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)　概要

1. 本仕様書の位置づけ

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合わせて記述する。

本書は、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「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)」として改訂したものである。

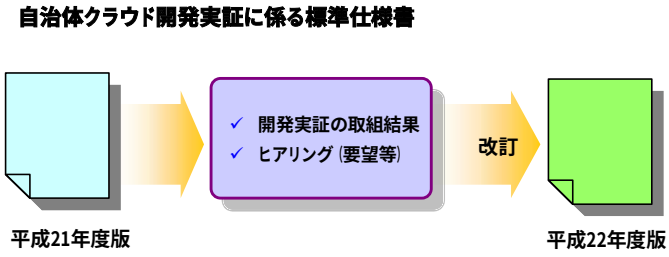

図 1-1　標準仕様書の改訂

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あれば併せて記述する。

本書では、上記①～③の基本方針に基づき、図 2-1 に示す範囲について記述する。

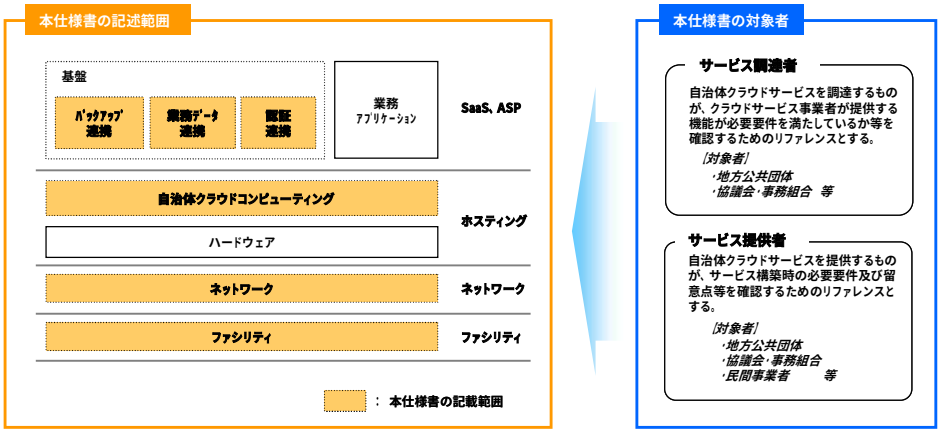

図 2-1 本仕様書の記述範囲

3. 標準仕様

3.1 ファシリティ(データセンター)

3.1.1 概要

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(DC)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示す。

3.1.2 機能

(1) 法令

日本国内法の適用および業務毎の関係法令を遵守する必要がある。

サービス提供者およびサービス調達者は、日本国内法が適用される国内に設置された DC でサービスの提供及び利用を行う。

また、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 の利用を利用すること。

(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、入退出管理、鍵の管理、監視、破壊対策、警備について定める。

また、情報セキュリティマネジメントシステム（ISO/IEC27001）等の認証を取得している DC を利用することを推奨する。

(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、電源の維持、火災・避雷・静電気からの防護、建物の災害対策、空調について定める

上記の各種対策に加えて、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ことが必要である。

3.2 ネットワーク

3.2.1 概要

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。

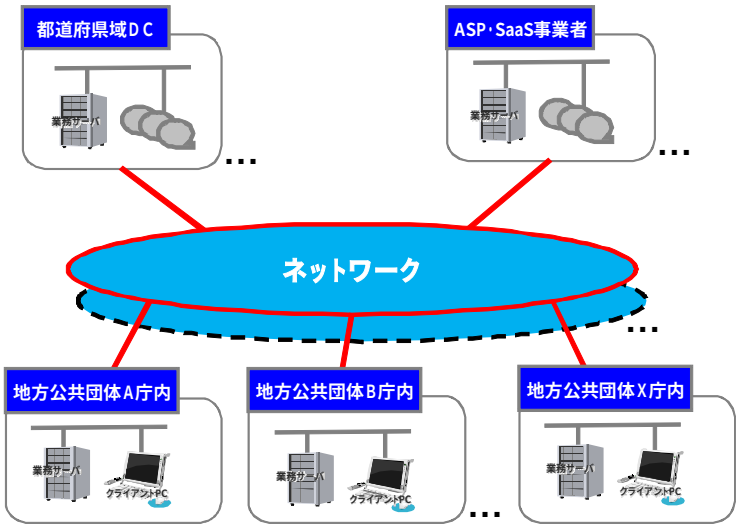

図 3-1 ネットワークの適用範囲

3.2.2 機能

(1) 通信

ア 性能

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。

また、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し、加えて侵入検知(IDS)を導入するなど、安定運用のためのシステム提供が必要である。

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

自治体クラウドのサービスを将来の帯域増大に対しても継続できるよう、回線網を選択すること。さらに、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、責任分界点を明確すること。

(3) SLA (**サービスレベル**)

SLA による運用品質の確保、サービス状況の把握や分析等による継続的な品質管理の確保が必要となる。

(4) **その他**

ネットワークの付加機能として、名前解決、電子メール及び時刻同期について記述する。

3.3 自治体クラウドコンピューティング

3.3.1 概要

都道府県域データセンター内において、仮想化技術を用いてシステム構築する場合の実装方法等の仕様について記述する。

また、地方公共団体の規模や業務特性に拠らず柔軟な環境構築を可能とする機能について以下に記載する。

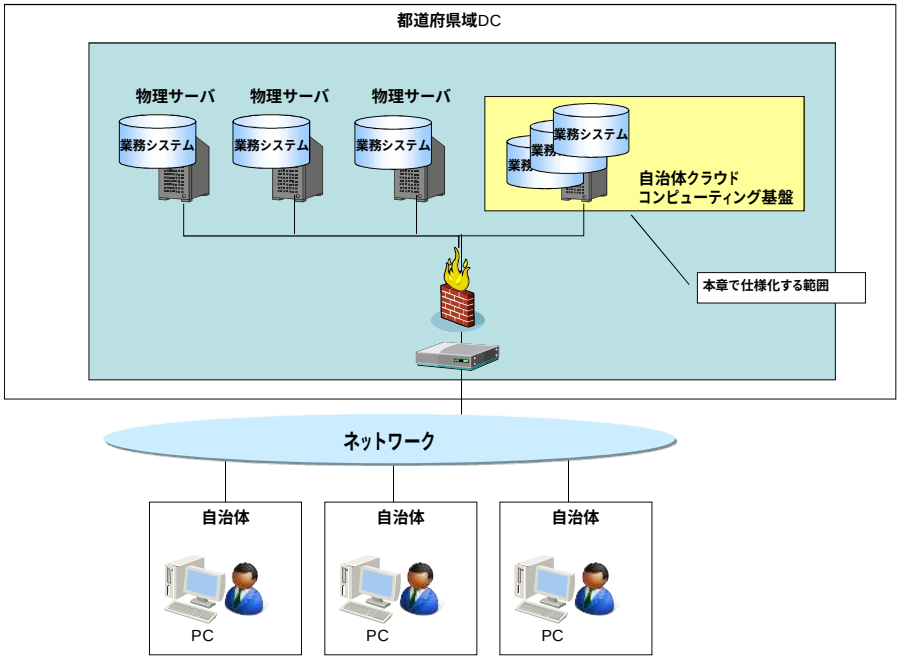

図 3-2 自治体クラウドコンピューティングの適用範囲

3.3.2 機能

都道府県域データセンター内において、仮想化技術を用いてシステム構築する場合の実装方法等の仕様について記述する。

(1) **仮想化機能**

サーバの仮想化とは、図 3-3 に示す通り、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であり、サーバの仮想化の特徴である、CPU の仮想化、サーバの仮想化、I/O の仮想化、ネットワークの仮想化等についての留意点を記述する。

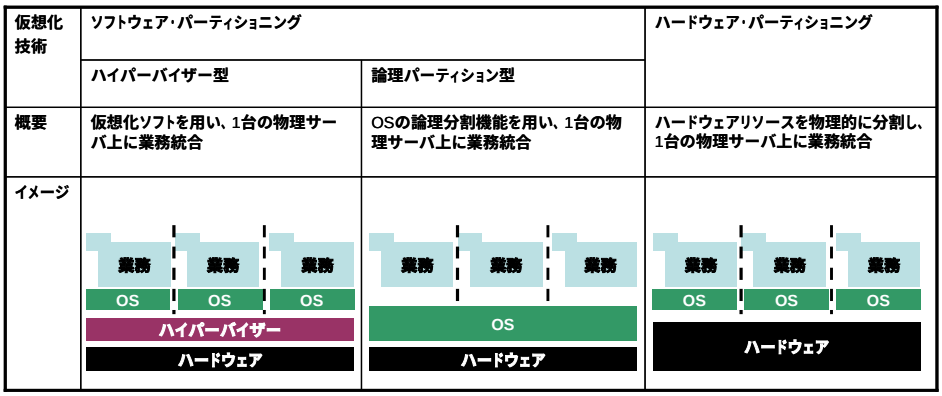

図 3-3　仮想化のイメージ

(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。

ここでは、システム管理に必要となるセキュリティ、VM のセキュリティ、ネットワークのセキュリティ及びログの運用等について記述する。

(3) **静的マイグレーション**[1]

静的マイグレーションにより、既存の業務システムを仮想化された環境に移行することが可能となる。仕様書では、静的マイグレーションに必要なハイパーバイザ製品（VMware 等）の機能や制限について記述する。

(4) **動的マイグレーション**

動的マイグレーションにより、業務を停止することなく他のサーバへ引き継ぐことが可能となり、ハードウェア障害等による業務停止時間を極小化することが可能となる。仕様書では、動的マイグレーションの実現方式や留意点を記述する。

[1] マイグレーション：プログラムやデータの移行、別なプラットフォームへの移植を指す。

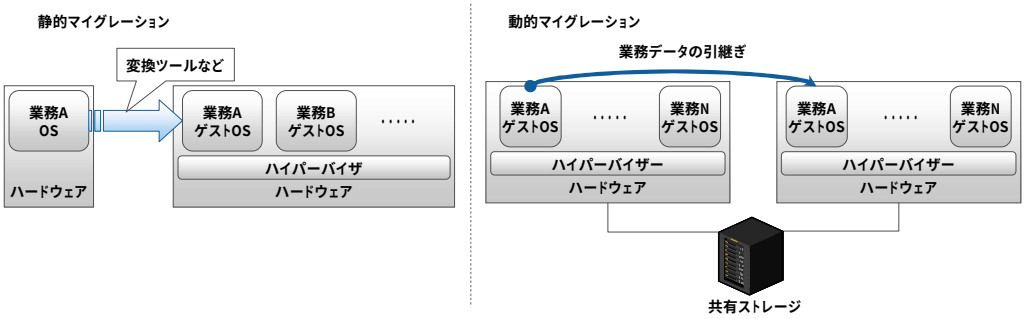

図 3-4　静的マイグレーションと動的マイグレーション

(5) **グリッド連携**

グリッド連携は、複数のハードウェアをハイパーバイザで集約することで、処理能力の向上および可用性の向上や、業務システムのリソースを動的に割り当てることを実現する機能である。仕様書では、グリッド連携の実現方式や留意点を記述する。

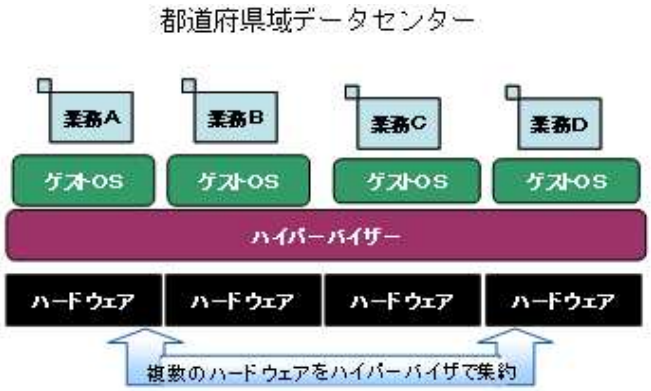

図 3-5　グリッド連携イメージ

3.4　認証連携

3.4.1　同一自治体内でのシングルサインオン

3.4.1.1　概要

自治体クラウドでは、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、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。

この問題を解決する対策として、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について記述する。

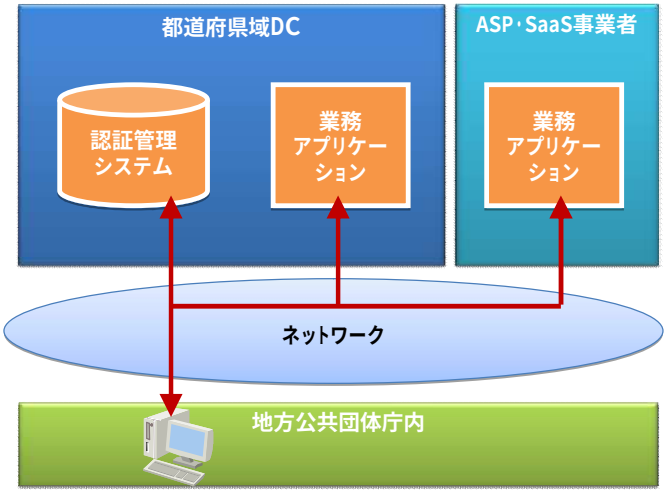

図 3-6　同一自治体内でのシングルサインオンの適用範囲

3.4.1.2 機能

(1) **ユーザ認証**

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ために必要となる、認証方式や認証レベルについての仕様を記述する。

(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必要となる、認証連携トランザクションの HTTPS 利用等の通信の秘匿性・完全性が確保するための要件を記述する。

(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して、SAML、Open ID、リバースプロキシ及び Cookie を用いた方式の特徴を提示する。

3.4.2 クラウドサービス間でのシングルサインオン

複数の ASP 事業者等、異なるサービス調達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。その場合、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、仕様書では運用面での留意事項も考慮しつつ、複数のクラウド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（SAML）について、実現方式、セキュリティ等を踏まえて記述する。

3.4.3 属性情報の連携

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。仕様書では属性情報を安全にクラウド間で流通させるための機能に関して、代表的な技術仕様(ID-WSF）や留意点について記述する。

3.5 業務データ連携

3.5.1 概要

データ連携されている業務アプリケーション（以下、業務 AP）が、ネットワークをまたがった地方公共団体外（都道府県域 DC、ASP・SaaS 事業者、他の都道府県域 DC）に配置される場合の業務 AP 間の業務データ連携仕様について記述する。また、複数の業務 AP 間のデータ連携に係る共通仕様を集約化した「業務データ連携機能」を、都道府県域 DC の機能としての装備する場合の仕様について、併せて記述する。

※「業務データ連携機能」の仕様は、「地域情報プラットフォーム標準仕様書」に基づいたものとしている。

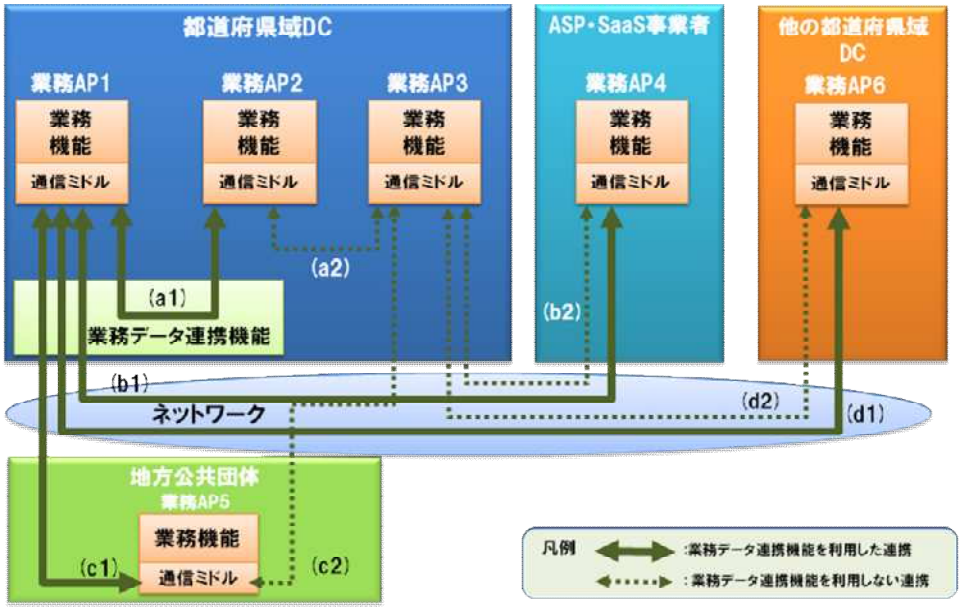

図 3-7　業務データ連携のユースケースと本節の適用範囲の概念図

表 3-1　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
		(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

3.5.2 機能

業務データ連携の概略アーキテクチャを図 3-8 に示す。

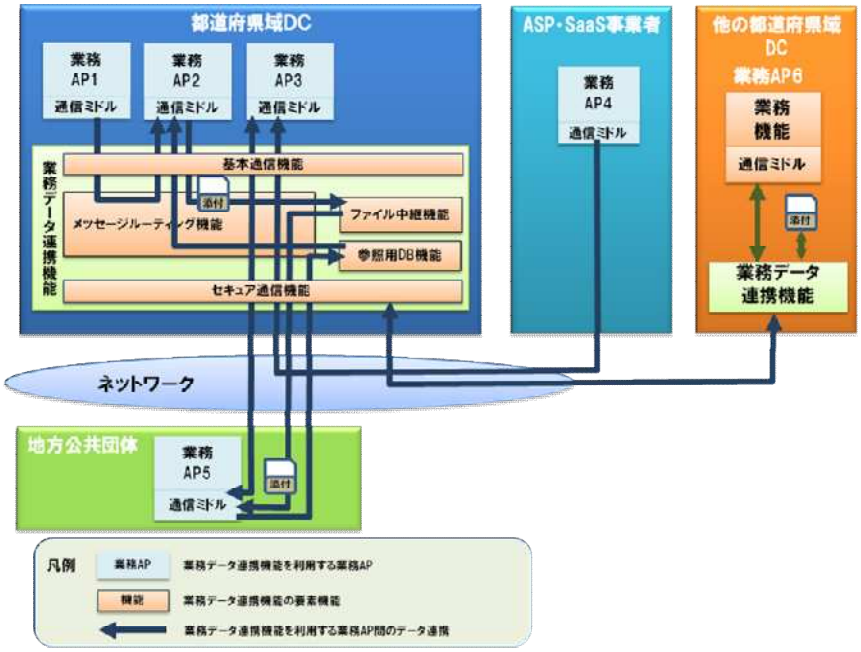

図 3-8　業務データ連携の概略アークテクチャ

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。なお、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。

(1) 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。

(2) 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。

(3) メッセージルーティング

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。

(4) 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。

(5) 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。

(6) 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）。

(7) 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機能である。

3.6 バックアップ連携機能

3.6.1 概要

大規模災害等におけるデータの消失回避を目的として、共同利用型業務アプリケーションなどのバックアップデータを、ネットワークを経由して遠隔地に保管するための機能について記述する。

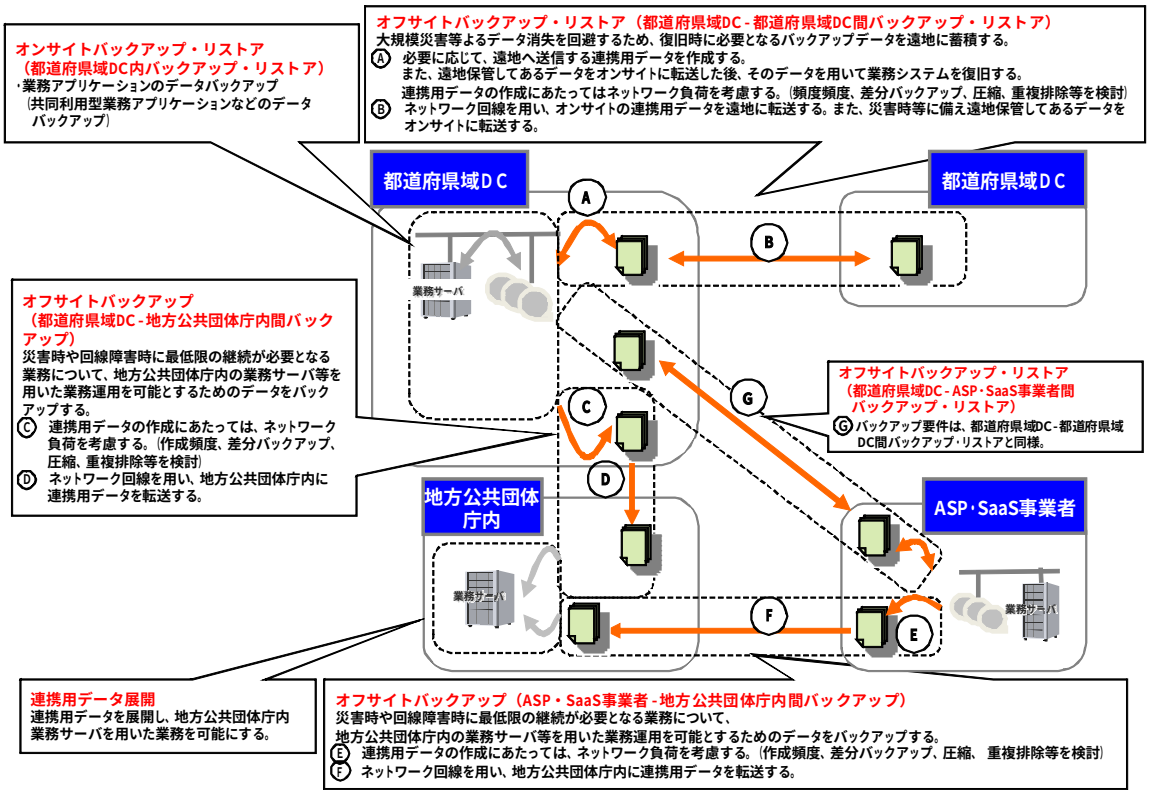

図 3-9 バックアップ連携の適用範囲

3.6.2 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

業務アプリケーション導入時に実装される機能であり、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、セキュリティを強く意識したデータ管理方法が必要となる。

(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)であり、連携データ作成、データの世代管理及び効率的に連携を行うための機能について記述する。

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)であり、ネットワーク負荷軽減に向けた効率的にデータ転送を行う機能、データの世代管理、ジョ

ブによる自動化等の効率的に連携を行う機能について記述する。

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)であり、処理の自動化を行うための機能について記述する。

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、通信時にセキュリティを確保する機能やセキュリティを強く意識したデータ管理が必要となる。

オ 性能向上に関する機能

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の性能向上を目的とした整備を行うことが望ましく、ネットワーク負荷軽減に向けた効率的にデータを転送、データの世代管理、効率的にデータ連携を行う機能としてデータベースのレプリケーション機能について記述する。

(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)であり、業務継続に向けた最小限のデータを作成、データの世代管理、処理の自動化による効率的に連携を行うための機能について記述する。

イ データ連携に関する機能

オフサイトバックアップにおける、都道府県域 DC、ASP・SaaS 事業者と地方公共団体内へデータ連携するための処理(データ連携プロセス)であり、ネットワーク負荷軽減に向けた効率的にデータ転送を行う機能、ジョブによる連携動作等の効率的に連携を行う機能について記述する。

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機能であり、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るため、詳細な方式については規定しない。

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、通信時にセキュリティを確保する機能やセキュリティを強く意識したデータ管理について記述する。

オ 性能向上に関する機能

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、データベースのレプリケーション機能について記述する。