自治体情報セキュリティ対策の見直しについて

Ⅰ　はじめに

1　検討の背景

総務省は、「自治体情報セキュリティ対策検討チーム」（平成 27 年の日本年金機構における個人情報流出事案を受けて総務省が開催）の報告[1]を踏まえ、平成 27 年 12 月 25 日付け総務大臣通知「新たな自治体情報セキュリティ対策の抜本的強化について」により、自治体に対して、いわゆる「三層の対策」を講じるよう要請を行った。

要請を受けた各自治体においては、情報システム・ネットワークを三つのセグメント（マイナンバー利用事務系、LGWAN 接続系、インターネット接続系）に分離・分割すると同時に、インターネット接続系においては、都道府県と市区町村が協力し、原則、都道府県単位でインターネット接続口を集約した上で、「自治体情報セキュリティクラウド」の構築を行った。

これらにより、インシデント数の大幅な減少を実現するなど、短期間で自治体の情報セキュリティ対策の抜本的強化がなされている。

一方、自治体からは、ネットワークの分離・分割後、ユーザビリティへの影響を指摘する声があり、さらに、政府における「クラウド・バイ・デフォルト原則」などを受けたクラウド化、デジタル手続法[2]の成立による行政手続のオンライン化、働き方改革や業務継続のためのテレワークなど、自治体においても新たな時代の要請が日々増大している。

また、「自治体情報セキュリティクラウド」は、更新時期が迫っており、サイバー攻撃の増加やサイバー犯罪における手口の巧妙化などセキュリティ上の新たな脅威等も踏まえて、次期のあり方について検討する必要がある。

「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の改定等に係る検討会」（以下「検討会」という。）は、こうした状況を踏まえ、三層の対策の効果や課題、新たな時代の要請を踏まえ、効率性・利便性を向上させた新たな自治体情報セキュリティ対策について検討を行った。

---

[1] 新たな自治体情報セキュリティ対策の抜本的強化に向けて ～自治体情報セキュリティ対策検討チーム報告～（平成 27 年 11 月 24 日）

[2] 情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るための行政手続等における情報通信の技術の利用に関する法律等の一部を改正する法律（令和元年法律第 16 号）

２　本とりまとめの位置付け

本とりまとめは、検討会において、自治体情報セキュリティ対策の見直しに係る具体的施策をとりまとめたものである。

今後、検討会では、本とりまとめを踏まえ、更なる詳細や残された課題等について引き続き検討を行うこととするが、総務省においては、本とりまとめを踏まえ、次期自治体情報セキュリティクラウドの在り方についての自治体への助言や「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」（以下「ガイドライン」という。）の改定など必要な対応を行うべきである。

Ⅱ　具体的施策

１　「三層の対策」の見直し

検討会では、新たなセキュリティ対策の検討を行う基本的な前提として、住民情報については引き続き情報流出を徹底して防止する必要があること、従来の「三層の対策」による強靭化モデルは、自治体の情報セキュリティレベルの大幅な向上を短期間に実現しており、その基本的な枠組みは維持すること（ただし、サイバー攻撃の増加や手口の巧妙化など最新の脅威、昨今の重大インシデントを踏まえた対策の強化は必要）が挙げられた。

こうした基本的な前提の下、クラウド化、オンライン手続、テレワークなどの利便性・効率性の向上に関する新たな時代の要請への対応方策について検討した。

自治体へのアンケートや検討会での議論等を踏まえると、マイナンバー利用事務系は、住民情報の流出を徹底して防止する観点から慎重な検討が必要な一方、人手不足などを背景に eLTAX[3]やぴったりサービス[4]などのシステムと連携することで円滑に業務を遂行できる仕組みの構築が必要である。また、効率性・利便性向上の観点からは、特に、LGWAN 接続系とインターネット接続系との分割や無害化通信に関して課題があることが指摘されている。さらに、一部の自治体においては、効率性・利便性の向上方策として、インターネット接続系に業務端末・システムを配置するモデルが既に導入・検討されている。

以上を踏まえ、「三層の対策」については、以下の見直し等を行うことが必要である。

---

[3] 「eLTAX」（エルタックス）は、地方税ポータルシステムの呼称で、地方税における手続きを、インターネットを利用して電子的に行うシステム

[4] 「ぴったりサービス」は、マイナポータルを活用した子育て・介護・被災者支援の分野に限らず、あらゆる分野の手続のオンライン申請実現に活用できるシステム

(1)マイナンバー利用事務系の分離の見直し

住民情報の流出を徹底して防止する観点から他の領域との分離は維持すべきであるが、十分にセキュリティが確保されていると国が認めた特定通信（ガイドラインに明記、ex.eLTAX、ぴったりサービス）に限り、インターネット経由の申請等のデータの電子的移送を可能にする必要がある。

(2)LGWAN 接続系とインターネット接続系の分割の見直し

効率性・利便性の向上は、ネットワークの分割のいわば例外を設けるものとなるため、より高度なセキュリティ対策を実施することが必要となるが、人的・財政的リソースの制限等により、自治体によって対応可能なセキュリティ対策のレベルには差がある。

このため、業務端末及び人事給与、財務会計等の内部管理系のシステムを LGWAN 接続系に配置する従来型の強靭化モデルについて必要な改善を行ったモデル（αモデル）を基本形として提示するべきである。

さらに、クラウド・バイ・デフォルト原則やテレワーク等の新たな時代の要請を踏まえて効率性・利便性の高いモデルとして、インターネット接続系に業務端末・システムを配置した「新たなモデル」（βモデル）を提示するべきである。ただし、情報資産単位でのアクセス制御、監視体制や CSIRT など緊急時即応体制の整備、個々の職員のリテラシー向上など十分な人的セキュリティ対策を確実に実施することを採用の条件にするべきである。

(3)自治体の情報セキュリティ対策におけるリスク評価の実施

適切なセキュリティ対策を実施（対策の漏れの防止、過剰投資の抑止）するためには、システム構成、保有情報等に応じたリスク評価を実施することが重要となる。

上記（1）、（2）の「三層の対策」の見直しにあたっては、総務省は、一部の自治体の協力を得て自治体が保有する情報資産を対象としてリスク評価を実施し、リスクに対して必要なセキュリティ対策を整理することが必要である。

2　業務の効率性・利便性向上

(1)自治体の内部環境からパブリッククラウドへの接続

現在、政府では、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（平成 30 年6月7日 CIO 連絡会議決定）を定め、情報システム調達に際しては、コスト削減や柔軟なリソースの増減等の観点から、クラウドサービスの利用を第一候補として検討を行うこととする（クラウド・バイ・デフォルト原則）などクラウドサービスの利活用が進められている。自治体においても、住民等の多様なニーズに迅速に応え

た行政サービスを提供する観点も踏まえながら、その利活用が求められている。

一方、自治体においては、総務省の主導により、情報セキュリティ対策として、平成27 年度以降、いわゆる「三層の対策」を講じ、マイナンバー利用事務系や LGWAN 接続系の内部ネットワーク環境とインターネット接続系のネットワークの分離・分割がなされたことによって、インターネット接続系以外の領域から安全にパブリッククラウドを利活用する方策が検討課題となっている。

このため、検討会においては、自治体の検討に資するよう、LGWAN 接続系のネットワークから、セキュリティを確保しつつ、パブリッククラウドに接続するための技術的要件について検討を行い、令和2年1月に中間報告をとりまとめた。

今後、国のクラウドサービスの安全性評価制度や当該中間報告を踏まえて安全にパブリッククラウドを利活用する方策について更なる検討・整理を進め、必要に応じガイドラインの改定を行うべきである。

(2) 自治体の内部環境へのリモートアクセス

自治体においては、働き方改革や業務継続の観点から、テレワーク等のリモートアクセスに対するニーズが高まっている。一方、セキュリティへの懸念等から、活用は限定的になっている。

このため、検討会においては、テレワーク等の導入検討に資するよう、インターネット回線を使用せず閉域網を使用した LGWAN 接続系へのリモートアクセスの技術的要件等について検討を行い、令和2年1月に中間報告をとりまとめた。

今後、インターネットを経由した LGWAN 接続系へのテレワークについても、早急に技術的要件等の整理を行うべきである。

さらに、これらの検討結果を踏まえ、ガイドラインの改定を行うべきである。

(3) 庁内無線 LAN

現行のガイドラインにおいては、職員が主に利用する LGWAN 接続系において、無線 LAN の利用は避けることが望ましいとされている。

一方、自治体においては、業務効率化の観点から、庁内無線LANによる柔軟な職場環境の実現に対するニーズが高まっており、既に導入されている例もある。

庁内無線 LAN の利用によって、例えば、ノートPCを持ち込んでのペーパーレス会議やフリーアドレスの実現等が可能となるが、セキュリティ対策が不十分な場合、不正アクセス等のリスクも懸念される。

このため、検討会においては、利用ニーズの高い LGWAN 接続系における庁内無線 LAN の利用に関するセキュリティ要件を整理した。

今後、当該検討結果を踏まえ、ガイドラインの改定を行うべきである。

3　次期「自治体情報セキュリティクラウド」の在り方

「自治体情報セキュリティクラウド」を都道府県毎に構築し、運用を開始した平成 29 年度以降、マルウェアへの感染等は大幅に減少している。また、自治体へのアンケートや検討会での議論では、自治体における情報セキュリティ対策が浸透したこと、県と市町村間の連携が密に実施され、インシデント対応や二次被害防止が実現されていることも効果として挙げられている。

しかしながら、各自治体情報セキュリティクラウドによって、導入している機能や監視を委託されている事業者のレベルに差異があること、調達方式等において非効率な面があること、災害発生時の可用性などに課題があることが指摘されている。

以上を踏まえ、次期「自治体情報セキュリティクラウド」のあり方については、以下のとおりとすることが適当である。

また、総務省は、早急に次期「自治体情報セキュリティクラウド」のあり方を決定し、自治体に助言すべきである。さらに、自治体の予算要求時期等を見据え、技術的要件等の詳細について検討を行い、助言すべきである。

(1) 基本的な考え方

次期自治体情報セキュリティクラウドは、標準要件を総務省が提示し、民間事業者がクラウドサービスを開発・提供することにより、セキュリティ水準の確保とコストの抑制を実現することが望ましい。

また、各団体の求める水準に応じて、オプション機能を柔軟に選択できること、可用性・コストを考慮し、接続回線（インターネット回線・専用回線サービス等）を柔軟に選択できることが必要である。

運用形態については、引き続き、都道府県が主体となり調達・運営し、市区町村のセキュリティ対策を支援する形態（複数の都道府県の共同調達・運営も可能）とすることが適当である。

(2) サイバー攻撃の増加など新たな脅威や現行課題への対応

高度なセキュリティレベルを確保するため、セキュリティ専門人材による監視機能（SOC）を強化することが必要である。また、監視を行う事業者のレベルを確保するため、総務省が提示する標準要件において、SOC の仕様を盛り込むことが適当である。さらに、災害時等に住民や企業への情報発信が中断することがないよう、業務継続のための負荷分散機能（CDN）や、暗号化通信の増加に伴う暗号化された通信に対する監視機能の追加を検討することが必要である。さらに、インターネット接続系に業務端末・システムを配置した「新たなモデル」（βモデル）を採用する自治体のエンドポイントを監視する機能をオプションとして選択可能にすることも考えられる。

（3）その他のオプション機能の例示

標準要件においては、自治体事務の効率化に資するメールやファイルの無害化機能等をオプション機能として例示するべきである。

4　昨今の重大インシデントを踏まえた対策の強化

（1）神奈川県における情報流出事案を踏まえた対策強化

令和元年 12 月、神奈川県において、リース契約満了により返却したハードディスクの盗難による情報流出が発覚した。総務省では、同日、当面の対応として、住民情報が大量に保存された記憶装置の廃棄等の方法を物理的な破壊又は磁気的な破壊の方法により行うとともに、自治体の職員が当該措置の完了まで立ち会いを行うなど確実な履行の担保を要請した。その後、検討会及びその下に設置した「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の改定等に係る検討会ワーキンググループ」（以下「ワーキンググループ」という。）において、情報資産や機器の廃棄等について、情報の機密性に応じた適切な手法等を整理した。

今後、当該検討結果を踏まえ、ガイドラインの改定を行うべきである。

（2）クラウドサービスの大規模障害を踏まえた対策強化

令和元年 12 月、日本電子計算株式会社が提供する自治体向けクラウドサービス「Jip-Base」に障害が発生し、全国 53 団体 453 システムに影響を与え、その一部については、要介護認定、各種証明書の発行、ホームページの閲覧等に長期間の支障が発生した。

その後、検討会及びワーキンググループにおいて、原因の検証と再発防止策について整理した。

今後、総務省は、システムに求められる可用性等のレベルに応じたクラウドサービスの選択や SLA を含む適切な契約等を推進するよう取り組むとともに、当該検討結果を踏まえ、ガイドラインの改定を行うべきである。

5　各自治体の情報セキュリティ体制・インシデント即応体制の強化

平成 27 年の日本年金機構の情報漏えい事案発覚後、インシデント即応体制の強化が図られたが、自治体へのアンケートの結果では、CSIRT の整備状況は市区町村で 65%にとどまり、役割の明確化についても、市区町村の半数で明確化できていない状況にあった。また、情報システム担当者等に対する実践的サイバー防御演習（CYDER）も開催されているが、未受講の自治体が多い状況にある。さらに、標的型メールへの対応や USB による情報持ち出し等職員のセキュリティ・リテラシーが求められる事案も多いことから、今後、職員に向けた情報セキュリティの啓発や訓練が継続

して必要である。

以上を踏まえ、総務省は、地方公共団体情報システム機構と連携して、以下事項について、引き続き積極的に取り組むべきである。

(1)実践的サイバー防御演習(CYDER)の確実な受講

総務省は、国立研究開発法人情報通信研究機構(NICT)を通じ、国の機関、指定法人、独立行政法人、自治体及び重要インフラ事業者等の情報システム担当者等を対象とした体験型の実践的サイバー防御演習(CYDER)を実施している。

受講率の向上に向け、各自治体の受講計画の策定とそのフォローアップ、オンラインでの受講を可能とする演習実施環境の整備等の実施により、未受講の自治体を中心とした計画的な受講を推進する必要がある。

(2) インシデント対応チーム(CSIRT)の設置及び役割の明確化推進

CSIRT 未設置の小規模市町村向けに「小規模自治体のための CSIRT 構築の手引き」を作成するとともに、作成した手引きを基に CSIRT 構築のポイントや必要性について説明会を開催するなど CSIRT の設置及び役割の明確化を推進すべきである。

(3) 演習等を通じた各自治体の職員のセキュリティ・リテラシーの向上

地方公共団体情報システム機構が実施しているインシデント対応訓練の取組を引き続き実施することが重要である。また、内閣サイバーセキュリティセンター（NISC）主催の「分野横断的演習」等の参加自治体を増加させる取組を検討すべきである。

(4) 啓発や訓練を通じた各自治体の職員のセキュリティ・リテラシーの向上

地方公共団体情報システム機構が実施しているリモートラーニングによる情報セキュリティ研修（e ラーニング)、情報セキュリティ対策セミナー（集合研修)、情報セキュリティに関する技術講習会等の取組を引き続き実施することが重要である。

６　ガイドラインの適時の改定

総務省は、次回のガイドラインの改定において、平成 30 年７月に改定された「政府機関等の情報セキュリティ対策のための統一基準」（NISC）の改定についても反映すべきである。また、今後は統一基準等の改定後早期に改定を行うべきである。

Ⅲ　スケジュール

総務省は、自治体の予算要求時期等を見据え、早急に自治体に提示すべき事項（次期「自治体情報セキュリティクラウド」の在り方等）は、自治体へ助言することが必要である。さらに、総務省は、本とりまとめを踏まえ、ガイドラインについて、2020 年夏を目途に改定を行うべきである。

Ⅳ　検討会の概要

１　検討会

【構成員名簿（※ 敬称略、五十音順)】

■　構成員

	石井夏生利	中央大学国際情報学部教授
	上原哲太郎	立命館大学情報理工学部教授
	岡村　久道	弁護士　京都大学大学院医学研究科講師
（座長）	佐々木良一	東京電機大学総合研究所特命教授
	庄司　昌彦	武蔵大学社会学部メディア社会学科教授
	長峯　道宏	千葉市総務局情報経営部業務改革推進課長 （令和２年４月から）
	塗師　敏男	横浜市総務局しごと改革室 ICT 担当部長
	半田　嘉正	富山県経営管理部情報政策課情報企画監
	三輪　信雄	総務省最高情報セキュリティアドバイザー
	若杉　健次	港区総務部情報政策課長（令和２年４月まで）

■　オブザーバ

総務省自治行政局住民制度課

総務省サイバーセキュリティ統括官室

地方公共団体情報システム機構

【開催実績】

	主な議題
第１回 （令和元年 12 月 3 日）	(1) 検討会の運営について (2) 新たな自治体情報セキュリティ対策について
第２回 （令和元年 12 月 23 日）	(1) ワーキンググループの設置について (2) 新たな自治体情報セキュリティ対策について (3) ユーザビリティの改善について
第３回 （令和２年１月 31 日）	(1) ワーキンググループでの検討状況について (2) 新たな自治体情報セキュリティ対策について
第４回 （令和２年 2 月 28 日）	(1) ワーキンググループでの検討状況について (2) 新たな自治体情報セキュリティ対策について
第５回　※書面会議 （令和２年４月 20 日）	(1) 自治体情報セキュリティ対策の見直しについて（素案）
第６回 （令和２年５月 15 日）	(1) 自治体情報セキュリティ対策の見直しについて（案） (2) 今後の進め方及びワーキンググループの設置について

２　ワーキンググループ

【構成員名簿（※ 敬称略、五十音順】

■　構成員

上原哲太郎　　立命館大学情報理工学部教授

塗師　敏男　　横浜市総務局 ICT 担当部長

半田　嘉正　　富山県経営管理部情報政策課情報企画監

三輪　信雄　　総務省最高情報セキュリティアドバイザー

若杉　健次　　港区総務部情報政策課長

■　オブザーバ

総務省サイバーセキュリティ統括官室

【開催実績】

	主な議題
第１回 （令和元年 12 月 23 日）	(1) ワーキンググループの運営について (2) 神奈川県からのヒアリング (3) 事務局提出資料について
第２回 （令和２年１月 15 日）	(1) 第１回ワーキンググループを踏まえた議論 (2) 日本電子計算株式会社ヒアリング
第３回 （令和２年 2 月 28 日）	(1) 日本電子計算株式会社における再発防止策について (2) 「Jip-Base」で発生した障害を踏まえた再発防止策（案）について