Vol.2022-EIP-95 No.9
2022/2/18

地方公共団体における外部サービス利用の実態と課題の研究

小田信治[1]　藤本正代[1]

概要：地方公共団体では，住民サービスや業務生産性の向上を「外部サービス」の利活用により実現していく動きが高まっている．しかしながら，地方公共団体は，機微な情報資産を扱うため，利便性と安全性の両輪の対応が求められる．地方公共団体が「外部サービス」を利用し，安心・安全な行政運営に繋げていくために，地方公共団体の「外部サービス」利用の実態と課題について情報セキュリティマネジメントの観点から考察する．

キーワード：地方公共団体，外部サービス，情報セキュリティマネジメント

Research on the actual situation and issues of the use of external services by local governments

SHINJI ODA[†1]　MASAYO FUJIMOTO[†1]

Abstract: Local public organizations are increasingly moving to improve resident services and business productivity by utilizing external services. However, since local public organizations handle sensitive information assets, it is required to deal with both convenience and safety. In order for local governments to use external services and lead to safe and secure administrative management, we will consider the actual conditions and issues of using external services by local governments from the perspective of information security management.

Keywords: Local public organizations, External services, Information security management

1. はじめに

1.1 行政に関するデジタル化の方向性

行政手続のオンライン化，ワンストップ・ワンスオンリー化（以下「行政のデジタル化」という．）を抜本的に進めることが 2020 年 7 月 17 日に閣議決定され，デジタル関連 6 法案が 2021 年 5 月 12 日に参議院で採決された．今後，クラウドサービスをはじめとした「外部サービス」を活用し，誰もがインターネットで簡単に行政手続きができる社会の実現を目指していくことになる．一方，地方公共団体（以下「自治体」という．）は，人口規模が大小様々であり組織の規模や体制が異なるものの，住民の要配慮個人情報，所得情報や特定個人情報などの機微な情報資産を保有していることは，全ての自治体が同じであり，その組織単位で行政のデジタル化を進めることになる．国はそうした現状を踏まえて，デジタル関連 6 法案の 1 つとして「地方公共団体情報システムの標準化に関する法律案」を制定した．地方公共団体の基幹系情報システム（17 業務＋戸籍，戸籍の附票及び印鑑登録事務）について，国が基準を策定し，当該基準に適合した標準化システムの利用を求める法的枠組みである．また，この標準化システムはガバメントクラウド上で運営する計画が記載[1]されており，クラウド・コンピューティングの技術を活用した「外部サービス」を利用し，行政のデジタル化の進展を図るものと考えられる．このように，国の政策面の後押しの中で行政のデジタル化を自治体が促進していくことになるが，機微な情報資産を保有する自治体が安心・安全な行政運営を行うためには，各自治体で行政のデジタル化と情報セキュリティ対策の両輪の対応を行う必要がある．

1.2 自治体における情報セキュリティに関するインシデント事例

自治体が「外部サービス」を利用する中でインシデントが発生し公表されている．2019 年 12 月 4 日，日本電子計算株式会社が提供する地方公共団体向け IaaS サービス「Jip-Base」の大規模障害（以下「自治体 IaaS インシデント」という．）が発生した．この障害により，全国 53 団体 453 システムで業務が停止した．その上，サービスの復旧に時間を要し，行政サービスに関する各業務に大きな影響をもたらした[2]．また，2021 年 2 月 1 日，株式会社両備システムズが提供する地方公共団体向けクラウド型システムに第三者からアクセスされる事案（以下「自治体 SaaS インシデント」という．）が発生した．両備システムズが，セールスフォース上で構築した住民向けの検診予約などのアプリケーションサービスを提供していたが，クラウドサービスの設定不備が原因となりサービスを利用していた神戸

1 情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

市，船橋市，西条市等で不正アクセスの被害が発生した[3][4]．さらに，2021 年 9 月 9 日，株式会社 TKC が提供する「TASK クラウド住基システム」に障害が発生した．これにより，142 団体において，9 月 9 日朝から 14 時 50 分まで，住民票や印鑑登録証明書などの印刷・発行ができない状態となった[5]．このようにインシデントが発生すると住民へのサービスを継続することが難しくなる．

これらのインシデントの経緯や再発防止策を確認すると「外部サービス」を提供する事業者（以下「外部サービス事業者」という．）との報告や連絡体制等に不備があったことが判明している．例えば「自治体 IaaS インシデント」が発生した中野区では，Web サイト上に再発防止策の内容が公開されている[6]．その中で“今回の障害においては，障害の状況や復旧見込み等に関する日本電子計算株式会社からの報告が頻度・内容ともに不足しており，区の対応に支障をきたしていた”，“そのため，日本電子計算株式会社と区において，平常時・障害発生時・障害発生後の連絡体制について協議し，必要な情報が必要なタイミングで共有されるよう体制の再整備を図る”，と記載されている．こうした実態を踏まえると住民側は，インシデント事例の団体と同様に，自治体と外部サービス事業者間の各役割において曖昧な点が存在したままの状態で「外部サービス」を利用していないかという不安や不信感を抱きかねない．万が一，自治体と外部サービス事業者間の各役割において曖昧な点が存在しているとなれば，インシデント発生時の被害がさらに広がることが予測される．また，インシデント発生時の対策が不十分なものとなり，住民サービスをはじめとした行政運営に対する影響も懸念される．

1.3 本研究の概要

以上のことから本研究では，自治体が「外部サービス」の利用を進めていく中で，自治体が「外部サービス」を利用する際の課題を抽出し解決することが重要と考え，特に自治体の「外部サービス」利用の際のマネジメントの観点にフォーカスして考察する．まず,「外部サービス」利用とオンプレミス環境との相違におけるマネジメントについて考察した先行研究，自治体の情報システムに関する先行研究について調査した．次に,「外部サービス」の利用実態について確認し，自治体の「外部サービス」の類型化を試みた．また，総務省から自治体向けに発出されている「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 2 年 12 月版）」[7]（以下「総務省セキュリティポリシーガイドライン」という．）の「外部サービス」に関する記載内容を確認した．さらに，自治体で発生した「外部サービス利用」におけるインシデント事例を調査し，そこで明らかになった「外部サービス」利用の際の留意すべきポイントに関して,「総務省セキュリティポリシーガイドライン」上の記載の有無について照合した．これらの結果を踏まえて,「自治体が「外部サービス」を利用する際の留意すべきポイント」を明らかにし,その内容については，自治体が「外部サービス」を利用する際の留意すべき「確認項目」として整理した．そして,「確認項目」の内容を各自治体へのアンケート・ヒアリングを通して評価・検証を行い，自治体が「外部サービス」を利用する際の課題をマネジメントの観点から整理した．

なお本研究では,「外部サービス」とは,「自治体以外の者が一般向けに情報システムの一部又は全部の機能を提供するもの」,「自治体が管理運営するドメイン以外でサービスを提供されるもの」と定義し，クラウドサービス，ソーシャルメディア，ホスティングサービス（共同利用型の業務システム等含む）等を示すものとしている．ただし，先行研究や参考文献を引用する場合は，表現された各呼称をそのまま用いて記述している．

2. 先行研究

渡邉ら（2017）[8]は，学術機関に対するクラウドサービスの導入に関して，ISMS や情報セキュリティガバナンスの考えをベースに成熟度モデルを 4 つの評価基準と 5 つの評価軸（成熟度ステージ）を算出することにより，情報セキュリティガバナンスの観点で評価することを提案している．クラウドサービスは外部委託の一つとして位置づけられるため，オンプレミスからクラウドサービスに情報システムの一部を転換していく際には，転換により生じる差異を確認し，必要に応じて不足を補うプロセスの構築が重要であると述べている．また，渡邉ら（2019）[9]は，これまで研究してきた成熟度モデルに関して 2016 年度から学術機関に対する実態調査を行っているが，その結果から，継続して実態調査を実施している機関は，成熟度モデルの各指標が向上しているとして，自組織の成熟度を定量的に可視化することの有効性を示している．

伊藤ら（2020）[10]は，利用者のクラウドサービスの仕様の認識不足，障害発生時の可用性への対策不足が一因でクラウドサービスの障害発生時に大きな業務影響に繋がっていると指摘した上で，利用者，クラウドサービスを構築する事業者（Sier）とクラウドサービス事業者といった関係者間のクラウドサービスにおける各情報の認識を共有化することが可用性を高められる解決策であると提言している．本先行研究では IaaS 型のクラウドサービスに限定した研究となっているが，IaaS 型のクラウドサービスを構築する場合は，要件定義の段階で各関係者が構築する業務の運用に合わせた可用性レベルを認識することが重要と指摘し，可用性レベルに関する「サービス切替時間」,「業務継続の要求度」,「稼働率」の各指標を用いたガイドラインを提案している．また実際に，各インシデント事例をガイドライン記載内容に当てはめ，その有効性を立証している．

自治体に関する先行研究は,「自治体クラウド」,「電子自治体」等，国の施策に関係するものが多く，自治体におけ

る「外部サービス」全般の取り扱いやマネジメントに関して触れられている研究は見当たらなかった．このため，自治体の「外部サービス」の利用実態や自治体の「外部サービス」におけるインシデント事例を調査することで，自治体が「外部サービス」を利用する際の課題を明確にする必要がある．

3. 本研究の手法

まず，自治体の「外部サービス」利用の実態に合わせた課題を明らかにするため，自治体の「外部サービス」の利用実態を調査し，自治体がどのような業務で「外部サービス」を利用しているのか確認する．次に「総務省セキュリティポリシーガイドライン」の記載内容を調査し,「外部サービス」の利用実態に即した管理項目が記載されているのか確認する．また，自治体の「外部サービス」利用におけるインシデント事例を調査し，実際のインシデントにおいて被害が拡大したポイントがどこにあるのか確認する．さらに，インシデント事例においてインシデントの被害が拡大したポイントが「総務省セキュリティポリシーガイドライン」に記載されているのか確認することで, 自治体が「総務省セキュリティポリシーガイドライン」を遵守できていないことが課題なのか, そもそも自治体が「外部サービス」を利用するにあたり留意すべきポイントが定まっていないのか，明らかにする．確認した結果を基に自治体が「外部サービス」を利用する際の対応を整理し，自治体アンケートにより内容の評価・検討を行う．

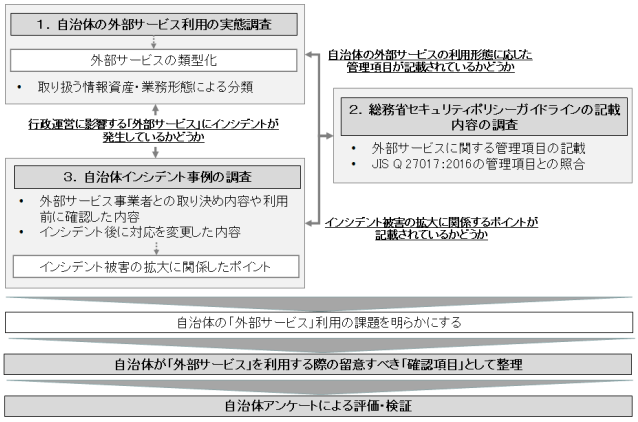

図１　本研究の手法

(1) 「外部サービス」の利用実態の調査

対象自治体は，神奈川県内 33 市町村とし，各自治体での現在の「外部サービス」の利用状況と各自治体での今後の「外部サービス」の利用計画を確認した．調査方法は，各市町村の Web サイト，情報化計画書，総務省「地方行政サービス改革の取組状況等に関する調査等」（令和 2 年 3 月 27 日公表）」[11]，事業者が公開している導入事例等を利用した．調査は 2021 年 8 月 28 日から 2021 年 9 月 24 日に実施した．なお，図書館蔵書検索・予約，国・県が運営する申請手続き（ぴったりサービス・電子申請サービス等）は「外部サービス」として含めていない．

(2) 「総務省セキュリティポリシーガイドライン」の調査

「総務省セキュリティポリシーガイドライン」の基本方針及び対策基準（例文）における「外部サービス」の記載内容の確認と基本方針及び対策基準（例文）における「外部サービス」の記載内容と，「JIS Q 27017：2016」箇条 5 から 18 と附属書 A の管理項目[12]との比較照合を行った．

(3) 自治体の「外部サービス」におけるインシデント事例の実態の調査

自治体の不正アクセスや業務停止の被害をもたらした「自治体 IaaS インシデント」,「自治体 SaaS インシデント」の各事例から「外部サービス」の特性の理解とインシデントの際の被害拡大の関係性を明らかにすることを目的として調査を行った.「自治体 IaaS インシデント」,「自治体 SaaS インシデント」の事例の自治体を対象として，ヒアリングの実施（「自治体 IaaS インシデント」事例の自治体 1 団体）とアンケートの実施（「自治体 SaaS インシデント」の事例公開 17 団体の内コロナウイルス対応部門を除く 10 団体にアンケートを送付）を行った．また，各自治体の Web サイトで各インシデントの内容を確認した．

4. 自治体の「外部サービス」利用に関する調査と分析

4.1 自治体の「外部サービス」利用の実態の調査結果

調査した自治体では，様々な業務で「外部サービス」を利用していることが判明した．住民情報，税や福祉・介護といった業務を扱う基幹業務系の「外部サービス」については「自治体クラウド」,「単独クラウド」合わせて 19 団体（神奈川県内導入率 58%）であった．住民に関する機微な情報を扱う業務において「外部サービス」の利用が浸透していることが明らかである．Covid-19 ワクチン予約の申請に関しては，32 団体が利用していることが確認できた．1 団体は確認した時点で Web サイトによる Covid-19 ワクチン予約申し込みが終了していたため「外部サービス」の利用可否の詳細が確認できなかったが，利用団体数の多さから考えて突発的に対応が必要となる業務について「外部サービス」を利用することは，自治体にとって有効であると言える．また，自治体の公式 Web サイトによる情報発信以外に，ソーシャルメディアを活用した広報や情報発信を実施している団体が多い．スマートフォンの普及等を背景に様々なソーシャルメディアのツールを利用して積極的に住民への情報発信を行う姿勢が伺える．さらに LINE を情報発信以外に相談や行政手続きの申請に活用したり，スマートフォン用のアプリケーションをダウンロードしてプッシュ型の情報発信や予防接種の申し込みに活用したりするなど，様々な工夫を自治体がしていることが分かった．これらのオンラインによる申請手続きに関しては，国や県で申請システムが構築されているが，利便性の観点で地域独自に運

用されている実態があった．例規集・会議録・地図情報・窓口の混雑状況・チャットボットによる質疑応答等の情報公開に関しても「外部サービス」を利用して積極的になされていた．このように行政は住民との接点なくしては成り立たないため，手段として「外部サービス」を積極的に活用することで行政運営の効率化を図っていると考える．

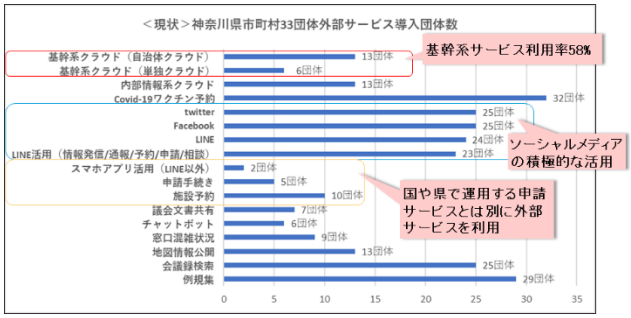

図 2　神奈川県市町村 33 団体別外部サービス導入状況

また，確認した各「外部サービス」を同様な業務の分類に合わせ，「外部サービス」を業務の種別で整理したものが次の図である．

外部サービス区分名	サービス内容	用途
基幹系サービス	自治体クラウド	住民情報・税・国保等の基幹系業務
	単独クラウド	
申請系サービス	Covid-19ワクチン予約	ワクチン予防接種申込
	スマホアプリ活用	行政手続き申請・予防接種申込・保育園入園申請等
	申請手続き	行政手続き申請（事前申請含む）等
	施設予約	自治体管理の施設予約申し込み、空き状況の検索等
内部情報系サービス	内部情報系クラウド	財務会計・文書管理・庶務事務等の内部業務
ソーシャルメディアサービス	twitter	公式アカウントによる広報・情報発信
	Facebook	
	LINE	
	LINE活用（情報発信/通報/予約/申請/相談）	公式アカウントによる広報意外に相談や行政手続きの申請等で利用
情報提供サービス	議会文書共有	議会文書のペーパーレス化と共有化で利用
	チャットボット	住民向けのQ＆A等に利用
	窓口混雑状況	窓口の混雑状況を住民にWebサイトで開示
	地図情報公開	都市計画・ハザードマップ・各施設の案内等に地図情報を公開
	会議録検索	議会の会議文書を公開
	例規集	例規集を公開

図 3　外部サービスの区分

次に，今後の「外部サービス」の利用計画について示したものが次の図である．

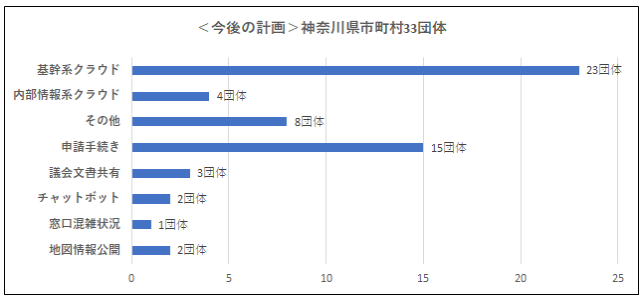

図 4　「外部サービス」利用の今後計画予定団体数

このように自治体では様々な「外部サービス」の利用の実態があったことから，自治体の「外部サービス」利用の実態調査から得られた結果を「機密性」と「住民影響」の 2 軸で分類した．個人情報を扱う「外部サービス」の場合は「機密性 3」．一般公開されていない行政事務手続きに関する情報等を扱う場合は「機密性 2」．Web サイト等で公開されている情報提供サービスについては「機密性 1」．なお，「機密性」については，「総務省セキュリティポリシーガイドライン対策基準 2．情報資産の分類と管理（1）情報資産の分類」を参照して具体的に定義した．また，「住民影響」については，住民の暮らし（各手続きが止まってしまうもの，給付やサービス判定に影響するもの）に直結するものを「住民影響 3」．行政事務上の起案に関わる事務，入札等に係る手続き，また，役所に出向けば代替可能なサービスは「住民影響 2」．ソーシャルメディアの活用は，Web サイトで代替えが可能であり，メインの情報発信ではないため「住民影響 1」とした．さらに，個人情報が漏えいした場合の影響を考慮するために，日本ネットワークセキュリティ協会（JNSA）が想定損害賠償額の算定で用いているモデル[13]を参考に「経済的損失」と「精神的苦痛」という 2 種類の尺度を追加して類型化を試みた．

種別	高	中	低
機密性	3	2	1
住民影響	3	2	1
精神的苦痛	3	2	1
経済的損失	3	2	1

図 5　項目別のレベル

外部サービス区分	機密性	住民影響	精神的苦痛	経済的損失	現状の利用状況	今後の利用計画
基幹系サービス	高	高	高	高	多	多
申請系サービス	高	高	低	低	少※	多
内部情報系サービス	中	中	低	高	中	少
ソーシャルメディアサービス	低	低	低	低	多	少
情報系サービス	低	低	－	－	多	少
※．Covid-19ワクチン予約の申請を含まない場合						

図 6　外部サービス区分別状況

「機密性」，「住民影響」，「精神的苦痛」，「経済的損失」の各項目のレベルを図 5 の通りとして，「外部サービス」の区分ごとに各項目の状況をまとめたものが図 6 である．また，各項目におけるレベルの数値を掛け合わせて，各「外部サービス」の区分に対する「行政運営影響度」を求めたものが図 7 である．

外部サービス区分	数値	行政運営影響度
基幹系サービス	81	大
申請系サービス	9	中
内部情報系サービス	12	中
ソーシャルメディアサービス	1	少
情報系サービス	1	少

図 7　外部サービス区分別行政運営影響度

これらの結果を踏まえると自治体では，「機密性」，「住民影響」，「精神的苦痛」，「経済的損失」の各項目の指標が高い「基幹系サービス」の利用が現状多く，今後の利用計画も多い．「申請系サービス」は，住民情報を取り扱うため「機密性」は高いが，情報漏えいの観点から考慮すると「精神

的苦痛」,「経済的損失」は共にレベルは低いため,「行政運営影響度」は「基幹系サービス」の数値ほど大きな数値となっていない．一方,「内部情報系サービス」は，主に自治体内部の情報を扱っているが，口座情報の管理をしていることから「経済的損失」が高く，行政運営に対する影響が一定程度あることが判明した．これらの「外部サービス」の利用に際しては，情報セキュリティに対する十分な考慮が求められる．

4.2 「総務省セキュリティポリシーガイドライン」の調査結果

「外部サービス」に関しては，対策基準「8．外部サービスの利用」に管理項目が示されているが，情報資産の取り扱いに関する分類に応じたクラウドサービス利用の可否の判断について記述があるものの，自治体が実際に利用している「外部サービス」の業務種別に関しての具体的な記述はなかった．

対策基準8.外部サービスの利用の構成	主な記述内容
8.1外部委託	外部委託事業者の選定基準,契約項目,確認・措置
8.2約款による外部サービスの利用	約款による外部サービスの利用に係る規定の整備,約款による外部サービスの利用における対策の実施
8.3ソーシャルメディアサービスの利用	運用手順の整備,機密性2以上の取り扱いの制限,利用にあたっての責任者の配置,アカウントの乗っ取りの対策
8.4クラウドサービスの利用	情報資産の取り扱いに関する分類に応じたクラウドサービス利用の可否,国内法が適用されない場合のリスク（準拠法・裁判管轄の指定）,クラウドサービスの特性の考慮,情報セキュリティ監査による客観的な評価

図 8　対策基準「8.外部サービスの利用（例文）」の構成と記述内容

次に,「総務省情報セキュリティポリシーガイドライン」の対策基準の例文と「JIS Q 27017 : 2016」箇条 5 から 18 と附属書Aを比較照合した．その結果，32 項目の差分があることが判明した.「総務省情報セキュリティポリシーガイドライン」は ISMS ベースで策定されており,「外部サービス」に対する詳細な管理項目の記載は少ない．

	対策基準（例文）項目	差分項目
1	組織体制	1
2	情報資産の分類と管理	4
3	情報システム全体の強靭性の向上	1
4	物理的セキュリティ	1
5	人的セキュリティ	4
6	技術的セキュリティ	14
7	運用	4
8	外部サービスの利用	2
9	評価・見直し	1
	合計	32

図 9　「JIS Q 27017：2016」との各対策基準項目別差分数

4.3 自治体の「外部サービス」におけるインシデント事例の調査結果

「自治体 SaaS インシデント」,「自治体 IaaS インシデント」の事例団体に対して，アンケート及びヒアリングを実施して「外部サービス」の特性の理解やインシデントの際の被害拡大のポイントについて確認した．なお，これらのインシデントの事例における「外部サービス」の区分は,「基幹系サービス」,「申請系サービス」,「内部情報系サービス」であった．

	アンケート項目	A自治体	B自治体	C自治体	D自治体
(1)	サービス利用形態（複数のサービス利用）の説明が利用前に事業者からあったか	有	無	有	有
(2)	外部サービスと自治体との責任分担についての説明が利用前に事業者からあったか	無	無	有(ホワイトペーパーで提示)	インシデント後に見直しを実施
(3)	約款の形態について（自治体形式か事業者形式か）	自治体	自治体	自治体	自治体
(4)	SLAの締結の有無	有	無	無	インシデント後に内容を変更
(5)	SLAに不正アクセスやデータ保護に関する記載の有無	無	-	-	非機能要件は一部記載有
(6)	インシデント発生時の対応に関する文書化の有無	有	無	有	インシデント後に見直しを実施
(7)	サービスのバージョンアップ時の対応に関する文書化による合意の有無	インシデント後に仕組みを構築	無	インシデント後に仕組みを構築	インシデント後に見直しを実施
(8)	機微な情報がクラウドサービス内に保存される場合の情報漏えい対策の有無	通信の暗号化（HTTPS）	無	無	インシデント後に見直しを実施
(9)	サービスが利用できなくなった場合の代替手段の有無	無	無	無	インシデント後に仕組みを構築

図 10　インシデント事例自治体に対するアンケート及びヒアリングの主な結果

確認の結果，自治体では自治体の約款を利用して契約を行っていた．そのため自治体は，自ら扱う情報資産の重要度に応じた情報セキュリティリスクの意識を持ち，外部サービス事業者に情報セキュリティに関する要求をすると共に契約を締結することが求められる．また,“アンケートの各項目について対応できていない”,“インシデント発生時に委託事業者や外部サービス提供事業者との連携が悪くインシデントの対応が遅れた”,“オンプレミス環境を IaaS サービスに移行した際に「外部サービス」利用における情報セキュリティに関して全体的な評価ができていなかった”という回答があった．このように,「外部サービス」の利用における留意点が認識されないまま「外部サービス」を利用し，インシデント発生時の対応が遅れた実態が見受けられた．

4.4 自治体の「外部サービス」利用に関する調査と分析のまとめ

自治体では,「行政運営影響度」が高い「外部サービス」の利用実態があり，実際にこれらの「外部サービス」の区分でインシデントが発生していた．しかし,「総務省セキュリティポリシーガイドライン」の「外部サービス」に関する記述は，自治体の「外部サービス」の利用実態に即した詳細な管理項目の記述にはなっていなかった．また，インシデント事例の団体では，インシデント発生の前後で自治体が情報セキュリティ対策を変更した内容があることが判明した．

- インシデント発生時の報告体制や内容
- バックアップの仕組みの見直し
- 外部サービス側のバージョンアップ等の変更管理
- 緊急時の対応計画（ICT-BCP）の自治体側の策定
- SLA の記載内容の見直し

これらの項目は,「総務省セキュリティポリシーガイドライン」には具体的な記述はなかったが,「JIS Q 27017：2016」の管理項目には記述されている内容であった．以上

のことから自治体の「外部サービス」利用に関する課題は，自治体が「外部サービス」を利用する際に留意すべきポイントに関して「総務省セキュリティポリシーガイドライン」の管理項目に示されておらず，自治体が認識できていないことにあると考える．そこで，インシデント事例においてインシデント発生の前後で自治体が情報セキュリティ対策を変更した内容について「総務省セキュリティポリシーガイドライン」には具体的な記述はなく「JIS Q 27017 : 2016」の管理項目には記述されている内容を，「自治体が「外部サービス」を利用する際の留意すべき確認項目」として次の図の通りに整理した．

項目	カテゴリ	留意すべき確認項目	JIS Q 27017 : 2016
(1)	インシデント報告	情報セキュリティインシデントの報告内容について外部サービス事業者に確認し，内容について合意ができているか	16.1.1 責任及び手順
		情報セキュリティインシデント報告の仕組みについて外部サービス事業者に確認し，内容について合意ができているか	16.1.2 情報セキュリティ事象の報告
(2)	情報資産管理	情報資産について定期的にバックアップを実施すること	12.3.1 情報のバックアップ
(3)	アクセス制御	アクセス制御方針を定めているか	9.1.2 ネットワーク及びネットワークサービスへのアクセ
		アクセス制御方針に従って「外部サービス」がアクセスの制限ができているか	9.4.1 情報へのアクセス制限
(4)	情報セキュリティ要求事項	情報セキュリティ要求事項を定め，「外部サービス」が要求事項を満たせるか否か	14.1.1 情報セキュリティ要求事項の分析及び仕様化
(5)	変更管理	「外部サービス」の設定を変更した場合，サービス仕様書等の変更履歴が作成されているか	2.1.2 変更管理
(6)	脆弱性管理	「外部サービス」に影響し得る技術的脆弱性の管理に関する情報を外部サービス事業者に要求し，自治体の業務影響や保有するデータへの影響について特定できているか	12.6.1 技術的ぜい弱性の管理
(7)	緊急時対応計画	緊急時対応計画の策定ができているか	16.1.1 責任及び手順
(8)	SLA	SLAの記載内容の情報セキュリティの役割及び責任が明確になっているか	15.1.2 供給者との合意におけるセキュリティの取扱い
		「外部サービス」がSLAを遵守できているか	
		複数の「外部サービス」で構成される場合，構成される各サービスがSLAを満たし，遵守できているか	15.1.3 ICT サプライチェーン
(9)	監査	「外部サービス」が情報セキュリティポリシーを遵守しているか確認のための監査を定期的に行えているか，または，監査報告書によって遵守状況を確認できているか	18.2.1 情報セキュリティの独立したレビュー

図 11　「自治体が「外部サービス」を利用する際の留意すべき確認項目」

5. 「自治体が「外部サービス」を利用する際の留意すべき確認項目」の評価検証

「自治体が「外部サービス」を利用する際の留意すべき確認項目」の各項目の「重要度（必要性）」，「確認の難易度」，「確認の有無について」等に関して，実際に自治体の意見を求め評価検証を行った．35 自治体（人口規模 10 万人未満，10 万人以上 30 万人未満，30 万人以上の各人口区分単位で抽出）に対してアンケートを実施し，15 自治体より回答を得た．アンケートは各項目に対して，「重要であり確認・合意すべきである」，「重要ではあるが確認・合意が難しい」，「特に留意しなくても良い」，を選択し，その理由を記載する形とした．アンケートの結果，「重要であり確認・合意すべきである」または，「重要ではあるが確認・合意が難しい」の回答が占める割合が 100%となる項目が 6 項目あった．「特に留意しなくても良い」の回答がある項目（7）については，“重要な情報資産を取り扱う場合は，外部サービスで利用しない”といったリスク回避の考えを示していた自治体が存在した．また，（6）の項目は，“外部サービス側で実施すべき内容であり外部サービスの利用者側で確認すべき点ではない”という回答が 4 団体あった．ただし全体的には，「特に留意しなくても良い」の回答があった（6）の項目でも「重要であり確認・合意すべきである」または，「重要ではあるが確認・合意が難しい」の回答が占める割合が 7 割以上であり，「自治体が「外部サービス」を利用する際の留意すべき確認項目」に関する 9 カテゴリの各項目における重要度について妥当性があることが明らかになった．

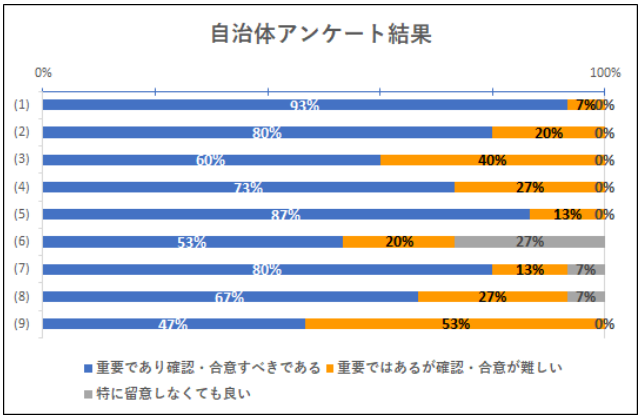

図 12　自治体アンケート回答割合（留意点 9 カテゴリ n=15）

次に「重要ではあるが確認・合意が難しい」と回答した割合が多かった項目の理由については (9) の項目では，“自治体が外部サービス事業者を定期的に監査することが難しい”という意見があった．(3) の項目では，“外部サービス事業者との定期的な報告の合意が難しい”，“自治体内で外部事業者のセキュリティ対策の内容や報告を評価できる人材がいない”という意見があった．このような回答結果を踏まえると，自治体では情報セキュリティ対策の仕組みや実施状況等「外部サービス」そのものの仕組みについて外部サービス事業者に確認することは難しいという実態があることが判明した．

また，自治体がこれらの各項目の実施について「外部サービス」の利用前に確認しているかどうかについては次の図の通りである．

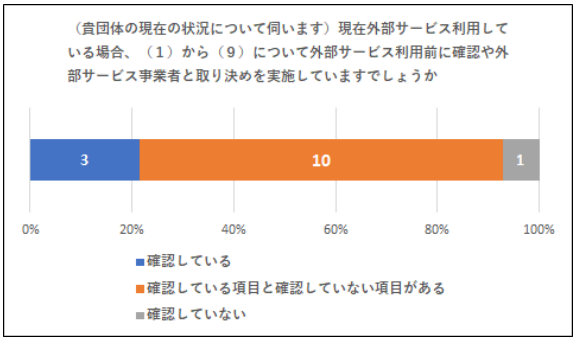

図 13　自治体アンケート結果グラフ（外部サービス利用

前の確認状況 n=14）

「確認している項目と確認していない項目がある」の回答が全体の 7 割弱を占めた.「確認していない項目」についての内容は，項目（6）と項目（9）が確認できていないという回答が多かった.

情報セキュリティポリシー（基本方針・対策基準等）に定めているかどうかについては次の図の通りである.

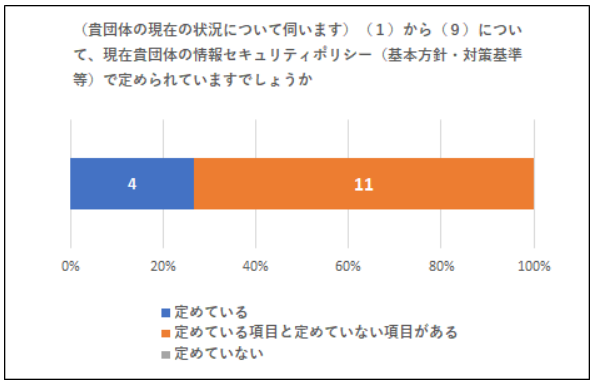

図 14　自治体アンケート結果グラフ（情報セキュリティポリシーへの各項目の反映状況 n= 15）

「定めている項目と定めていない項目がある」の回答が全体の 7 割を占めた.「定めていない項目」の内容は，項目（2），項目（5），項目（6），項目（7），項目（8），項目（9）で，情報セキュリティポリシーに定めていないという回答が多かった.“総務省セキュリティポリシーガイドライン」を参考に作成しているため概ね定められているが，ざっくりとした文言で定められている部分もあり完全とは言いきれない”という意見もあった.

6. 本研究のまとめ

6.1 本研究の成果

行政のデジタル化が進展する中，自治体での「外部サービス」の利活用が進むことが想定されるため,「外部サービス」利用の実態に合わせた課題を明らかにする必要があると考え，自治体の「外部サービス」の利用実態,「総務省情報セキュリティポリシーガイドライン」,自治体のインシデントの事例を調査した．その結果，自治体が外部サービス事業者との取り決めが不十分なまま「外部サービス」を利用している実態があることが判明した．そのため，インシデント発生時の対応が遅れ被害が拡大した項目を自治体のアンケートとヒアリングから抽出し，これらの項目について「総務省セキュリティポリシーガイドライン」の記載内容を確認したが，抽出した項目に関する詳細な記載がなかった．そこで，これらの項目を「自治体が「外部サービス」を利用する際の留意すべき確認項目」として 9 カテゴリ 12 項目に整理し，その項目の内容と各項目の重要性について自治体にアンケートを実施し，評価検証を行った．その結果，整理した各項目は,「自治体が「外部サービス」を利用する際の留意すべき確認項目」として重要度が高い項目として評価を得ることができた．ただし，実際に各項目を全て確認できている団体は，アンケートの結果では 2 割程度である．また各項目全てが，各団体の情報セキュリティポリシーに定められている割合も 3 割弱となっている．各自治体は様々な理由で自治体が自ら基準を定めることが難しいといった課題を抱えながらも，総務省のガイドラインを参照しながら情報セキュリティポリシーを策定している．しかしながら，当の「総務省セキュリティポリシーガイドライン」には,「外部サービス」利用の留意点が自治体の「外部サービス」利用の実態に即して詳細に記載されていないため，具体的な対策基準に落としきれていないということが各自治体の課題になっていると考える．自治体が「外部サービス」を利用する際の課題は,「基幹系サービス」,「申請系サービス」,「内部情報系サービス」といったインシデント発生時に行政運営に影響を与える可能性が高い「外部サービス」を利用するにあたり，従来のオンプレミス環境とは異なる「外部サービス」の特性に合わせた留意すべきポイントへの対策が定まっておらず，インシデント発生時の対応が不十分となっていることである.本研究において,「自治体が「外部サービス」を利用する際の留意すべき確認項目」を明らかにすることができた.

6.2 新たな課題

自治体アンケートの結果から，自治体は,「外部サービス」のセキュリティ対策の仕組みやセキュリティ対策の実施状況を外部サービス事業者に確認し，情報セキュリティ要件に適合しているか判断することが困難であるという課題が判明した．オンプレミス環境であれば，自治体が仕様を定め，その仕様内容に沿って納品されているか確認すれば良いが,「外部サービス」は外部サービス事業者側がセキュリティ対策の仕組みや実施状況を管理しているため，自治体側から情報開示を求めていかないと内容を正確に把握することができない．自治体は,「外部サービス」を利用する際の管理項目を定め，外部サービス事業者に対応状況を確認し問題がないか判断していく必要がある．一方，外部サービス事業者側としては，第三者認証の取得が浸透していないという課題が挙げられる．APPLIC（一般財団法人全国地域情報化推進協会／自治体地域情報 PF 標準仕様推進）普通会員 89 社（一般財団法人・団体を除く）の第三者認証の取得状況を確認すると，クラウドサービスの国際認証である ISO/IEC27017（JIS Q 27017：2016）を取得している事業者や SOC 監査報告書の提供が可能な事業者が少なかった．ISO/IEC27017（JIS Q 27017：2016）を認証している外部サービス事業者の多くが IaaS に関する認証取得であり，自治体向け業務アプリケーションで認証を取得しているサービスは非常に少なかった.こうした状況から自治体では,「「外部サービス」の信頼性」や「情報セキュリティに関する対策の実装状況」に関する情報を客観的に得ること自体が難しい状況下にあると言える.

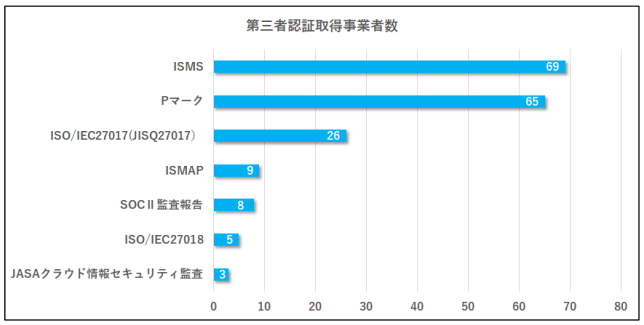

図 15　第三者認証取得事業者数（APPLIC 普通会員 89 社）2021 年 5 月調査

6.3 提言

「総務省セキュリティポリシーガイドライン」はソフトローとしての位置づけであり，自治体が「外部サービス」を利用する際の情報セキュリティ要件や仕様として定めていく際のより所になっている．本研究で明らかになった「自治体が「外部サービス」を利用する際の留意すべき確認項目」が対策基準の管理項目に示されることで，自治体の情報セキュリティポリシーに反映されることが期待でき，「外部サービス」の特性に合わせた留意すべきポイントへの対策が定まっておらずインシデント発生時の対応が不十分となっている，という自治体の課題の解決に繋がると考える．また，「外部サービス」とオンプレミス環境の相違やインシデント発生時におけるリスクについては，自治体向けの「外部サービス」に特化したガイドラインを国が策定し，自治体と共有していくことで，自治体が「外部サービス」を利用する際に必要となる情報セキュリティに対する理解が浸透していくと考える．

7. おわりに

本研究では「自治体が「外部サービス」を利用する際の留意すべき確認項目」を明らかにしてきたが，自治体では，“外部サービス事業者に対して情報セキュリティに関する対策状況といった各種情報を確認していくことは難易度が高く，確認や合意が困難である”という意見があった．これらの課題に対する解決策については，本研究では深堀りできていない．今後自治体では，「外部サービス」の利用の計画があることから，「外部サービス」を利用するにあたって効率的な運用が図られると共に，運用が適切に行われているか評価していくことが重要となってくる．自治体が「外部サービス」を利用して住民サービスの向上と業務効率化を進展させていくことは，住民の暮らしをより豊かにしていくことに繋がる．このため，自治体が「外部サービス」を利用する際の情報セキュリティマネジメントに関する研究について継続して進め，自治体が安心・安全に「外部サービス」を利用し，行政の運営ができるよう貢献していきたい．

謝辞　コロナ禍の多忙な行政運営の中，アンケート及びヒアリングにご協力頂いた各自治体の職員の皆様に，謹んで感謝の意を表する．

参考文献

[1] デジタル庁．デジタル社会の実現に向けた重点計画,p.96-97．https://www.digital.go.jp/policies/priority-policy-program（2022 年 1 月 10 日アクセス）．
[2] 総務省．総務省からの地方公共団体向け IaaS サービスの障害事案を踏まえたクラウドサービスの提供に係る対応要請について,別添 1（2020）．
[3] 両備システムズ．クラウド型システムへの第三者からのアクセスについて（更新）．https://www.ryobi.co.jp/news/notification20210212（2022.1.24 アクセス）．
[4] 読売新聞オンライン．https://www.yomiuri.co.jp/national/20210502-OYT1T50200/（2021.10.15 アクセス）．
[5] TKC．TASK クラウド住基システムの障害発生に関するお詫び https://www.tkc.jp/lg/topics/20210909_1/（2022.1.10 アクセス）．
[6] 中野区．https://www.city.tokyo-nakano.lg.jp/dept/152000/d029106.html,（2022.1.10 アクセス）．
[7] 総務省．地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 2 年 12 月版）．
[8] 渡邉英伸，晏康庄，西村浩二，相原玲二，合田憲人，吉田浩．クラウドサービス利用に向けた学術機関のための情報セキュリティガバナンスの実態調査．情報処理学会報告（2017）．
[9] 渡邉英伸，西村浩二，合田憲人，吉田浩．情報システムのクラウド化における組織的な情報セキュリティガバナンスの重要性．学術情報処理研究,No.23,p.102-111（2019）．
[10] 伊藤吉史，後藤厚宏．クラウドサービス利用における利用者視点での可用性確保についての考察－IaaS に関して－．情報処理学会第 82 回全国大会（2020）．
[11] 総務省．「地方行政サービス改革の取組状況等に関する調査等」（令和 2 年 3 月 27 日公表）」．https://www.soumu.go.jp/iken/02gyosei04_04000134.html（2022 年 1 月 9 日アクセス）．
[12] 日本規格協会．情報技術－セキュリティ技術－JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範（2016）．
[13] 日本ネットワークセキュリティ協会．情報セキュリティインシデントに関する調査報告書別紙第 1.0 版（2018）．