自治体クラウドの情報セキュリティ対策等に関する調査研究　報告書

2013 年 5 月

総務省

はじめに

自治体クラウドによる地方公共団体の情報システム集約と共同利用の推進は、新たな情報通信技術戦略（平成 22 年 5 月 11 日、ＩＴ戦略本部）における「国民本位の電子行政の実現」のための重点施策の一つとして位置づけられているほか、新成長戦略～「元気な日本」復活のシナリオ～（平成 22 年 6 月 18 日閣議決定）におけるⅤ．科学・技術・情報通信立国戦略の中でも明示されており、地方公共団体における財政面等の負担軽減、行政事務の効率化、住民サービスの品質向上等を図るものである。さらに、「東日本大震災からの復興の基本方針」（平成 23 年 7 月 29 日東日本大震災復興対策本部）においては、「地方公共団体をはじめ幅広い分野へのクラウドサービスの導入推進など情報通信技術の利活用促進を行う。」が盛り込まれており、外部のデータセンターの活用による災害に強いシステムの構築が求められている。

自治体クラウドの推進に当たっては、情報セキュリティへの懸念から導入が躊躇されるケースも想定されているところである。また、社会保障・税番号制度（以下、「番号制度」という。）の導入が予定されている中で、自治体クラウドによるシステムの共同利用を図ることにより、番号制度に伴うシステム改修経費の抑制等にも寄与する可能性がある。番号法案附則第 6 条には、複数の地方公共団体の情報システムの共同化又は集約の推進について言及されている。

本事業は、上記を踏まえ、今後自治体クラウドに取り組もうとする自治体が留意すべき事項について調査研究を行い、その成果を普及することにより、自治体クラウドの一層の推進に資することを目的とするものである。

目 次

1. 自治体クラウドの取り組み状況

本章では、これまでの自治体クラウドの取り組み状況について、既存の検討資料を基に示す。

1.1 自治体クラウドの概要

本節では、自治体クラウドの概要について示す。

従来の地方公共団体における情報システムの導入に当たっては、自団体が管理する設備にハードウェア等を設置し、そのハードウェア上にソフトウェアを独自開発またはパッケージ利用等により導入する形が一般的であった。加えて、運用についても、基本的には当該団体が中心となって（必要に応じて、ハードウェア導入業者や運用業者等の支援を受けて）運用を行う「自庁導入（オンプレミス）」の形態が一般的であった。

近年、自庁内にハードウェア等を設置せず、予め事業者が所有するデータセンター等の設備に設置されたハードウェア及びソフトウェア等から、インターネットや専用線等のネットワークを経由してサービスとして利用する「クラウドコンピューティング技術（以下、「クラウド」という。）」が登場し、自庁導入に代わる情報システムの導入形態として注目を集めている。

「自治体クラウド」とは、上記のクラウドの進展、普及を踏まえ、地方公共団体においてクラウドを用いた情報システム導入を行うことを指す。自治体クラウドの推進のために、これまで総務省を中心に推進のための取り組みが実施されてきた。特に、複数の地方公共団体が一体となって、情報システムの共同化と集約化を進めることで、運用経費の削減等を図ることを目的としている。自治体クラウドの導入イメージについて、以下に示す。

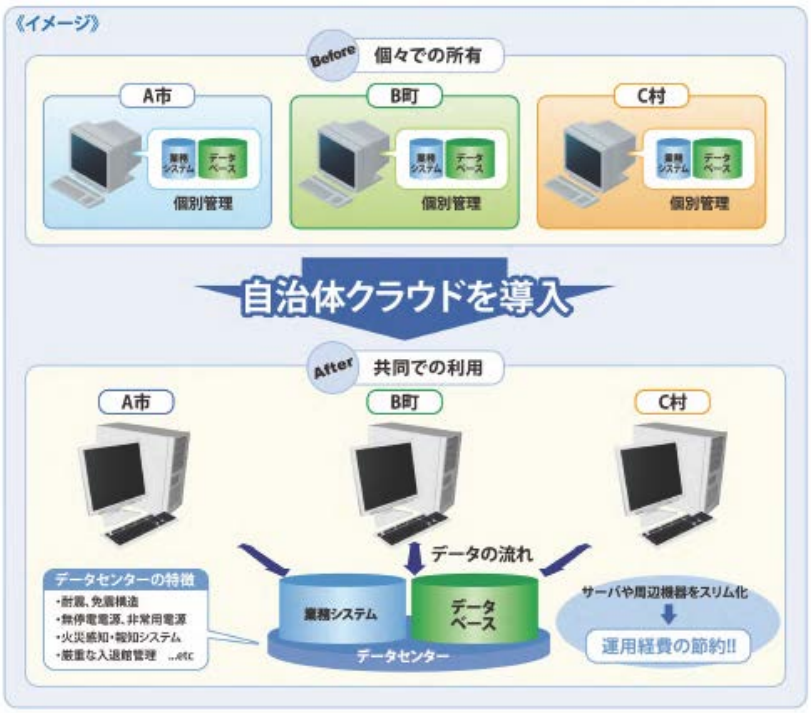


図 1-1 自治体クラウドの導入イメージ
（出典：「自治体クラウド解説用リーフレット」より抜粋
http://www.soumu.go.jp/main_content/000153859.pdf）

1.1.1　総務省における取り組み

本項では、総務省における自治体クラウドに関する取り組みについて示す。

(1) 自治体クラウド開発実証事業

総務省では、平成 21 年度から平成 22 年度にかけて「自治体クラウド開発実証事業」を実施し、6 都道府県、78 市町村において自治体クラウドの導入に係る実証実験が実施された。都道府県毎の参加団体及び実証の特色について、以下に示す。

表 1-1　参加団体及び実証の特色

開発実証団体	参加市町村	実証の特色
北海道	三笠市、深川市、恵庭市など計 29 団体	平成１５年から、「住民サービスの向上」や「行政の効率化・高度化」、「地域経済の活性化」を図ることを目的とした北海道独自の共同アウトソーシング構想である「北海道電子自治体プラットフォーム構想」を推進してきた。自治体クラウド開発実証においても自治体クラウドコンピューティングを利用した基盤に関する実証を重点的に行った。
京都府	福知山市、舞鶴市、綾部市など計 25 団体	京都府内では、平成９年度から京都府町村会事業として、自治体情報化推進事業（京都府町村会情報センター）を立ち上げるなどして、府内のシステム共同化を推進してきた。自治体クラウド開発実証において、さらなる共同化に向け基盤の共同化等を実証するとともに、自治体クラウドとして求められる都道府県域を越えたバックアップを確認した。
徳島県	徳島市、阿南市、吉野川市など計 8 団体	徳島県では、県内におけるＯＳＳ（オープンソースソフトウェア）の普及促進を目指し、産学官等で構成する徳島県ＯＳＳ勉強会を設立し、その活動を進めている。自治体クラウド開発実証においては、これら国産のプログラミング言語であるＲｕｂｙで開発した業務アプリケーションによる接続実証を行うとともに、京都府のデータセンターを利用し、ＬＧＷＡＮ経由で実施する文書管理システムでの実証及び遠隔会議の実証を行った。
佐賀県	武雄市、鹿島市、嬉野市など計 6 団体	県内全市町の情報システム共同化等を目指して知事及び全市町長によって構成される佐賀県ＩＣＴ推進機構を設立し、市町の情報システムにおける共同化の推進を図っている。自治体クラウド開発実証では、共同利用化の効果の大きい住民情報、税、国民健康保険関係の業務について参加市町の業務改善を行った上で、業務アプリケーションプログラムに関する権利を確保した持続的発展可能な、新たな共同利用アプリケーションの開発とともに、仮想化等新たなクラウドコンピューティングを支える技術の実証を行った。
大分県・	（大分県）	大分県・宮崎県では、両県及び市町が一体となり、事務共通化の

開発実証団体	参加市町村	実証の特色
宮崎県	日田市、臼杵市、杵築市など計５団体 （宮崎県） 延岡市、日向市、串間市など計５団体	運用実証を実施。県域を越える業務アプリケーションの共同化を行い、今後の自治体クラウドの取り組みの一つのモデルとなる成果を提示した。また、ネットワーク障害等が発生しても住民票の発行等が窓口で行えるよう利用拠点バックアップ（市町村バックアップ）の実証を実施した。さらに、ＬＧＷＡＮの帯域がクラウドの実運用に耐えうることを確認するため、ＬＧＷＡＮの性能テストを実施した。

（出典：「自治体クラウド開発実証事業　調査研究報告書」
第２章「自治体クラウド開発実証の概要」より弊社作成
http://www.soumu.go.jp/main_content/000127520.pdf）

(2) 地方公共団体における ASP･SaaS 導入活用ガイドライン

上記の事業を踏まえ、地方公共団体が ASP・SaaS を活用する際の具体的課題や実効性のある取り組み方策等について検討が行われ、平成 22 年 4 月に「地方公共団体における ASP･SaaS 導入活用ガイドライン」として公開された。

同ガイドラインでは、ASP・SaaS の地方公共団体における活用領域として、調達仕様が比較的シンプルないわゆる情報系／庁内系システムにおける利用が中心となっていることが示されている。また、今後は、自治体クラウドなどによる情報システムの集約と共同利用の進展に合わせ、業務フローの複雑な基幹系業務（フロントオフィス業務）においても積極的な活用が期待される。

図 1-2　ASP・SaaS の活用分野

（出典：「地方公共団体における ASP･SaaS 導入活用ガイドライン」を一部加工
http://www.soumu.go.jp/main_content/000061414.pdf）

また、サービスの導入企画から利用（調達、利用、変更・中止）までの各プロセスにおいて、地方公共団体が検討すべき事項や留意点について記載されている。また、ASP・SaaS

の導入に当たっての SLA（Service Level Agreement）の考え方や、契約の進め方についても示されている。

図 1-3　ASP・SaaS 利用のプロセス

（出典：「地方公共団体における ASP･SaaS 導入活用ガイドライン」より抜粋
http://www.soumu.go.jp/main_content/000061414.pdf）

(3) 自治体クラウド推進本部の創設

平成 22 年 7 月に「自治体クラウド推進本部」が設置され、さらなる自治体クラウドの全国的な導入に向けた体制が構築された。

同本部では、「自治体クラウド推進本部有識者懇談会」が計 4 回にわたって行われ、その結果として、平成 23 年 6 月に「自治体クラウド推進本部有識者懇談会とりまとめ」及び「クラウドサービス導入による効果提案項目（例）」が示された。

同とりまとめでは、クラウドサービスを活用したデータ連携が、今後の電子自治体を実現するための各種機能の基盤として位置付けられている。「7　クラウド導入により期待される最適化社会を支えるシステムの方向性について」において、以下のように記載されている。

> クラウドサービスを活用したデータ連携が実現すれば、各自治体においても、プル型情報提供機能（ホームページによる情報提供等）、カスタマイズ機能（情報やレイアウト等を自由に設定する機能）、インテリジェント検索機能（複雑な行政手続きや書類名などの情報でも容易に検索できる機能）、プッシュ型情報提供機能（各自治体等から希望する利用者に情報を発信する機能）、エージェント型情報提供機能（利用者に関係する情報を収集）の実装等への道筋も明確になってくる。電子自治体は新たなステージに突入し始めたと言える。
>
> （出典：「自治体クラウド有識者懇談会とりまとめ」より抜粋
> http://www.soumu.go.jp/main_content/000121262.pdf）

(4) 被災地における自治体クラウドの導入支援

また、平成 23 年 3 月 11 日に発生した東日本大震災によって、多くの地方公共団体の情報システムが被災した。被災した地域の早期復興に資するために、被災地の地方公共団体における情報システムの早期復旧や災害に強い情報基盤の早期整備の促進を目指して、平成 23 年度から平成 24 年度にかけて、被災地における自治体クラウドの導入支援が実施された。

具体的には、計 21 団体に対して、住民情報に関するシステムのクラウド化に要する経費に対する補助金の交付を行った。加えて、クラウド化だけでなく、ネットワークの断絶に備えた庁内バックアップ等、付加的な取り組みを実現した団体も存在した。

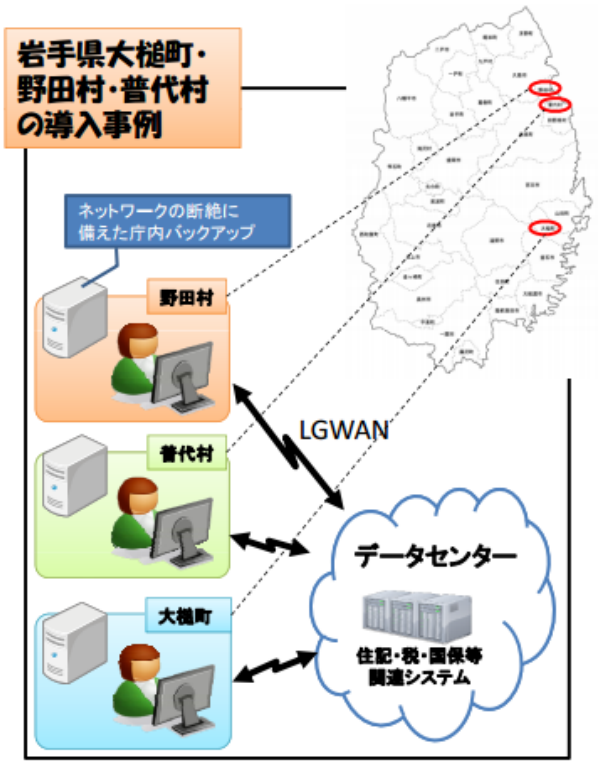


図 1-4　ASP・SaaS 利用のプロセス

（出典：自治体クラウド推進セミナー資料のうち
総務省「自治体クラウドの推進」より抜粋
https://www.lasdec.or.jp/cms/9,29258,21,119.html）

従来の自庁導入と比較した自治体クラウドの効果の一つとして、データセンター等の事業者側設備の利用に伴う迅速な導入、サービスの提供が可能である点が挙げられる。一刻も早い復旧が求められる被災地に対して、自治体クラウドの導入はニーズも多く、高い効果が得られるものと考えられる。今後の地方公共団体における業務継続計画（BCP：Business Continuity Plan）策定等にあたっても、自治体クラウドは有用な取り組みになりうると考えられる。

1.1.2　地方自治情報センターにおける取り組み

本項では、財団法人地方自治情報センター（LASDEC）における取り組みについて示す。

LASDEC では、自治体クラウドを促進するため、市区町村（政令指定都市を除く。）及び一部事務組合等（以下「市町村」という。）を対象に、「自治体クラウド・モデル団体支援事業」（平成 22 年度は、「自治体クラウド・共同アウトソーシング移行促進事業」として実施）を実施している。当事業における選定団体（地域）について、以下に示す。

表 1-2　自治体クラウド・モデル団体支援事業における選定団体（地域）

実施年度	選定団体（地域）
平成 22 年度	・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 ・奈良県基幹システム共同化検討会 （計 3 地域）
平成 23 年度	・北海道深川市、留萌市、弟子屈町 ・岐阜県美濃加茂市、坂祝町 ・熊本県錦町、宮崎県都農町、高原町、川南町 （計 3 地域）
平成 24 年度	・北海道名寄市、士別市、今金町 ・新潟県聖籠町、出雲崎町、関川村 ・愛知県岡崎市、豊橋市 ・愛知県豊川市、新城市、設楽町、東栄町、豊根村 （計 4 地域）

加えて、上記事業の成果等を基に、自治体クラウド導入促進の取り組みの一環として、自治体クラウド導入事例の調査結果をまとめた「地方公共団体におけるクラウド導入の取組み」が作成、公開されている。

当資料では、自治体クラウドの導入推進方法として、標準的な作業項目及びスケジュールが示されている。また、各作業項目における具体的な検討事項や留意点について示されており、将来的に自治体クラウドを導入することを検討している地方公共団体にとって参考となる点が記載されている。

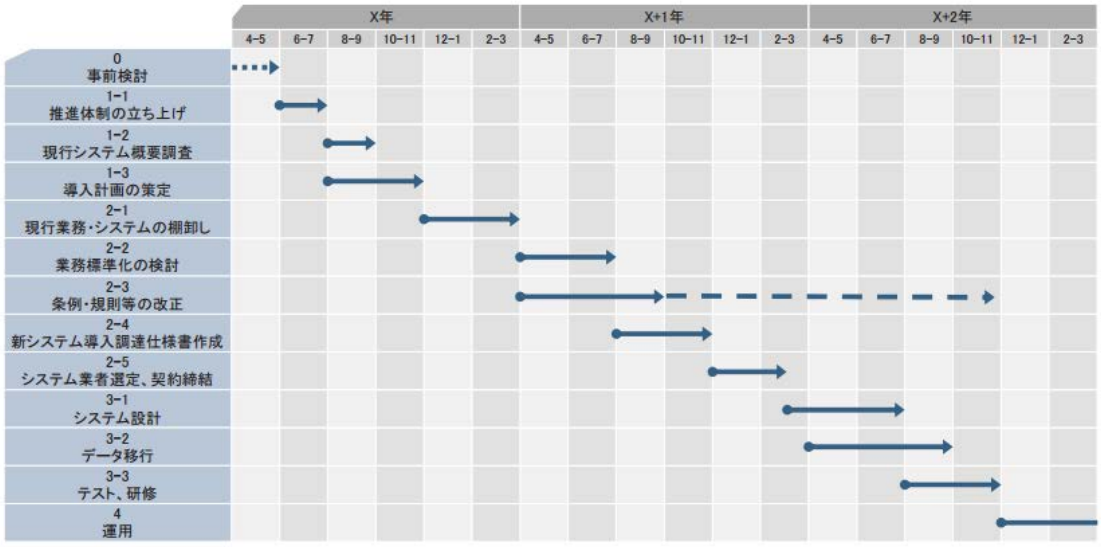


図 1-5　自治体クラウドの標準的な導入スケジュール
（出典：「地方公共団体におけるクラウド導入の取組み」より抜粋
https://www.lasdec.or.jp/cms/9,26589,21.html）

1.1.3　自治体クラウドの効果及び課題

本項では、自治体クラウドの導入によって期待される効果、及び導入に当たっての課題について、既存の調査、検討結果を基に示す。

(1) 自治体クラウド導入による効果

自治体クラウド導入による効果として、「地方公共団体におけるクラウド導入の取組み」では、以下のような例が示されている。

表 1-3　自治体クラウド導入による効果

項番	効果	概要
1	情報システムに係るコスト削減	自治体クラウド導入の各フェーズ（計画立案、仕様検討・システム選定、導入・移行、運用）で発生する各種経費について、「割り勘効果」等により１団体当たりの経費負担は少なくなる。
2	情報システムの管理・運用業務軽減	自治体クラウドでは、情報システムの管理・運用を含めてのサービス提供を受けるため、地方公共団体側の情報システム部署職員の作業負担軽減が見込まれる。さらに、各種の法制度改正等で必要となる情報システム対応の迅速な実施にも効果がある。
3	業務プロセス標準化による業務効率化	自治体クラウド導入には、情報システムの標準化・共同化を進めることが必要であり、参加団体それぞれの業務改革を通じて、事業者が提供するサービス（パッケージ機能）に合わせた業務プロセスの標準化を実施

項番	効果	概要
		することで、情報システム部署のみならず、基幹系業務等を行う部署にとっても、業務の効率化が期待できる。
4	情報セキュリティの確保	自治体クラウドでは、ハードウェア機器を厳重な入退室管理、24 時間 365 日の有人監視及び最新のセキュリティ技術を導入しているデータセンターに設置するため、個人情報を含む行政情報の保管について高いセキュリティが確保される。
5	住民サービスの向上	自治体クラウド導入を共同で進めることにより、中核となる地方公共団体の情報システム利用スキル（例：住基カードの共同発行、コンビニでの証明書交付や公金収納等）が、他の地方公共団体にも波及する効果が期待できる。
6	災害への対応強化	自治体クラウドは、ハードウェア設置場所の耐震性確保のほか、バックアップデータの遠隔地保管や地方公共団体間の相互支援を実現しやすい環境として、BCP 対応の観点からも効果的である。

（出典：「地方公共団体におけるクラウド導入の取組み」
「２．３　自治体クラウドの導入効果」を基に作成
https://www.lasdec.or.jp/cms/9,26589,21.html）

(2) 導入に当たっての課題

自治体クラウド導入に当たっての課題として、「地方公共団体におけるクラウド導入の取組み」では、以下のような例が示されている。

表 1-4　自治体クラウド導入に当たっての課題

項番	課題	概要
1	カスタマイズの制約	パッケージに対して利用団体ごとの独自仕様となるカスタマイズを行うことで、割り勘効果を通じた財源創出効果が減るため、パッケージに合わせた業務標準化を行う必要がある。
2	相互運用性の確保	データ移行に多額のコストが発生する場合、自治体クラウドのサービスを乗り換えることが難しく、ベンダロックインに陥る可能性があり、データ表現形式（データフォーマットやインターフェイス）の標準化によるサービス選択の柔軟性を高める必要がある。
3	情報セキュリティに係る技術的対策	クラウドサービス利用固有のセキュリティ問題（他の利用者によるクラウドシステム内部のデータへの攻撃）の解消や故障・障害への技術的対策、サービス提供事業者の信頼性確認が必要となる。

項番	課題	概要
4	情報セキュリティに係る法的留意点	データセンター設置場所やアクセス区域について国内限定とすることや情報セキュリティに係る監査体制の確保、利用団体における庁内 LAN やパソコンのセキュリティ対策といった点に留意する必要がある。

（出典：「地方公共団体におけるクラウド導入の取組み」
「３．３　自治体クラウド導入推進に係る動向」を基に作成
https://www.lasdec.or.jp/cms/9,26589,21.html）

1.2　ヒアリング調査の概要

本項では、本調査研究において実施したヒアリングの概要について示す。

1.2.1　ヒアリング調査項目

本調査研究では、「はじめに」に示したとおり、「情報セキュリティ対策」及び「番号制度の導入」という 2 つの観点から、自治体クラウド導入可能性や留意点等を調査し、自治体クラウドの一層の推進に資することを目的としている。ヒアリングに当たっても、上記 2 つの観点について、地方公共団体の現状及び課題認識を把握することを目的として実施した。

ヒアリング調査における調査項目について、以下に示す。

表 1-5　ヒアリング調査項目

１．自治体クラウドの情報セキュリティ対策等について

（１）クラウド環境にて留意すべきセキュリティリスクについて

- 自治体でクラウド環境を導入する上で、次に挙げるリスクの中で特に留意すべき項目はどれですか？（複数あれば３つ程度選択してください）
  - 共同利用時の料金負担の公平性
  - 不明瞭な SLA
  - ノンカスタマイズの場合の業務改革コスト
  - ベンダロックイン
  - セキュリティモデル、品質モデルのカスタマイズ
  - 既存システムとのデータ連係
  - アクセス権限の管理（クラウド事業者側を含む）
  - アプリケーションの応答速度
  - データ保管場所と法制度
  - ソフトウェアライセンスの移行
- そのうち、クラウド環境を導入した後に課題となったものはありますか？

（２）自治体とクラウド事業者の責任分界のあり方について

- 現在使用しているクラウド環境で取り決めているサービス水準(SLA 等)では、次の SLA 項目を定めていますか？

- サービス時間（24 時間 365 日、など）
- サービス稼働率（99.9%、など）
- ディザスタリカバリ方法（遠隔地へのデータバックアップ、など）
- 障害発生時等に提供されるバックアップデータ形式（標準フォーマット、など）
- 平均復旧時間（1 時間以内、など）
- サービス提供状況の確認方法（ホームページ上で公開、など）
- カスタマイズ性（利用者側でのカスタマイズ可能な項目、など）
- 同時接続利用者数（同時 50 ユーザ、など）
- データバックアップの方法
- バックアップデータの保管期間

● 現在取り決めていないが、今後は取り入れていきたいと考えている SLA 項目はありますか？

● クラウド事業者との責任分界を考える上で、自治体側の課題にはどのようなものがありますか？
（例：サービス水準を高くするとコスト高になる、専従者がいないために適切なサービス水準が定められない、など）

● SLA の各項目の評価方法を定めていますか？

● 判定結果をもとに、SLA の見直しを行ったり、試験運用期間を設けたりする予定はありますか？

（3）クラウド環境の障害発生時の対応について

● クラウド環境やネットワークに障害が発生した場合の、業務継続のために自治体側で実施している対策はありますか？
（例：データのバックアップ、バックアップ回線の準備、他のクラウド環境への移行計画、バックアップデータの標準化、障害対応訓練の実施、など）

● 現在は実施していない対策のうち、今後優先的に取り組む予定のものはありますか？

（4）クラウド環境におけるセキュリティポリシーについて

● 現在利用しているクラウド環境では、どのようなセキュリティポリシーを定めていますか。

● 個人情報等、機微な情報をクラウド環境で扱う場合に、現状のセキュリティポリシーで改善すべき点はありますか？

（5）自治体クラウドの導入効果について

● 自治体クラウドを導入した結果、どのような効果がありましたか？
（例：コスト削減、職員の負荷軽減、障害などの発生件数の減少、住民向け情報

サービスの向上、など）

- そのうち、定量的に確認出来ている項目はありますか？
- 上記の導入効果から派生して現れている効果や、今後期待される波及効果はありますか？

（削減したコストの住民サービスへの振り分け、職員の負荷軽減による新たな住民サービスの立ち上げ、など）

２．　番号制度対応に関する質問事項

（１）業務システムの共同化、クラウド化の状況について

- 別表第 1（別添参照）、別表第 2（別添参照）に記載された事務を行うための業務システムのうち、既に共同利用している業務システムはありますか？
- 別表第 1、別表第 2 に記載された事務を行うための業務システムのうち、既に団体個別にクラウド利用している業務システムはありますか？

（２）検討・推進体制について

- 番号制度対応について共同で検討・推進する体制はできていますか？どのようなものですか？
- 団体内において、共同検討のための体制はできていますか？どのようなものですか？
- 団体内において、番号制度対応検討のための体制はできていますか？どのようなものですか？

（３）調達について

- 番号制度に対応するために、以下の調達が発生すると考えられます。
  - 既存システムの改修・機能追加
    - イ）個人番号及び符号の取得
    - ロ）別表第 1 に記載されている事務についての番号対応（法人番号、個人番号の登録機能と番号による検索機能の開発、画面や帳票への番号表示・番号印字のための改修）
    - ハ）別表第 2 に記載されている事務についての番号対応（別表第 2 に記載されている事務ごとの特定個人情報のデータ抽出機能、対応する業務システムに共通する統合宛名番号の生成、登録、検索機能の開発）
    - ニ）統合宛名番号と符号との紐づけ機能の開発
    - ホ）照会した特定個人情報に対する回答電文の取込機能の開発
    - ヘ）中間サーバとの OLTP 接続機能の開発（任意）
  - 中間サーバの稼動準備、運用
    - イ）中間サーバのアプリケーション（個別部分）の設計開発・導入
    - ロ）ハードウェア及びネットワーク等中間サーバの稼動環境整備

ハ）中間サーバのアプリケーションの導入（セットアップ、既存システムとの接続、権限設定等）

ニ）中間サーバの運用

・ インターフェイスシステムの稼動準備

イ）インターフェイスシステムの稼動環境整備

ロ）インターフェイスシステムの導入（セットアップ、情報提供ネットワークシステム（コアシステム）との接続等）

- 上記に関して、共同で検討を始めていますか？
- 上記に関して、共同で取り組む予定はありますか？
- 共同で取り組むためにどのような準備をしていますか？

（4）中間サーバのクラウド利用について

- 中間サーバをクラウドにて運用する場合、クラウドベンダ選定に関してどのような点を重視しますか？
- 中間サーバをクラウドにて運用する場合、契約主体はどのように考えていますか？（団体ごと、事務組合、代表団体など）
- 団体ごとに、仮想化サーバを個別に契約する予定ですか？
- ファイアウォールの設置、ネットワーク整備など、現時点ではどのような課題があると考えていますか？

（5）費用負担、参加団体について

- 番号制度対応に係る費用負担はどのようにする予定ですか？
- 番号制度対応を機に、参加団体に変化はありますか（新たに募集するなど）？

（6）法制度・規約類の対応について

- 団体における業務システムのセキュリティポリシーは、情報提供ネットワークシステムに接続することができるようになっていますか？
- 団体における個人情報保護条例は、情報提供ネットワークシステムに接続することができるようになっていますか？
- 団体における文書管理規定等、他団体との情報授受について定めた規定類は、情報照会、情報提供する上で、支障ないもの（送受信のつどの決裁は不要等）になっていますか？
- 第 17 条を活用して、別表第 2 に記載された事務以外に、条例を定めて共同利用参加団体間で情報連携しようと考えている事項はありますか？
- これまでにクラウドや外部のデータセンターを利用した際に実施した手続きなどについて、番号制度対応時に活用できる事項はありますか？

以上

別添

1. 別表第 1、別表第 2 について

- 別表第 1 とは、法案第 6 条（利用範囲）にて、個人番号を利用することができる者及び利用できる事務を記載した一覧、別表第 2 とは第 17 条（特定個人情報の提供の制限）にて、国が用意する情報提供ネットワークシステムを使用して、提供すべき特定個人情報の種類、当該特定個人情報を提供する者及び提供できる事務を記載した一覧である。
- 別表第 1、別表第 2 では市町村は、「市町村長」「医療保険者（国民健康保険組合）」「教育委員会」「共済」等の事務遂行者として登場する。

2. 別表第 1 への対応について

- 別表第 1 では、市町村は、市民および職員の地方税の賦課徴収等の事務や、児童福祉、障害者福祉、高齢者福祉等の福祉に係る事務、国民健康保険、介護保険の保険給付の支給や保険料の徴収等の事務などに個人番号を利用することとなっている。
- 個人番号の利用は、法案審議の状況にもよるが、平成 28 年からと見込まれており、上記事務を行うシステムに関して、個人番号の入力機能、個人番号を使った検索機能、帳票類への個人番号の出力機能等を追加する必要がある。

3. 別表第 2 への対応について

- 別表第 2 では、市民および職員の地方税の賦課徴収等の事務や、上記に上げた福祉、保健業務に必要な特定個人情報を他機関に照会できること、および他機関から照会を受けて提供すべきこととなっている。
- 情報提供ネットワークシステムを使用した情報連携は、番号利用開始の 1 年半後をめどに、順次開始することが予定されているため、上記事務を行うシステムと中間サーバとのデータ受け渡しのための機能追加などが必要である。

1.2.2　ヒアリング対象団体の概要

本節では、ヒアリング対象団体の概要について示す。

表 1-6　ヒアリング団体の概要

項番	ヒアリング団体	共同利用対象地域	概要
1	神奈川県町村情報システム共同事業組合	羽山町、寒川町、大磯町など （県下の全 14 町村）	・基幹系、内部系合わせて 46 業務システムを共同化し、H23 年 9 月より共同システムが稼動している。 ・コスト削減効果として、各団体 61%～30%の削減を達成した。
2	新潟県三条市	新潟県長岡市、三条市、魚沼市、見附市、粟島浦村（計 4 市 1 村）	・左記 4 市 1 村における住民情報系システムの共同利用についての検討を実施している。 ・団体間で人口規模の差が比較的大きい。
3	福岡電子自治体協議会	（検討中）	・福岡県内の地方公共団体について、共同利用についての検討を実施している。
4	熊本県錦町	熊本県錦町、宮崎県都農町、高原町、川南町 （計 4 町）	・平成 23 年度自治体クラウド・モデル団体支援事業の対象団体である。 ・県と市町村との両システムについて、県域をまたいだ形での共同利用を実現している。
5	岐阜県美濃加茂市	岐阜県美濃加茂市、坂祝町 （計 1 市 1 町）	・平成 23 年度自治体クラウド・モデル団体支援事業の対象団体である。 ・一部業務において、単一のデータベース・アプリケーションを用いたマルチテナント形態の共同利用を実現している。

2. 自治体クラウドの情報セキュリティ対策

2.1 国内外におけるセキュリティ事案の動向

2.1.1 国内外のサイバー攻撃の事例

(1) サイバー攻撃等のセキュリティ事案の動向

サイバー攻撃等の情報セキュリティ事案（インシデント）とは、情報資産が損なわれた状態であり、何らかの脅威により、以下のような事象が発生した状態を示す。

- 運用停止（業務停止）
- 情報消失・破壊
- 不正アクセス（改ざん、盗聴、なりすまし、踏み台）
- 情報漏洩

IPA（独立行政法人情報処理推進機構）では、ウィルスやウェブ改ざんなどの届出を受けて各種インシデントを把握しており、毎年 10 大脅威としてまとめている。2012 年版の脅威として、4 位にはソフトウェア脆弱性、5 位ウェブサイト改ざんなどが挙げられている。以下に、IPA による 2012 年版の 10 大脅威を示す。

表 2-1 IPA による 2012 年版 10 大脅威

1 位 機密情報が盗まれる!? 新しいタイプの攻撃(標的型攻撃)
2 位 予測不能の災害発生！引き起こされた業務停止
3 位 特定できぬ、共通思想集団による攻撃
4 位 更新忘れのクライアントソフトを狙った攻撃
5 位 ウェブサイトを狙った攻撃
6 位 スマートフォンやタブレットを狙った攻撃
7 位 大丈夫 !? 電子証明書に思わぬ落し穴
8 位 身近に潜む魔の手・あなた職場は大丈夫？(内部犯行・情報漏洩の脅威)
9 位 危ない！アカウントの使まわしが被害を拡大
10 位 利用者情報の不適切な取扱いによる信用失墜(プライバシーに係る問題)

（出典：IPA「2012 年版 10 大脅威　変化・増大する脅威！」）

NISC（内閣官房情報セキュリティセンター）では、政府機関等を含む重要インフラ分野の情報システムを守るために、「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」改定版を 2012 年 4 月に発行している。ここでは 2013 年度までに国として取り組むべき施策や重要インフラ事業者等に期待する事項がまとめられているが、特に改定版においては、次の観点での改定が行われている。

- 東日本大震災発生時における複数の IT システムの同時的障害発生の考慮
- IT システム （制御システムを含む）に対するサイバー攻撃等の環境変化
- BCP 等の充実
- 環境変化を踏まえた安全基準の改善

・　情報共有体制の強化、等

前項の情報セキュリティ事案と、IPA や NISC における取り組みを踏まえると、近年のサイバー攻撃として特に注目すべき内容は次の通りである。

1）標的型攻撃

標的型攻撃とは、組織内の従業員・職員等を標的として巧妙に作られたメールを送り付けてシステムにウィルスを感染させ、外部からの侵入口を作り、情報搾取などを行うものである。IPA の 2012 年版 10 大脅威では 1 位となっており、新たに顕在化した脅威として挙げられている。

標的型攻撃は APT（Advanced Persistent Threat : 先進的で執拗な脅威）とも呼ばれており、従業員の情報を電話などのオフラインで入手するなど、ソーシャルエンジニアリングの手法を組み合わせることもあり、手口が年々巧妙化している。

2）不正アクセス

大手企業や官庁を攻撃対象にした悪意を持つ集団による攻撃が増えている。不正アクセス自体は古くから行われている攻撃手法だが、ソフトウェアの脆弱性が絶え間なく発見されるため、不正アクセスの脅威は継続していると言える。IPA の 10 大脅威でも、ウェブサイトを狙った攻撃は 2007 年から毎年取り上げられている。

近年では、不正アクセスが組織化しており、悪意を持つものと不正アクセスを行うものが分業化しているため、不正アクセスの対象になりやすい大手企業や官庁の脅威は増している。

3）制御システムに対する攻撃

従来は外部ネットワークとの接続を行っていないために、サイバー攻撃等とは無縁と考えられてきた制御システムにおけるセキュリティインシデントが増加している。NISC の第 2 次行動計画においても制御システムに対する注意喚起が行われており、IPA においても制御システムに対するセキュリティ対策に関する取り組みが始まっている。

とりわけ、2009 年にイランの核施設における遠心分離器の破壊を狙った Stuxnet（スタックスネット）と呼ばれるマルウェアは、標的型攻撃を制御システムに対して行った代表的な事例として注目されており、同様の手法で多くの制御システムが攻撃できる可能性を示した。

(2) サイバー攻撃等のセキュリティ事案

以下では、近年発生したセキュリティ事案の中で、特徴的なものを示す。

1）標的型攻撃

■ 三菱重工業における情報漏洩の可能性
2011 年 9 月、三菱重工業の機密情報（ミサイルや宇宙関連）を狙った攻撃が行われ、情報が漏洩した可能性がある。社員に対してマルウェア付きのメールを送信する標的型攻撃と考えられる。三菱重工業以外にも、同様な機密情報を取り扱う企業に対して、同時期に類似の攻撃が仕掛けられたものと思われる。

■ JAXA における情報流出
2012 年 1 月、JAXA のパソコンが標的となり、機密情報（物資補給機やロケット関連）が漏洩した可能性がある。2011 年 7 月に新種のウィルスが仕込まれた標的型メールが職員に送られ、アプリケーションソフトウェアの脆弱性を突かれて感染したものと思われる。

2）不正アクセス

■ PSN（プレイステーションネットワーク）における個人情報流出
2011 年 4 月、Sony のゲーム機「プレイステーション」向けのオンラインサービスである「PlayStation Network (PSN)」のサーバに対して、ソフトウェアの脆弱性（SQL インジェクション）を悪用した不正アクセスが行われた。全利用者 7,700 万人分の個人情報が盗まれた。

3）制御システムに対する攻撃

■ Stuxnet（スタックスネット）
2009 年の終わりから 2010 年の初頭にかけて、イランにある遠心分離器を含むシステムが Stuxnet と呼ばれるマルウェアに感染し、遠心分離器が破壊された。制御システムの SCADA と呼ばれるソフトウェアの脆弱性を狙われたもので、当該システムを事前に綿密に調査して実施された標的型攻撃と考えられる。

■ オーストラリアにおける下水処理システムに対する攻撃
2000 年にオーストラリアの SCADA ソフトウェアを開発する企業の元従業員が、上下水処理場の運営会社の職に応募したものの不採用とされたことに恨みを抱き、2 カ月間の間 46 回にわたって同社の下水処理の制御システムに侵入し、下水排水施設のデータを書き換えたりオペレーションを妨害し、結果として 264,000 ガロンもの未処理の下水を河川や公園に放出した。

■ 米国のビル設備監視制御システムに対する攻撃
2012 年 2 月に、米国ニュージャージー州の空調会社のビル制御システムに対して不正アクセスが行われた。制御システムのミドルウェアの脆弱性をついたもので、不正アクセスは確認されたが、実際の被害が起きる前に発見された。攻撃者側が SHODAN と呼

ばれるハッカー向け検索エンジンを使って当該ミドルウェアの脆弱性を調査して攻撃を行ったものと推測されている。

2.1.2　国内外のクラウドに関連したサイバー攻撃等のセキュリティ事案

(1) クラウドに関連したサイバー攻撃等のセキュリティ事案

クラウドに関連したサイバー攻撃等のセキュリティ事案として、近年発生した特徴的な事例を以下に示す。

- Vaserve へのゼロデイ攻撃
  英国の ISP Vaserv 社は、仮想化ソフト HyperVM を用いた安価なホスティングサービスを提供していた。2009 年 6 月に、HyperVM の未知の脆弱性を突いた攻撃（ゼロデイ攻撃）が行われた。多くの顧客は、バックアップなしでこのサービスを利用していたため、複数顧客のデータが消失した。影響は、10 万ウェブサイトに及んだ。

- Gmail 消失
  2011 年 2 月、Gmail の一部のメールが消失する障害が発生した。障害の影響は全 Gmail ユーザの 0.08%に及んだ。発生から約 24 時間経過した時点でも、全 Gmail ユーザの 0.02%がメールにアクセスできない状態となっていた。原因は、ストレージソフトウェアをアップデートした際にバグが混入したためであった。障害復旧のために、ストレージソフトウェアのバージョンを元に戻すことにより対応した。

- Amazon EC2 の大規模障害
  2011 年 4 月、Amazon の米国東海岸データセンターで稼動する EC2 の仮想マシンや、仮想マシンの外付けディスクである Amazon EBS の一部が利用できなくなった。障害発生当初は、Amazon EBS の障害が原因とされたが、実際にはネットワークの設定ミスであった。Amazon EBS 内のハードディスクを結ぶネットワークがダウンしたことが原因であった。ネットワーク設定が正常に戻った後、ミラーリングサーバが溢れ、コントロールプレーンも輻輳状態となった。障害は 4 日間継続し、EC2 を利用する他社のクラウドサービスも停止した。

- NTT PC コミュニケーションズの Cloud9 停止
  2011 年 5 月、NTT PC コミュニケーションズのクラウドサービス Cloud9 において、全仮想サーバへの接続が不可となった。ファイルシステムの不具合が原因であったが、長期に渡ってクラウドサービスが再開せず、利用者にはデータの取り出し方法と代替サービスの提供がアナウンスされた。

- 富士通クラウド上の自治体向け電子申請システム
  2011 年 11 月、電子自治体向けの電子申請システムで利用されていた富士通のクラウドに対して、30 あまりの IP アドレスから DDoS 攻撃に近いトラフィック集中が起こった。クラウドサービスを一時停止したため、10 県・約 200 市町村の電子申請サービスが一

時的に利用できない状況となった。

■ ファーストサーバにおけるファイル消失

2012 年 6 月、ファーストサーバのクラウドサービスにおいて、基盤ソフトウェアに対する更新プログラムの適用を、管理者の独断で本番サーバすべてに適用したところ、誤って全てのデータを削除してしまった。データ削除の対象にバックアップサーバも含まれていたため、多くのバックアップデータも消失した。

加えて、データ復元を試み、復元できたデータを顧客に渡したところ、別の顧客のデータを含んだものを渡してしまい、情報漏洩事故も発生した。

データ保全に対する備えが、保守要員を含めた保守運用で不十分であった。

(2) クラウドに関連したサイバー攻撃等のセキュリティ事案の動向

クラウドサービスの脆弱性を考える上での特徴として、以下のことが挙げられる。

- データセンターにリソース（サーバ、データベース、ミドルウェア、通信回線・機器、電源装置等）が集中している。
- 仮想化ソフト等基盤ソフトウェアには、データセンター内で共通製品を使っていることが多い。
- 仮想化ソフトには通常ハイパーバイザーの機能がある。

上記の特徴と、前項で示したセキュリティ事案を考えると、次のことが言える。

- ハイパーバイザー等の仮想化ソフトの脆弱性を突かれると、クラウド事業者のサービス全体に障害が発生する。
- 共有リソース（通信機器、電源装置、ミドルウェア等）の故障やそれに対する攻撃等により、被害が拡大する傾向がある。
- クラウド事業者の運用保守の手違いなどにより、障害が及ぶ範囲が広くなる傾向にある。

2.2　クラウド事業者におけるセキュリティ対策の評価

2.2.1　クラウド事業者のセキュリティ対策への取り組み事例

クラウド事業者のセキュリティ対策への取り組み状況として、特徴的な事業者における状況を以下に示す。

(1) IBM におけるセキュリティ対策の取り組み状況

IBM では、ビジネス要求に基づくセキュリティ要件を定義した「IBM セキュリティ・フレームワーク」があり、クラウドのセキュリティもこのフレームワークに基づいて実装している。以下に、「IBM セキュリティ・フレームワーク」に基づくクラウドセキュリティ要件を示す。

表 2-2　IBM セキュリティ・フレームワークとクラウドセキュリティ要件目

セキュリティ・ガバナンス、リスク・マネジメント、コンプライアンス
・　セキュリティの可視化 ・　コンプライアンス（法令遵守）の証明 ・　監査及び犯罪捜査への協力
人とアイデンティティー
・　認証、ID 連携、シングルサインオン ・　認可 ・　特権ユーザの監視
データと情報
・　保管データおよび伝送データの暗号化、暗号鍵の管理 ・　保管データの隔離 ・　個人情報、暗号化されたデータに対する法規制の遵守 ・　情報の機密区分の維持
アプリケーションとプロセス
・　安全な開発プロセスの遵守と維持 ・　提供するクラウドサービスのコンプライアンス
ネットワーク、サーバとエンドポイント
・　他のクラウド利用者とのネットワークの分離 ・　侵入検知／防止 ・　提供されるシステムイメージの安全性確保 ・　新しい脅威を想定した定期的見直し
物理インフラストラクチャー
・　物理セキュリティの確保（入退室管理、カメラによる監視）

（出典：http://www-935.ibm.com/services/jp/ja/it-services/presssum/jp-rs-its-cloud-security-2__a898080v14545y57.html を基に MRI 作成）

(2) ニフティクラウドにおけるセキュリティ対策の取り組み状況

ニフティクラウドにおけるクラウドセキュリティにおける主な実施項目を以下に示す。

表 2-3　ニフティクラウドセキュリティ対策実施項目

インフラを外部の攻撃から守る対策	
ネットワークセキュリティ	ニフティクラウドの管理システムについては、ネットワークを独立させることで外部からの侵入を防ぎ、さらにコントロールパネルは IDS による通信回線の監視により侵入検知を行っている。
センターセキュリティ	データセンターは赤外線センサーと監視カメラによる警備で守られており、施設内では生体認証装置など多階層のセキュリティポイントを設け、強固なセキュリティ対策をしている。
インフラを災害から守る対策	
センターの災害対策（耐震・免震対策、電源対策、火災対策）	直下型地震が起きても影響を受けにくい強固な地盤にセンターを設置、さらに免震構造で耐震型の二重床構造になっている。 火災対策については、超高感度煙探知機や窒素ガス消火設備の設置、停電対策についても複数系統受電、冗長化した UPS 設備設置、自家発電設備を完備している。
顧客の情報資産の保護	
システムの冗長化	サーバ、ストレージ、ネットワークはすべて完全二重化され、またストレージについては RAID6 相当の冗長化を行っている。これによりニフティクラウドのサービスを安定して継続提供し、顧客の情報資産を守っている。

（出典：http://cloud.nifty.com/policy/security.htm）

(3) 富士通におけるセキュリティ対策の取り組み状況

富士通クラウドのセキュリティ対策では、「仮想環境を外から守る」、「仮想環境の中を守る」、「ポリシーで守る」の 3 つの視点で実施している。

表 2-4　富士通クラウドのセキュリティ対策（3 つの「守る」）

仮想環境を外から守る	
脆弱性診断・管理	物理環境や仮想化環境にある OS やミドルウェアに潜む脆弱性を発見し結果をレポート提供。
ログ統合モニタリング	富士通のセキュリティオペレーションセンター（SOC）より、セキュリティに精通した専任技術者が 24 時間 365 日常時監視。
仮想環境の中を守る	
仮想化ファイアウォール、ウィルス対策	従来のネットワーク型セキュリティ対策では防げないゲスト OS 間の攻撃や不正なトラフィックを検知/防御。

特権ユーザ管理	管理者も含めた全てのユーザに対する強制アクセス制御を実施し、必要最小限のアクセス権限を付与することで、管理者に対しても機密情報へのアクセスをブロックして情報漏えいを防止、サーバのセキュリティを強化。
ポリシーで守る	
セキュリティコンサルティング	クラウドセキュリティガイドライン作成やポリシー見直し支援を実施。
統合 ID 管理（認証／シングルサインオン）	物理環境と仮想化環境、さらにプライベートクラウドとパブリッククラウドで構成される企業のシステム環境においてアカウント情報を一元管理。また、1 回のログオンのみでクラウドサービスを含む複数システムの業務画面を利用できるシングルサインオン環境を提供。

（出典：http://jp.fujitsu.com/solutions/cloud/support/security/）

2.2.2　クラウドサービスにおける情報セキュリティ対策に関するチェックリスト

クラウド事業者が提供する情報セキュリティ対策に関するチェックリストとして､特徴的なチェックリストの例を以下に示す。

(1) ニフティクラウドチェックリスト

ニフティクラウドでは､顧客からのセキュリティに関する問い合わせ内容について､以下のような確認事項を決めている。

表 2-5　ニフティクラウドチェックリスト

データ（情報）の保護
・　ログなどに関する確認事項 ・　アカウントの認証機能に関する確認事項 ・　システム運用・保守に使用する業務用アカウントの認証機能に関する確認事項 ・　インターネット、電話回線などのネットワークを利用に際する確認事項 ・　開発者や運用・保守者のアクセス権限に関する確認事項 ・　ファイアウォールに関する確認事項 ・　脆弱性情報等に関する確認事項 ・　データセンターの管理における確認事項 ・　システムの開発・検証の際の確認事項 ・　システムを構成するコンポーネントとして、外部の事業者が提供する製品、ソフトウェアを組み込む際の確認事項 ・　システムのセットアップ時の確認事項 ・　システム障害の影響を最小に抑えるための確認事項
サービス品質について
・　サービスレベル（SLA）に関する確認事項 ・　サービスサポートの稼動率、サービス稼働率に関する確認事項

事故・障害対策
・　障害、情報セキュリティ事項に関する確認事項
サポート・保守・監視
・　メンテナンスの告知に関する確認事項 ・　サーバにパッチをあてる際の確認事項 ・　運用と運用手順の記録に関する確認事項 ・　システムやネットワークの構成を示した仕様書や構成図などの管理情報に関する確認事項 ・　情報セキュリティ事故が発生した際の確認事項 ・　システムの開発者に関する確認事項 ・　ファイアウォールなどのポリシーや設定を変更した場合の確認事項 ・　サーバのソフトウェア、ハードウェアを変更した場合の確認事項 ・　ユーザ、ベンダの役割分担に関する確認事項
データセンターの災害対策
・　データセンターの地震、火災、雷対策に関する確認事項 ・　データセンターの電源、電源経路、UPS（無停電電源装置）に関する確認事項 ・　データセンターの自家発電設備に関する確認事項 ・　データセンターの空調設備に関する確認事項 ・　災害発生時の対応に関する確認事項

（出典：http://cloud.nifty.com/policy/security_faq.htm）

(2) JASA「クラウド情報セキュリティ管理基準」

特定非営利活動法人日本セキュリティ監査協会(JASA)が 2011 年度の経済産業省委託事業の一部として作成した「クラウドセキュリティ監査基準」では、クラウドサービスにおける情報セキュリティ対策に関するチェックリストの例を示している。以下に、チェックリスト中で示されている「リスクの種類」を示す。

表 2-6　JASA「クラウド情報セキュリティ管理基準」におけるリスクの種類

・　クラウドサービスにおける高集約化がもたらす悪影響 ・　クラウドサービスを構成する仮想システムで障害が発生することによる被害 ・　クラウドサービス内の他利用者の活動による悪影響 ・　クラウドサービスの提供に必要な資源の枯渇による被害 ・　クラウドサービスにおいて他利用者が自分のデータにアクセスすることによる被害 ・　クラウドサービスの基盤インフラへの攻撃がもたらす被害 ・　クラウドサービス事業者内での内部不正による被害 ・　クラウドサービスの管理用システムが不正利用されることによる被害 ・　クラウドサービスと利用者の間の通信回線上での攻撃による被害 ・　クラウドサービス上で消去したはずの情報の残留による被害 ・　クラウドサービスに対するサービス妨害攻撃による被害 ・　クラウドサービスにおける特定の規格への依存による悪影響 ・　クラウドサービスを利用することによるお客様におけるガバナンスへの影響

- クラウドサービスが利用している外部委託先での障害による被害
- クラウドサービス利用者の経済的損失を狙ったサービス妨害攻撃による被害
- クラウドサービスで用いる暗号鍵の不適切な扱いによる被害
- クラウドサービスに対する不正な探査による被害
- クラウドサービスに対する証拠提出命令と電子的証拠開示による悪影響
- クラウドサービス提供国との司法権の違いがもたらす悪影響
- クラウドサービス事業者が、所有者の許可なくデータを利用することによる被害
- クラウドサービス上でのライセンス管理に関するトラブル

（出典：http://www.jasa.jp/about/result/pdf2011/2011_cloud_doc05.pdf）

2.2.3　自治体クラウドとして留意すべき情報セキュリティ対策項目

自治体クラウドとして留意すべき情報セキュリティ対策項目について、今年度実施した5団体に対するヒアリング調査にて明らかになった点を以下に示す。

(1) ヒアリング結果のまとめ

ヒアリング調査の結果､各自治体において留意している自治体クラウドのセキュリティリスクは以下のとおりであった。

表 2-7　各自治体が留意しているセキュリティリスク

情報セキュリティ項目	ヒアリング対象団体				
	A	B	C	D	E
共同利用時の料金負担の公平性		○		○	
不明瞭な SLA			○		
ノンカスタマイズの場合の業務改革コスト	○			○	
ベンダロックイン		○			○
セキュリティモデル、品質モデルのカスタマイズ		○	○	○	
既存システムとのデータ連係					○
アクセス権限の管理（クラウド事業者側を含む）					○
アプリケーションの応答速度	○				○
データ保管場所と法制度		○	○	○	
ソフトウェアライセンスの移行					

記号：○=留意している

(2) セキュリティリスクに対するヒアリング結果

ヒアリングにおいて提示した各セキュリティリスクに対する各自治体のコメントを以下に示す。

1）共同利用時の料金負担の公平性

- 団体の規模により、システムの規模も異なる。中小規模の団体は規模の大きな団体が必要としている機能をそのまま使うことが考えられる。その場合の費用負担の割合については検討が必要である。
- 共同化に際して、団体ごとに個別にカスタマイズすることが必要となり、共通部分とは切り離して料金を設定した。一方で、人口規模が同じ団体同士が共同化を行う場合は、規模の違いによる課題は発生しなかった。
- 料金負担の公平性については、算定方法を工夫することにより解決可能である。

2）不明瞭な SLA

- 不明瞭な SLA を留意すべきセキュリティリスクととらえ、SLA 項目をクラウド業者と定めている。明確な SLA の締結は可能であると考えるが、ペナルティに関しては曖昧である。
- SLA を提示している業者は、その達成度合いに応じて利用料金の減額が定められている。未達成の場合には、その規定をそのまま課すことを考えている。

3）ノンカスタマイズの場合の業務改革コスト

- 事務の業務フローは人口規模によって異なる。例えば、小規模な団体などは受付から審査までを一人の職員が行うが、大規模な団体などは受付や審査などを分業で実施することが多い。
- 共同利用の対象が町村のみである場合は、事務の業務フローのすり合わせは、市などに比べると容易であった。一方、比較的大規模な団体とのすり合わせや、例外処理への対応は困難であった。
- カスタマイズがなるべく不要となるようなパッケージを選定した。クラウドの共同利用に当たっては、住民情報と税情報などのデータ連携を考慮することが必要不可欠である。データ連携機能については、従来は SI（システム・インテグレーション）で作り込んでいたが、小規模団体はその余裕がなく SI が難しい状況である。そのため、パッケージ選定の重要性は高い。
- 機能の共通化やカスタマイズについては、従来の業務フローを合わせるのではなく、パッケージの業務フローに自治体側が合わせた。

4）ベンダロックイン

- クラウド導入によって、ベンダロックインされる度合いは下がると考えられる。これは、クラウドの共同利用と、単独利用や自庁導入と比較した現時点での評価である。具体的にどのような箇所がベンダロックインになり得るかは、今後の評価による。
- ベンダロックインになり得る箇所として、データ移行のところがある。業者選定時に円滑な移行を可能とする旨を調達仕様書や契約書などに明記して合意している。しかし、業者を切り換える時などに実作業として円滑に移行が行えるどうかについては懸念している。

・　データ移行に関しては、ベンダロックインの問題がある。技術面だけでなく、料金面でもデータを出すだけでかなり高額な料金を請求された。価格交渉も困難であった。

5）セキュリティモデル、品質モデルのカスタマイズ

・　プライベートクラウドにおいては､セキュリティや品質に係るカスタマイズの柔軟性は確保されており、要求は満たしている。
・　クラウドへの移行に伴い、ネットワーク統合という意味で、物理的に切れていたものが統合された。庁内の自席で業務ができるようになるなど、利便性が上がったが、その分職員のセキュリティ意識を徹底する必要がある。セキュリティ対策はあまりしていなかったが、統合に伴い投資をすることで、統合後のセキュリティレベルを上げることができた。
・　セキュリティは自治体ごとの考えで設定できる。基となるセキュリティポリシーは共同利用団体間で一緒に最終審議した。セキュリティポリシーは全団体が作っていたが、内容にばらつきがあったため、見直しをして再度作り直した。

6）既存システムとのデータ連携

・　既存システムとのデータ連携は、調達仕様書で現行システムに合わせた対応を求めた。
・　既存システムではクライアント･サーバを使ってきたが､それをクラウド化することで、結果として業者を切り替えることになった。その際に、業者間でデータ連携が課題となった。業者間でデータ形式がまったく異なるため、どういう形で受け渡しをするかはかなり困難であった。前業者がデータをそのまま出すと技術流出になるため、加工したデータを新業者が取り込むことになった。

7）アクセス権限の管理（クラウド事業者側を含む）

・　従来のクライアント・サーバモデルでは、アクセス権限は「ユーザ」と「管理者」の 2 種類に大別されていた。クラウド共同利用モデルでは、管理者が「町村側の管理者」と「データセンター側の管理者」に分かれる。両管理者の役割分担や責任分界が曖昧な状況にあり、今後検討が必要である。
・　団体の業務データのセキュリティを考慮して、業務データにアクセスできないように、データセンターの管理者側には利用者用端末を配置していない。このため、障害発生時などに、データセンター側の管理者が、利用者用端末を用いて状況を把握することができないことが課題となっている。
・　クラウド導入後は、各個人のアクセス権限の設定が複雑で多岐にわたることから、その設定が行き届かなく､本来見られてはいけない内容が他の部署で見ることができることなどが発生した。そのようなことを個別に指摘して対応するという状況が多くあった。

8）アプリケーションの応答速度

・　稼働直後は､応答時間に係る SLA を達成できないこともあり､復旧にも時間を要した。原因の一つとして、画面上のデータ表示件数が挙げられる。当初は一画面で全件のデー

タを表示する仕様であったが、データ読み込みの待ち時間が大きいため、一画面で表示される件数を少なくするよう変更することで対応した。

- クラウド導入前のクライアント・サーバシステムよりも応答時間が遅くなった。サーバをスペックアップしても劇的に応答が速くなることはなかった。

9）データ保管場所と法制度

- 調達仕様書には、バックアップサイトの他に災害対策ということも含めたいと考えている。災害対策に対するコスト負担については、これまではベンダからの指摘はなかったが、RFI（情報提供依頼書）で情報提供された費用以上に求められることはないと考えている。
- バックアップサイトについては、災害発生後すぐに稼動するようなことは求めていない。最低限データが無くならないこと、その後は何日かかっても良いから業務が再開できることを求めている。
- 住民情報をパブリッククラウドの中に入れることについては団体の中で抵抗がある。
- 震災後、データの遠隔地バックアップを導入した。
- IaaS 利用の場合、ハードウェア障害などは IaaS 業者の責任であり、その上のアプリケーションとデータについてはアプリケーション業者に責任がある。このため、各層においてバックアップを取得する必要がある。
- ベンダが自社にデータセンターを持っていないケースでは、有事の場合に備えて、ベンダからの距離が近いデータセンター業者を選定した。

10）ソフトウェアライセンスの移行

留意すべき事項としてあげる団体はなかった。

2.2.4　クラウド事業者のセキュリティ対策を評価する仕組み

前項までに整理した、クラウド事業者側のセキュリティ対策と、自治体クラウドとして留意すべき情報セキュリティ対策項目を比較し、評価を行う仕組みを検討した。検討結果を以下の表に示す。

表 2-8 クラウド事業者のセキュリティ対策を評価する仕組み

セキュリティリスク	クラウド事業者評価の仕組み（案）
共同利用時の料金負担の公平性	自治体の規模の違いによる料金負担が適切かどうかを確認する。小規模な自治体に不要な機能により、料金が高くなっていないことの確認が必要である。
不明瞭な SLA	SLA の内容を確認する。 具体的な SLA 項目については「2.3 責任分界の在り方」に示す。
ノンカスタマイズの場合の業務改革コスト	従来システムからクラウドシステムへの移行時において、エンドユーザへの説明会等の開催、エンドユーザにとってわかりやすいマニュアル類の提供などを確認する。
ベンダロックイン	ベンダロックインについては、特にデータ移行の際に注意を要する。中間フォーマットなどの標準形式でデータをエクスポートできる機能や、それらのエクスポートデータ作成のコストなどの確認が必要である。
セキュリティモデル、品質モデルのカスタマイズ	セキュリティや品質に係るカスタマイズの柔軟性が確保されていることを確認する。クラウドとして標準的に提供されるセキュリティの水準に加えて、セキュリティを強化するためのオプションが選択可能かどうかを確認する。
既存システムとのデータ連携	自治体クラウドへの移行の過渡期において、庁内の既存システムとのデータ連携が可能かどうか確認する。
アクセス権限の管理（クラウド事業者側を含む）	クラウドの管理者に対する役割分担と責任分界が定められていることを確認する。 団体毎の管理者や、複数団体を束ねた管理者など、クラウド共同利用の形態に即した管理者権限、ユーザ権限が付与可能か確認する。
アプリケーションの応答速度	アプリケーション応答速度に関して SLA で定めているか、また定めたとおりのパフォーマンスが出ていることを利用者側で確認する仕組みがあるかを確認する。
データ保管場所と法制度	データセンター、バックアップの管理について確認をする。特にバックアップデータの取得頻度や保管先、個人情報等の機微情報に対する特別な取扱いの有無について確認をする。

2.3　責任分界の在り方

2.3.1　クラウド事業者の提供する SLA の事例

クラウド事業者が提供する SLA の事例として、国内の代表的なクラウド事業者が提示している SLA 項目やグレードの例を以下に示す。

(1) ニフティクラウド

国内の代表的な ISP（インターネット・サービス・プロバイダ）であるニフティが提供するパブリック・クラウドサービス「ニフティクラウド」が、2013 年 3 月現在公表している品質保証制度(SLA)では、稼働率についてサービス品質の水準を表 2-9 のように定めている。

表 2-9　ニフティクラウドにおける SLA

■サービス品質の水準
月間のサーバ稼働率が 99.95%以上であること。
■稼働率の考え方
月間稼働率＝（月間総稼動時間－累計障害時間）÷月間総稼動時間×１００
※ネットワーク環境やディスクの動作異常については、それによって影響を受けたサーバの台数を基準に、サーバ稼働率として換算します。
※5 分未満は切り捨てとします。
※累計障害時間については、5 分以上継続して以下のいずれかに定める状態にあったと、ニフティが確認した時間
（１）お客様が利用中のサーバに電源が入らない
（２）お客様が利用中のサーバに全くアクセスできない状態
（３）お客様が利用中のサーバに接続されているディスクに全くアクセスできない状態
■適用の除外
・　定期保守に伴うサービスの中断
・　サービスの保守を緊急に行う場合
・　本サービスの機能としての中断（HA 機能）
・　ユーザが本利用規約に違反したことによる場合
・　ドライバー又は OS 上の不具合による場合
・　ユーザ環境、インターネット環境の不具合又は DNS サーバの不具合によるドメインの停止など
・　仮想化ソフトウェアの不具合による場合
・　VPN 通信又はセキュアネットワーク機能の不具合による場合
・　オートスケール機能の不具合による場合
・　コントロールパネルの不具合による場合
・　第三者からの攻撃、妨害による場合
・　原因の如何を問わず、障害が継続した時間をユーザが測定できない場合

・　火災､停電等により本サービスの提供ができなくなった場合
・　地震､噴火､洪水､津波等の天災により本サービスの提供ができなくなった場合
・　戦争､動乱､暴動､騒乱､労働争議等により本サービスの提供ができなくなった場合
・　その他運用上あるいは技術上の理由により、ニフティが本サービスの一時的な中断が必要と判断した場合

（出典：http://cloud.nifty.com/sla/）

稼働率が 99.95%以上とは、例えば 1 ヶ月 30 日間連続稼働させた場合に、障害による停止時間が 20 分程度以内となる。

障害の停止時間に関しては、ニフティが確認した時間に限定すると共に、仮想化ソフトウェアの不具合や第三者からの攻撃・妨害については適用外としている。

⑵ NTT コミュニケーションズ「クラウド・エヌ」

国内最大手の広域通信会社である NTT コミュニケーションズが提供するパブリック･クラウドサービス「クラウド・エヌ」では、2013 年 3 月時点での仮想サーバにおけるサービスレベルアグリーメント(SLA)として、表 2-10 に示す事項を規定している。

表 2-10　クラウド・エヌにおける SLA

■仮想サーバに係る SLA サービス
本サービスにおいて、仮想サーバの稼働率を対象とする 99.99%のサービスレベルアグリーメントサービス（SLA）を提供します。
■計算方法
月間稼働率＝（１－累積障害時間÷月間総稼動時間）×１００
※累積障害時間は、料金月ごとに対象となる障害が発生した仮想サーバの障害時間（当社の責めに帰すべき理由により、仮想サーバが利用不可能になった状態が継続して発生した時間とし、1 分未満の時間は切り捨てるものとします。）を合算した時間とします。
■適用除外事項
・メンテナンス（緊急メンテナンスを含む）による停止の場合
・サービス利用者または第三者からの攻撃、妨害等による場合
・本サービスの機能としての中断（HA 機能）による場合

（出典：http://www.ntt.com/cloudn/data/sla.html）

前項のニフティクラウドと比較して、稼働率は 99.99%と高く、また 1 分以上の停止を累積するなど、厳しい条件を課している。適用除外事項については、ニフティクラウドと同程度と考えられる。

⑶ GMO クラウド

国内のビジネス向けパブリック･クラウドサービスの大手である GMO クラウドでは､2013 年 3 月時点で、表 2-11 に示すサービス品質保証制度（SLA）を規定している。

表 2-11　GMO クラウドにおける SLA

■サービス品質の水準

月間のサーバ稼働率：99.95%

■品質保証制度の概要

・対象の仮想サーバ：基盤システム上の不具合に起因する仮想サーバ

・障害発生の時間：障害発生時間が月 720 時間の 0.05%を越えた場合。

・稼動時間：月間とは、暦月の初日から末日までの期間

・障害時間：以下の時点から起算し、障害復旧を当社が確認するまでの期間

（1）お客さまが当社に対して障害が発生している旨を通知し、当社が障害の事実を確認した時。

（2）当社が障害の事実を確認し、これをお客さまに通知した時。

・障害復旧：仮想サーバがマイグレーションされ、サービスが立ち上がった時

・申告期限：障害復旧日から翌月の 20 日まで

■適用範囲

・基盤システムに起因する障害が稼働中の仮想サーバに発生した場合

・当社で管理しているネットワークに障害が発生した場合

■適用の除外

・米国ロケーションおよびマレーシアロケーションをご利用の場合

・ユーザによって仮想サーバが停止された場合

・クラウドコンソールの操作や閲覧ができない場合

・停止中の仮想サーバに対して障害が発生した場合

・当社のネットワークに接続するための回線に障害が発生した場合

・当社管理外の設備に起因して障害が発生した場合

・ユーザもしくは第 3 者が提供するサービスに起因して障害が発生した場合

・当社が保守作業を行う場合

・天災、疫病の蔓延、悪意の第三者による妨害行為により障害が発生した場合

・仮想サーバにインストールしたソフトウェア等に不具合があった場合

・利用約款の定める義務に違背する行為により障害が発生した場合

（出典：http://www.gmocloud.com/service/sla.html）

SLA の水準としては、ニフティクラウドと同程度といえる。データセンターのロケーションが海外の場合に SLA の適用範囲外としているが、これらは海外における電力事情や通信の安定性に起因しているものと考えられる。

2.3.2　自治体クラウドで必要とされる SLA 項目

本調査におけるヒアリング調査では、自治体クラウドにおいて必要とされる SLA 項目について確認をおこなった。以下の確認した結果を整理する。

表 2-12　必要とされる SLA 項目

SLA 項目	ヒアリング対象団体				
	A	B	C	D	E
サービス時間 （24 時間 365 日、など）	○	○	○	○	○
サービス稼働率 （99.9%、など）	○	○	○	○	○
ディザスタリカバリ方法 （遠隔地へのデータバックアップ、など）	○	○			
障害発生時等に提供されるバックアップデータ形式 （標準フォーマット、など)				○	
平均復旧時間 （1 時間以内、など）	○				○
サービス提供状況の確認方法 （ホームページ上で公開、など）	○	○	○	○	
カスタマイズ性 （利用者側でのカスタマイズ可能な項目、など）					
同時接続利用者数 （同時 50 ユーザ、など）					
データバックアップの方法	○	○	○	○	
バックアップデータの保管期間	○	○			

記号：○=規定している

各 SLA 項目に対する個別の状況については次の通りであった。

(1) サービス時間

- サービス時間については､開庁日の業務時間＋前後 1 時間程度をオンライン稼動の基本としている｡バッチ処理についてはオンライン稼動時間帯を外した夜間帯を想定している。
- クラウド環境における 24 時間 365 日の稼動は、自治体クラウドにおいては必ずしも求められていない。
- ただし、住民サービス等については 24 時間稼動が求められるため、今後そうしたサービスを拡張するためには、クラウド環境の強みが活かせる可能性が高い。

(2) サービス稼働率

- 昨今のクラウド環境におけるサービス稼働率 99.9%までは求めていないという意見が多かった。サービス稼働率を高く設定することでコスト増加が引き起こされるため、現実的な稼働率を設定することで、コスト削減を狙うケースが多い。
- 具体的には、99%～99.5%程度という意見が多かった。

(3) ディザスタリカバリ方法

- 東日本大震災の教訓から、ディザスタリカバリについてのニーズが高まっており、検討を進めている団体が多かった。
- 特に、遠隔地バックアップについては、自治体の地元業者が保有するデータセンターが地理的に近接していて、想定する広域災害に対応出来ない可能性を指摘する声があった。
- 複数の自治体の連携による遠隔地バックアップへの取り組みが有効と考えられる。

(4) 障害発生時等に提供されるバックアップデータ形式

- バックアップデータの形式としては、標準的なバックアップソフトウェアの出力形式や、データベースからのエクスポートなどを定めているケースがあった。
- ただし、それらは調達仕様書には記載するが、SLA で求めないとしているケースがあった。
- 平常時の障害に備えたバックアップに加えて、障害時の緊急対応に向けたバックアップデータの形式について、今後検討する必要がある。

(5) 平均復旧時間

- システムの冗長構成（物理的な二重化、仮想化による多重化など）により、短時間での復旧が可能な工夫はされている。
- 復旧時間短縮に向けた構成や、目標とする復旧時間については、調達仕様書には記載するが、SLA では求めないとしているケースがある。
- 一方、平均復旧時間を稼働率と同様の SLA 評価指標と考えて、定期的に評価を行っているケースもある。

(6) サービス提供状況の確認方法

- パブリッククラウドでは、エンドユーザがサービス稼働状況をリアルタイムに確認する方法を提供しているケースが多いが、自治体クラウドではクラウド事業者側からの連絡に頼っているケースが多い。
- 自治体側からクラウドサービスの稼働状況を確認する手段としては、エンドユーザとし

てサービスにアクセスしてメニューを表示するなどの方法がとられている。
・ 長期的なサービス提供状況については、運用サービス実績報告書を定期的（四半期毎など）に提出させているケースが多い。

(7) カスタマイズ性

・ カスタマイズ性については、自治体側で簡単な帳票修正ができることを確保したいとの意見があった。
・ データ利用については、EUC（エンド・ユーザ・コンピューティング）が可能な状態で、CSV 形式などで提供を求めているケースが多い。

(8) 同時接続利用者数

・ 同時接続利用者数を SLA で規定しているケースは少ないものと思われる。その理由としては、町村の規模が小さい場合には、現実的に同時利用が非常に少ないことが挙げられる。
・ ただし、自治体クラウドにおける複数市町村での共同利用において、繁忙期や突発的な事象で多数の同時利用が発生するケースも考えられるため、コストが過大にならない範囲で同時接続利用者数を SLA で定める必要がある。
・ バッチ処理については、市町村間で時期が重なることがあるため、実施スケジュールの調整が必要となる場合もある。

(9) データバックアップの方法

・ データバックアップの方法については、出力に使うソフトウェアや出力媒体（テープなど）を定めているケースがある。
・ バックアップの頻度や方法（フルバックアップ、差分バックアップなど）は特に規定していないため、バックアップやリストアの方法やそれらにかかる時間などは、クラウド事業者にゆだねられているケースが多いと考えられる。

(10) バックアップデータの保管期間

・ バックアップデータの保管期間について、特に明示していないケースがある。この場合に、何らかの理由により過去のデータを参照することや、障害発生時にバックアップデータでどこまでさかのぼれるかなど、クラウド事業者側の運用にゆだねられている可能性がある。

2.3.3　自治体クラウドにおける SLA のグレードの検討

自治体クラウドで必要とされる SLA 項目について、前項までに確認した自治体の取り組みなどを参考として、求めるべきグレードの案を検討した。検討結果を以下に示す。

表 2-13　SLA のグレードの検討

SLA 項目	求めるべきグレード（案）	検討のポイント
サービス時間	・市民向けサービスについては 24 時間 365 日（サービス停止時間は別途定める） ・職員向けサービスについては、開庁日時を基準に個別の事情に合わせて定める。 ・夜間バッチ処理に必要なサービス時間も別途定める。	・将来の市民サービス拡充を視野に入れて、24 時間 365 日の対応が可能なクラウドサービスを視野に入れる必要がある。 ・職員向けサービスについては、コストを中心に検討する。
サービス稼働率	・99%～99.5%程度を基本とする。	・将来のクラウドサービスの向上により、サービス稼働率をある程度高めてもコストに大きく影響しない可能性もある。
ディザスタリカバリ方法	・広域災害を想定した遠隔地へのバックアップが行われていること。 ・遠隔地のバックアップデータを用いた緊急対応の方法が定められていること。	・バックアップデータが確保出来ることに加えて、そのバックアップデータの利用方法についても確認しておく必要がある。
障害発生時等に提供されるバックアップデータ形式	・EUC（エンドユーザコンピューティング）で利用可能なデータ形式でデータが提供されること。	・EUC については、対応可能な職員の有無も重要な要件となるため、自治体毎の事情を勘案する必要がある。
平均復旧時間	・3 時間程度を基本とする。	・平均復旧時間を短くすることでコストが増加する場合が多いため、コストを中心に検討する。
サービス提供状況の確認方法	・オンラインでリアルタイムにサービス稼働状況が確認できること。 ・障害発生時には、自治体の管理者宛に電話やメールなど複数手段で自動的に連絡すること。	・クラウドの稼働状況については、自治体のシステム管理者が迅速に把握できる手段が必要である。

SLA 項目	求めるべきグレード（案）	検討のポイント
カスタマイズ性	・簡易な帳票の変更が利用者側で可能なこと。 ・EUC で利用可能なデータ形式で出力可能なこと。	・帳票の変更については、コストが大幅に増加したり、クラウド事業者のパッケージが対応していない可能性もあるため、個別に検討が必要である。
同時接続利用者数	・平常時に利用可能な同時接続利用者数を定めること。 ・特別な理由で同時接続利用者数が増えた場合に、一時的に増やす手段や手続きを定めること。	・平常時の同時利用者数を過大にすると、コストが増加してしまうため、平常時と平常時以外の対応を分けて考える必要がある。
データバックアップの方法	・バックアップの頻度、方法（フル、差分など）、保管媒体、バックアップデータ形式を定めること。	・クラウド事業者側でのバックアップの方法を自治体側でも把握しておき、業務継続に役立てる必要がある。
バックアップデータの保管期間	・バックアップの保管期間、保管する世代数、廃棄時の方法を定めること。	・確保可能な過去のデータを把握するとともに、廃棄方法についても定める必要がある。

2.3.4　クラウドの責任分界の考え方

前項までに整理した、自治体クラウドにおける SLA 項目やグレードに基づき、自治体クラウドを推進した場合の責任分界等の考え方の検討結果を以下に示す。

(1) 運用状況の確認について

- 障害発生を確認する主体はクラウド事業者だが、同時に自治体側のシステム管理者でも把握できる必要がある。
- 障害発生の一次報告を素早くシステム管理者に連絡することが重要である。原因の把握などはその後時間をかけても問題ないケースが多い。
- 自治体クラウドを共同利用しているケースでは、システム管理者側にはハードウェアに関する障害しか把握できない場合がある。エンドユーザが使うアプリケーションへのアクセス権が設定されていないと、自治体のエンドユーザから連絡を受けて、初めてシステム管理者が気づく場合がある。アプリケーションの稼働確認まで、自治体のシステム管理者ができる機能が必要である。
- エンドユーザからの問い合わせ対応として、クラウド事業者側に障害受付のコールセンター機能を設けることで、システム管理者の負荷を軽減すると共に、問い合わせ内容を記録することによる SLA 評価などへの活用も期待できる。

(2) SLA 未達に関する考え方

- SLA の各項目の達成度合いによって、利用料金の減額でペナルティを課すことも可能である。この場合に、運用サービス実績報告書などを定期的に求めて、SLA の達成状況を確認することが必要となる。
- セキュリティインシデントの発生については、最低限のペナルティは取り入れる必要がある。
- 一方、ペナルティを強くすると、「ペナルティを払えば済み」とクラウド事業者が曲解することや、大きなペナルティを課された事業者が撤退するなどの恐れがある。ペナルティのみならず、インセンティブへの配慮も必要である。
- 障害発生時のクラウド事業者の金銭的な負担と、障害発生に伴う市町村の担当者の負担等のバランスについては、対応要員の駆け付けに伴う実費などの負担のみとするか、それ以上の対応を求めていくか、今後の議論が必要である。

(3) SLA 見直しについて

- SLA の見直しについては、最低限年 1 回、場合によっては年に数回（四半期毎など）行うことが望ましい。
- SLA の見直しにあたっては、クラウド事業者から提出される運用サービス実績報告書などによる確認が基本となるが、自治体側でも独自に計測・評価が行える仕組みを持つことが望ましい。
- 例えばシステムのレスポンスタイムなどは、システム管理者や職員が手動で計測することも可能である。クラウド上にリアルタイムで確認可能なツールを用意することも検討すべきである。

(4) 複数事業者の責任分界について

- IaaS 事業者やパッケージベンダ、複数のアプリケーションベンダが自治体クラウドの各種機能を提供している場合、各事業者の責任分界を明確にしておく必要がある。
- 例えば、IaaS 事業者は仮想化ソフトウェアまで、ゲスト OS からミドルウェアまではパッケージベンダ、それ以外はアプリケーションベンダ、のように、対応する各事業者と調整の上、定める必要がある。
- 複数事業者が対応している場合に、運用開始後の責任分界の変更や SLA の変更は困難となるため、調達段階での明確化が重要である。
- 障害発生時の対応については、複数事業者による原因究明が困難な場合もおこりやすいため、対応体制の確立や、一次切り分け事業者の明確化などを行う必要がある。

2.4　ネットワーク障害時に備えた対策

2.4.1　ネットワーク障害パターンの整理

ネットワーク障害パターンとして、平常時の機器故障や、通信事業者やクラウド事業者側の障害、大規模災害時の広域障害などを類型化し、それぞれの状況を整理した。整理結果を以下に示す。

表 2-14　ネットワーク障害パターンの整理

ネットワーク障害のパターン	通信事業者			クラウド事業者			自治体庁舎	
	基幹網	局舎	アクセス回線	ハードウェア	基盤ソフトウェア	アプリケーション	通信機器	端末
(1)単独の通信障害			×					
(2)大規模通信障害	×							
(3)クラウドのハードウェア障害				×				
(4)クラウドのソフトウェア障害					×	×		
(5)自治体の通信機器障害							×	
(6)自治体の端末障害								×
(7)局所的な停電							×	×
(8)大規模災害時の広域障害（停電なし）	×	×	×					
(9)大規模災害時の広域障害（停電あり）	×	×	×				×	×

記号：×=障害発生

2.4.2　ネットワーク障害発生時の対策の検討

ネットワーク障害発生時の対策について、前項のネットワーク障害パターン別に検討した結果を以下に示す。なお、ネットワーク障害パターンと主な対策の対応については、下表の通りである。

表 2-15　ネットワーク障害パターンと主な対策の対応

ネットワーク障害のパターン	主な対策					
	アクセス回線を多重化	自庁社内機器の代替機を確保	自庁舎内にバックアップサーバを設置	自庁舎内にデータバックアップを確保	自庁舎に非常用発電装置等を備える	クラウド側の冗長化をSLA等で規定
(1)単独の通信障害	○		○			
(2)大規模通信障害			○	○		
(3)クラウドのハードウェア障害			○			○
(4)クラウドのソフトウェア障害			○			○
(5)自治体の通信機器障害	○	○				
(6)自治体の端末障害		○				
(7)局所的な停電	○				○	
(8)大規模災害時の広域障害（停電なし）			○			
(9)大規模災害時の広域障害（停電あり）			○		○	

記号：○=障害のパターンに関係する対策

(1) 単独の通信障害

- 単独の通信障害で通信事業者のアクセス回線に障害が発生した場合、障害が発生した地域の自治体庁舎からクラウドサービスが一時的に利用不能となる。
- 対策としては、異なる通信事業者を用いて、アクセス回線を 2 重化することが考えられる。
- アクセス回線の 2 重化のためには、その分のコストが余分に必要となるが、本調査でヒアリングを実施した小規模自治体では、バックアップ用回線を ADSL にすることでコスト削減を図る方策をとっている。
- アクセス回線の障害発生は起こりうるものとして、自庁舎内に重要な機能のみを搭載したサーバを設置するケースもある。

(2) 大規模通信障害

- 大規模通信障害により、通信事業者の基幹網に障害が発生した場合、自治体庁舎からクラウドまでの経路の一部に障害が発生することが予想され、その場合には自治体庁舎からクラウドサービスが一時的に利用不能となる。
- 通信障害の回復を待たずに業務を継続する場合には、平時から自庁舎内にバックアップサーバを準備し、データを定期的にアップデートしておく必要がある。
- バックアップサーバを自庁舎内に持つと、クラウド化によるコスト削減メリットが大幅に損なわれる可能性がある。このため、中小規模の自治体においては、EUC に必要なデータのバックアップのみを自庁舎内に置くことによる業務継続について検討する必要がある。

(3) クラウドのハードウェア障害

- クラウド事業者側のサーバやネットワーク機器のハードウェア障害により、一時的にクラウドサービスが利用不能となる。
- 一般にクラウド事業者側のハードウェアは冗長化されているが、複数機器が同時に故障することや、ネットワーク機器の新しいファームウェアの不具合や運用操作ミスによるサービス停止も想定できる。
- 対策としては、調達仕様書や SLA でハードウェアの冗長性を担保することや、クラウド事業者における運用状況の報告を求めることで、ハードウェア障害の発生確率を抑えることが考えられる。
- クラウドサービスの復旧を待たずに業務を継続するためには、代替サーバを自庁舎に設置する必要があるが、コストを抑えるためには最低限の機能のみを代替サーバに備えるようにする必要がある。

(4) クラウドのソフトウェア障害

- クラウド事業者側の基盤ソフトウェア（OS やミドルウェア）やアプリケーションの不具合により、一時的にクラウドサービスが利用不能となる。
- ソフトウェアのアップデートによる不具合であれば、クラウド事業者が以前のソフトウェアに戻すことで早期に回復が望めるが、ソフトウェアにゼロデイ脆弱性（修正プログラムが用意できていない脆弱性）が見つかった場合には、障害が長期化する恐れがある。
- 対策としては、調達仕様書や SLA でクラウド側のソフトウェアをマルチベンダにすることも考えられるが、コストを大幅に高くする要因となるため、多くのクラウド事業者では対応できないと考えられる。
- クラウドサービスの復旧を待たずに業務を継続するためには、代替サーバを自庁舎に設置する必要があるが、コストを抑えるためには最低限の機能のみを代替サーバに備えるようにする必要がある。

(5) 自治体の通信機器障害

- 自治体の通信機器の障害により、当該自治体の庁舎からクラウドサービスが一時的に利用不能となる。
- 通信機器には冗長化機能を備えたものが多いため、多くの自治体では主要な通信機器で冗長構成を取っているが、コスト上の制約から一部の通信機器で冗長構成を取っていないために、それが単一障害点となり、通信不能に陥ることがある。
- 対策としては、代替の通信機器をコールドスタンバイとして庁舎内に備えておき、故障発生時に速やかに交換できる体制を構築することが考えられる。
- 小規模自治体においてコスト削減を目指す場合には、クラウドと端末をインターネットなどの安価な通信回線上の VPN で接続する方法が考えられるが、セキュリティ上の課題を考慮して、是非を検討する必要がある。

(6) 自治体の端末障害

- 自治体の端末の障害により、当該端末からクラウドサービスが一時的に利用不能となる。
- クラウドサービスを利用する端末は、汎用のパソコンであるため、代替のパソコンは問題なく調達可能と考えられる。
- ただし、端末の OS やブラウザなどに脆弱性が発見された場合には、庁舎内の多くの端末で同じ問題を抱えることになるため、異なるブラウザや異なるバージョンの OS などで回避する方策も検討する必要がある。一時的な利用であれば、職員所有の端末（パソコンやタブレット端末など）の活用も検討すべきである。

(7) 局所的な停電

- 局所的な停電を想定すると、自治体庁舎内の通信機器や端末が利用できず、クラウドサービスが利用不能となる。
- 通信機器については、自治体庁舎に非常用発電装置の備えがあれば給電が可能となるが、端末への給電まで備えているケースは少ないため、バッテリー駆動可能なノートパソコンなどの利用が対策となる。
- 通信機器への給電が困難な場合に備えて、携帯電話網などの代替回線を用いた VPN 接続の利用についても検討すべきである。

(8) 大規模災害時の広域障害（停電なし）

- 停電を伴わない大規模災害により、通信事業者の設備に対する広域障害が起こった場合には、自治体庁舎からクラウドまでの通信経路に障害が発生して、クラウドサービスが利用不能となる。
- 対策としては、自治体庁舎内にバックアップサーバを設置して業務継続することが挙げられるが、「(2)大規模通信障害」と同様に、コスト対効果について検討する必要がある。大規模災害発生時には、最低限の業務（非常時優先業務）が限定されるため、それらの業務に必要な機能をバックアップサーバに備える必要がある。

(9) 大規模災害時の広域障害（停電あり）

・ 停電を伴う大規模災害により、通信事業者の設備に対する広域障害が起こった場合には、自治体庁舎からクラウドまでの通信経路に障害が発生するとともに、自治体庁舎においても端末の利用が困難となり、クラウドサービスが利用不能となる。
・ 対策としては、自治体が備える業務継続計画（BCP）において、最低限の業務（非常時優先業務など）をクラウドサービス無しで遂行できるように、代替手段を準備する必要がある。
・ 対策としては、非常用発電装置等を備えた自庁舎内のバックアップサーバによる業務継続が挙げられるが、コスト対効果について検討する必要がある。

2.4.3 ネットワーク障害発生時のその他の考慮点

ネットワーク障害発生時のその他の考慮点として、ヒアリング調査により得られた内容を以下に示す。

(1) 自治体側で実施するバックアップについて

・ バックアップサーバを自治体庁舎内に備えるにはコスト増加要因が大きいため、データのバックアップのみを自治体庁舎側に置くという考え方もある。
・ バックアップデータを自庁舎に置くだけで無く、2 次バックアップを他の遠隔の自治体に置くことで冗長性を高めることが可能となる。

(2) 障害対応の訓練について

・ 障害対応の訓練として、システム停止時を想定したパソコンによる業務や、計画停電を想定した自家発電装置への切替テストを実施した。訓練を行った結果、サーバやネットワークの切替がスムーズに行かなかったという例もあった。
・ クラウドにおいても、障害時にバックアップサイトに切り替える訓練を行って、動作を確認する必要がある。
・ クラウドを共同利用する場合には、クラウド事業者だけでなく、共同利用する自治体間での連絡体制の確立も必要である。

2.5　クラウド環境におけるセキュリティポリシー

2.5.1　自治体クラウドにおける個人情報保護条例への対応

(1) 個人情報保護条例の動向

個人情報保護に関する法律として、特に自治体クラウドにおける対応に留意するものには、自治体等の行政機関における個人情報の取扱いを定めた「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」（1988 年制定）がある。この法律では、自治体は個人情報の適切な取扱いを確保するため必要な施策を制定・実施するよう努力すべき旨が規定されており、自治体ではその対策を講じると共に、自治体個別の個人情報保護条例を制定する動きにもつながっている。自治体別の個人情報保護条例については、平成 20 年 4 月 1 日時点で、すべての都道府県（47 団体）・市区町村（1,811 団体）において策定されている。

(2) クラウドにおける個人情報取扱いに関する課題

自治体が保有する情報システムにおいては、上述した個人情報保護条例に基づいて個人情報の取扱いを実施してきたが、自治体クラウドへの取り組みが進むにつれて、様々な課題が明らかになってきた。以下にクラウドにおける個人情報取扱いに関する課題を示す。

1）信頼性および可用性

- データの格納場所
  クラウドにおいては、データの格納場所が特定できない場合があり、また自動的に移動してしまうことがある。これによりデータが確実に保管されていることを保証しにくくなる。特に、パブリッククラウドの場合は、個人情報が国境を越えて海外に持ち出されるリスクを想定する必要がある。
- データ保管ポリシー
  データのバックアップ方法や頻度など、データ保護の方法がクラウド側で定められ、自治体で自由に決められない可能性がある。また、一度定めたデータ保管ポリシーが、運用の途中で変更される可能性もある。
- プライバシー侵害の監視
  データ利用及び保管の運用をクラウド事業者にゆだねることになるため、プライバシー侵害が行われていないことを確認するために、クラウド事業者を監視する手段を確保する必要がある。
- 情報主体に対するアクセスの提供
  情報主体に対して、個人情報へのアクセス方法をどのような方法で提供するかが課題となる。セキュリティを確保しつつアクセス手段を提供する場合に、特別なセキュリティ対策が必要となり、自治体クラウドによるコスト削減効果を薄める可能性がある。

2）完全性

- データの確実な削除
  情報主体がデータの削除を求めたとき、クラウド事業者が情報を確実に削除したことを確認する必要がある。クラウドではデータ保護のために、冗長化や多重のバックアップが行われている可能性があり、それらを完全に削除できない可能性がある。
- 断片化された情報の取扱い
  クラウド上では冗長性確保のために、データを断片化して複数のサーバに分散して保持する場合がある。個別のサーバに格納され断片化された情報を、個人情報としてどのように取り扱うかが課題となる。

3）個人情報保護条例への対応

- 自治体が制定している個人情報保護条例で、データの外部持ち出しの禁止や、個人情報の庁内からの持ち出しの禁止を規定している場合、クラウドに個人情報を格納できなくなる可能性がある。

(3) 自治体クラウドにおける個人情報保護条例への対応

自治体クラウドにおいては、上述したような個人情報取扱い上の課題があるが、現時点で考慮されている対応について以下に示す。

1）信頼性及び可用性

- 従来の自庁に設置したサーバに対して、自治体クラウドではデータセンターにサーバが設置されることから、信頼性および可用性の向上が期待できる。
- 東日本大震災における教訓から、庁舎被災を想定したデータの管理体制や業務継続が重要であり、その確保のためには、セキュリティ対策が確保されたクラウドの利用が有効である。

2）完全性

- 完全性については、従来型の自治体システムにおける対策に加えて、上述したクラウド独自の課題に対して対応する必要がある。
- 特にデータの確実な削除については、クラウド事業者が運用中に確実に実施するように、契約等で保証する必要がある。

3）個人情報保護条例の改定について

- 自治体クラウド導入の先進的な取り組み事例のうち、個人情報保護条例に対応した自治体の例を表 2-16 に示す。

表 2-16　自治体クラウドにおける個人情報保護条例への対応

団体名	個人情報保護条例への対応
岐阜県美濃加茂市・坂祝町	住民情報を含むデータを外部のデータセンターで保管する点について、データセンターや接続回線の信頼性を評価した上で、各団体での個人情報保護審査会により許可を得た。
福井坂井地区広域市町村圏事務組合	各構成団体側の個人情報保護条例では、「通信回線を用いた電子計算機等と結合して実施機関以外に保有する個人情報を提供することができない」と定められている。しかし、例外として外部結合することがただし書きの規定に該当するかを確認するため、各団体の個人情報保護審査会に諮問するよう依頼した。諮問に対して、それぞれの個人情報保護審査会から、「公益上の必要がある」「個人の権利利益を不当に侵害するおそれがない」と判断する答申があった。

（出典：https://www.lasdec.or.jp/cms/resources/content/26589/5_Chapter5.pdf）

2.5.2　セキュリティポリシーの見直しのポイント

自治体クラウドにおける個人情報取扱いに関する課題を含めて、従来のセキュリティポリシーを自治体クラウド向けに見直す場合の、検討のポイントなどをヒアリング結果からまとめた。

(1) セキュリティポリシーの共同化と適用の範囲

- 複数団体で共同化を進める場合、クラウド環境のデータセンターやネットワークまでを共通化するセキュリティポリシー適用の範囲とし、各団体内のネットワークについては共同化の対象外とするケースがある。このように切り分けることで、比較的容易にセキュリティポリシーの共同化が可能である。ただし、あるべき姿としては、自治体の庁内ネットワークも統合されることが望ましい。
- クラウドによる共同化で、各団体でばらばらであった個人情報の取扱いが共通化される。この際に情報審議会にかけるかどうかは、団体毎の条例の解釈の違いに依存する。外部と接続することから、情報審議会にかけるケースもある。

(2) クラウド環境に適応したネットワーク構成

- ネットワーク構成は団体間で大きく異なる。業務システム毎にネットワークが異なる団体もあれば、統合されている団体もある。クラウド環境では、従来のクライアント・サーバ型向けの垂直統合的なネットワーク構成はそぐわない面もある。電話のように P2P で直結するようなネットワーク構成が実現できないか議論している。将来的には、ネットワークも含めたクラウド化、共同化もあり得ると考える。

・　ネットワーク構成の変更に伴い、セキュリティポリシー見直しの要否も検討が必要となる。

(3) クラウド化対象の違いによる見直しの要否

・　公共施設、電子申請などでクラウド化を実施した際にはセキュリティポリシーは変えなかった。しかし、住民情報系のクラウド化に際しては、セキュリティポリシーを見直す必要があると感じている。
・　従来のセキュリティポリシーの程度によっても要否は異なる。クラウドに変更する以前から基本的な ID・パスワードの管理、個人情報の管理、メディアの管理などを厳格に定めていた団体では、クラウド化によっても変更せずに対応できるケースもある。

(4) クラウド事業者の選定基準

・　個人情報を扱う場合には、適切なクラウド事業者の選定基準が必要である。
・　サービス要件定義書において、クラウド事業者に対して、ISO27001/ISMS やプライバシーマークの取得を求める団体もある。

(5) クラウド化に特化したセキュリティポリシー見直し項目

・　クラウド化を前提としたセキュリティポリシーにおいては、従来システムにおけるセキュリティポリシーに加えて、データの保管場所、暗号化、バックアップ、通信の暗号化、強固なユーザ認証、アクセス制限、セキュアなアプリケーションなども検討する必要がある。

3. 番号制度を踏まえた自治体クラウドの推進のあり方

番号制度の対応に当たり、地方公共団体は、住基、税務、福祉等の既存システムの改修に加え、新たな情報システムとして、中間サーバ等の構築を行うことが想定されている。加えて、既存システム及び中間サーバ等について、自治体クラウドを活用することも想定される。

本章では、既存システム及び中間サーバ等について、自治体クラウドを活用している、又は新たに活用することを検討している地方公共団体を主な読み手と想定し、番号制度の対応に当たって留意すべき事項について示す。なお、以下に示す内容は、2013 年 3 月時点の公開情報に基づく想定であり、番号制度に係る今後の詳細検討によって、変更が生じる可能性がある。

3.1 番号制度の概要

本節では、番号制度の概要について示す。

3.1.1 番号法案の検討経緯

番号制度とは、社会保障の充実・安定化と、そのための安定財源確保と財政健全化の同時達成を目指す社会保障と税の一体改革を推進するために必要な基盤として導入が検討されている制度であり、政府・与党社会保障改革本部により検討が進められてきた。「社会保障・税番号大綱（平成 23 年 6 月 30 日、政府・与党社会保障改革本部決定）」では、番号制度により実現できること及び必要な仕組みについて、以下のように記載されている。

表 3-1 番号制度により実現できること及び必要な仕組み

２．番号制度で何ができるのか

（１）よりきめ細やかな社会保障給付の実現
（２）所得把握の精度の向上等の実現
（３）災害時における活用
（４）自己の情報や必要なお知らせ等の情報を自宅のパソコン等から入手できる
（５）事務・手続の簡素化、負担軽減
（６）医療・介護等のサービスの質の向上等

３．番号制度に必要な３つの仕組み

付番 新たに国民一人ひとりに、唯一無二の、民 - 民 - 官で利用可能な、見える「番号」を最新の住所情報と関連づけて付番する仕組み

情報連携 複数の機関において、それぞれの機関ごとに「番号」やそれ以外の番号を付して管理している同一人の情報を紐付し、紐付けられた情報を活用する仕組み

本人確認 個人や法人が「番号」を利用する際、利用者が「番号」の持ち主であることを証明するための本人確認（公的認証）の仕組み

（出典：社会保障・税番号大綱 概要
（平成 23 年 6 月 30 日、政府・与党社会保障改革本部決定）より抜粋
http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/110630/gaiyou.pdf）

上記の検討に基づき、平成 25 年 3 月 1 日、番号制度を実現するための法律案として「行政手続における特定の個人を識別するための番号の利用等に関する法律案（以下、「番号法案」という。）」が第 183 回通常国会に提出された。番号法案では、番号制度の目的（第一条）や基本理念（第三条）のほか、用語の定義が以下のように示されている。

表 3-2　番号法案における用語の定義（抜粋）

項番	用語	定義	該当条文
1	個人情報	行政機関個人情報保護法第二条第二項に規定する個人情報であって行政機関が保有するもの、独立行政法人等個人情報保護法第二条第二項に規定する個人情報であって独立行政法人等が保有するもの又は個人情報の保護に関する法律第二条第一項に規定する個人情報であって行政機関及び独立行政法人等以外の者が保有するもの	第二条第三項
2	個人番号	住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるもの	第二条第五項
3	特定個人情報	個人番号をその内容に含む個人情報	第二条第八項
4	個人番号利用事務	行政機関、地方公共団体、独立行政法人等その他の行政事務を処理する者が第九条第一項又は第二項の規定によりその保有する特定個人情報ファイルにおいて個人情報を効率的に検索し、及び管理するために必要な限度で個人番号を利用して処理する事務	第二条第十項
5	個人番号関係事務	第九条第三項の規定により個人番号利用事務に関して行われる他人の個人番号を必要な限度で利用して行う事務	第二条第十一項
6	情報提供ネットワークシステム	行政機関の長等の使用に係る電子計算機を相互に電気通信回線で接続した電子情報処理組織であって、暗号その他その内容を容易に復元することができない通信の方法を用いて行われる第十九条第七号の規定による特定個人情報の提供を管理するために、第二十一条第一項の規定に基づき総務大臣が設置し、及び管理するもの	第二条第十四項

（出典：「行政手続における特定の個人を識別するための番号の利用等に関する法律案」より抜粋
http:/ http://www.cas.go.jp/jp/houan/130301bangou/houan_riyu.pdf）

加えて、番号法案別表第一では、個人番号を利用できる者及び事務の一覧が示されている。また、番号法案別表第二では、特定個人情報の情報照会者及び事務に対して、情報照会できる特定個人情報及びその情報提供者の一覧が示されている。

地方公共団体は、以下の機関として情報照会者及び情報提供者となることが想定され、各機関として行うべき事務及び特定個人情報について、情報照会及び情報提供を行うことが規定されている。

- 都道府県知事、市町村長
- 都道府県教育委員会、市町村教育委員会
- 国民健康保険組合
- 後期高齢者医療広域連合
- 地方公務員共済組合（地方職員共済組合、公立学校共済組合、警察共済組合、東京都職員共済組合、指定都市職員共済組合、市町村共済組合）、全国市町村職員共済組合連合会
- 地方公務員災害補償基金（支部）
- 都道府県社会福祉協議会、市町村社会福祉協議会　など

別表第一の抜粋を以下に示す。

表 3-3　番号法案別表第一（抜粋）

別表第一		
1	厚生労働大臣	健康保険法第五条第二項又は第百二十三条第二項の規定により厚生労働大臣が行うこととされた健康保険に関する事務であって主務省令で定めるもの
2	全国健康保険協会又は健康保険組合	健康保険法による保険給付の支給又は保険料等の徴収に関する事務であって主務省令で定めるもの
3	厚生労働大臣	船員保険法（昭和十四年法律第七十三号）第四条第二項の規定により厚生労働大臣が行うこととされた船員保険に関する事務であって主務省令で定めるもの
4	全国健康保険協会	船員保険法による保険給付、障害前払一時金若しくは遺族前払一時金の支給若しくは保険料等の徴収又は雇用保険法等の一部を改正する法律（平成十九年法律第三十号。以下「平成十九年法律第三十号」という。）附則第三十九条の規定によりなお従前の例によるものとされた平成十九年法律第三十号第四条の規定による改正前の船員保険法による保険給付の支給に関する事務であって主務省令で定めるもの
5	厚生労働大臣	労働者災害補償保険法（昭和二十二年法律第五十号）による保険給付の支給又は社会復帰促進等事業の実施に関する事務であって主務省令で定めるもの
6	都道府県知事	災害救助法（昭和二十二年法律第百十八号）による救助又は扶助金の支給に関する事務であって主務省令で定めるもの
7	都道府県知事	児童福祉法（昭和二十二年法律第百六十四号）による里親の認定、養育里親の登録、療育の給付、障害児入所給付費、高額障害児入所給付費、特定入所障害児食費等給付費若しくは障害児入所医療費の支給、医療の給付等の事業若しくは日常生活上の援助及び生活指導並びに就業の支援の実施、負担能力の認定又は費用の徴収若しくは支払命令に関する事務であって主務省令で定めるもの

（出典：「行政手続における特定の個人を識別するための番号の利用等に関する法律案」より抜粋
http:/ http://www.cas.go.jp/jp/houan/130301bangou/houan_riyu.pdf）

別表第二の抜粋を以下に示す。

表 3-4　番号法案別表第二（抜粋）

	情報照会者	事務	情報提供者	特定個人情報
1	厚生労働大臣	健康保険法第五条第二項の規定により厚生労働大臣が行うこととされた健康保険に関する事務であって主務省令で定めるもの	医療保険者（医療保険各法（健康保険法、船員保険法、私立学校教職員共済組合法、国公務員等共済組合法をいう。以下同じ。）により医療に関する給付の支給を行う全国健康保険協会、健康保険組合、日本私立学校振興・共済事業団、共済組合、市町村長又は国民健康保険組合をいう。以下同じ。）又は後期高齢者医療広域連合	医療保険各法又は高齢者の医療の確保に関する法律による医療に関する給付の支給又は保険料の徴収に関する情報（以下「医療保険給付関係情報」という。）であって主務省令で定めるもの
			市町村長	地方税法その他の地方税に関する法律に基づく条例の規定により算定した税額若しくはその算定の基礎となる事項に関する情報（以下「地方税関係情報」という。）、住民基本台帳法第七条第四号に規定する事項（以下「住民票関係情報」という。）又は介護保険法による保険給付の支給若しくは保険料の徴収に関する情報（以下「介護保険給付関係情報」という。）であって主務省令で定めるもの
			厚生労働大臣若しくは日本年金機構	国民年金法、私立学校教職員共済法、厚生年金保険法、国家公務員共済組合法又は地方公務員等共済組合法による年金である給付の支給又は保険料の徴収に関する情報（以下「年金給付関係情報」という。）であって主務省令で定めるもの
2	全国健康保険協会	健康保険法による保険給付の支給に関する事務であって主務省令で定めるもの	医療保険者又は後期高齢者医療広域連合	医療保険給付関係情報であって主務省令で定めるもの
			健康保険法第五十五条又は第百二十八条に規定する他の法令による給付の支給を行うこととされている者	健康保険法第五十五条又は第百二十八条に規定する他の法令による給付の支給に関する情報であって主務省令で定めるもの
			市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
			厚生労働大臣若しくは日本年金機構又は共済組合等	年金給付関係情報であって主務省令で定めるもの
3	健康保険組合	健康保険法による保険給付の支給に関する事務であって主務省令で定めるもの	医療保険者又は後期高齢者医療広域連合	医療保険給付関係情報であって主務省令で定めるもの
			健康保険法第五十五条に規定する他の法令による給付の支給を行うこととされている者	健康保険法第五十五条に規定する他の法令による給付の支給に関する情報であって主務省令で定めるもの
			市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
			厚生労働大臣若しくは日本年金機構又は共済組合等	年金給付関係情報であって主務省令で定めるもの
4	厚生労働大臣	船員保険法第四条第二項の規定により厚生労働大臣が行うこととされた船員保険に関する事務であって主務省令で定めるもの	医療保険者又は後期高齢者医療広域連合	医療保険給付関係情報であって主務省令で定めるもの
			市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
			厚生労働大臣若しくは日本年金機構又は共済組合等	年金給付関係情報であって主務省令で定めるもの

（出典：「行政手続における特定の個人を識別するための
番号の利用等に関する法律案」より抜粋
http:/ http://www.cas.go.jp/jp/houan/130301bangou/houan_riyu.pdf）

3.1.2　番号制度に係る情報システムの概要

番号制度の導入にあたっては、国は情報照会、情報提供及び提供記録の記録、保管のために情報提供ネットワークシステムを設置することとなっている（番号法案第二十一条、第二十三条）。また、地方公共団体においては、既存システムと情報提供ネットワークシステムとの接続に当たり、中間サーバを導入することが検討されている。

中間サーバの機能概要について、以下の機能が予定されており、具体的な機能要件等については、引き続き検討が行われている。

表 3-5　中間サーバの機能概要

項番	機能名	機能概要
1	情報照会／提供支援機能（仮称）	・インターフェイスシステム（情報提供ネットワークシステムの一部）から受領した情報を既存システムへ引継ぎ、また、既存システムで作成された情報照会者へ提供される情報をインターフェイスシステムへ引き渡す機能。
2	符号管理機能（仮称）	・既存システムの利用番号と符号を紐付け、管理する機能。

（出典：内閣官房　情報連携基盤技術ワーキンググループ（第 8 回）
資料 4-2「情報提供ネットワークシステム等の機能の概要（案）」
http://www.cas.go.jp/jp/seisaku/jouhouwg/renkei/dai8/siryou4-2.pdf）

3.2　中間サーバの共同利用

中間サーバは、地方公共団体にそれぞれ一台ずつ設置されることが想定されている。しかしながら、必ずしも物理的にハードウェアを分ける必要はなく、仮想化等で論理的に分割することで対応できるため、中間サーバ及びインターフェイスシステムについて、自治体クラウドを活用した共同利用が可能と考えられる。

本節では、中間サーバの共同利用による効果及び課題について、地方公共団体単独で自庁導入、運用を行う場合と比較した特徴を示す。また、既存システムを自治体クラウドで共同利用する場合との比較についても行う。

3.2.1　中間サーバの共同利用による効果

中間サーバの共同利用により実現できる効果について、中間サーバで特に配慮すべき特徴や留意点について検討する。

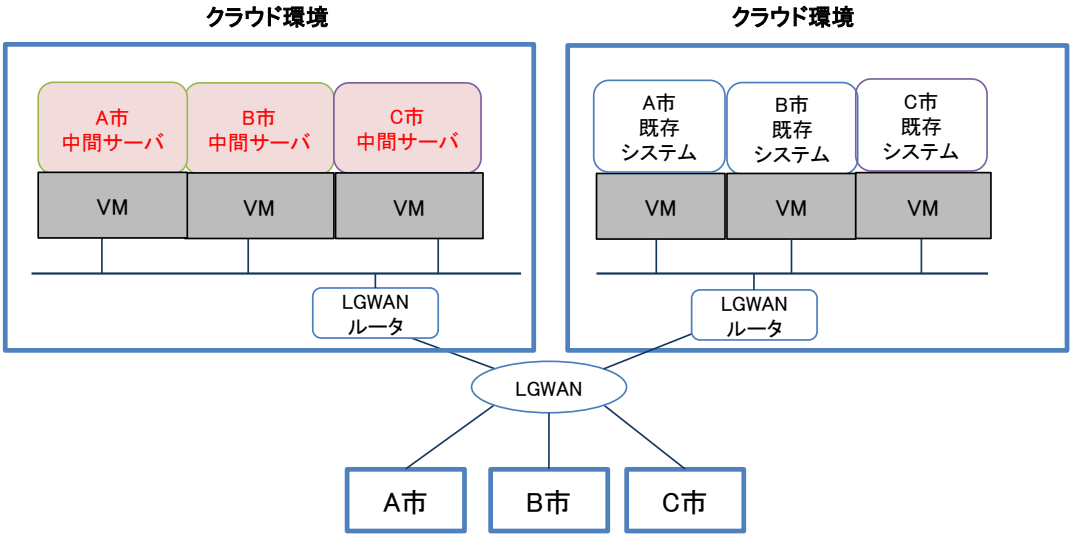
(1) コスト削減

中間サーバについては、既存システムと同様、導入に係る各種経費を共同利用団体間で按分することで、「割り勘効果」により一団体あたりの経費負担を少なくする効果が見込まれる。

また、中間サーバは国の政策に基づき開発されるシステムであるため、既存システムと異なり、基本的な機能は全国統一のものである。そのため、コスト削減を実現するために重要

な要素である「カスタマイズの最小化」については、中間サーバの機能のうち、既存システムとの接続に係る一部機能の範囲にとどまり、既存システムと比べてカスタマイズの必要性は少ないと考えられる。したがって、中間サーバを自治体クラウドによって導入することで、コスト削減効果の余地は大きいことが考えられる。

加えて、中間サーバの運用に係るコストについても削減が見込まれる。中間サーバの運用時間帯は検討中であるが、各団体がそれぞれ自庁で運用することは非常にコストが高くなることが想定される。データセンター等による共同利用を行うことで、運用コストの削減も期待される。



VM:Virtual Machine（仮想マシン）の略。

図 3-1　中間サーバ共同利用のイメージ

(2) 情報セキュリティの確保

中間サーバは、情報提供ネットワークシステムを介して外部システム（他の情報保有機関等）との情報照会、情報提供を実施する。そのため、中間サーバは従来の既存システムと比べて、適切な情報セキュリティ対策を講じることが重要となる。

自治体クラウドによる共同利用を行う場合は、ハードウェアは一定のセキュリティレベルが確保されたデータセンター等に設置されることになる。そのため、自庁内の導入と比べ、情報セキュリティのレベルは向上し、情報セキュリティ確保に係る団体の負荷も減少することが見込まれる。

3.2.2　中間サーバの共同利用に当たっての課題

共同利用に当たって検討すべき課題について、中間サーバで特に配慮すべき特徴や留意点について検討した。

(1) カスタマイズの制約

従来の既存システムに対する自治体クラウドの活用では、業務アプリケーションの機能要件も異なり、共同で利用する業務アプリケーションの検討に関して、利用団体毎間で調整が困難な場合も多かった。また、調整がついた場合でもパッケージをカスタマイズすると、費用が発生し、かえって割高になってしまう場合もあった。そのため、カスタマイズを極力制約し、パッケージに合わせた業務標準化を行うことが地方公共団体にとっての課題であった。

一方、中間サーバは国がソフトウェアを一括開発し、地方公共団体に配布することが予定されており、カスタマイズの必要性はかなり限定的なものになると考えられること、中間サーバに格納するデータに関しては、国によりデータ標準が示されることから自治体クラウドによる導入は進めやすいものになることと期待される。しかしながら、カスタマイズが完全に不要になる訳ではないこと、加えて共同利用団体間での仕様の差異が発生することが想定されることから、共同利用団体間で、カスタマイズを極力抑えるような調整を行う必要がある。

(2) データの移行方策

自治体クラウドの課題として、上述のカスタマイズの制約に加えて、データ移行の制約により、ベンダロックインにつながる点についても認識されている。クラウドサービス間の相互運用性確保のために、平成 23 年度に中間標準レイアウトの検討及び推進がなされてきた。中間サーバの導入に当たっては、前述した特定個人情報に対するデータ項目の標準化について、中間標準レイアウトの検討結果等が参考となる。

そのため、中間サーバのクラウドサービス間でデータ項目が著しく異なることは、既存システムのクラウド利用時に比べて少なく、データ移行の制約という観点からも、中間サーバの自治体クラウドによる導入は進めやすいものになることと期待される。

番号制度対応は全ての地方公共団体において必要なことから、その導入を見据え、既存システムベンダも中間標準レイアウトを意識した対応を行っていくことが想定され、番号制度の導入がより円滑に推進されることと考えられる。

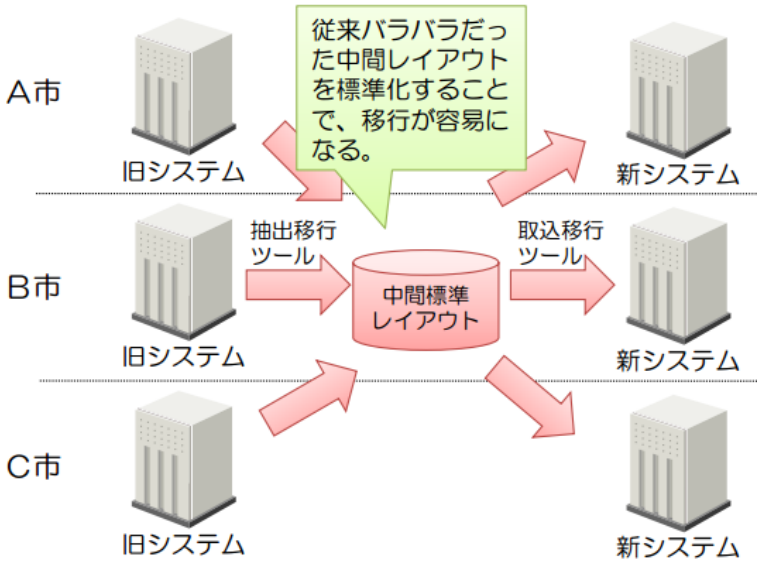


図 3-2　中間標準レイアウトによるデータ移行作業イメージ

（出典：「自治体クラウドの円滑なデータ移行等に関する研究会とりまとめ　（概要）」より抜粋
http://www.soumu.go.jp/main_content/000164375.pdf）

(3) 費用按分の方法

中間サーバにおける望ましい費用按分の方法についても課題となることが想定される。

自治体クラウドにおけるコスト削減効果を高めるためには、前述したカスタマイズの最小化とともに、団体間で適切な費用按分の方法を設定する必要がある。

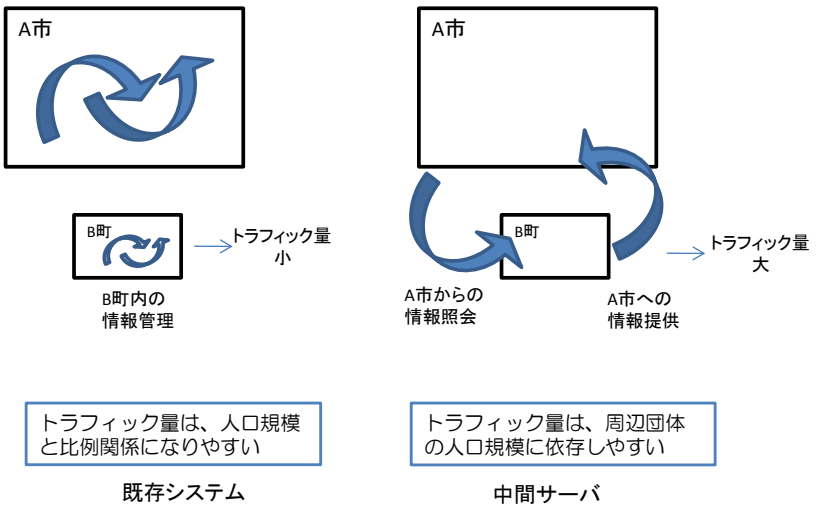


図 3-3　トラフィック量に関する既存システムと中間サーバの違い

トラフィック量に関する既存システムと中間サーバの違いについて、図 3-3 に示す。

既存システムにおいては、各業務システムのトラフィック量に応じた従量制を基本とし、個別に調整を行う方式が採用されることが多い。その場合、各業務システムは、原則自団体内の住基や税情報等の管理を行うものであるため、トラフィック量は人口規模と比例関係になることが多いと考えられる。

一方、中間サーバにおいて同様の方式を採用する場合は、トラフィック量は自団体の人口規模だけでなく、他団体からの情報照会、情報提供の量にも依存すると考えられる。その場合、人口規模の多い大規模団体の周辺に位置する団体などは、当該大規模団体からの情報照会（又は大規模団体への情報提供）が多くなると考えられ、必ずしも自団体の人口規模と比例関係にない可能性も多いと考えられる。

中間サーバの共同利用に当たっては、上記のような特徴も踏まえ、望ましい費用按分の方式検討や、共同利用団体間での調整を密に実施する必要がある。

3.3　想定される共同利用の形態（ネットワーク構成のあり方等）

本節では、既存システム及び中間サーバの共同利用や、想定されるネットワーク構成等について示す。

3.3.1　既存システムの共同利用形態

既存システムの共同利用形態は、「自治体クラウド標準仕様書」において、以下のようなパターンに分類されている。

表 3-6　既存システムの共同利用形態

項番	形態	概要
1	同一業務統合型	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。
2	地方公共団体内業務統合型	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。
3	複数地方公共団体／多種業務統合型	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。

（出典：「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）」をもとに作成 https://www.lasdec.or.jp/cms/9,17362,21.html）

3.3.2　中間サーバの共同利用形態

中間サーバの共同利用形態を検討する上で、共同利用にあたっての既存システムとの相違点について、以下に示す。

(1) 集約範囲

クラウドによる集約の範囲は、大きく分けて以下の 3 種類に分類される。

表 3-7　集約範囲のパターン

パターン	概要
SaaS （Software as a Service）	アプリケーション（ソフトウェア）をサービスとして提供する
PaaS （Platform as a Service）	アプリケーションを稼働させるための基盤（プラットフォーム）をサービスとして提供する
IaaS （Infrastructure as a Service）	サーバ、CPU、ストレージなどのインフラをサービスとして提供する

（出典：総務省「スマート・クラウド研究会報告書」を基に作成
http://www.soumu.go.jp/menu_news/s-news/02ryutsu02_000034.html）

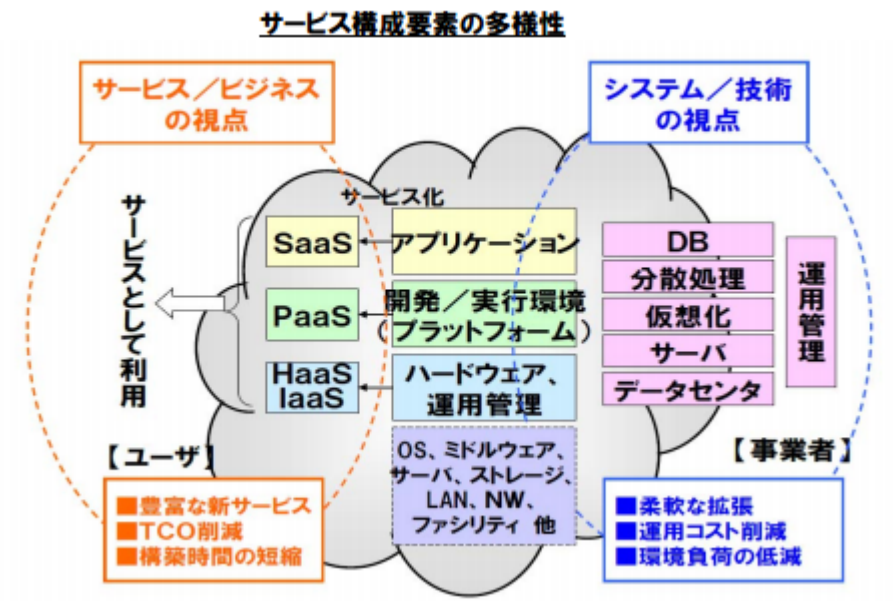


図 3-4　SaaS、PaaS、IaaS の集約範囲
（出典：総務省「スマート・クラウド研究会報告書」
http://www.soumu.go.jp/menu_news/s-news/02ryutsu02_000034.html）

上記を踏まえた中間サーバの特徴について、以下に示す。

中間サーバについては、前述のとおり、ソフトウェアの仕様は共通性が高いものと想定される。また、既存システムのように、複数の業務システムのソフトウェアが搭載されるので

はなく、単一のソフトウェアとして提供される可能性が高いと考えられる。そのため、ソフトウェアをサービスとして提供する SaaS の適用が比較的容易であり、既存システムと比べて、集約範囲の拡大が容易になると想定される。

(2) 対象団体

既存システムについては、地方公共団体の地域性や業務内容の違いが存在するため、共同利用の対象団体を無条件に増やすことは難しいと考えられる。

反面、中間サーバは、番号制度導入の前提として進められるものであるため、連携試験等の実施のために、同時期に、原則として全地方公共団体で一斉に稼働することが求められる可能性が高い（稼働方針や具体的な稼働日等は未定であるため、今後の検討により変わる可能性がある）。また、前述のとおり、ソフトウェアの仕様は比較的共通性が高いものと想定され、団体毎の独自機能のカスタマイズの必要性が少ないと考えられることから、従来の既存システムの自治体クラウドに比べ、共同利用の対象団体を広げる（複数の都道府県をまたぐ等）ことも比較的容易と考えられる。円滑な番号制度の導入という観点からは、全国一律または地方単位で共同化するなど、対象団体をなるべく増加させた方が望ましいとも考えられる。

表 3-8　共同利用における既存システムと中間サーバの特徴

観点	既存システムの特徴	中間サーバの特徴
集約範囲	業務システムの要件が団体毎に異なるため、SaaS の導入は調整を要する	ソフトウェア仕様の共通性が高いため、SaaS の導入が容易と考えられる
対象団体	地域性や業務内容に違いがあるため、無条件な対象団体の増加は調整を要する	番号制度導入時に、同時期、全団体の一斉稼働が求められる場合、対象団体を広げることが比較的容易

上記のような背景から、中間サーバの共同利用は、集約範囲及び対象団体ともに、既存システムに比べて集約の余地が広いといえ、共同利用に適している可能性が高いと考えられる。

3.3.3　ネットワーク構成のあり方

中間サーバを共同利用する場合において想定されるネットワーク構成のあり方は、以下のような観点から検討を行う必要があると考えられる。

(1) 責任分界点の明確化

中間サーバは、既存システムと情報提供ネットワークシステム（インターフェイスシステム）との中間で必要な処理を行うものであるが、その調達主体や運用主体は国と地方公共団体で異なることが想定される。そのため、ネットワーク構成の検討に当たっては、各システムの責任分界点が明確になるような構成とする必要がある。

(2) セキュリティの確保

中間サーバは、情報提供ネットワークシステムを介して他の情報保有機関とやり取りを行うため、十分なセキュリティを確保できるようなネットワーク構成とする必要がある。

ネットワークセキュリティ上、インターフェイスシステムと中間サーバの責任分界点の明確化のために、両者の間にファイアウォール（FW）を設置することが望ましいと考えられる。

上記の構成に加え、中間サーバは外部（他の情報保有機関など）からアクセスされるため、既存システムと同じセグメントに配置することで、既存システムのセキュリティが確保できなくなる恐れがある。従って、既存システムと異なるセグメントに、中間サーバを設置する構成がより望ましいと考えられる。

中間サーバを既存システムと同じセグメントに置く構成の例について、以下に示す。

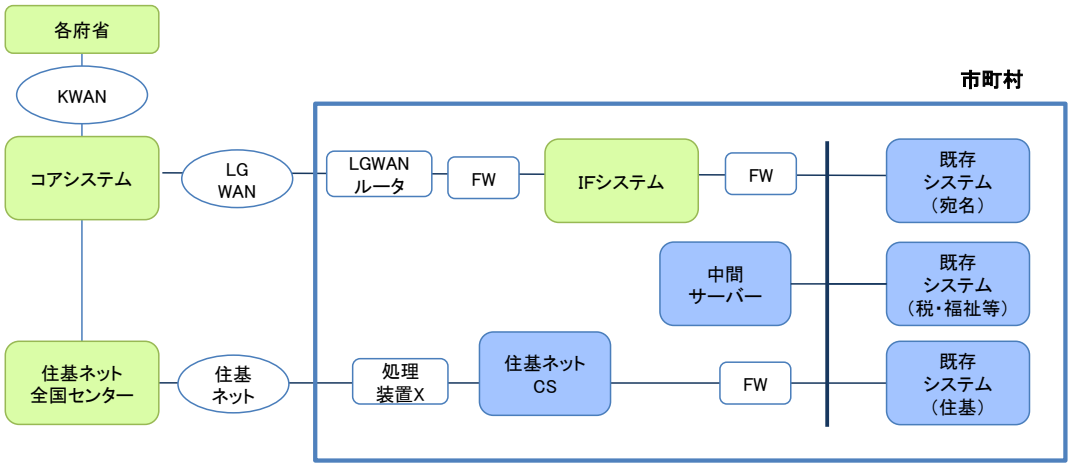


図 3-5　同じセグメントに置く構成例

中間サーバを既存システムと異なるセグメントに置く構成の例について、以下に示す。

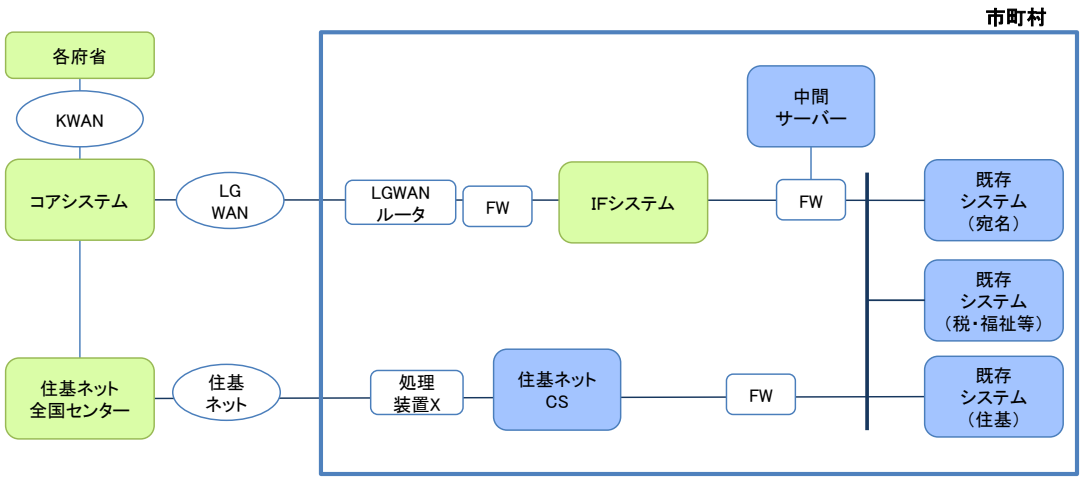


図 3-6　異なるセグメントに置く構成例

(3) 自庁内ネットワーク

自庁内ネットワークについて、基幹系 LAN と情報系 LAN が分かれている場合については、中間サーバを情報系 LAN に接続するか、中間サーバと情報系 LAN との間に FW を設置するか等の検討が必要となる。

基幹系 LAN と情報系 LAN が分かれている場合の構成例として、情報系 LAN に直接接続するケースを図 3-7 に、直接接続しないケースを図 3-8 に示す。いずれのケースにおいても、基幹系 LAN と情報系 LAN を接続している既設のルータ等の接続ポリシーの再検討が必要である。

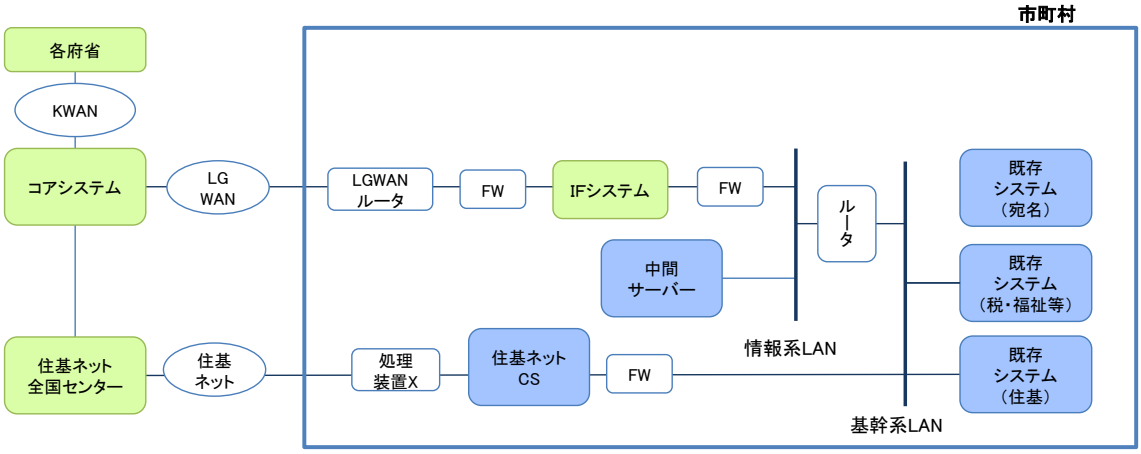


図 3-7　基幹系 LAN と情報系 LAN が分かれている場合の構成例（１）
中間サーバを情報系 LAN に直接接続するケース

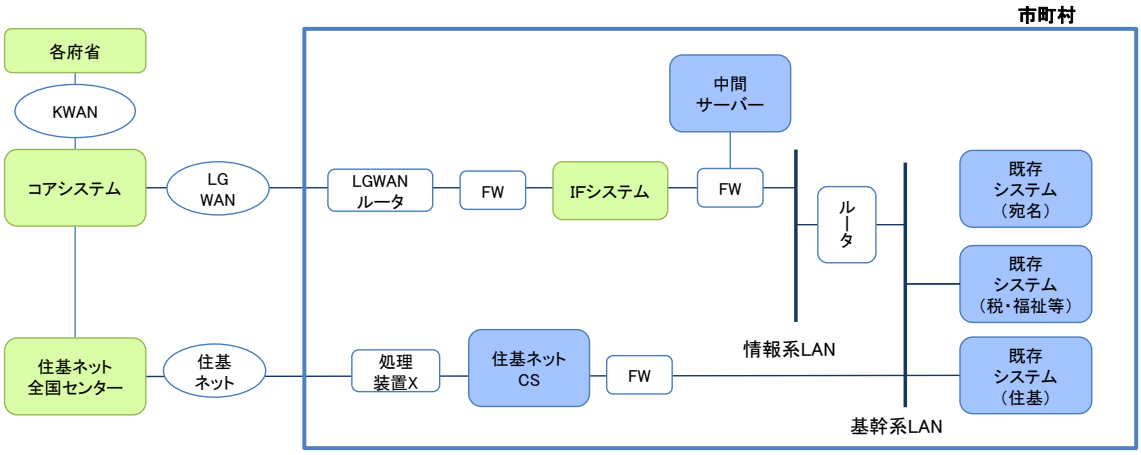


図 3-8　基幹系 LAN と情報系 LAN が分かれている場合の構成例（２）
中間サーバを情報系 LAN に直接接続しないケース

3.4　導入スケジュール（想定）

本節では、番号制度の導入にあたり想定されるスケジュールについて示す。

番号制度の導入に当たっての作業項目及びスケジュールについては、平成 24 年度における番号法案の提出時には、以下のようなロードマップ（案）が想定されていた。

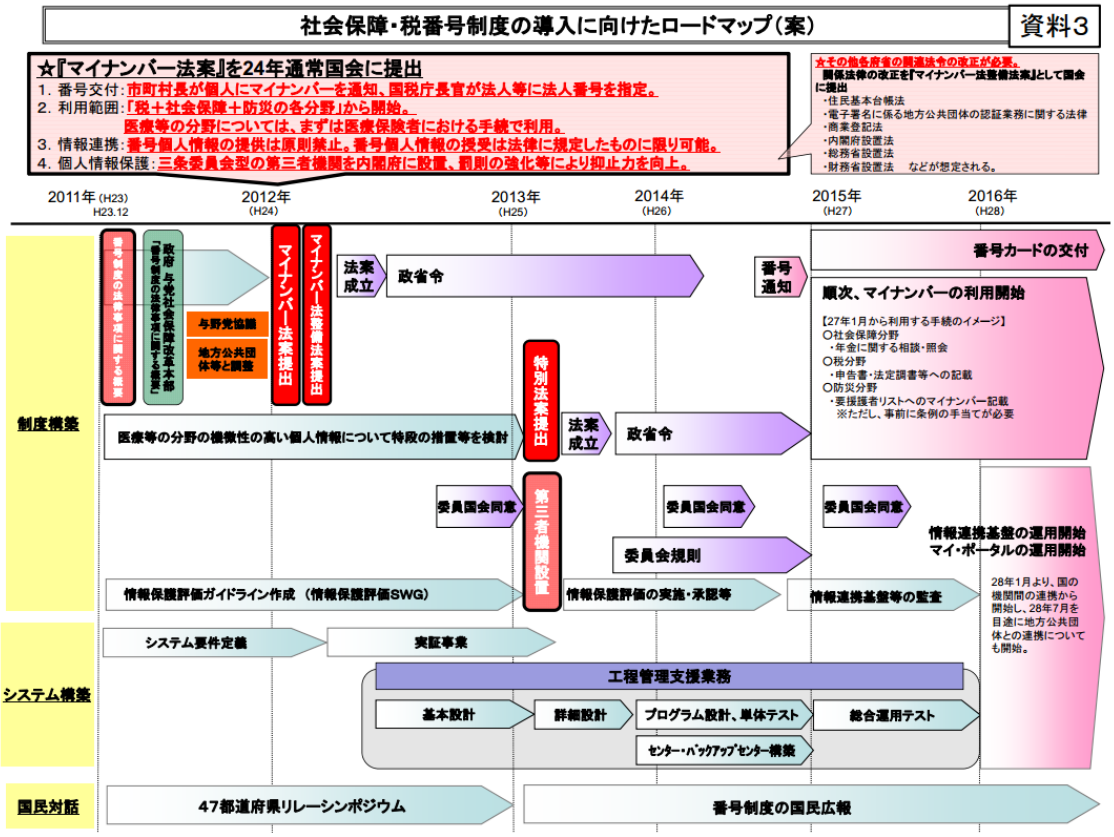


図 3-9　番号制度の導入に向けたロードマップ（案）（平成 24 年度国会提出時点）
（出典：社会保障・税に関わる番号制度に関する実務検討会（第 14 回）「（資料３）社会保障・税番号制度の導入に向けたロードマップ（案）」より抜粋 http://www.cas.go.jp/jp/seisaku/bangoseido/dai14/siryou3.pdf）

上記のロードマップそのものは、平成 24 年 11 月の衆議院解散に伴う廃案により見直しとなった。しかしながら、平成 25 年 3 月に新たに国会提出された番号法案では、必要な作業項目に概ね変化はない見通しである。また、スケジュールについては、概ね上記から 1 年程度後ろ倒しで進められることが予想されている。

上記を踏まえると、今後の番号制度の導入スケジュールは、表 3-9 のようになると想定される。

表 3-9　想定される導入スケジュール

項番	時期（想定）	マイルストーン（想定）
1	2015(H27)年 秋頃	・住民へのマイナンバーの通知（通知カードの交付・送付）開始
2	2016(H28)年 1 月	・個人番号カードの交付開始（通知カードと引換）
3	2017(H29)年 1 月	・情報提供ネットワークシステムの運用開始 ・国の機関間における情報連携の開始 ・情報提供等記録開示システムの稼働
4	2017(H29)年 7 月	・地方公共団体を含めた情報連携の開始

3.5　番号制度の導入に係るヒアリング結果について

本節では、本調査研究で実施したヒアリング調査のうち、番号制度に係る調査結果について示す。

3.5.1　ヒアリング結果（概要）

番号制度の導入に係るヒアリング結果の概要について、以下に示す。

表 3-10　番号制度の導入に係るヒアリング結果（概要）

項番	調査項目	概要
1	業務システムの共同化、クラウド化の状況について	・番号法案別表第 2 で示された事務のうち、基幹系業務については、概ねクラウドによる共同利用を実施している（又は実施予定である）団体が多い。 ・一方、福祉系の事務については、共同利用やシステム化が行われていない場合も多い。その場合は、別途システム化を行うか、専用端末からの入力が必要となると考えられる。
2	検討・推進体制について	・自治体クラウドの取り組みを実施している（又は実施予定である）ため、それとは別に番号制度の導入のために、別途推進体制を設けたというヒアリング団体は存在しなかった。今後は、既存システムの自治体クラウドに係る協議会や定例会等において、番号制度の導入についても検討していく意向の団体が多い。 ・番号制度に関する情報は、内閣官房が実施した説明会（シンポジウム）への参加や、ベンダからの提案等を通じて取得している団体が多かった。
3	調達について	・自治体クラウドを実施している（又は実施を予定している）ため、従来の契約（又は予定している契約）と同等の方式で調達する方針である。 ・新規に調達を行うのではなく、制度改正による対応の一環として、（費用の有無は別として）既存契約内での対応を想定している団体が多い。
4	中間サーバのクラウド利用について	・全てのヒアリング団体について、既存システムと同様に、中間サーバについてもクラウドによる共同利用を行う意向であった。 ・クラウドの利用形態（SaaS、PaaS、IaaS など）についても、現在実施中の自治体クラウドの利用形態（又は予定している形態）を踏襲する方針の団体が多いが、複数のパターンを想定している団体も存在する。

5	費用負担、参加団体について	・費用負担についても、現在実施中の自治体クラウドの利用形態（又は予定している形態）を踏襲する方針の団体が多いが、具体的な按分方法等まで検討していない団体もあった。 ・参加団体については、番号制度を機に、参加団体を増加させる意向を持つ団体も存在したため、番号制度の導入が、自治体クラウド推進のトリガーとなり得ると考えられる。
6	法制度・規約類の対応について	・自治体クラウド実施団体では、すでに外部接続に関する条例等の対応は完了しているため番号制度の導入に当たり、新たな対応は予定していない（必要がない）。ただし、新規に取り組む団体では、新たに外部システム（情報提供ネットワークシステム等）との接続が必要になるため、外部接続に伴うセキュリティポリシーの修正を見込んでいる団体が存在した。 ・個人情報保護条例については、除外規定として、「法令に定めのあるとき」という条項を設けているため、特段の対応を講じる必要はないとのことであった。 ・情報照会、情報提供に当たっては、文書管理規程等で課内決裁等が必要になりうる団体が存在する。そのため、番号制度の導入に当たって文書管理規程を変更する、情報照会、情報提供に当たって電子決裁機能を具備する等の対応が必要になる可能性がある。
7	その他のテーマ	上記以外に、以下のような意見があった。 【同一庁内の連携】 ・実態として同一庁内に存在する複数の情報保有機関（「市区町村」と「市区町村教育委員会」等）について、番号法案では、自庁内で連携するためには条例を策定する必要があるとされている（番号法案第十九条第九号）。しかしながら、現行のシステムで実現できていることを引き続き行うために条例を制定するのは現実的でない。 【画面上での情報確認について】 ・所得証明書などの町村間の情報照会は、紙媒体で実施している。原課としては、番号制度対応により、これまで紙で確認していたものを画面で確認することになるため、切り替えのハードルは高いと思われる。また、データの真正性をどう担保するかも課題となる。 【既存システムの宛名統一】 ・番号制度の導入に当たっては、個人番号又は符号と紐付ける既存システム側の宛名番号について、団体内で

		統一されていることが望ましい可能性がある。しかしながら、宛名の統一がなされていない団体も存在し、それらの団体については、予め宛名を統一する必要があり、団体の負担となりうる。

3.5.2　ヒアリング結果（詳細）

個々の団体におけるヒアリング結果（詳細）について、以下に示す。

(1) 業務システムの共同化、クラウド化の状況について

1）ヒアリング対象団体 A

- 基幹系業務システムの共同利用を行っている。各団体の自庁内については、個人番号がなくとも既存の宛名で統一されている。
- 既存システムの共同利用は実現できているため、今後導入される中間サーバについても共同利用する方向で検討している。市町村側も、番号制度に係る情報が見えない中、共同で対応することが暗黙の認識になりつつある。
- 平成 25 年度中に、住基ネット CS（コミュニケーションサーバ）の共同化を検討している。端末は団体毎に入札を行う。仮想化などにより、サーバの台数などは町村側が意識しなくてもよい形としている。
- 団体内の既存システムの運用時間帯は 7 時から 22 時まで、365 日運用している。中間サーバの運用時間帯も、それらと合わせた時間帯になると想定している。
- 所得証明書などの団体間の情報照会は、紙媒体で実施している。原課としては、番号制度対応により、これまで紙で確認していたものを画面で確認することになるため、切り替えのハードルは高いと思われる。また、データの真正性をどう担保するかも課題となる。
- 情報提供ネットワークシステム上の情報照会者、事務、情報提供者及び特定個人情報を定めている番号法案別表第 2 では、市と教育委員会は別機関として定められている。そのため、自庁内で連携するには条例を策定する必要があるが、既存のシステムで実現できていることを引き続き行うために条例を制定するのは現実的でない。
- 自団体内の条例で、「他団体からデータを提供すること」をルール化できるのか、効力が及ぶのかは疑問である。そもそも全国一律で対応する制度について、条例対応を求めるのがそぐわないのではないか。

2）ヒアリング対象団体 B

- 2013 年 4 月に共同で住民情報系の業務システムをクラウドで調達することになっているため、現時点で共同利用している業務システムはない。

3）ヒアリング対象団体 C

- 現段階で共同利用及びクラウド利用している業務システムはない。今後、番号制度対応

した業務システムを調達した IaaS 上で稼働させることを想定しており、その際は共同で利用することになると考えている。

4）ヒアリング対象団体 D

・ 団体独自に保有している個別のシステムを除き、基幹系については共同化が完了している。クラウド化を検討したきっかけは、住基法改正対応である。

5）ヒアリング対象団体 E

・ 基幹系業務及び内部管理業務について、共同化を実施している。

(2) 検討・推進体制について

1）ヒアリング対象団体 A

・ 番号制度対応の検討に当たっては、プロジェクト推進責任者会議において団体側に情報提供を実施すると共に、業者の説明会などを実施している。
・ クラウド化のメリットは、制度改正時の柔軟な対応であると考えている。業者との契約においても、制度改正時への対応は仕様として含まれている。番号制度対応も、費用の要否は別として、制度改正への対応として実施する想定である。

2）ヒアリング対象団体 B

・ 2011 年に、クラウド化に関して費用対効果を中心に検討を開始した。その際は、効果を見極めてから実際に参加するかどうかを考えるという程度の緩やかな検討体制だった。
・ 2012 年に「効果あり」と判断した団体の間で、自治体クラウドに取り組むことを決定した。番号制度対応もその中で検討している。

3）ヒアリング対象団体 C

・ 今年度設置した「クラウドサービス検討部会」において、中間サーバやインターフェイスシステムの共同構築を含め番号制度対応していくことを想定している。
・ 国から中間サーバ等の仕様が提示された段階で、共同構築について検討を開始したい。
・ 参加団体内における番号制度対応検討体制については、詳細には把握していない。団体が実施すべき事項がいまだ明確でないことから、整備が進んでいない状況と推察している。

4）ヒアリング対象団体 D

・ 番号制度対応のために特別の検討・推進体制は設けていないが、自治体クラウド導入時に設立した総合行政システム共同化推進機構や、定例で実施している会議体等で議論していくことになると思われる。

・ 基幹系システムを共同化しているため、番号制度についても共同で対応していくことになると思われる。
・ ベンダからは、これまでに 3 回程度情報提供を受けているが、具体的な仕様等については情報を得られていない。

5）ヒアリング対象団体 E

・ 現時点で、番号制度のための検討、推進体制は整備していない。
・ 昨年末に実施された内閣官房による説明会に出席した。それ以上の情報は特に得られていない。
・ ベンダとは、毎月一回定例会を開催しているが、現時点で特に提案等は受けていない。

(3) 調達について

1）ヒアリング対象団体 A

・ 基本的には、現行採用しているパッケージの番号制度対応版を導入することになると想定している。
・ 構築の他にも、実運用、調達等で共同化できる範囲については取り組みたい。

2）ヒアリング対象団体 B

・ 番号対応については、今後の調達仕様書に盛り込む予定である。その際は、他の業務システム同様、サービスとして調達する。
・ 仕様には、新規に調達する住民情報系システムについては、本ヒアリング調査の質問票に書かれていることに加え、制度変更による項目追加等について柔軟に対応すること、と記載するつもりでいる。
・ 一部の団体では、介護・福祉業務システムと他のシステムでベンダが異なるものの、宛名統合は完了している。しかし、他団体がすべて宛名統合しているわけではない。

3）ヒアリング対象団体 C

・ 中間サーバやインターフェイスシステムの共同構築を含めて、番号制度対応を検討することを想定している。具体的には、現在調達中の IaaS 基盤を活用して PaaS を構成する共通機能の一部として整備することを考えている。
・ 既存システムの改修や機能追加については、具体的な進め方を含め未検討である。

4）ヒアリング対象団体 D

・ 具体的な調達方式の検討には至っていないが、一括調達を行うものと思われる。
・ 新たな調達を行うのではなく、既存の契約に含まれている「制度改正対応」の一環としてベンダが対応することになると思われる。

5）ヒアリング対象団体 E

・　調達方式の検討は、現時点では行っていない。
・　国による制度改正、法律改正は、パッケージのバージョンアップでベンダが対応することとしている。番号制度についても、同様の対応をベンダが行う想定である。

(4) 中間サーバのクラウド利用について

1）ヒアリング対象団体 A

・　中間サーバのクラウドベンダ選定に当たっては､稼働中の共同総合住民システムとの整合性や､ハードウェア等の整備に必要な価格の優位性を重視することになると思われる。
・　契約主体は不明であるが、複数団体が一括で調達・契約することになると思われる。
・　ネットワークの整備に当たっては､団体の自庁ネットワークが共同化されていない点は今後の課題になり得ると思われる。

2）ヒアリング対象団体 B

・　業務アプリケーションとデータセンターはセットで調達することになるが､中間サーバの物理的条件にこだわりはない。そもそもクラウドなので、サーバの物理配置はサービサーの責任範囲と考えている。
・　国が仕様を決めてくれれば、それに従った仕様とする。クラウドは認めない、というのは困る。
・　庁内 LAN の中に残る業務システムとしては、別表第 2 に記載されている公営住宅周りの事務を行うための公営住宅管理システムがあり、これをどうするかは課題である。

3）ヒアリング対象団体 C

・　中間サーバについては、具体的な技術仕様、運用要件、セキュリティ要件が示されていないため、詳細な検討ができていない状況である。ただし、中間サーバには団体の保持する住民情報が格納されることから､団体ごとに仮想化サーバを準備する必要があると考えている｡そのため､契約主体は団体ごとになると考えている｡そもそも当団体では、仮想化サーバの利用については各団体で契約することとしているため､整合性は取れる。
・　また､情報提供ネットワークとの接続にはLGWANの利用が想定されていることから、クラウド環境と LGWAN のノード間をどのように接続するかが課題になると考えている。

4）ヒアリング対象団体 D

・　中間サーバについても、既存システムと同様に、共同によるクラウド利用を検討していくことになると思われる。
・　後継の新たなパッケージとして導入するか､既存パッケージのバージョンアップになるかは現時点で不明。ベンダの対応状況を見て検討していきたい。

5）ヒアリング対象団体 E

・　中間サーバについても、クラウド利用を行うことになると思われる。
・　契約主体は、現在はそれぞれの団体で行っているため、同一の契約主体になると考える。

(5) 費用負担、参加団体について

1）ヒアリング対象団体 A

・　現行サービス額の算定に準じて、番号制度関連の負担割合も決めることになると思われる。
・　現在の構成団体でハードウェアの最適化がなされているため、現時点では、番号制度対応を機に、新たに参加団体を募集するなどの取り組みは想定していない。

2）ヒアリング対象団体 B

・　中間サーバのハードスペックが住基ネットと同じように団体の規模によらず全国統一であったとしても、人口差のある団体間で利用料にそれを理由とした差を設けるつもりはなく、あくまでコストの削減率目標値（各団体最低 2 割）の確保を基準に負担割合を考える。
・　現在、当団体では住基カードにて住民票のコンビニ交付サービスを提供しているが、これを個人番号カードに乗り換えたいと考えている。その際には、当団体だけでなく他団体に広げたいと考えており、個人番号カードに住民票のコンビニ交付機能が標準装備されることを期待している。
・　番号制度を契機として、今回の自治体クラウドの取り組みに参加する団体が増えるのではないかと思われる。

3）ヒアリング対象団体 C

・　中間サーバ及びインターフェイスシステムについては、ソフトウェアは国が開発したものを自治体に配布し、自治体ではそれを稼働させるハードウェアを整備することとされているため、これら 2 つの部分を仮想化サーバ上で稼働させることが可能であれば、必要な仮想化サーバの費用を各団体で負担してもらうことになると考える。IaaS 同様、サービス調達とするため、従量課金を採用することになるのではないかと考える。
・　番号制度対応は、加入団体に限らず県内の全団体で実施しなければならない作業であることから、番号制度対応を機に、未加入の団体にも共同整備を呼びかける予定で、中間サーバだけでなく、接続する業務システムについても共同化が進むのではないかと期待している。

4）ヒアリング対象団体 D

・　今後、1 団体が新たに共同利用の対象となる予定である。
・　上記の 1 団体のほかに、番号制度を契機に参加団体を増やすことは、現時点では考えて

いない。

5）ヒアリング対象団体 E

・　参加団体を増やすことは、現時点では想定していない。

(6) 法制度・規約類の対応について

1）ヒアリング対象団体 A

・　各団体のセキュリティポリシーに基づきクラウド化を実現しているため、情報提供ネットワークシステムへの接続にも対応できるという認識である。

2）ヒアリング対象団体 B

・　当団体では、電文はデータであり文書ではないとの解釈をしており、文書管理規定で定められた決済ルールは電子的データの送受信には適用されない。また、個人情報保護条例には、「法令で定められた場合」という例外規定が設けられている。
・　被災者台帳システムを共同利用する構想があり、その場合は災害時の住民情報について番号を利用するメリットがあるか検証したうえで、別表第 1 の事務として追加したいと考えている。これも条例対応が必要か確認したいところである。

3）ヒアリング対象団体 C

・　セキュリティポリシーで一部の業務システムについて外部ネットワークとの接続を禁止している団体が多く、情報ネットワークシステムとの接続に際して見直しをする必要が生じると考えている。
・　また、個人情報保護条例で外部ネットワークを介した情報提供に制限をかけている場合が多く、情報提供ネットワークシステムとの接続に際して見直しをする必要があると考えている。ただし、当団体の場合、個人情報保護条例中の「電子計算組織の結合による提供の制限」の除外規定として、「法令に定めのあるとき」という条項を設けているため、この条項により条例改定をしなくて済むのではないかとの見方もある。
・　文書管理規定について、団体の詳細情報は把握できていない。しかし、いくつかの団体に聞いたところでは、文書による情報照会、提供の手続きにおいては、都度あるいは運用により一括で決裁を行っており、情報提供ネットワークシステムを通じた情報照会、情報提供を中間サーバにより自動的に行うことについては、制度の見直しが必要との意見を頂いている。自動送信に関しては心理的な抵抗感もある。
・　団体内のネットワーク状況については整理はしていないので、個別に課題が出てくるかもしれない。

4）ヒアリング対象団体 D

・　情報提供ネットワークシステム等の外部ネットワークへの接続が必要となるため、見直

しが必要となる市町村も発生すると思われる。

・ 自治体クラウドの導入時にも、セキュリティポリシーや関連規定の内容は参加団体間で異なっていたため、見直しの必要性や範囲は団体毎に異なっていた。

5）ヒアリング対象団体 E

・ 番号制度に伴い整備される国のシステムに接続するため、セキュリティポリシーの改定は必要になると思われる。

4. まとめ

4.1 自治体クラウドの情報セキュリティ対策

自治体クラウドの情報セキュリティ対策として、クラウド事業者によるセキュリティ対策の評価、SLA 項目の設定による責任分界の在り方、ネットワーク障害に備えた対策、セキュリティポリシー見直し等について検討を行った。

- クラウド事業者によるセキュリティ対策の評価では、先進的に自治体クラウドに取り組んでいる自治体において、特に留意すべきセキュリティ項目と対策を確認し、それらを評価する仕組みを検討した。
- SLA 項目の設定による責任分界の在り方では、自治体クラウドで必要とされる SLA 項目とグレードについて検討し、自治体とクラウド事業者の責任分界の考え方を示した。
- ネットワーク障害に備えた対策では、障害のパターンを類型化し、パターン毎に対策を検討した。
- セキュリティポリシー見直しについては、自治体の個人情報保護条例への対応状況から、今後の自治体クラウド推進のためのセキュリティポリシー見直しのポイントを整理した。

自治体クラウドに先進的に取り組んでいる自治体では、クラウドシステム利用開始からちょうど 1 年程度経過している。この 1 年でクラウドのセキュリティ対策については多くの知見が蓄積されてきており、これらの知見は今後自治体クラウドに取り組む多くの自治体に有効と言える。

4.2 番号制度（マイナンバー制度）を踏まえた自治体クラウドの推進のあり方

中間サーバの導入に当たっては、既に既存システムの自治体クラウドを推進している団体はもちろんのこと、現時点で自治体クラウドに取り組んでいない団体に対しても、自治体クラウドの効果を訴求できるものと考える。加えて、中間サーバの導入をきっかけとして、既存システムの共同利用についても合わせて推進が期待されると考えられる。

番号制度の導入に当たって求められる情報システムの全体像や要件については、未だ検討段階である。しかしながら、番号制度は更なる自治体クラウド推進の契機と捉えられるため、今後の検討内容も踏まえ、番号制度と自治体クラウドをより一層、一体的に推進していくことが重要と考えられる。

4.3　自治体クラウドによる波及効果

本調査では、自治体クラウドにおけるセキュリティ対策や番号制度への対応等について検討してきた。本節では、自治体クラウドを導入した際の導入効果として、コスト削減以外の2次的な波及効果について、ヒアリング調査の結果を以下に示す。

(1) 職員の負荷軽減

- 情報システム担当部門の職員の負荷は減っている。トラブル時の問い合わせ窓口をクラウド事業者にアウトソースすることで、日常的な負荷が軽減された。
- 具体的には、日次のバックアップ作業、休日の稼働管理、SE の代理作業が不要となった。
- 一方、一般の職員については、自治体クラウド導入当初は、不慣れなために負荷が一時的に高まっている。このような負荷は、クラウドシステムに慣れるに従って軽減されると考えられる。

(2) 住民サービスの向上

- 従来システム化されていなかった業務について、他の自治体と共同利用することで、新しい住民サービスが開始できるケースがある。
- コンビニ収納などが代表的な例である。
- 住民サービスを行う会場で、VPN を利用してその場でクラウドサービスを利用し、作業レスポンスの向上が図られた。

(3) 同一システム利用による他自治体との連携

- 同一システムを使うことで、他の自治体と業務が共同化でき、業務効率化などの議論も共同でできるようになった。従来は業務のやり方やシステムが異なっていたため、議論を行うことも困難であった。
- 同一システムを使っているため、災害時などに被災地に支援で派遣された場合に、他の自治体のシステムをすぐに使えるようになる。

(4) 番号制度への効率的な対応

- 番号制度の対応に当たって、自治体クラウド導入団体は、既存契約の法改正改修として対応できる可能性がある、共同利用の検討体制が既に確立されているなどの理由により、導入していない団体に比べ、より効率的なリソース（人員面、金銭面）での対応が可能になると考えられる。
- それらのリソースを、更なる団体内の情報連携等の推進に活用することで、業務効率化や住民サービスの向上を実現することも可能になる。