が取り組んできた内容、さらに実証実験のプロセス及び結果から明らかとなった事項等を踏まえて標準仕様を記述する。

(2) クラウド技術の実現可能性

クラウド技術については、サーバの仮想化のように既に多数の実績があるものから、今後採用の拡大が期待されるものまで多様な技術が存在しており、その技術革新のスピードには目を見張るものがある。そこで本書では、現時点でのクラウド技術の実現可能性を考慮し、加えて今後行政情報システムへ採用が期待されている技術等も踏まえて標準仕様の記述を行う。

(3) 自治体クラウドの特性考慮

自治体クラウドは、地方公共団体が業務システム等をクラウドサービスへ移行して利用するものであり、その導入に当たっては、セキュリティや災害時の業務継続計画(BCP)等も含め、地方公共団体ならではの考慮点も多い。そこで本書では、このような自治体クラウド特有の考慮点を加味して標準仕様の記述を行うとともに、導入の検討に当たっての留意点等も併せて記述する。

3. 本書の記述範囲

本書での記述範囲及び本書を利用する対象者を図 3-1 に示す。

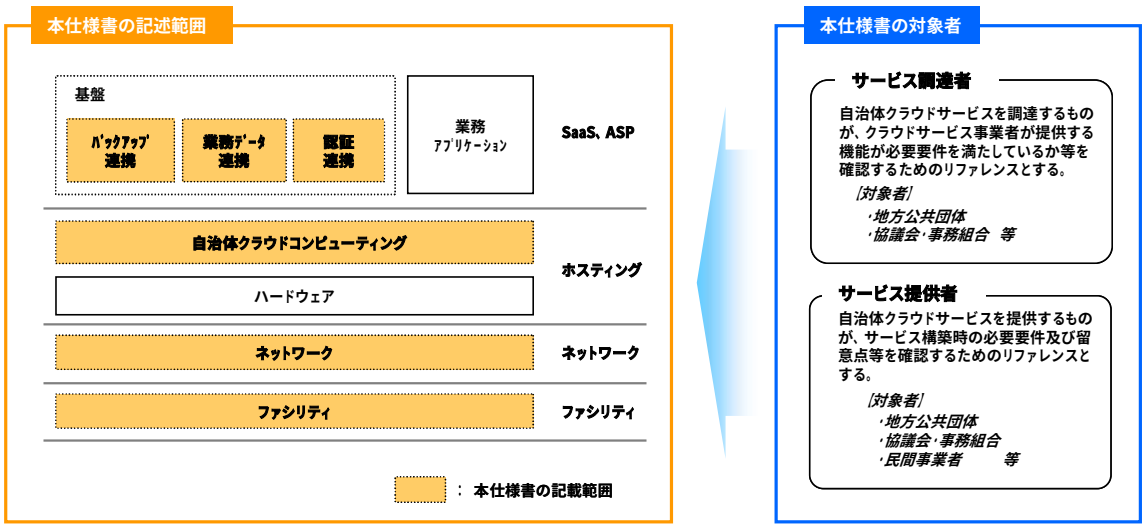


図 3-1 本書の記述範囲と対象者

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を記述したものであり、地方公共団体や ASP・SaaS 事業者から提供される業務アプリケーションについては、記述対象外とする。また、ハードウェアについても、地方公共団体の規模、業務アプリケーション及びサービス提供形態等により決定されるものであり、一般的な仕様を記述することが難しいことから、併せて記述対象外とする。
その他記述範囲の各項目の詳細については、4 章を参照されたい。

本書を利用する対象者としては、自治体クラウドサービスを提供する「サービス提供者」、自治体クラウドサービスを調達する「サービス調達者」を想定する。サービス提供者としては、地方公共団体、協議会・事務組合等の公的な組織が自治体クラウドサービスを提供する場合と、民間事業者が自治体クラウドサービスを提供する場合の２つを想定する。サービス調達者については、自治体クラウドサービスを選定、調達してサービスの提供を受ける地方公共団体、協議会・事務組合等（エンドユーザである自治体職員ではない。）を想定している。
サービス提供者がサービスを構築、提供するに当たって、またサービス調達者が自治体クラウドサービスを選定･調達するに当たって、要件や機能の充足度等の確認に本書を活用することを期待する。

なお、自治体クラウドは、LGWAN-ASP の形態で提供されるケースが多いと想定されるが、その場合は、LGWAN-ASP として要求事項をまとめた「総合行政ネットワーク ASP ガイドライン」等をはじめとする各種ドキュメントの遵守事項に従うことが必要となることに留意が必要である。

4. 標準仕様

4.1 ファシリティ

4.1.1 ファシリティ（データセンター）要件

4.1.1.1 概要

（1）目的

住民・企業等に関する重要情報を保護するため、データセンター（以下 DC という。）に必要な要件として、セキュリティ対策、災害対策などのファシリティ要件を整理する。

（2）適用範囲

ファシリティの適用範囲を図 4-1 に示す。

図 4-1 ファシリティの適用範囲

本仕様が対象とする範囲は図 4-1 に示すとおり、都道府県域 DC、ASP・SaaS 事業者の DC とする。

4.1.1.2 要件一覧

ネットワークの要件を表 4-1 に示す。

表 4-1　ファシリティの要件一覧

項番	要件	内容
1	法令	日本国内法の適用及び業務毎の関係法令を遵守。
2	セキュリティ対策	DC のセキュリティに対する対策要件。
3	災害対策	DC の災害（地震、停電、火災等）に対する対策要件。

4.1.1.3 機能

（1）法令

自治体クラウドのサービスを提供する場合、サービス提供者は、その取り扱う情報の重要性･機密性から日本国内法が適用される国内に DC を設置する必要がある。

また、サービス調達者は、自治体クラウドでサービスされる各種業務の法律、政令、省令、技術的基準及び条例に定められた条件を満たす DC 及び事業者を選定する必要がある。

（2）セキュリティ対策

「ASP・SaaS における情報セキュリティ対策ガイドライン」等、公共サービス向けのガイドラインを参照し、要件とされる以下の条件を満たす DC を利用すること。

ア　入退出管理

サーバ室等への入退出を管理･記録するため、本人認証を実施していること。

イ　鍵の管理

サーバ室への出入口及びサーバラック等の鍵を定められた場所に保管し、管理は特定者により行われていること。また、台帳等により鍵の貸出・返却が記録されていること。

ウ　監視

監視カメラを設置し、撮影された映像を一定期間保存すること。監視カメラの設置に当たっては、死角のないように設置されていることが望ましい。

エ　破壊対策

サーバ室への出入口には十分な強度を持つ防火扉を設置し、破壊等による不正侵入が防止されていること。

オ　警備

警備員を常駐させていること。

これらの対策に加えて、情報セキュリティマネジメントシステム（ISO/IEC 27001）等、国際標準の認証を取得している事業者の DC を利用することが望ましい。また、サービス調達者が定期的にサービス提供者のセキュリティ対策の実施状況を確認するため、訪問可能な DC を選定すること。

（3）災害対策

「ASP・SaaS における情報セキュリティ対策ガイドライン」等、公共サービス向けのガイドラインを参照し、要件とされる以下の条件を満たす DC を利用すること。

ア　電源の維持

自治体クラウドのサービスを提供する機器等を設置する場合は、停電や電力障害が生じた場合に電源を確保するための対策を講じられていること。

イ　火災、避雷、静電気からの防護

自治体クラウドのサービスを提供する機器等を設置する場合は、火災報知・通報システム及び消火設備が設置されていること。加えて消火設備の使用による汚損の対策が講じられていること。

また、避雷、静電気からの防護のための対策を実施されていること。

ウ　建物の災害対策

自治体クラウドのサービスを提供する機器等を設置する建物については、地震・水害に対する対策を講じられていること。

エ　空調

自治体クラウドのサービスを提供する機器等を設置する場合は、設置されている機器等による発熱を抑えるために十分な容量の空調が設置されていること。

4.1.1.4 留意事項

上記の各種対策が行われていることに加えて、自治体クラウドにおいては、事業の継続性・機密性が求められることから、サービス調達者は、サービス提供事業者がサービスを継続して提供できる運用体制を構築できているか確認する必要がある。

LGWAN-ASP によりサービスを提供する場合は、「総合行政ネットワーク ASP ガイドライン」等に示す各種規定・約款に準拠する必要がある。なお、LGWAN-ASP におけるファシリティサービス提供者として認定されている DC を利用する場合は、これらの規定・約款に準拠している。

4.2 ネットワーク

4.2.1 ネットワーク要件

4.2.1.1 概要

（1）目的

自治体クラウドのサービスを実施する場合、各都道府県域 DC、ASP・SaaS 事業者及び地方公共団体庁内をつなぐセキュリティの高いネットワークが必要となる。ここでは、自治体クラウドのサービス実施に必要なネットワーク要件を整理する。

（2）適用範囲

ネットワークの適用範囲を図 4-2 に示す。

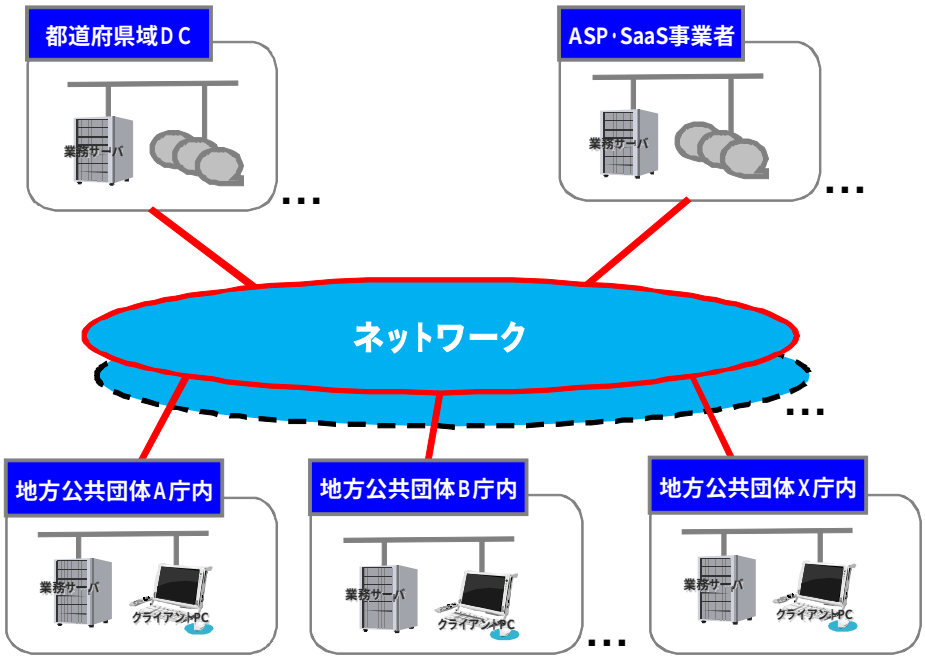


図 4-2 ネットワークの適用範囲

本仕様が対象とする範囲は図 4-2 に示すとおり、各都道府県域 DC、ASP・SaaS 事業者及び地方公共団体庁内をつなぐセキュリティの高いネットワークとする。

4.2.1.2 要件一覧

ネットワークの要件を表 4-2 に示す。

表 4-2　ネットワークの要件一覧

項番	要件	内容
1	通信	性能 ・ 円滑に業務の実施ができるよう、十分な帯域確保並びに障害時における代替ネットワークとの連携が可能なこと。 セキュリティ ・ 他のネットワークサービスの影響を受けることが無いよう、閉域性を保つこと。 広域性 ・ 地方公共団体を収容可能な通信網を提供できること。 拡張性 ・ 将来の帯域増大や異なるプロトコルに対しても、柔軟に対応できること。
2	運用	運用管理 ・ 国際標準に準拠した 24 時間 365 日の保守サービスを提供できること。 性能管理 ・ 性能管理を常に行うことで、安定した性能維持を提供できること。 障害対応 ・ 地方公共団体に対し、障害発生時早急に対応がとれること。 責任分界点 ・ 各都道府県域 DC、ASP・SaaS 事業者及び地方公共団体側との責任分界点を明確にすること。
3	SLA	サービスレベル ・ 適切な SLA を規定し、継続的な運用品質を確保できること。
4	その他	名前解決 ・ ネットワーク上に接続されている機器類を特定できる環境を備えていること。 電子メール ・ 地方公共団体に対し、電子メールによる連絡サービスが提供できること。 時刻同期 ・ ネットワーク上に接続されている機器類に対し、日本標準時刻を正確に配信できること。

4.2.1.3 機能

(1) 通信

ア 性能

(ｱ) 帯域

将来的に予想される自治体クラウドのサービス利用者増加を想定して、各都道府県域 DC、ASP・SaaS 事業者及び地方公共団体庁内をつなぐネットワークの帯域性能は、業務に耐えられる範囲まで拡張できる必要がある。

(ｲ) 代替ネットワークとの連携

大規模な災害・事故などによる障害から回避するため、各地方公共団体が利用しているネットワークと連携し、サービス提供が継続できること。

イ セキュリティ

自治体クラウドのサービスに利用するネットワークは、不正アクセスなどのセキュリティインシデント予防の観点から、暗号化及び VPN などを用いた独立した閉域網とすること。また、侵入検知(IDS)を導入するなど、安定運用のための対策も考慮することが望ましい。

ウ 広域性

自治体クラウドのサービスを提供するにあたり、各地方公共団体が容易に接続可能となるよう、広域性をもったネットワークの提供が必要である。

エ 拡張性

(ｱ) 帯域増大への対応

将来の帯域増大に対応できる回線網を選択すること。

(ｲ) IPv6 アドレスへの対応

将来的に予想される IPv4 アドレス枯渇に対応するため、IPv4 アドレスと IPv6 アドレスとが共存した状態でのサービス提供及び移行を可能とすること。

(2) 運用

ア 運用管理

(ｱ) 国際標準準拠の運用管理業務

自治体クラウドのサービスは、長期に渡り安定した運用が要求されるため、特定のベンダに依存しない、ISMS 及び ITSMS(ISO/IEC20000/ITIL)等に基づく運用管理業務が提供できること。

(ｲ) 24 時間 365 日体制の保守

自治体クラウドのサービスは、各地方公共団体での利用ニーズを吸収するため、原則 24 時間 365 日の保守体制がとれること。

イ 性能管理

自治体クラウドのシステム全体の構成管理を実施することで、トラフィック情報などを継続的に監視し、適切なサービス維持ができること。

ウ 障害対応

自治体クラウドのサービスを利用する各地方公共団体近辺に保守事業所などを設けることで、障害発生時早急にサービス復旧に向けた対応がとれること。

エ 責任分界点

自治体クラウドのサービスは、各地方公共団体による共同利用が前提となるため、責任分界点を明確にすること。

（3）SLA

ア サービスレベル

(ｱ) SLA 規定による運用品質の確保

SLA を規定し、自治体クラウドのサービス品質を明確にすること。

(ｲ) 継続的な品質管理の実施

サービス品質向上を目的とした、リアルタイムのサービス状況の把握を行うことができること。併せて、分析・評価結果に基づき SLA の見直しを含めた運用の改善を行う。

（4）その他

ア 名前解決

自治体クラウドのサービスでは、各地方公共団体の共同利用に伴い名前解決を実施するため、DNS 環境を提供できること。

イ 電子メール

自治体クラウドのサービスを利用する各地方公共団体に対し、電子メールによる連絡サービスを提供することで、信頼性の高い情報共有の推進を図れること。

ウ 時刻同期

自治体クラウドのサービスでは、各地方公共団体の共同利用に伴い一括した時刻同期が必要となるため、NTP 環境が提供できること。また時刻情報は、信頼できる機関などから入手すること。

4.3 自治体クラウドコンピューティング（仮想化）

4.3.1 サーバ仮想化

4.3.1.1 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。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 4-3 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。

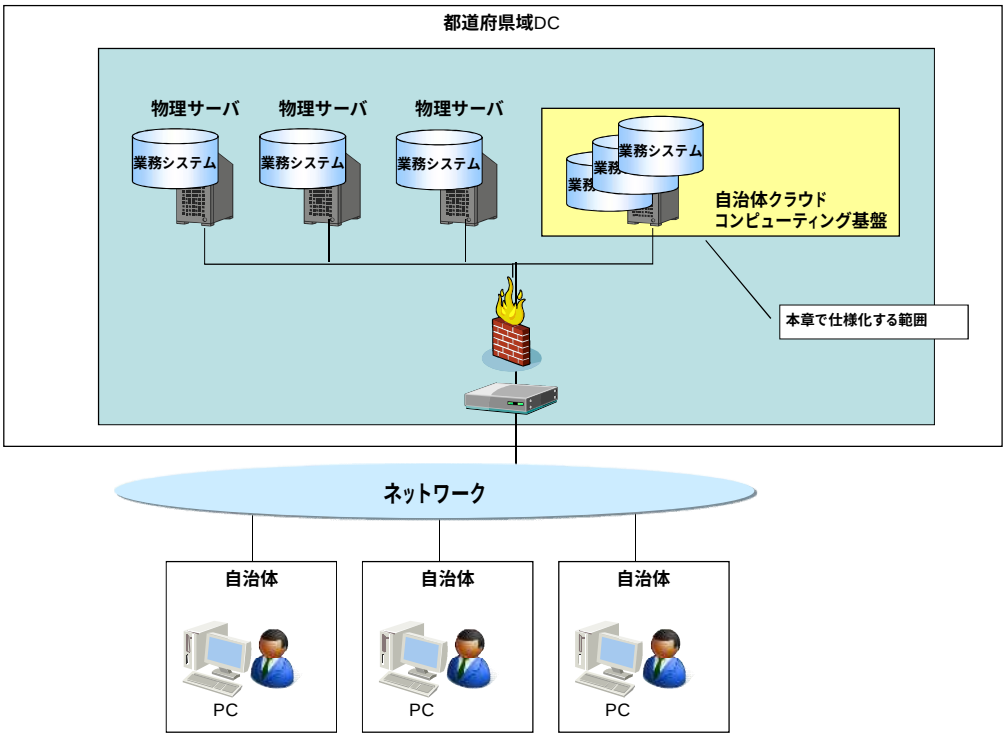


図 4-3　都道府県域 DC の実装イメージ

図 4-3 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。

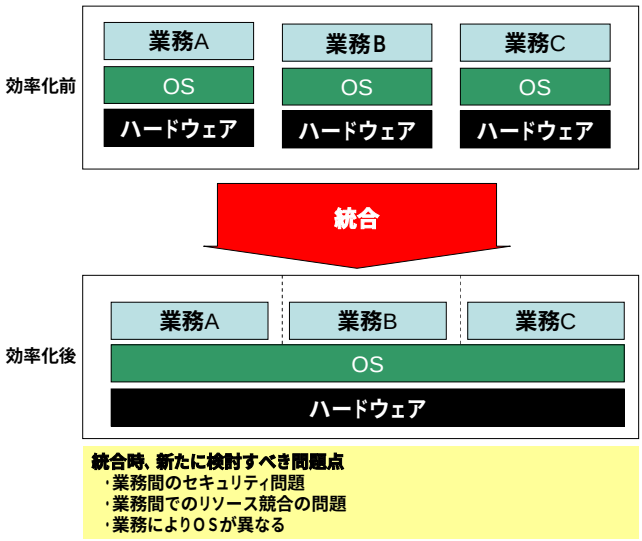


図 4-4　現状のハードウェア統合に対する課題

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。

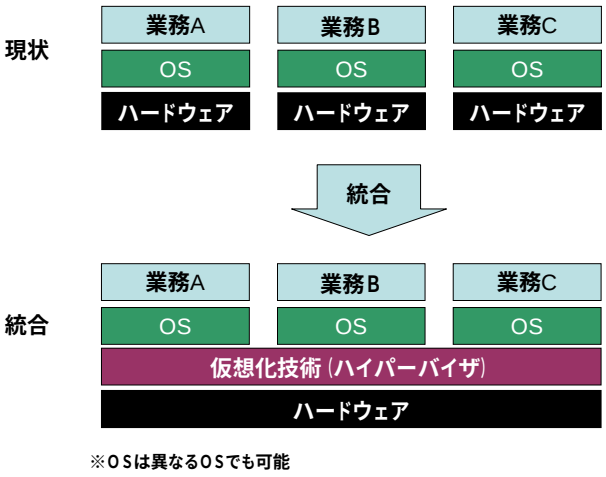


図 4-5　地方公共団体業務システムのハードウェア統合イメージ

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。

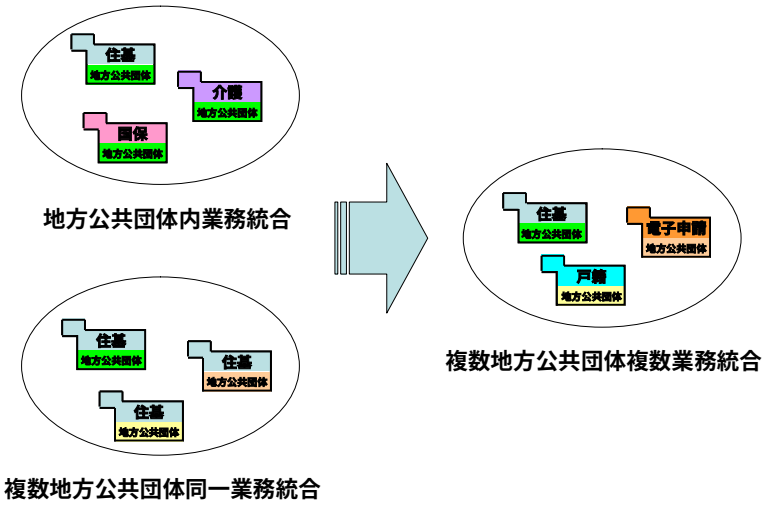


図 4-6　業務の段階的な統合

(2) 適用範囲

本節では都道府県域 DC で提供される、仮想化技術について記述する。適用範囲は、図 4-7 に示す仮想化サーバ部分とする。

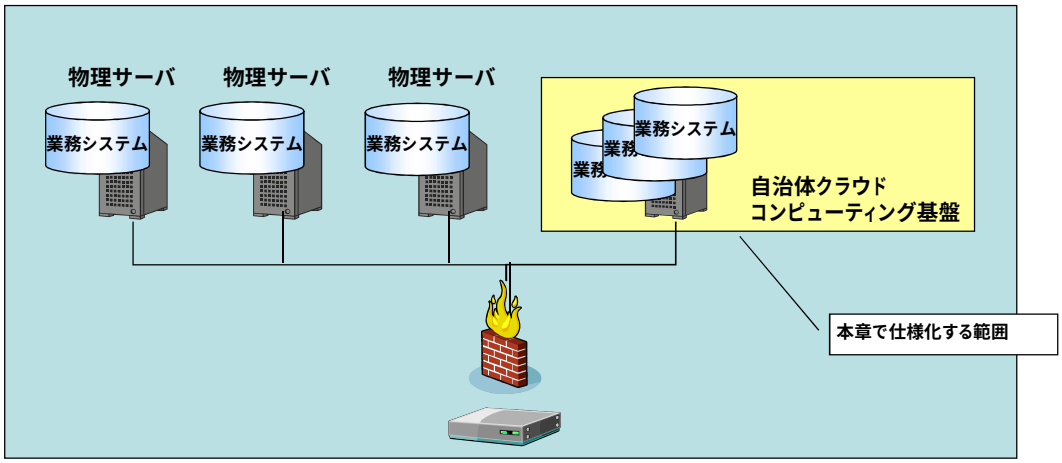


図 4-7　自治体クラウドコンピューティングの適用範囲

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 4-8 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 4-8 同一業務統合型

- 地方公共団体内業務統合型
  図 4-9 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 4-9 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 4-10 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 4-10 複数地方公共団体／多種業務統合型

(3) 制約事項

ア 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。

イ LGWAN-ASP **の制約**

都道府県域 DC で構築される業務システムを LGWAN-ASP として実装する場合、「総合行政ネットワーク ASP ガイドライン」等に従い構築されなければならない。

4.3.1.2 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 4-3 に示す。

表 4-3 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	静的マイグレーション	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機能。
4	動的マイグレーション	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働させる機能。
5	グリッド連携	複数のハードウェアをハイパーバイザにより集約することで、単独のハードウェアでは実現できないリソースを提供する機能。

4.3.1.3 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。

仮想化の特徴としては、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、下記アからオが挙げられる。

サーバの仮想化とは図 4-11 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 4-11　仮想化のイメージ

ア　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。

イ　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こと

  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。

ウ　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。

エ　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 4-12 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。

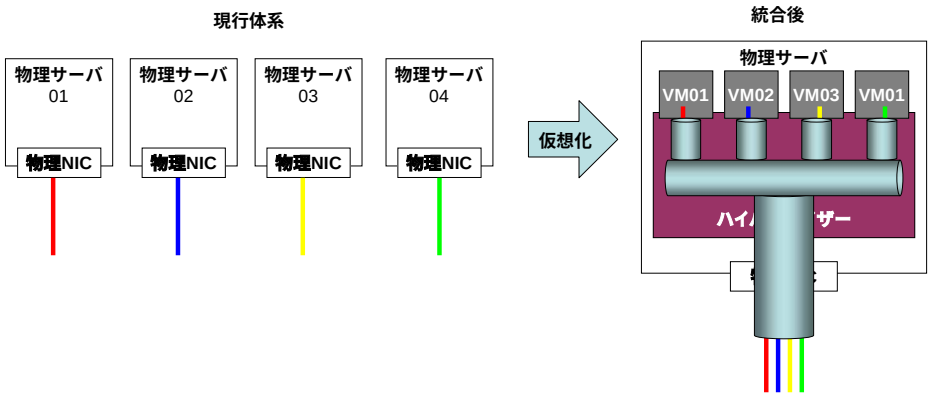


図 4-12　物理サーバへのアクセス集中

- 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。

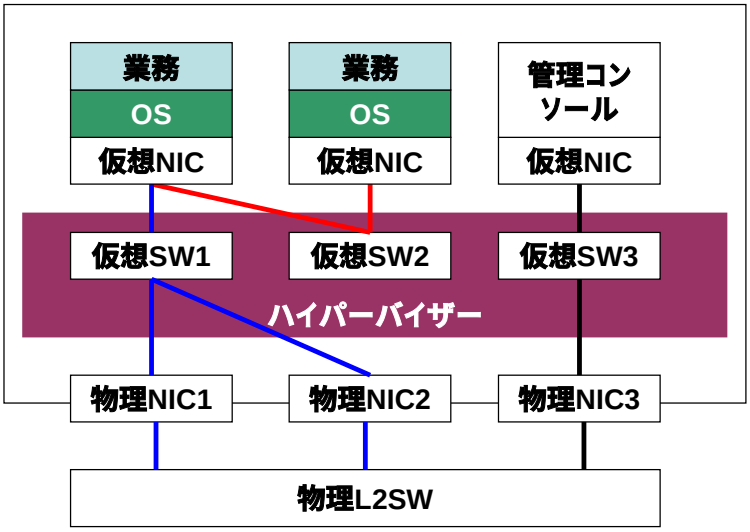


図 4-13　ネットワークの仮想化イメージ

オ　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。

(ｱ) 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。

(ｲ) 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。

(ｳ) 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。

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。

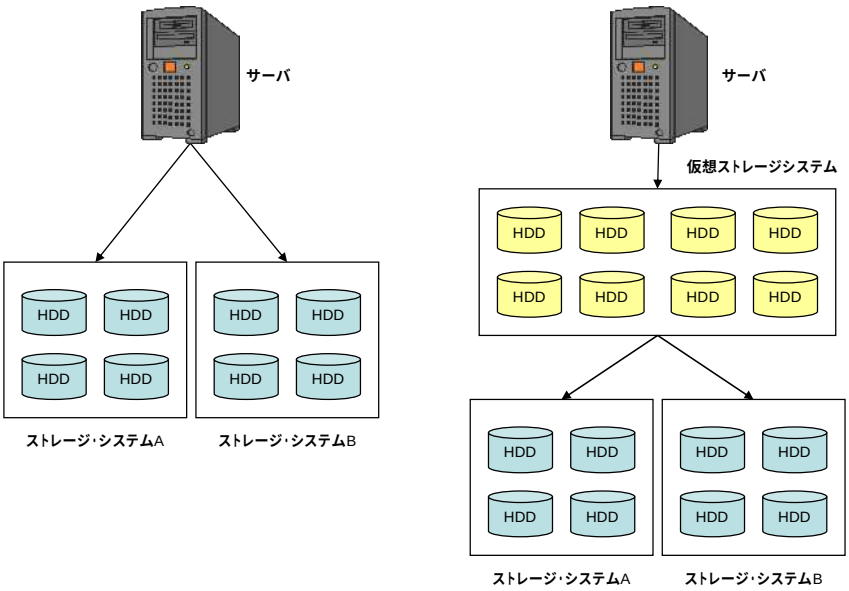


図 4-14　ストレージシステム筐体の境界をまたいだ統合

- 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。

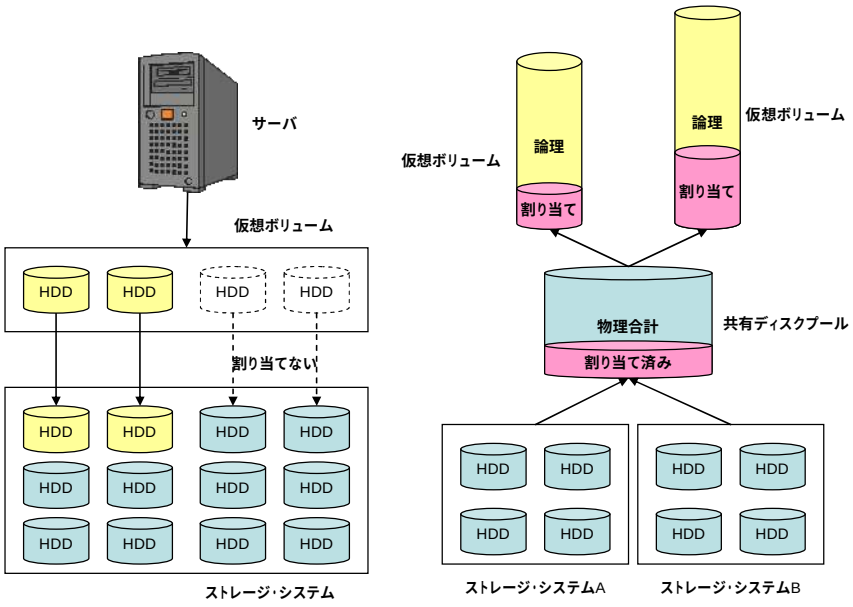


図 4-15　仮想プロビジョニング

- 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。

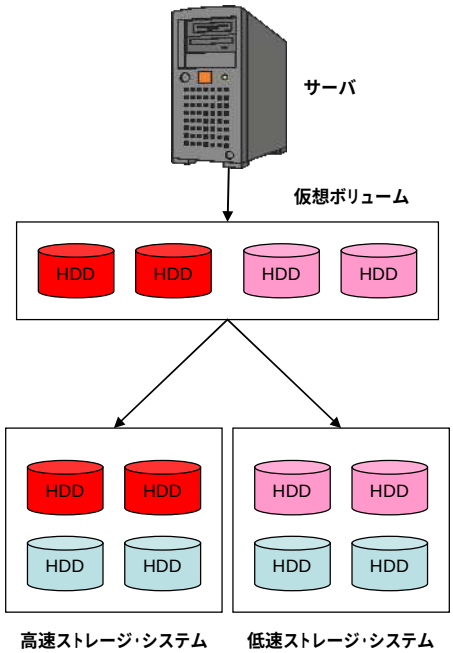


図 4-16　ILM

(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。

なお、LGWAN 上でサービスを展開する場合は、「総合行政ネットワーク ASP ガイドライン」等に準拠する必要がある。

ア 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 4-4 に示す。

表 4-4　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。

イ 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、OS のアップデート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。

ウ 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。

(ｱ) 物理サーバ間通信のセキュリティ

必要に応じて、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、外部ネットワークのアクセス制御を行う必要がある。

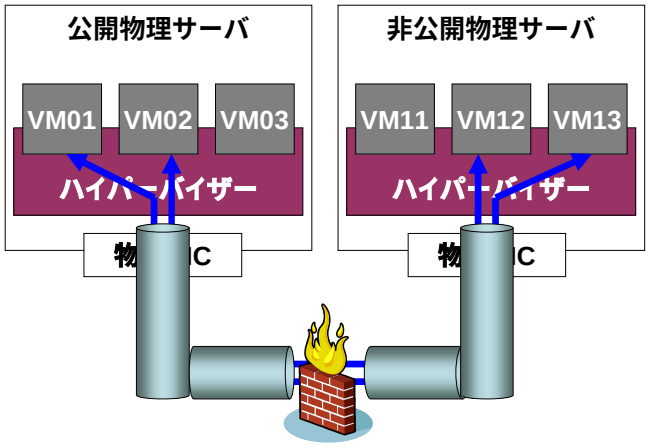


図 4-17　物理サーバ間通信のファイアウォール構成例

(ｲ) 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 4-17 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、図 4-18 に示す 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。

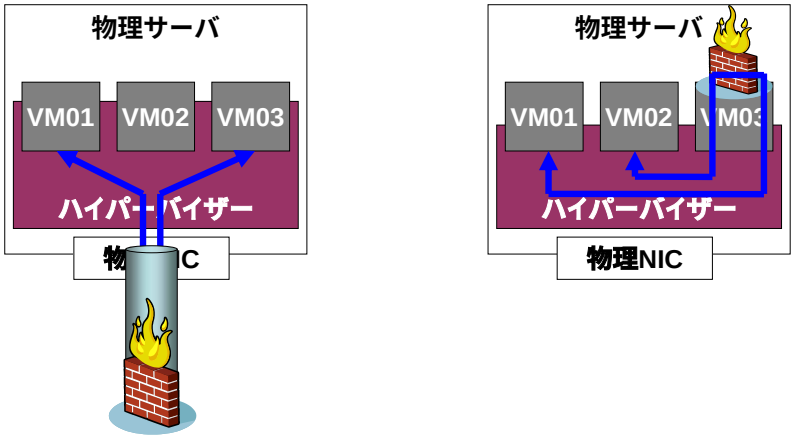


図 4-18　VM 間通信のファイアウォール構成例

エ 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) 静的マイグレーション

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。

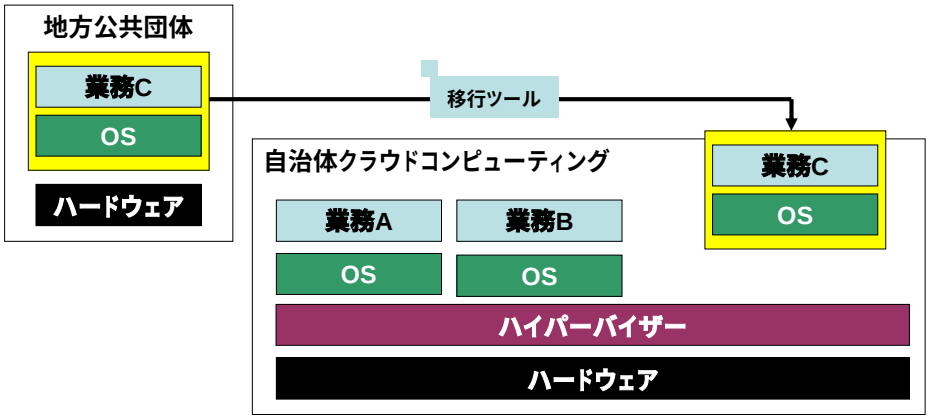


図 4-19 静的マイグレーション（例）

ア 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。

(ｱ) 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。

(ｲ) 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。

(ｳ) ネットワーク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、ネットワークを経由した外部との通信が発生する。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 等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。

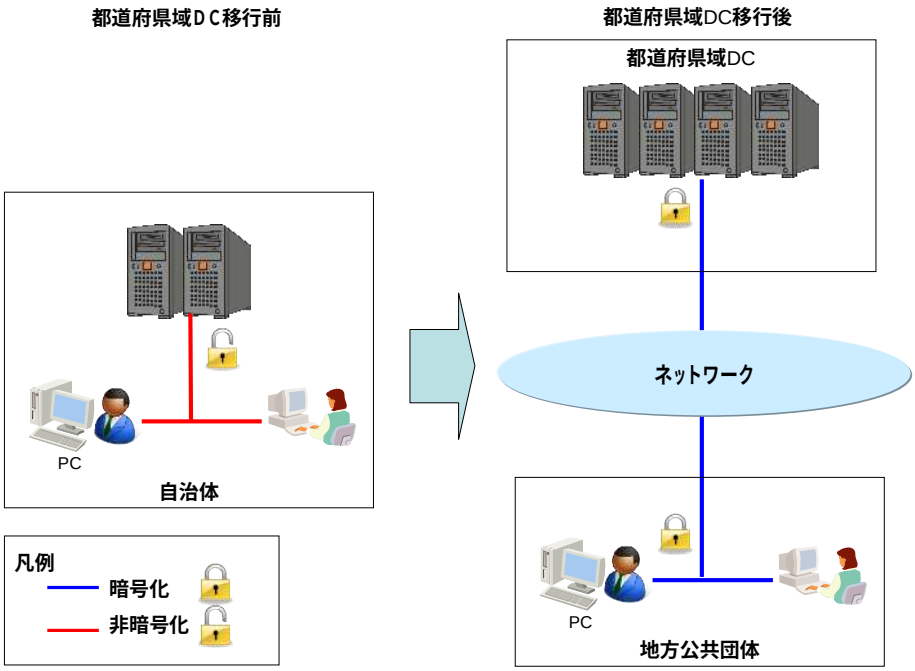


図 4-20　都道府県域 DC 移行前後の通信イメージ

(ｴ) ソフトウェア保守関連の留意事項

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) 動的マイグレーション

ア　動的マイグレーション（データセンター内）の概要

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。

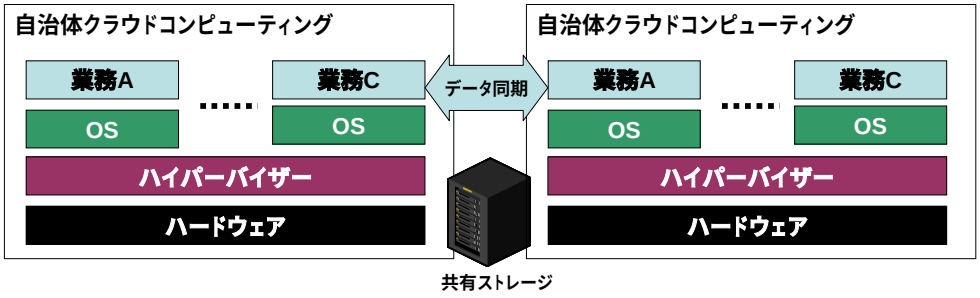


図 4-21　動的マイグレーション

イ　動的マイグレーション（データセンター間連携）の概要

図 4-22 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。

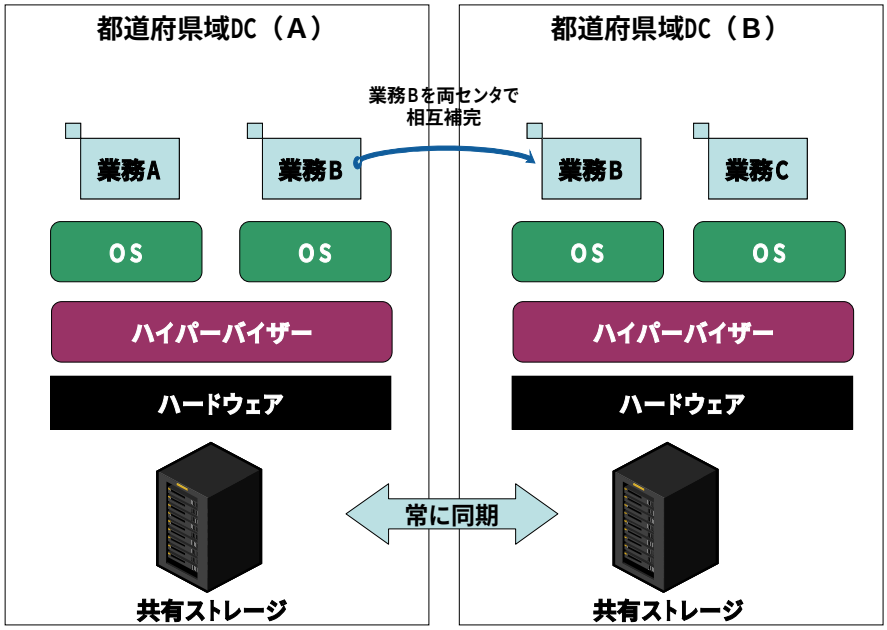


図 4-22　業務システム補完運用のイメージ

(ｱ) 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。ネットワーク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。

(5) グリッド連携

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 4-23 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、人口規模の大きい地方公共団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。

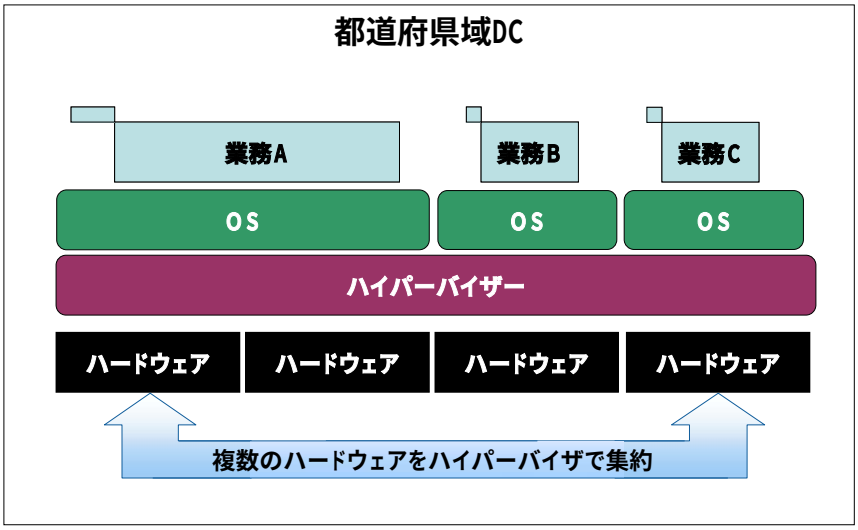


図 4-23　グリッド連携イメージ

ア　グリッド連携の留意事項

(ｱ) LGWAN の制約

LGWAN-ASP としてグリッド連携を実現する場合においては、「総合行政ネットワーク ASP ガイドライン」等に準拠する必要がある。

(ｲ) 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。

4.4 認証連携機能

4.4.1 同一自治体内でのシングルサインオン

4.4.1.1 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、適切に使い分けて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、その管理の煩雑さのため、ユーザがパスワードをメモに書き残す等、安全管理上の問題につながる可能性が懸念される。

このような問題を解決する対策の 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し、一度のログイン動作で複数の業務アプリケーションを利用できるシングルサインオンがある。このシングルサインオンを導入することにより、ユーザの利便性や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となる（図 4-24）。

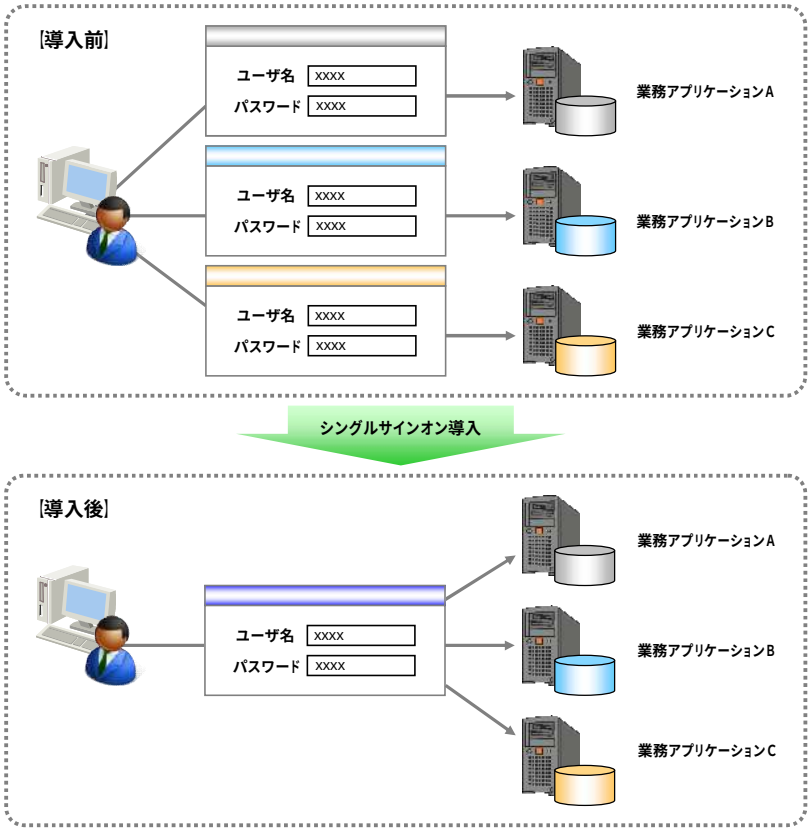


図 4-24　異なる業務アプリケーション間でのシングルサインオンの概念

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且つ安全に自治体クラウドの複数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

同一自治体内でのシングルサインオンの適用範囲を図 4-25 に示す。

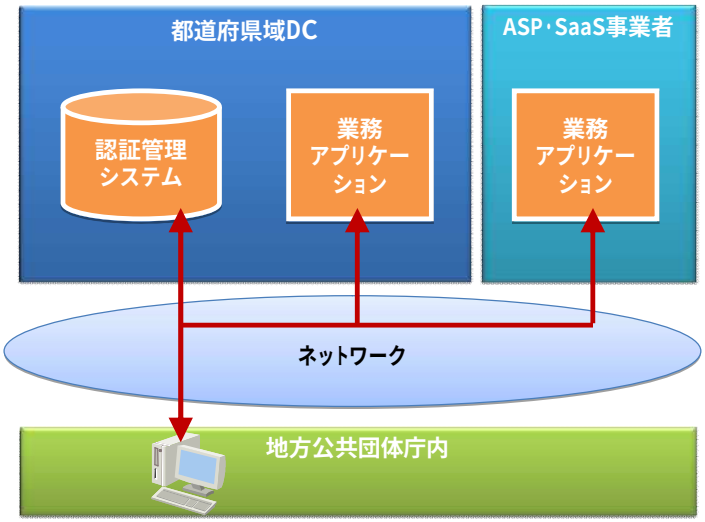


図 4-25　同一自治体内でのシングルサインオンの適用範囲

本仕様が対象とする範囲は、図 4-25 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、地方公共団体庁内のユーザ端末や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場合、セキュリティリスクも重要な考慮点の一つとなる。

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、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もある。

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、その結果として、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ことに注意が必要である。

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。

4.4.1.2 要件一覧

同一自治体内でのシングルサインオンの要件を表 4-5 に示す。

表 4-5　認証連携機能の要件一覧

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を許可する。
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を担保する。
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を利用可能にする。

4.4.1.3 機能

本節では、表 4-5 で挙げた要件を実現するための機能を提示する。

（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行うものであり、以下の要件を満たすことを推奨する。

- ユーザは、ユーザ 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。
- 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）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

シングルサインオンを安全に行うためには、ユーザ認証だけではなく、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 として導入する場合は、「総合行政ネットワーク ASP ガイドライン」で求められる通信のセキュリティに準拠する必要がある。

(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。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。

ア　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、認証情報を連携すること。
- ユーザ認証後に IdP から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。

この方式の概要を図 4-26 に示す。

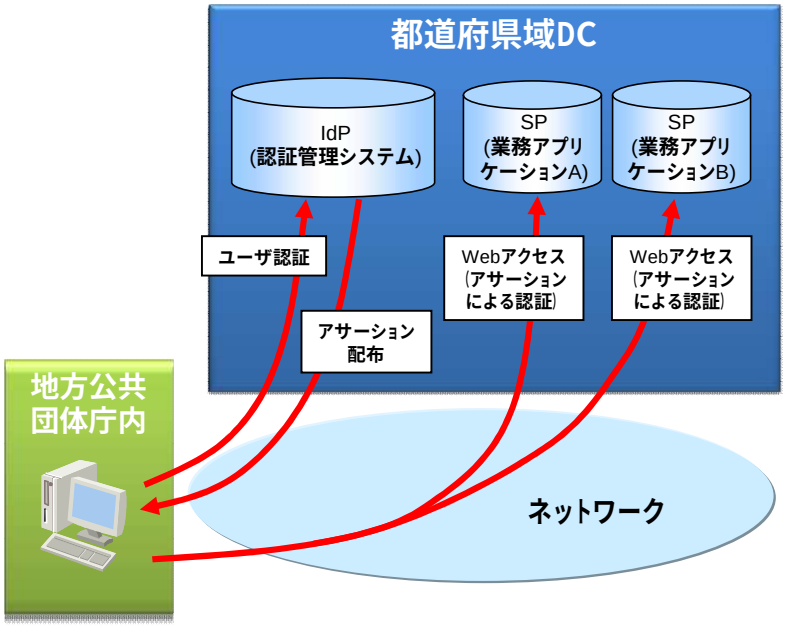


図 4-26　SAML を用いたシングルサインオン

イ　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。
- 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へログインできること。

【留意点】

- OpenID の方式は 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、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 のプライバシーに係る仕組みについては劣っており、導入に当たっては注意が必要である。

ウ　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へのアクセス経路上にリバースプロキシが介在してユーザ認証や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。

なお、リバースプロキシ方式では、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という特徴がある。

この方式の概要を以下の図 4-27 示す。

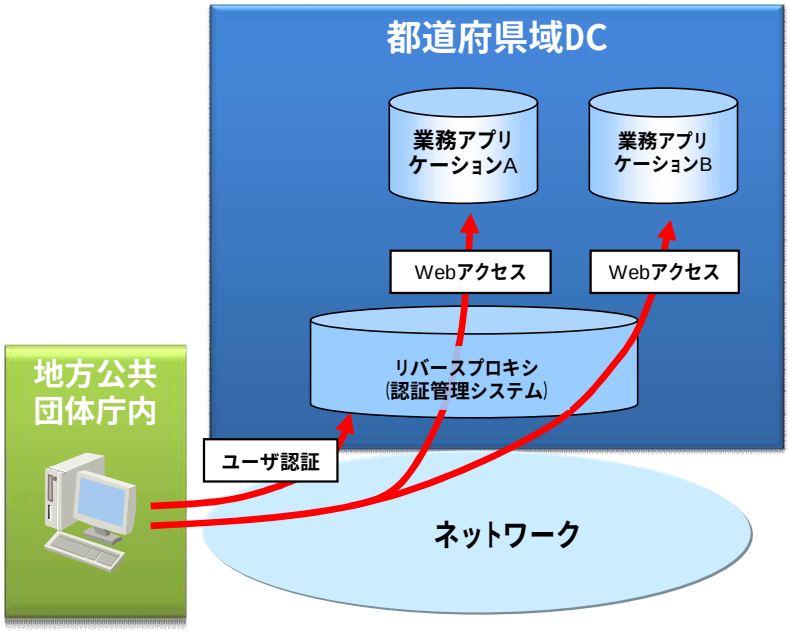


図 4-27　リバースプロキシを用いたシングルサインオン

【留意点】

- 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経由するため、ネットワーク構成の大きな制限となる。
- 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。

エ　Cookie を用いたシングルサインオン

OS 依存性を排除したシングルサインオンの手法として、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。

- 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 4-28 に示す。

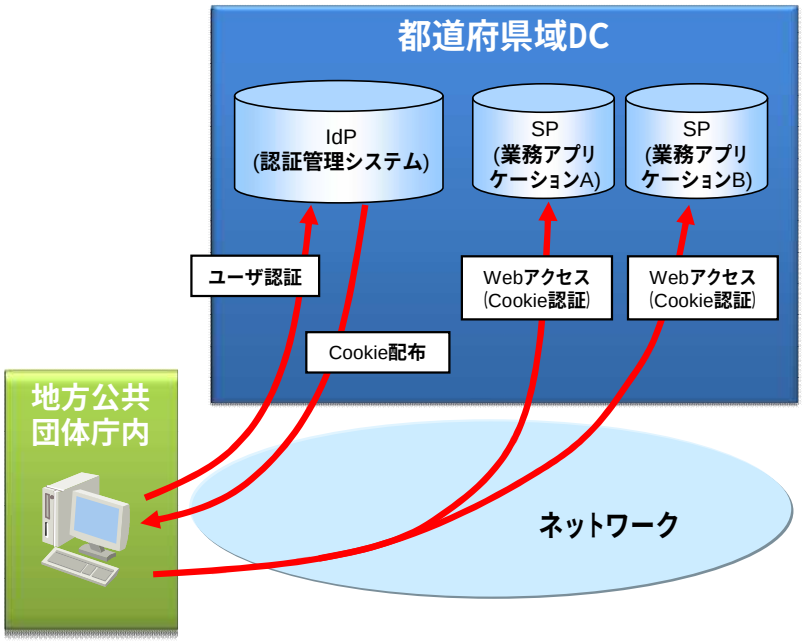


図 4-28　Cookie を用いたシングルサインオン

上記に取り上げたシングルサインオン方式には、それぞれ特長や考慮が必要な点があり、表 4-6 に一覧に示す。

表 4-6　シングルサインオン方式の比較

項番	方式	特長	考慮が必要な点
ア	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側の SAML 対応が必要である。
イ	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側の Open ID 対応が必要である。 ・ 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。
ウ	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である。
オ	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。

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、各方式のメリットとデメリットを検討した上で、実装を進める必要がある。

なお、将来的に地方公共団体間でシングルサインオンを実現する場合、方式のオープン性、セキュリティの強度等から 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。

4.4.2 クラウドサービス間でのシングルサインオン

4.4.2.1 概要

(1) 目的

本節では、今後各地方公共団体が幅広く認証連携機能を活用し、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として推奨される、クラウドサービス間でのシングルサインオンの仕様を記載する。

(2) 適用範囲

クラウドサービス間でのシングルサインオンの適用範囲を図 4-29 に示す。

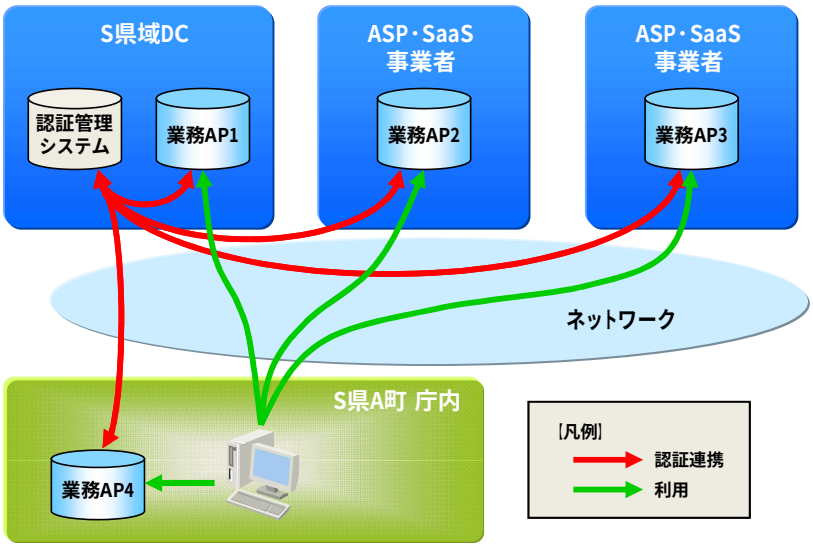


図 4-29　クラウドサービス間でのシングルサインオンの適用範囲

複数の ASP・SaaS 事業者等、異なるサービス提供者をまたぐ認証連携の実現が、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、ある市町村の原課が業務に応じて異なる ASP・SaaS 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、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・SaaS 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且つユーザ 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併せて考慮する。

4.4.2.2 要件一覧

クラウドサービス間でのシングルサインオンの要件を表 4-7 に示す。

表 4-7　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。
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にユーザ ID を隠蔽する。

4.4.2.3 機能

本節では表 4-7 で挙げた要件を実現するための機能を提示する。

(1) ユーザ ID の連携

図 4-30 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行う場合、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が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機能は、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 及び 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）の提供先が設定されていること。
- 各 SP にアサーションの取得先が設定されていること。

なお、ユーザ ID の管理（発行や削除など）は、通常は各サービス調達者の ID 管理者によって実施されるが、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。

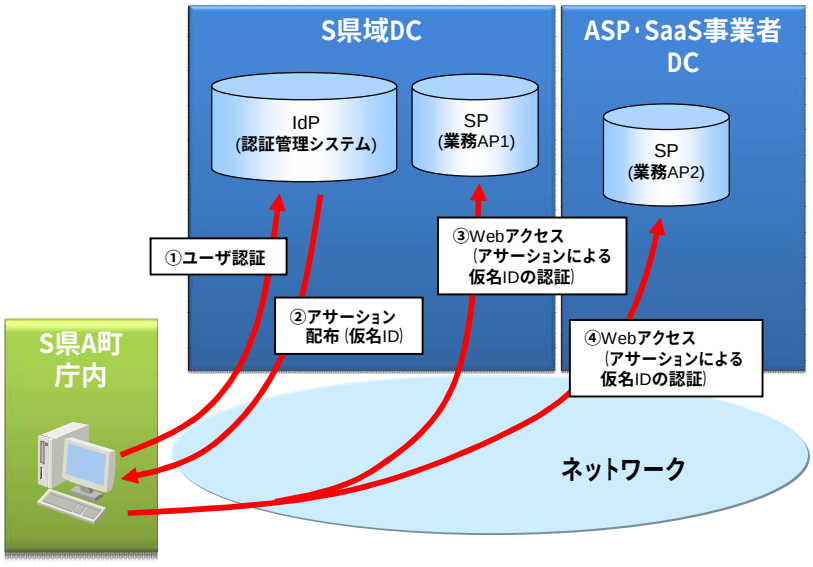


図 4-30　SAML を用いたクラウドサービス間でのシングルサインオン

（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、その結果として、各業務アプリケーションで保持しているユーザごとの操作履歴やプロファイル情報と簡単に割付けら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。

4.4.3 属性情報の連携

4.4.3.1 概要

（1）目的

本節では、クラウドサービス間でのシングルサインオンを前提とした、属性情報の連携の仕様を記述する。

（2）適用範囲

属性情報の連携の適用範囲を図 4-31 に示す。

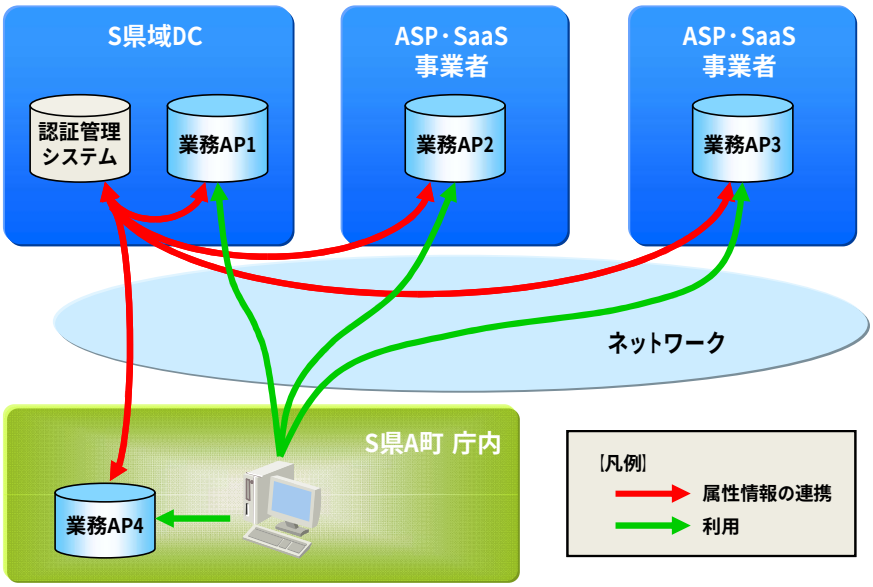


図 4-31　属性情報の連携の適用範囲

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）を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。

4.4.3.2 要件一覧

クラウドサービス間での属性情報の連携の要件を表 4-8 に示す。

表 4-8　クラウドサービス間での属性情報の連携の要件一覧

項番	要件	内容
1	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。

4.4.3.3 機能

本節では表 4-8 で挙げた要件を実現するための機能を提示する。

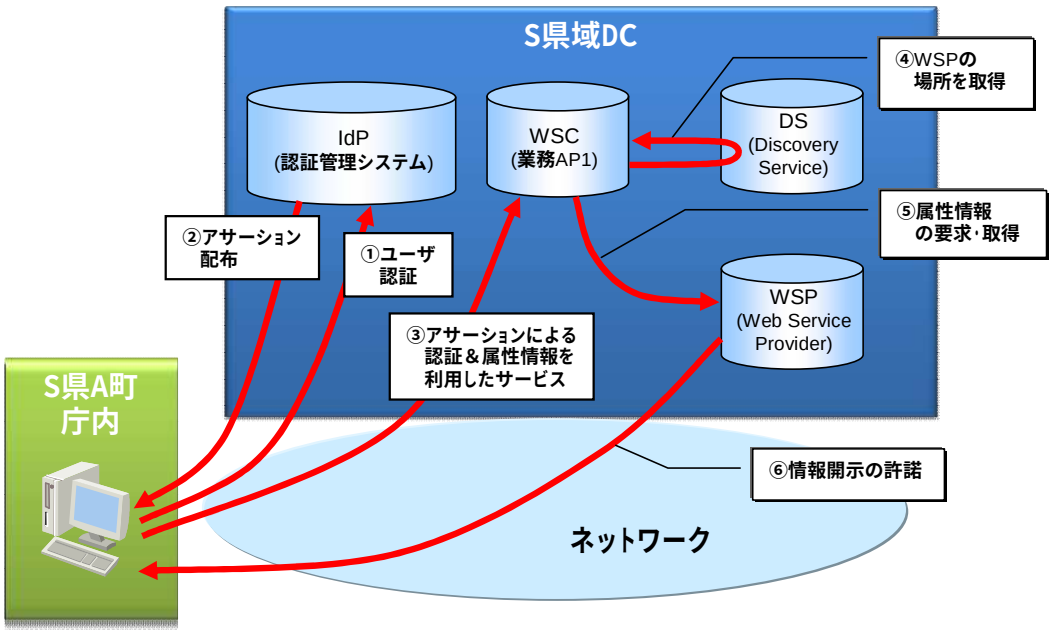
（1）属性情報の連携

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 では、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方式となる。

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 4-32 に示す手続きにて互いに連携動作を行う。



① 通常のSAMLの動作に従い、Idpでユーザ認証を行う。
② ユーザ認証後、Idpから配布されるアサーションを取得する。
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。

図 4-32　ID-WSF による属性情報の連携

このような ID-WSF による属性の連携により、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。

4.5 業務データ連携

4.5.1 業務データ連携要件

4.5.1.1 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（図 4-33 参照）。

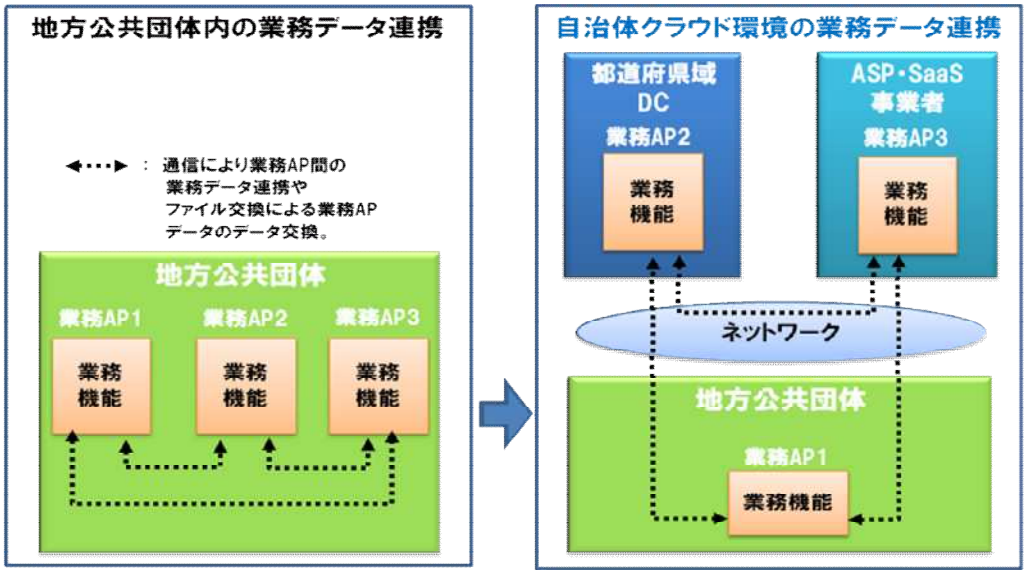


図 4-33　自治体クラウド環境の業務データ連携のイメージ

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）

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」（APPLIC-0010-2010）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 4-34 に示す。

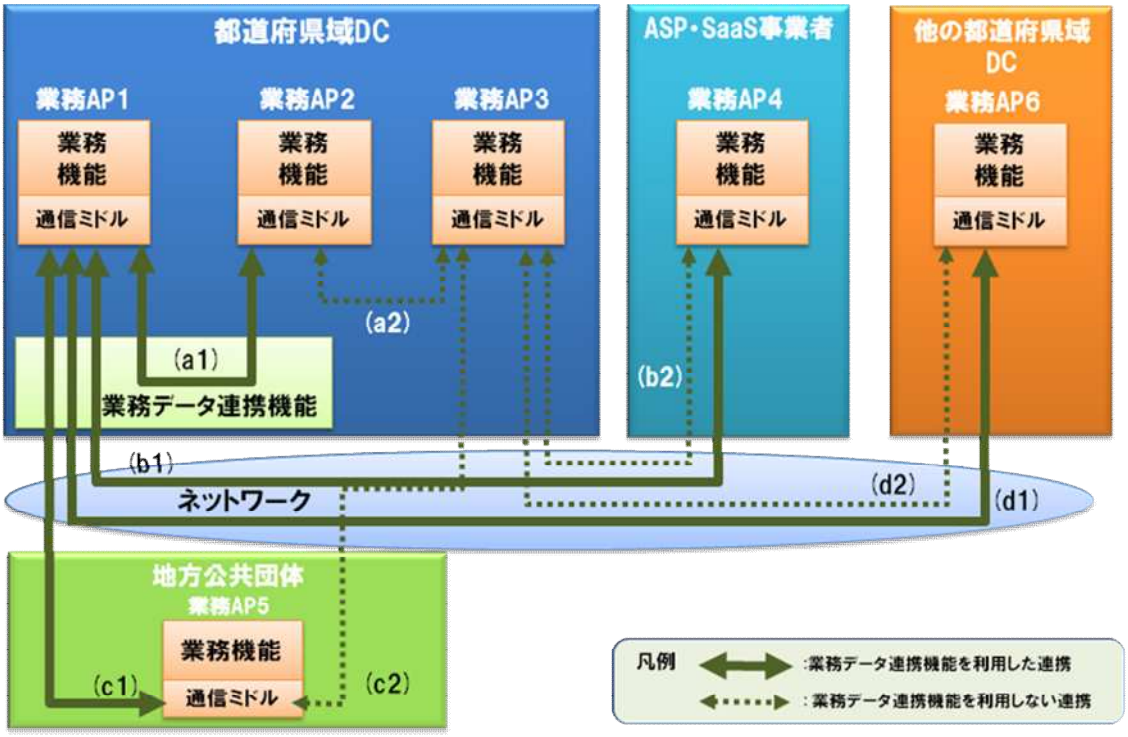


図 4-34　業務データ連携のユースケースと本節の適用範囲の概念図

表 4-9　業務データ連携のユースケースと本節の適用範囲

項番	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
		(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, d1）のユースケースについては、本節で記載する。

（3）業務データ連携機能を利用しない場合の留意事項

業務データ連携機能を利用しない場合（表 4-9 の a2, b2, c2, d2）のユースケースについては、本節の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 ごとに実装する際の留意事項について以下に示す。

ア　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。

イ　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ては、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。

ウ　そのほかの要件

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 が一つの場合、あるいは、オールインワンパッケージで提供され、且つ、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。

4.5.1.2 要件一覧

業務データ連携の要件を表 4-10 示す。

表 4-10　業務データ連携の要件一覧

項番	要件	概要	ユースケース（※1）				
			a1	b1	c1-1	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	セキュリティを確保したい場合は、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)	オフサイトへのアクセスが制限される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)	オフサイトへのアクセスが制限される場合のデータ取得（※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、公開されている NTP サービスを利用して同期を取ること。	○	○	○	○	○

【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、オフサイトへのアクセスが制限されない場合
(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、オフサイトへのアクセスが制限される場合
(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）

地方公共団体の通信セキュリティポリシーにより、外部からのアクセスを制限している場合、都道府県域 DC と地方公共団体庁内のオフサイトへのアクセスが制限される場合が想定される。このためユースケース c1 を c1-1 と c1-2 に分解する。アクセスが制限されない場合（c1-1）、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）オフサイトへのアクセスが制限される場合の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 4-35 に、業務 AP1 を都道府県域 DC 上の業務 AP、業務 AP2 を ASP・SaaS 事業者及び地方公共団体庁内の業務 AP とした場合の概念図を示す。

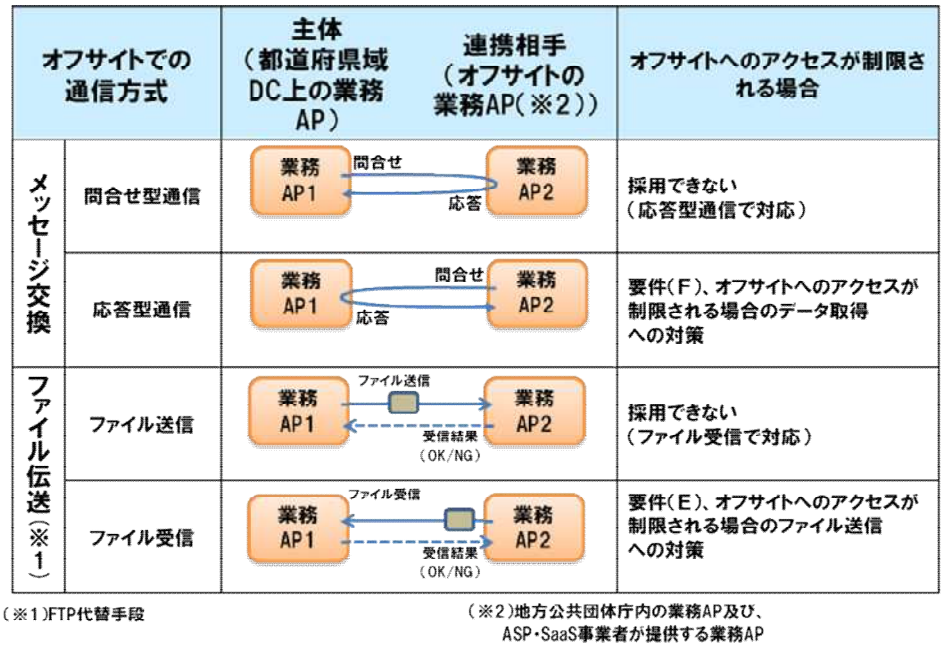


図 4-35　オフサイトのメッセージ交換とファイル伝送の 4 パターン

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 AP１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健康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 AP１が一定時間ごとにまとまったデータを業務 AP2 から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、オフサイトへのアクセスが制限される場合もあり、FTP プロトコルが使用できない場合の代替手段が必要となることもある。これを要件（D）に示す。

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できない場合の要件を要件（E）へ、オフサイトへのアクセスが制限されており、都道府県域 DC から地方公共団体庁内への問合せ型通信ができない場合の要件を要件（F）に示す。

4.5.1.3 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図 4-36 に示す。

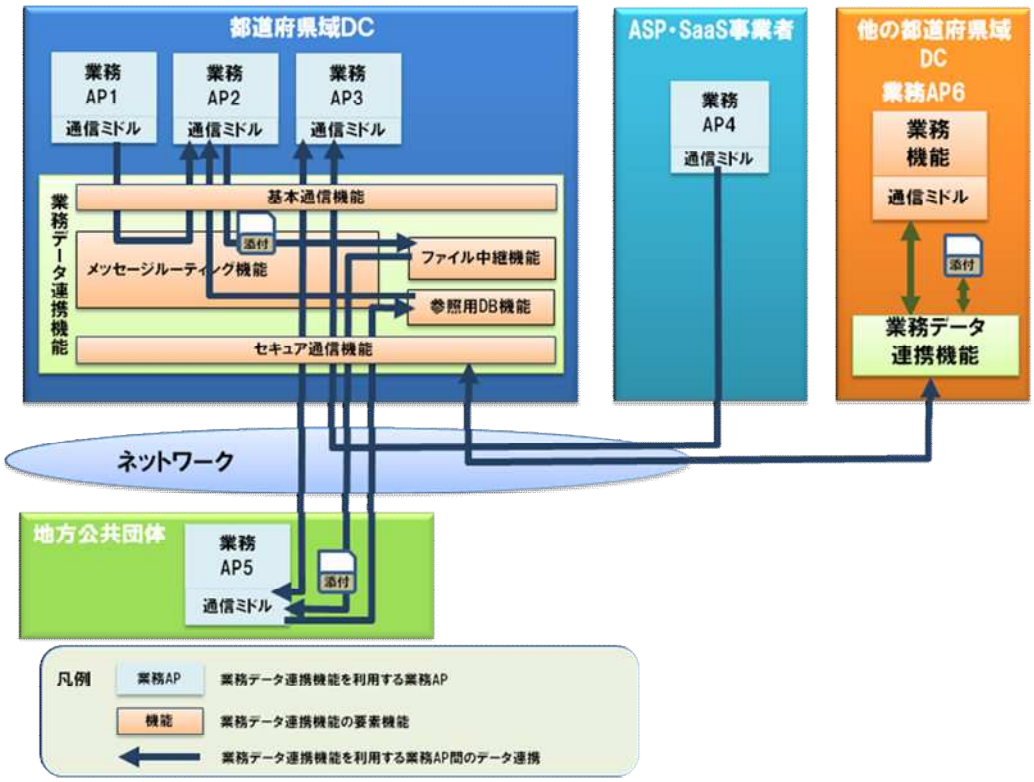


図 4-36　業務データ連携の概略アーキテクチャ

(2) 業務データ連携の構成要素である機能

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 4-10 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-0010-2010 である。

ア　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。

イ　セキュア通信機能

- SOAP 通信において、PKI 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。
- 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。

ウ　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。

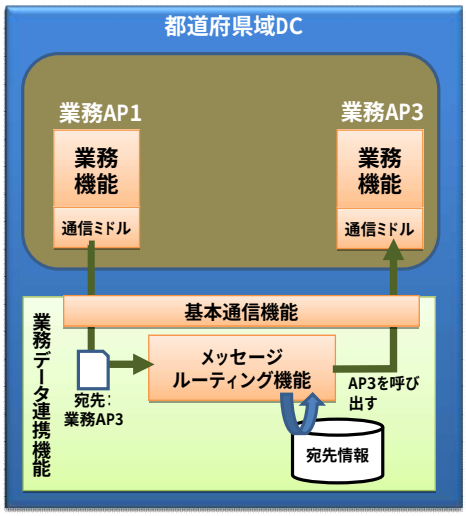


図 4-37　メッセージルーティング機能の例

- なお、他の都道府県域 DC 上の業務 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 上の業務 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。

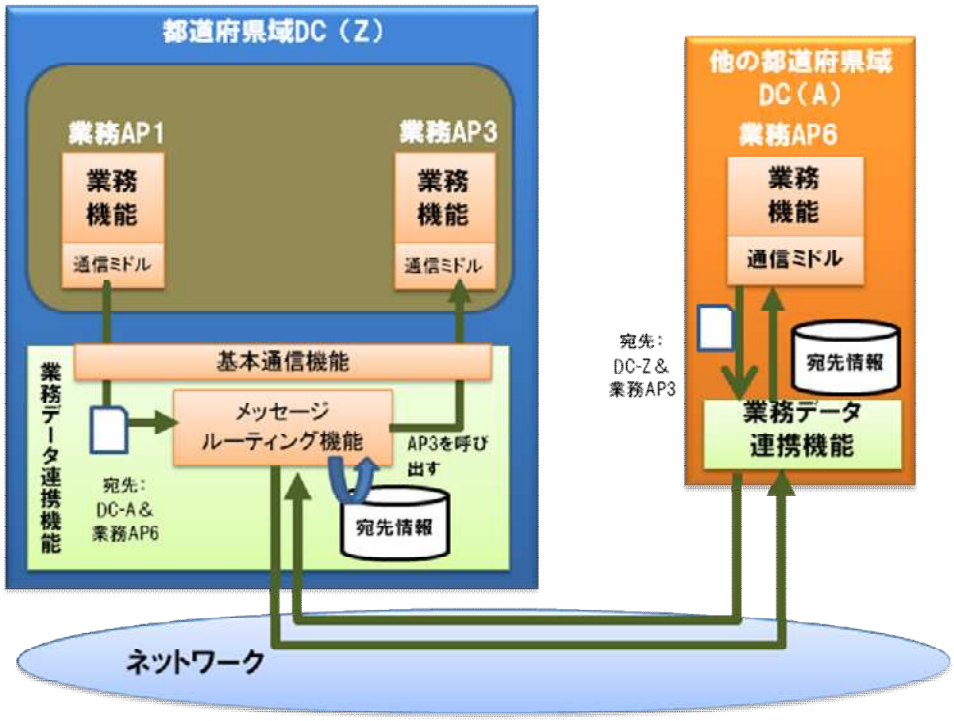


図 4-38　他の都道府県 DC 間のメッセージルーティング機能の例

エ　オフサイトのファイル伝送

- FTP プロトコルを利用する。ネットワークの通信制約等により、FTP プロトコルを利用できない場合は、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。
- 必要に応じて、セキュア通信機能を使って通信する。
- ネットワークの帯域を考慮し、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、一度に送付する業務データ量を減らすなどの運用設計を行う。

オ　オフサイトへのアクセスが制限される場合のファイル送信

オフサイトへのアクセスが制限されており、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できない場合、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。

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、「エ　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。
- 必要に応じて、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。
- ネットワークの帯域を考慮し、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、一度に送付する業務データ量を減らすなどの運用設計を行う。
- アクセス制限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。

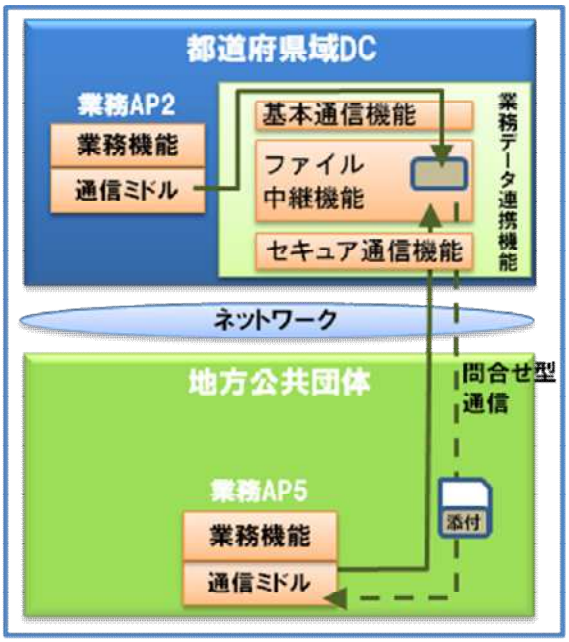


図 4-39　業務 AP5 から業務 AP2 へファイル送信
（オフサイトへのアクセスが制限される場合）の例

カ　オフサイトへのアクセスが制限される場合のデータ取得

オフサイトへのアクセスが制限されており、都道府県域 DC から地方公共団体庁内への問合せ型通信ができない場合、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（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。
- 必要に応じて、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。

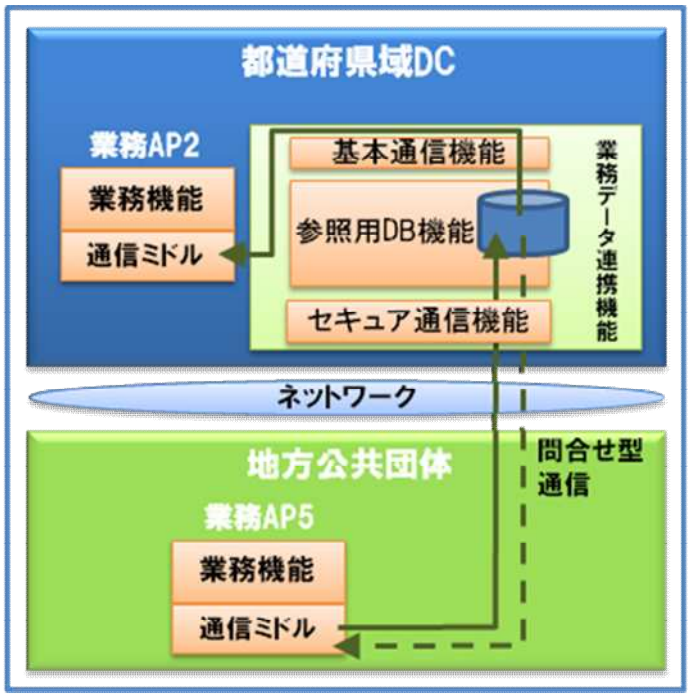


図 4-40　業務 AP5 から業務 AP2 へのデータ取得
（オフサイトへのアクセスが制限される場合）の例

キ　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、公開されている NTP サービスを利用して同期を取ること。

4.6 バックアップ連携

4.6.1 バックアップ連携要件

4.6.1.1 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・企業等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。これを前述の「4.1 ファシリティ」及び「4.2 ネットワーク」にて記述されている要件を満たした都道府県域 DC あるいは ASP・SaaS 事業者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構築する。

また、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。

そこで、上記バックアップデータを地方公共団体庁内に連携をすることにより、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ことが可能となる。

(2) 適用範囲

バックアップ連携の適用範囲を図 4-41 に示す。

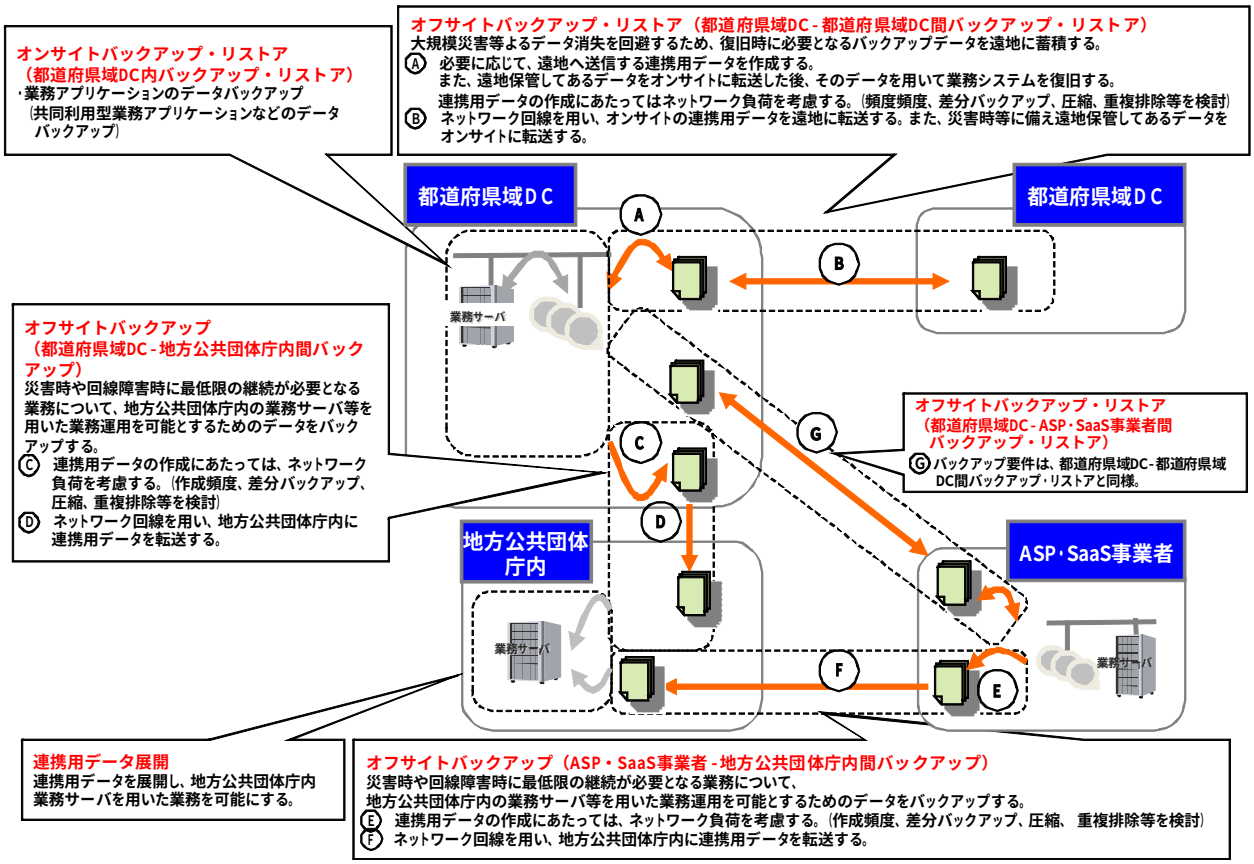


図 4-41　バックアップ連携の適用範囲

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。

ア　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。

イ　災害発生後復旧時に必要な業務を実施するための連携機能

- **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。

ウ　災害発生時に必要な業務を実施するための連携機能

- **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。

*取得したバックアップデータは、地方公共団体庁内において「連携用データ展開」を行うことで業務実施が可能となる。

なお、災害発生時において業務優先度が高い地方公共団体の業務については、災害発生時に必要な業務を実施するための連携機能を用いてデータのバックアップを行う。

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のように図 4-42 整理する。

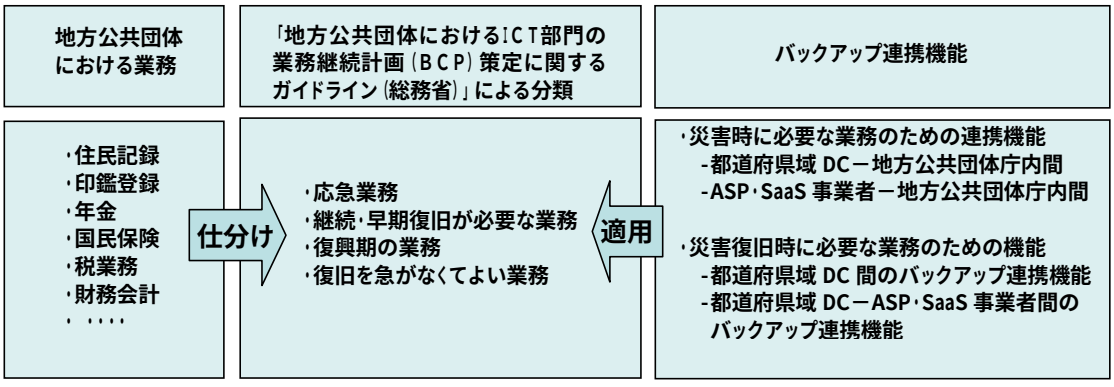


図 4-42　目標復旧時点（RPO）の適用

(ｱ) 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。

(ｲ) 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。

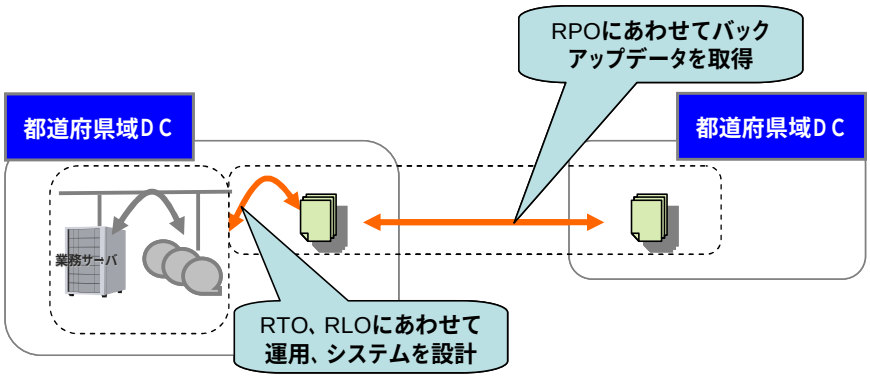
（注）
バックアップの頻度は、目標復旧時点（RPO）を基に定める。

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

また、「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。



4-43　目標復旧時点（RPO）の適用

4.6.1.2 要件一覧

バックアップ連携の要件を表 4-11 に示す。

表 4-11 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)	バックアップデータ作成に関する機能 ・ 業務アプリケーション等のバックアップデータを作成できること。
		データ復元に関する機能 ・ 業務アプリケーションで生成したデータからリストアできること。
		セキュリティに関する機能 ・ 適切にデータを管理すること。
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（図 4-41 内、Ⓐ） ・ 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（図 4-41 内、Ⓑ） ・ 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（図 4-41 内、Ⓐ） ・ 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)。
		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。
		性能向上に関する機能(任意要件) ・ 重複排除技術を有した専用ストレージを用いること(効率的なデータ転送によりネットワークの負荷軽減)。 ・ データベースのレプリケーション機能を有すること(障害発生から復旧までの作業時間短縮)。
3	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)	連携用データ作成に関する機能（図 4-41 内、Ⓒ及びⒺ） ・ 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（図 4-41 内、Ⓓ及びⒻ） ・ オフサイトバックアップにおける、都道府県域 DC、ASP・SaaS 事業者とデータ連携するための処理(データ連携プロセス)。
		連携用データ展開に関する機能 ・ 都道府県域 DC、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)。
		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。

		性能向上に関する機能(任意要件) ・ データベースのレプリケーション機能を有すること(障害発生から復旧までの作業時間短縮)。

4.6.1.3 機能

(1) オンサイトバックアップ・リストア

ア バックアップデータ作成に関する機能

イ データ復元に関する機能

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。

ウ 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、その管理に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、データを管理するすべての業務サーバにおいては、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。

(ｱ) データを管理する機能

a バックアップデータが蓄積されるサーバは、十分なセキュリティを考慮した運用がなされること(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。)。

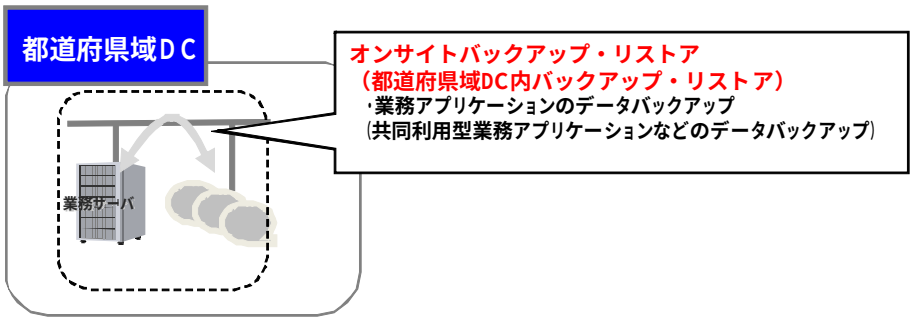


図 4-44 オンサイトバックアップ・リストア（都道府県域 DC 内処理)

(2) オフサイトバックアップ・リストア

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)。

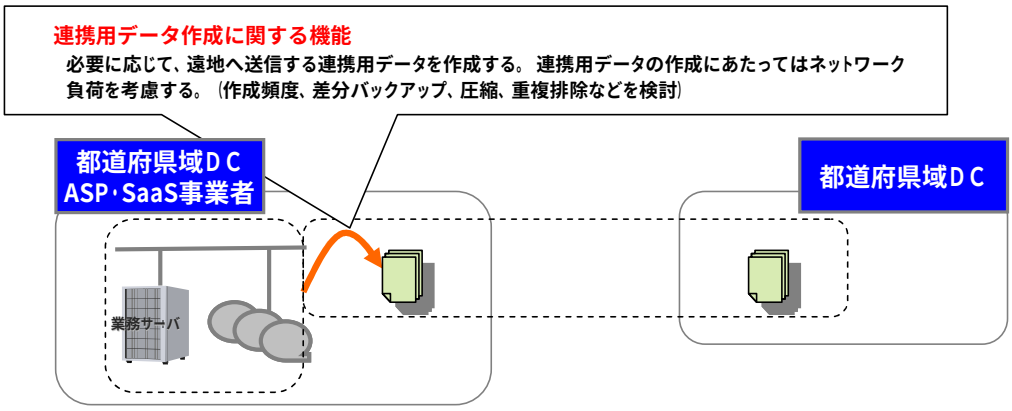


図 4-45　連携用データ作成に関する処理

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、ネットワーク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。

(ｱ) 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。

a　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。

b　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。

(ｲ)　データの世代管理を行うための機能

連携用データの作成日時、保存先などの管理ができる仕組みを提供する。

a　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、データの世代管理を行うための機能を用い、順次処理が実行される。

(ｳ)　データの世代管理を行うための機能

a　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。

b　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。

(ｴ)　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。

a　処理を自動で運転できること。

b　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。

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。

(ｵ)　拡張性を高めるための機能（推奨）

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。

a　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。

イ　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)。

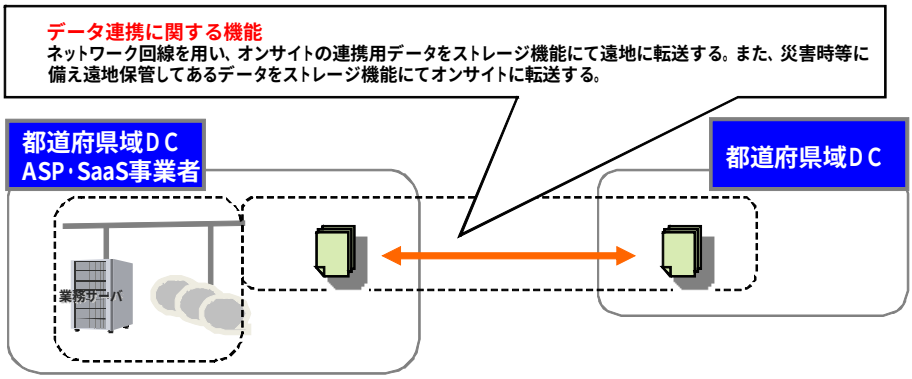


図 4-46　データ連携に関する処理

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。データの遠隔地保管場所は、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。この遠隔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。

(ｱ) 効率的にデータ転送するための機能

a 連携用データを転送できること。

b 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（重複排除機能）を用いることが望ましい。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。

(ｲ) データの世代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、必要に応じて長期間保存できること。

c 保存世代から外れたデータは削除し、データ領域を再利用できること。

(ｳ) 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 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。

c 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。

ウ 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)。

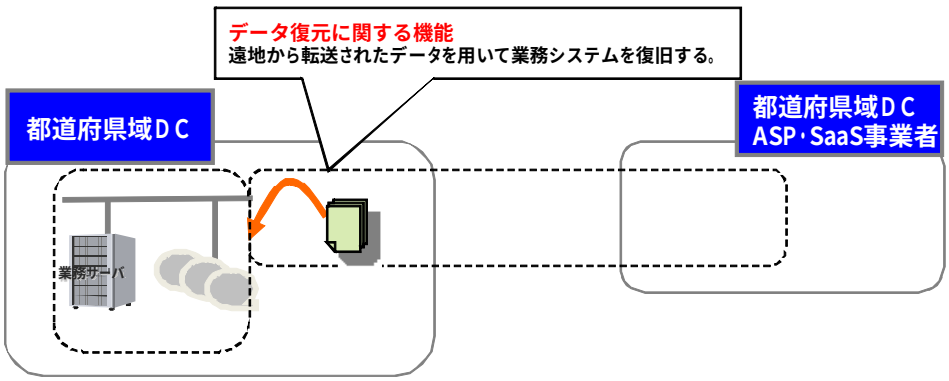


図 4-47 データ復元に関する処理

災害時等に備え遠隔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。

(ｱ) 処理の自動化を行うための機能

a 処理を自動で運転できること。

エ　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。

(ｱ) 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

a　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。
b　ネットワーク転送中は IPsec などで通信内容を秘匿できること。

(ｲ) データを管理する機能

a　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。
b　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。

オ　性能向上に関する機能

上記バックアップ連携に関する機能により、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)における一連の運用実施は可能となるが、ネットワークの効率的な利用による通信コスト削減や障害発生時における復旧時間の短縮の観点から、該当する業務サーバ並びにインフラについて、性能向上を目的とした整備を行うことが望ましい。

上記整備において、推奨される機能は以下となる。

(ｱ) 効率的にデータ転送するための機能

a　連携用データを転送できること。
b　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（重複排除・圧縮機能）をもちいること。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。

(ｲ) データの世代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、必要に応じて長期間保存できること。
c　保存世代から外れたデータは削除し、データ領域を再利用できること。

(ｳ) 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、必要に応じて長期間保存できること。
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。

(ｴ)　データベースのレプリケーション機能

リアルタイムによるデータ同期ができること。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。

(3) オフサイトバックアップ

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、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)。

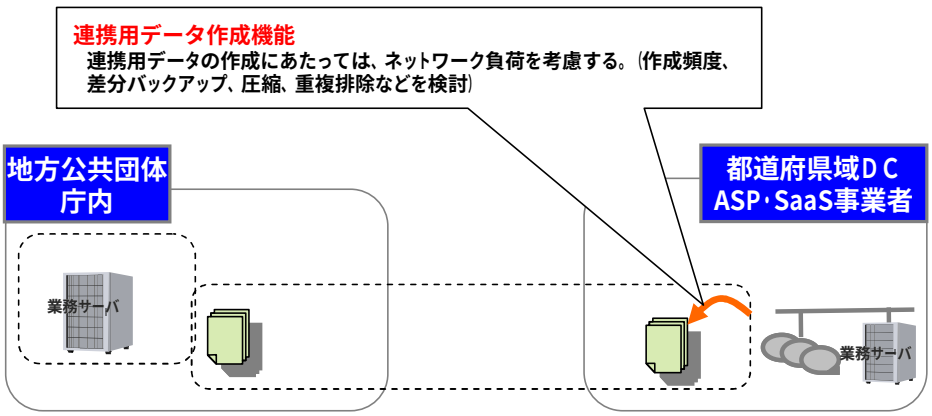


図 4-48　連携用データの作成処理

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。

(ｱ) 最小限のデータを作成するための機能
- a 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を取得できること。
- b 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。
- c 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。
- d データの圧縮等を行うこと。なお、複数のデータ間に存在する重複部分の排除する方式の導入も効果的である。

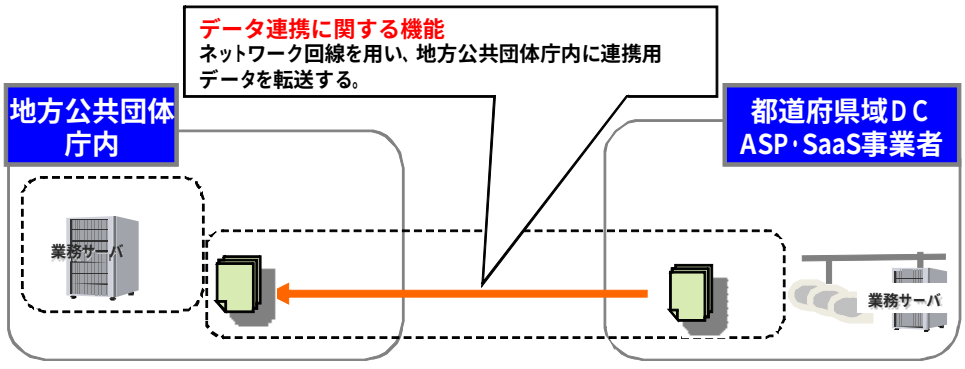
以降の機能は都道府県域 DC 間のオフサイトバックアップと同等である。

(ｲ) データの世代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、領域の再利用が可能なこと。

(ｳ) 効率的に連携を行う機能（推奨）
- a 処理を自動で運転できること。
- b 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。
- 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。

(ｴ) 拡張性を高めるための機能（推奨）
- a 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。

イ　データ連携に関する機能



4-49　データ連携に関する処理

(ｱ) データ転送時の効率化のための機能（推奨）
- a 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。

(ｲ) 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。

a　同時に複数連携が可能できること。
b　必要に応じて連携処理の頻度を変更・設定できること。
c　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　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。

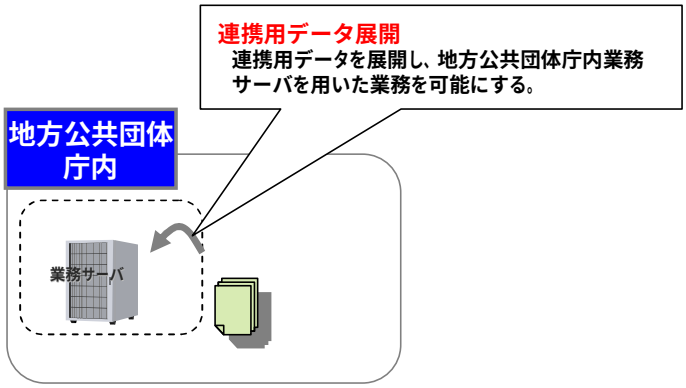


図 4-50　連携用データの展開処理

エ　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。このデータを地方公共団体庁内と他都道府県 DC 及び ASP・SaaS 事業者とで連携するため、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。

(ｱ) 通信時にセキュリティを確保する機能

a　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。
b　ネットワーク転送では、暗号化等による秘匿化を考慮すること。

(ｲ) データを管理する機能

a　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。)。

オ　性能向上に関する機能

上記バックアップ連携の関する機能により、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－地方公共団体庁内間バックアップ)における一連の運用実施は可能となるが、ネットワークの効率的な利用による通信コスト削減や障害発生時における復旧時間の短縮の観点から、該当する業務サーバ並びにインフラについて、性能向上を目的とした整備を行うことが望ましい。

上記整備において、推奨される機能は以下となる。

(ｱ) データベースのレプリケーション機能

リアルタイムによるデータ同期ができること。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。

付録１　参考資料

財団法人地方自治情報センターは、平成２２年度自治体クラウド・共同アウトソーシング移行促進事業において、「自治体クラウド開発実証事業に係る標準仕様書　平成 21 年度版」に準拠した自治体クラウドの構築及び業務システムの共同化を実施する３グループに、市町村の取組に係る経費を助成した。

団体名	構成団体	業務システム名
留萌地域電算共同化推進協議会	●（平成２４年４月から平成２７年度にかけて順次稼働） 増毛町、小平町、苫前町、羽幌町、初山別村、遠別町、天塩町	【基幹系】（住基、税、福祉） 【内部管理系】（財務会計、人事給与他）
福井坂井地区広域市町村圏事務組合	●（平成２３年１１月稼働） あわら市、坂井市、永平寺町	【基幹系】（住基、税、福祉） 【内部管理系】（財務会計、人事給与他）
奈良県基幹系システム共同化検討会	●（平成２３年４月稼働）河合町 ●（平成２４年４月稼働）香芝市、葛城市、田原本町 ●（平成２５年度稼働）上牧町、広陵町、川西町	【基幹系】（住基、税、福祉）

図　参考資料１　平成２２年度自治体クラウド・共同アウトソーシング移行促進事業

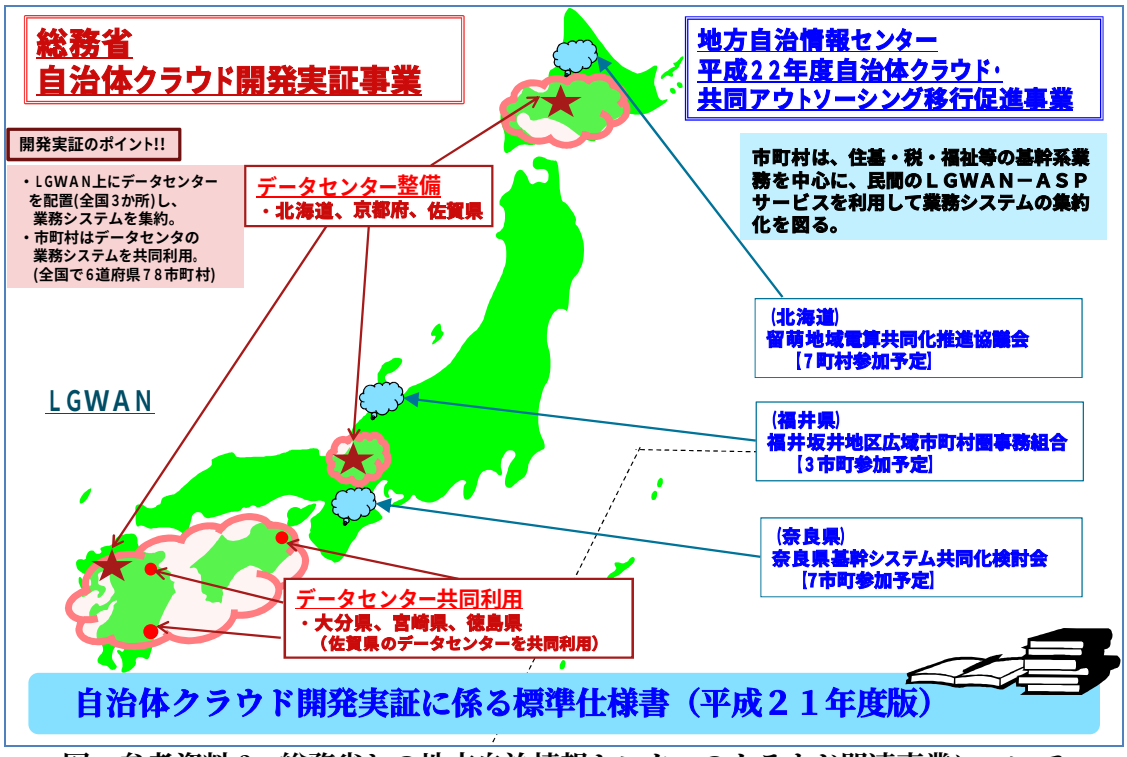


図　参考資料２　総務省との地方自治情報センターのクラウド関連事業について

付録 2　バックアップ連携構築時の考慮点

1.　バックアップ連携の構築

データセンター（都道府県域 DC、ASP・SaaS 事業者、地方公共団体）間のバックアップについては、バックアップデータを送信する側（以下、「送信側」という。）とバックアップデータを保管する側（以下、「保管側」という。）の両者によって、構築手段及び動作仕様を検討、協議しておく必要がある。

(1)　バックアップ連携の構築形態

構築形態は、保管側がどこまでのサービスを送信側に提供するかによって、表 付録 1-1 のように分類される。構築に当たっては、形態毎の特徴に留意する必要がある。

構築形態とその特徴に以下に示す。

表 付録 1- 1　構築形態の特徴

構築形態	概要	システム管理権の考え方	特徴
ハウジングサービス	保管側で場所、ラックを提供する構築形態	システム管理権限は、送信側が有する。	• 送信側にてバックアップサーバの調達、構築、業者の調達などの作業が発生する。 • 遠隔地での運用の検討が必要となる。
ホスティングサービス	保管側でサーバまでを提供する構築形態	システム管理権限は、保管側と送信側との調整により決める。	• 送信側にてバックアップソフトウェアの調達、構築、運用などの作業が発生する。 • 遠隔地での運用の検討が必要となる。 • バックアップデータを保管側に預けることになる。
アプリケーションサービス	保管側でバックアップソフトまで提供する構築形態	システム管理権限は、保管側が有する。	• 保管側の示すサービス提供条件に従う必要があり、サーバスペック、バックアップソフトウェアに制約が発生する。 • バックアップデータを保管側に預けることになる。

ア　ハウジングサービス

保管側がラックまでを提供し、送信側がラックにバックアップサーバなどの必要な機器、バックアップ用のソフトウェアを構築する形態である。

- 保管側は、場所（データセンター）、電源や回線などの設備及びサーバラックを準備する。
- 送信側は、保管側から提供を受けたサーバラックに、バックアップサーバ、バックアップ用ソフトウェアを調達、構築して利用する。

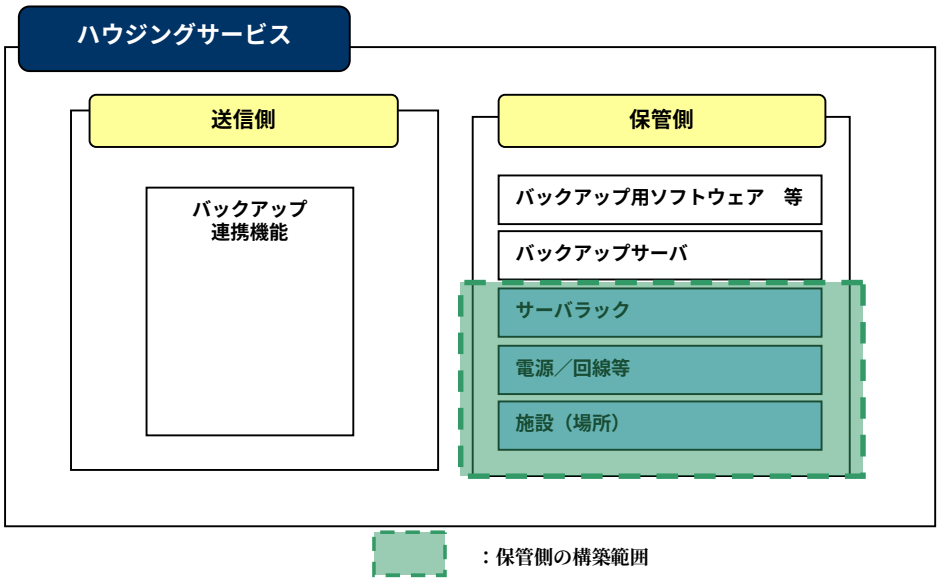


図 付録 1- 1　ハウジングサービスでの構築形態

イ　ホスティングサービス

保管側がバックアップサーバ（物理サーバ）までを提供し、送信側が提供されたバックアップサーバ上にバックアップソフトウェアなどを構築する形態である。

- 保管側が、場所（データセンター）、電源/回線などの設備、サーバラック及びバックアップサーバ（バックアップ連携データの格納に必要なディスクを含む）を準備する。
- 送信側は、提供されたバックアップサーバにバックアップソフトウェアを調達、構築して利用する。

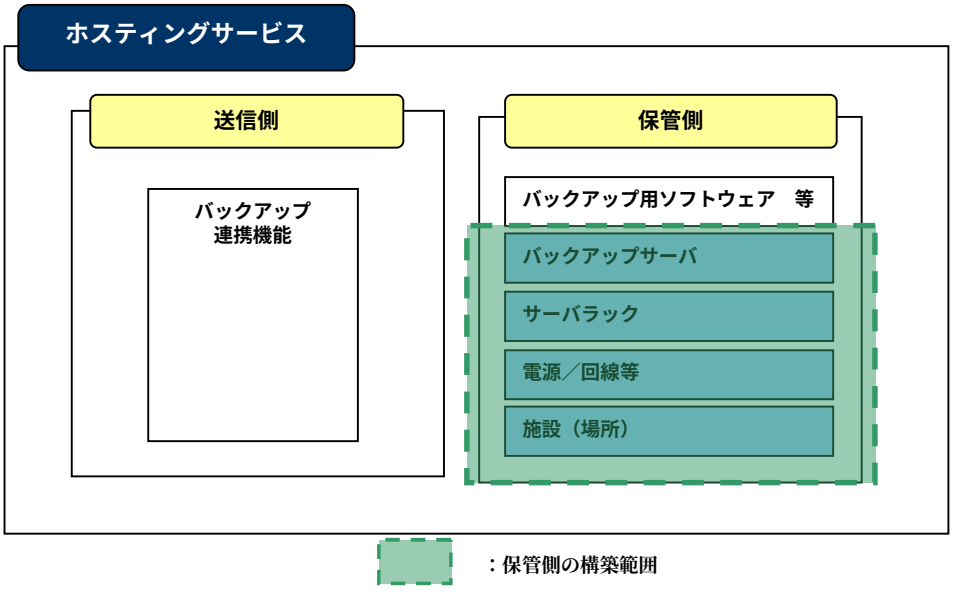


図 付録 1- 2　ホスティングサービスでの構築形態

ウ　アプリケーションサービス

保管側が提供するバックアップサービスを送信側が利用する形態であり、バックアップを行うためのバックアップソフトウェアまでが保管側から提供される形態である。

- 保管側がバックアップ連携に必要な場所からバックアップソフトウェアまでの全てを準備する。
- 送信側は、既に構築された保管側でのバックアップ環境を利用する。そのため送信側で新たにバックアップ連携の仕組みを構築する必要はない。

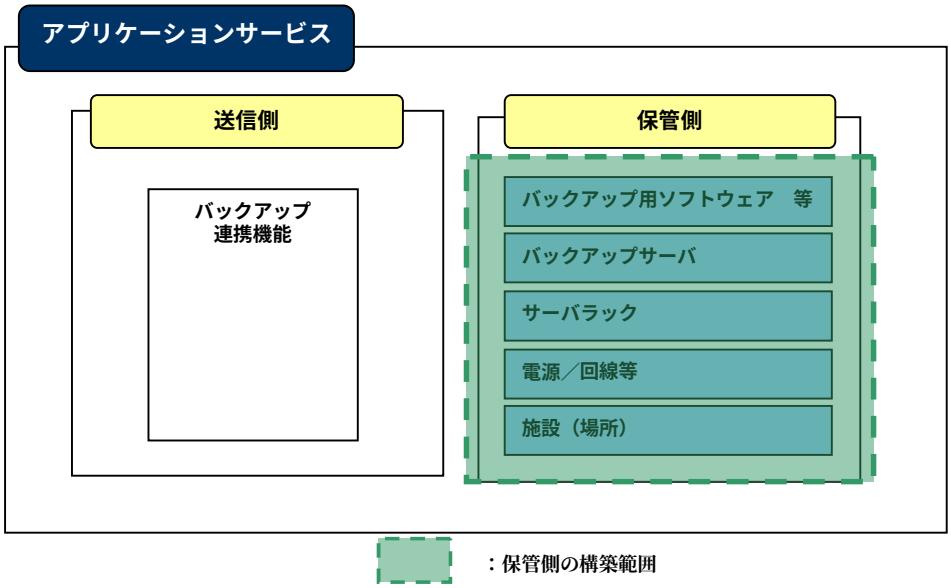


図 付録 1- 3　アプリケーションサービスでの構築形態

エ　留意事項

バックアップ連携を構築するに当たっての留意点を以下に示す。

- LGWAN 接続申請

  LGWAN を利用する場合は、以下を留意する必要がある。

  ハウジングサービスを利用して送信側がバックアップサーバを保管側 DC へ設置する場合、現在の LGWAN のルールでは、ASP-SS[2]を管理するものが LGWAN への接続申請を行うとされているため、保管側で「総合行政ネットワーク ASP ホスティングサービス変更申込書」 を LGWAN 運営主体へ提出し、承認を得る必要がある。

[2] ASP-SS:「総合行政ネットワーク基本要綱」に示された LGWAN に参加する団体が整備するサービス提供設備のこと。

(2) バックアップデータ送信方式の取り決め

バックアップデータの送信方式は、送信側からバックアップデータを送信する PUT 方式と、保管側からの取得要求への応答としてバックアップデータを送信する GET 方式が考えられる（図 付録 1-4）。バックアップ連携を行う場合は、以下のどちらの方式を採用するかを事前に送信側と保管側で取り決めておく必要がある。

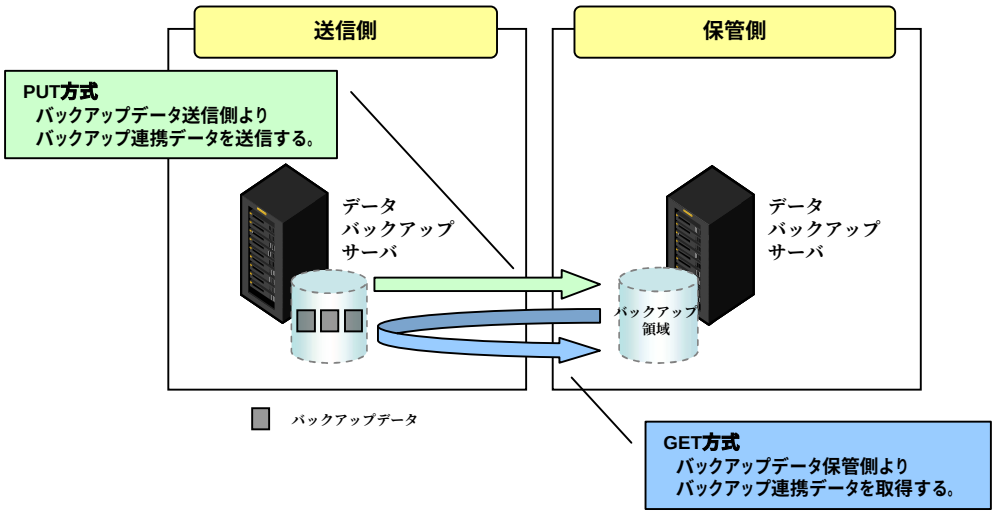


図 付録 1- 4　PUT 方式と GET 方式のイメージ

それぞれの送信方式の特徴を表 付録 1-2 に示す。

表 付録 1- 2　PUT 方式と GET 方式の特徴

データ送信方式	概要	特徴
PUT 方式	送信側から保管側へバックアップ連携データを送信する方式	• 送信側が主導となるため、バックアップタイミング、送達確認、障害が発生した際の対応について柔軟に行うことが出来る。
GET 方式	保管側からの取得要求に対する応答として送信側がバックアップ連携データを送信する方式	• 保管側が主導となる為、送信側ではバックアップデータの送信に関する組み込みなどが不要となる。 • 保管側が主導となる為、急なバックアップを行いたいなどの変則的な対応は困難となる。 • 保管側が主導となる為、バックアップタイミング、障害時の取り扱いにて調整･制約が考えられる。

2. SLA（Service Level Agreement）

サービス構築者がバックアップ連携サービスを提供する場合に適用すべき、またサービス調達者がバックアップ連携サービスを調達する場合に考慮すべき SLA の考え方を以下に示す。

(1) SLA の適用範囲

本項で対象とする SLA については、本編図 3-1 に示した「サービス提供者」と共同利用用途の各種業務システムをサービスとして調達する「サービス調達者」向けである。

ア SLA の要求項目

サービス提供者は、「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」より、サービス調達者である地方公共団体で対応が求められる以下の項目を SLA 要求事項として構築を行うことが必要である。

① 目標復旧時点（RPO： Recovery Point Objective）
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、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のこと。

② 目標復旧時間（RTO： Recovery Time Objective）
非常時において情報システムが停止した場合、いつまでに復旧する必要があるかという復旧に必要な時間のこと。

③ 目標復旧レベル（RLO： Recovery Level Objective）
通常の何割の処理ができればよいのか、情報システムが動かなければ全く仕事にならないのかという復旧時のレベルのこと。

イ SLA 項目への対応

「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」より想定する SLA のうち、「目標復旧時点」、「目標復旧時間」の 2 つに関する対応を以下に示す。

⑺ 目標復旧時点への対応

目標復旧時点を考慮して、バックアップを取得する頻度を定める必要がある。
目標復旧時点毎のバックアップ頻度を表 付録 1-3 に示す。

表 付録 1-3 目標復旧時点への対応

項番	目標復旧時点	バックアップ頻度
1	災害直前のデータが必要不可欠（データの喪失は許容できない）	リアルタイムレプリケーション（標準仕様書に定義した機能での実現は出来ない）
2	災害発生前日のデータを喪失しても許容できる	毎日のバックアップデータ取得が必要
3	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	3日周期でのバックアップデータ取得が必要
4	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	週次でのバックアップデータ取得が必要
5	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	月次でのバックアップデータ取得が必要

(ｲ) 目標復旧時間への対応

災害時においても応急業務として継続が必要な場合と必要ない場合に分類した対応が必要である。

a 応急業務として継続が必要な場合
応急業務として継続が必要な業務については、都道府県域 DC―地方公共団体庁内間、ASP･SaaS 事業者―地方公共団体庁内のバックアップにより、地方公共団体の庁内にデータのバックアップを配置する。

b 応急業務としての継続が必要ない（復旧を急がない）場合
応急業務として継続が必要ない業務については、都道府県域 DC 間、都道府県域 DC―ASP・SaaS 事業者間のバックアップを利用する。

3. 運用

(1) バックアップ連携に関する運用

バックアップデータを遠隔地（オフサイト）と連携、保管する場合の運用に関する留意事項を以下に示す。

ア データ容量について

バックアップ連携の構築形態がハウジングサービス及びアプリケーションサービスの場合、保管側にて送信側のデータを保管するためのディスク領域を確保するが、送信側は以下の項目について保管側と事前に合意しておく必要がある。

(ｱ) 初期データ容量

初期段階で保管側に必要となるバックアップデータの容量について、送信側が事前に調査し、保管側と取り決める必要がある。また、初期段階で確保するデータ容量は、バックアップデータの成長率を踏まえて保管側と取り決めすることが望ましい。

(ｲ) データ領域拡張

バックアップデータの保管に必要なデータ容量は、利用者数やシステム構成の変更などによって増加することが考えられる。初期段階で取り決めたデータ容量を超過した場合を考慮し、データ容量の拡張が必要となった際の取り決めが必要である。取り決めが必要な項目を以下に示す。

a 拡張性の有無
データ容量の拡張可否

b 拡張時に想定される制約の許容度合い
拡張に伴うバックアップシステムの長期間停止やシステム構成の変更有無など、システムに与える影響度合い

c 拡張時の費用体系
拡張を行う際の追加費用

イ 保守について

バックアップデータを遠隔地と連携している場合、障害や停電などの事象が発生することを想定して、送信側と保管側は、以下のような運用上の取り決めについて検討し、合意する必要がある。

(ｱ) 運用体制、連絡ルート

障害や停電などの事象が発生した場合の運用体制及び連絡先など。

(ｲ) バックアップサーバの死活監視・障害監視

バックアップサーバの死活監視・障害監視の実施主体について。

(ｳ) ハードウェア、ソフトウェアの保守
ハードウェア及びソフトウェア保守（故障対応やセキュリティパッチの適用など）の実施主体について（バックアップ連携の構築形態がアプリケーションサービスの場合を除く。）。

ウ　リストアについて
災害復旧時等に円滑にサービスの復旧を図るため、バックアップデータのリストアに関しては、以下の事項に留意が必要である。

(ｱ) 復元に必要なデータの入手経路（保存先から復元元へのデータ搬送に係る手順）を明確化しておくこと
(ｲ) リストアの手順を明確化しておくこと
※　リストア時に必要となる元データ（全件、差分）の種類やデータの取得方法（ネットワーク経由、テープ搬送）など。
(ｳ) リストアに要する時間が SLA を満たしていること
(ｴ) 定期的な訓練を実施し、バックアップデータから実際にリストアが可能であることを確認すること

4. セキュリティ

(1) システムのセキュリティ対策

LGWAN 上で自治体クラウドサービスの構築を行う場合、LGWAN-ASP として構築することなるため、サービス導入に当たっては、LGWAN-ASP として要求されるセキュリティ条件を満たす必要がある。

(2)データ管理に関するセキュリティ対策

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、データ管理には十分なセキュリティ対策が必要である。セキュリティ対策では「総合行政ネットワーク基本要綱」などを参照するとともに、バックアップ連携においては、他都道府県域 DC 及び ASP・SaaS 事業者へデータを預けることが想定されるため、保管側にてデータ参照などが行えないよう、暗号化などの対策も併せて検討する必要がある。

(3) データ通信時のセキュリティ確保

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、データ通信時には十分なセキュリティが必要である。セキュリティ対策では「総合行政ネットワーク基本要綱」などを参照するとともに、バックアップ連携においては、他都道府県域 DC 及び ASP・SaaS 事業者間とのデータ通信が想定されるため、VPN トンネリング等の対策も併せて検討する必要がある。

付録 3 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。

No.	用語	説明
21	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。
22	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。
23	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。
24	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。
25	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。
26	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。
27	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。
28	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。
29	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。
30	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。
31	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）
32	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。
33	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。
34	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。
35	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。
36	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。
37	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。
38	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地方公共団体内あるいは 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。
39	参照用 DB 機能	地方公共団体のセキュリティポリシー等により、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。
40	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、地方公共団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（27 業務を規定）。

No.	用語	説明
41	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。
42	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。
43	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。