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）
補足資料

平成２２年３月

財団法人　地方自治情報センター

目次

1. 本書の位置付け

本書は、財団法人地方自治情報センターの事業である「自治体クラウド開発実証に係る標準仕様書作成等研究開発事業」の成果物である標準仕様書を参照して、自治体クラウドサービスを構築、利用するに当たっての留意すべき事項及び考え方を示すものである。

1.1 本書の構成

本書は、標準仕様書を参照して自治体クラウドサービスを構築、利用する際に、特に検討が必要な以下の項目について記述している。また、自治体クラウドの構築、利用に関連する表 1-1 のガイドライン及び報告書等ですでに定められている項目については、当該文献を参照している。

① バックアップ連携の構築
② SLA（Service Level Agreement）
③ 運用
④ セキュリティ

表 1-1　参照文献一覧

参照文献名	発行元
公共 IT におけるアウトソーシングに関するガイドライン	総務省
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
地方公共団体 ASP・SaaS 活用推進会議　第一次 中間報告	総務省
総合行政ネットワーク ASP ガイドライン	財団法人地方自治情報センター
総合行政ネットワーク 基本要綱	財団法人地方自治情報センター
総合行政ネットワーク ASP 基本綱領	財団法人地方自治情報センター

本書と参照文献の関係を図 1-1 に示す。

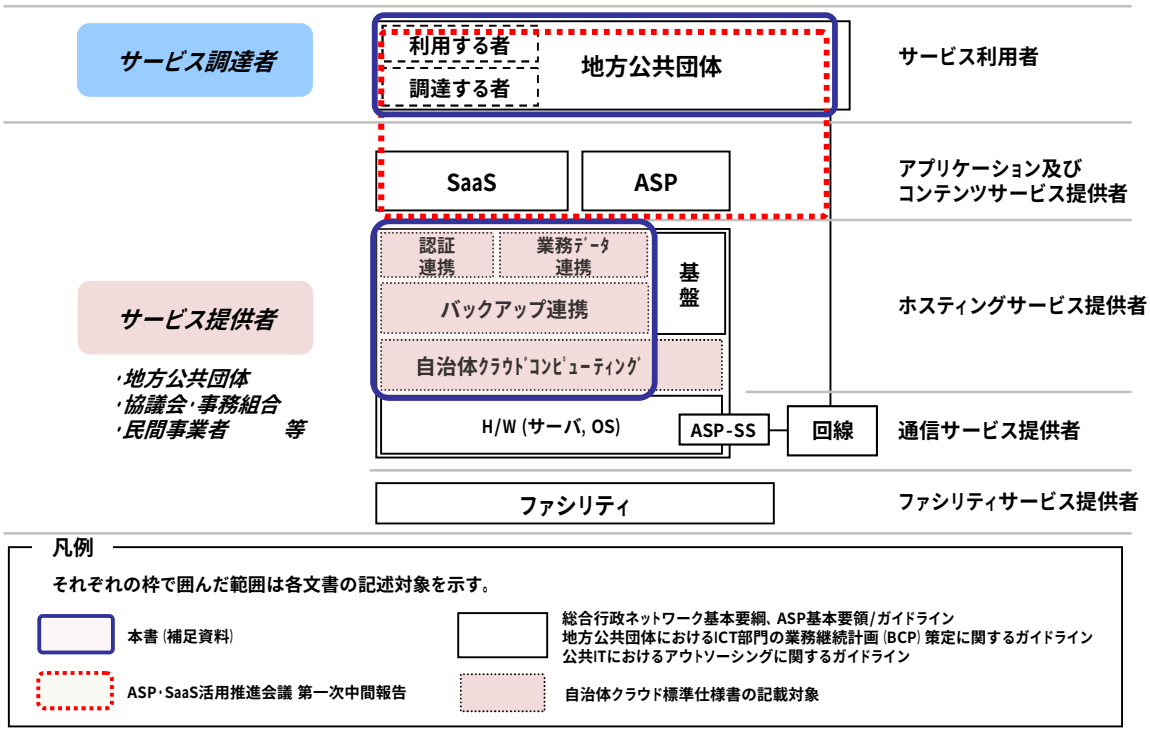

図 1-1　参照文献と補足資料の関係

2. 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。

2.1 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 2-1 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を以下に示す。

表 2-1　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。

2.1.1 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。

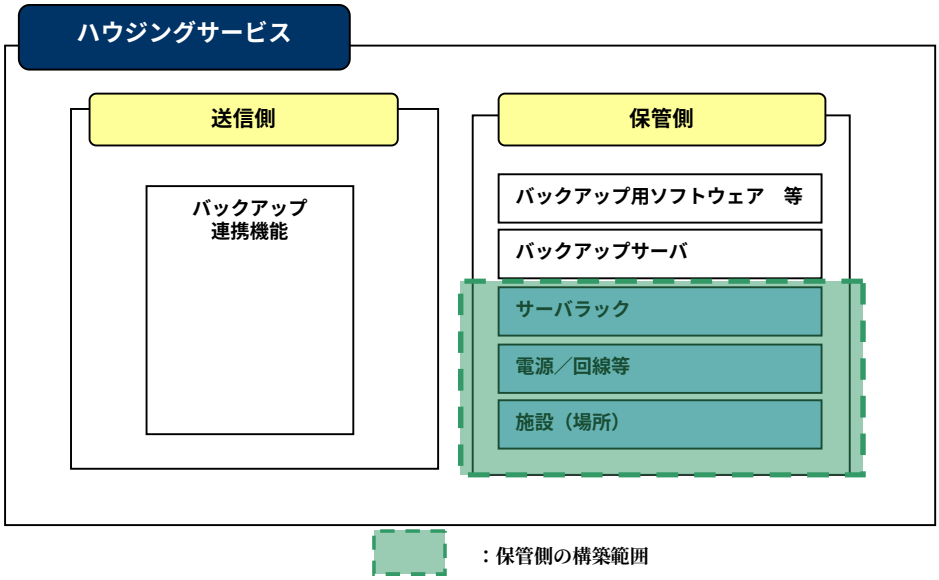

図 2-1　ハウジングサービスでの構築形態

2.1.2 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。

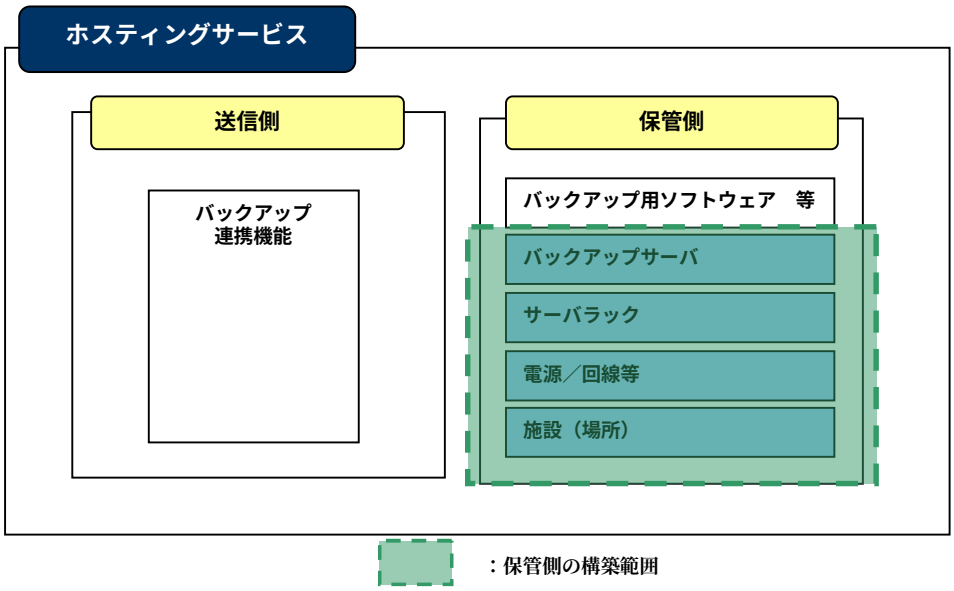

図 2-2　ホスティングサービスでの構築形態

2.1.3 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。

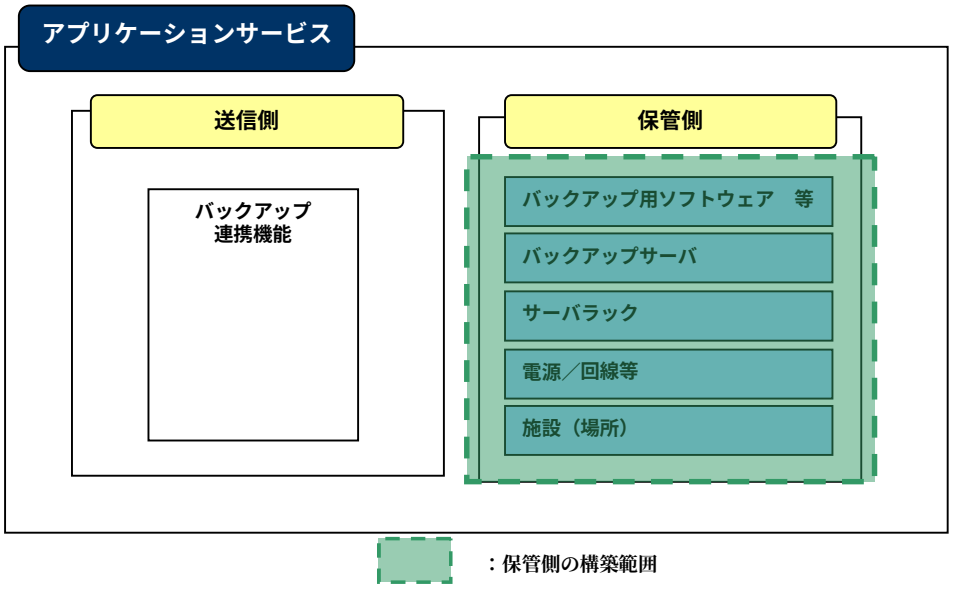

図 2-3　アプリケーションサービスでの構築形態

2.1.4 留意事項

バックアップ連携を構築するにあたっての留意点を以下に示す。

- LGWAN 接続申請

  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[1]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。

2.2 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 2-4）。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。

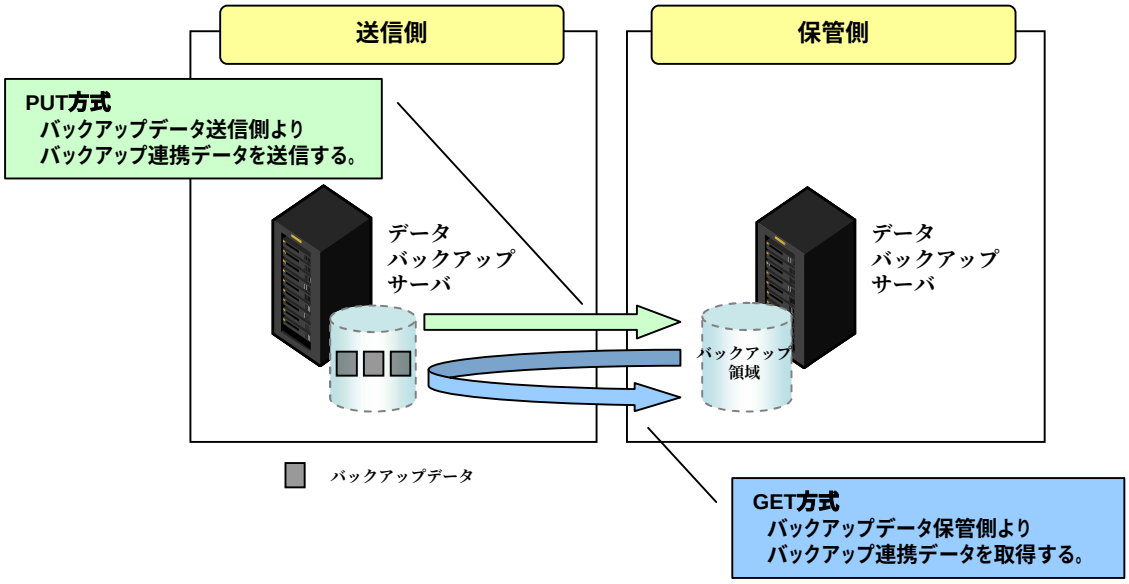

図 2-4　PUT 方式と GET 方式のイメージ

それぞれの送信方式の特徴を表 2-2 に示す。

表 2-2　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。

[1] 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。

2.3 バックアップ連携用通信経路の確保

バックアップ連携を行うためには、採用するバックアップ方式の要求するプロトコルが LGWAN において利用できることが必要である。しかし、現在の LGWAN で利用できるプロトコルには制限があるため、図 2-5 に示すとおり、トンネリング VPN を利用して、バックアップサーバ間の仮想的な直結通信回線を確立する必要がある。

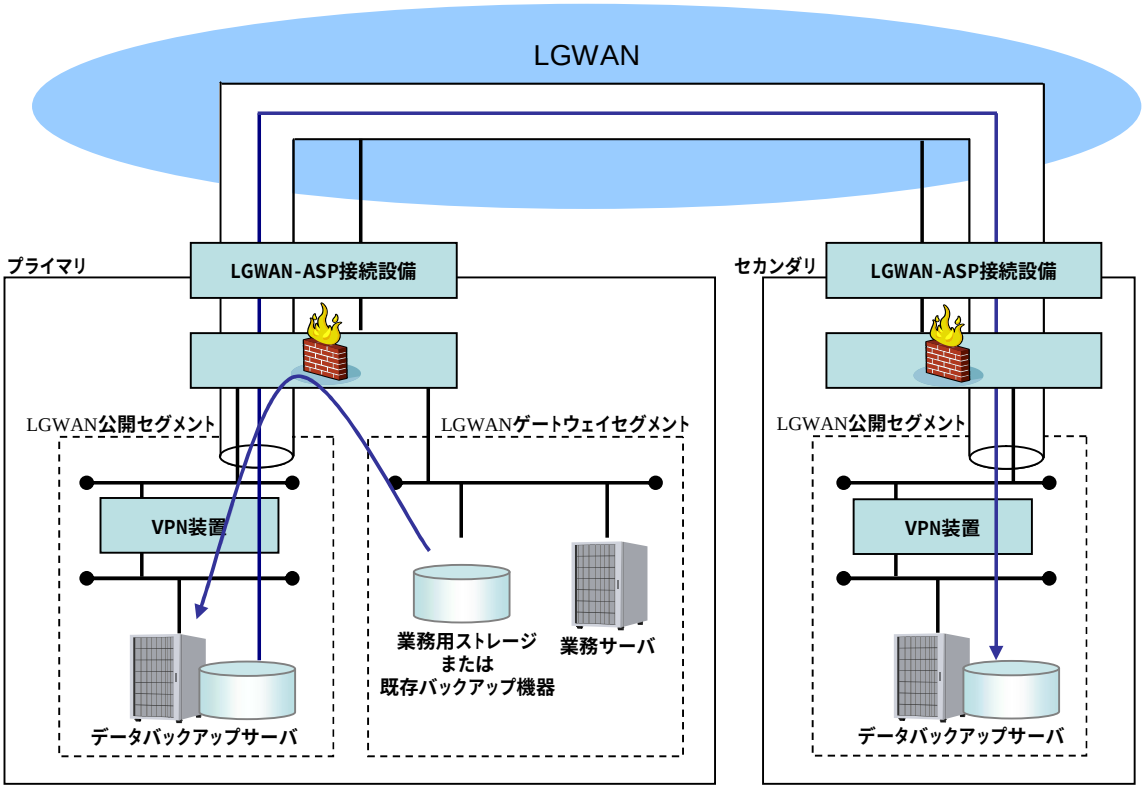

図 2-5　トンネリング VPN の構成イメージ

なお、LGWAN でのトンネリング VPN の実現に当たっては、「LGWAN-ASP 接続技術仕様書」、「LGWAN-ASP 接続手引き」にて示されている以下のいずれかの方法を選択する必要がある。

① Ethernet フレームの TCP/IP カプセル化
送信側、保管側のバックアップサーバのフロントに VPN ルータを設置し、その VPN ルータ間で VPN トンネリングを構成する。

② IPSec over TCP
送信側、保管側のバックアップサーバに VPN ソフトウェアをインストールし、バックアップサーバ間で VPN トンネリングを構成する。

また、都道府県域 DC 間、都道府県域 DC―地方公共団体庁内でトンネリング VPN を利用する場合は、LGWAN 運営主体への申請が必要であり、変更申請の場合は 2 週間程度、LGWAN-ASP の新規申請の場合は 3 ヶ月程度の審査期間を要することに留意が必要である。

3. 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 SLA の考え方を以下に示す。

3.1 SLA の適用範囲

本項で対象とする SLA については、図 1-1 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。

3.1.1 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。

3.1.2 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。

① 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 3-1 に示す。

表 3-1　目標復旧時点への対応

#	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

② 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。

ア 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。

イ 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。

4. 運用

4.1 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。

4.1.1 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。

① 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。

② 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。

ア 拡張性の有無
データ容量の拡張可否

イ 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

ウ 拡張時の費用体系
拡張を行う際の追加費用

4.1.2 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。

① 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。

② 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。

③ 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。）。

4.1.3 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。

① 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
② 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。
③ リストアに要する時間が SLA を満たしていること
④ 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

4.2 管理者に関する運用

標準仕様書に記述している自治体クラウドサービスを構築、利用する場合は、通常のシステム運用に係る管理者（サーバ管理者、ネットワーク管理者等）に加え、以下の管理者の設置を検討する必要がある。自治体クラウドサービスで必要な管理者を以下に示す。

4.2.1 バックアップ連携の管理者

① バックアップシステム管理者
バックアップシステム管理者はバックアップ連携のサービス提供者側にて必要であり、バックアップ領域（バックアップデータを配置する領域）及びバックアップスケジュール、バックアップデータの管理を行う必要がある。

4.2.2 自治体クラウドコンピューティングの管理者

① システム管理者
システム管理者は自治体クラウドコンピューティングのサービス提供者側にて必要であり、VM の追加、削除を行う必要がある。
② VM 管理者
VM 管理者は自治体クラウドコンピューティングのサービス提供者側にて必要であり、VM の起動・停止を行うが、システム管理者と兼務しても良い。

※ 自治体クラウドコンピューティングをクラウドサービスとして提供（仮想サーバを提供）する場合、VM 管理者はサービス調達者の役割であり、システム管理者は VM 管理者に対して、異なる VM への操作が行えないようにするなどのセキュリティ制限を設ける必要がある。

4.2.3 認証連携の管理者

① システム管理者
システム管理者は、認証連携のサービス提供者側にて必要であり、ID システム（IdP、SP など）の管理者として、利用者がシステムを正常に利用できるよう、運用・管理を行う必要がある。
② ID 管理者
ID 管理者は、認証連携のサービス調達者側にて必要であり、認証連携されているシステムの ID 発行や削除等の管理を行う。

5. セキュリティ

5.1 システムのセキュリティ対策

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。

5.2 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。

5.3 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。