地方公共団体におけるサイバーセキュリティに関する支援策及び実効性確保の検討に係るワーキンググループ　報告書

令和８年４月

地方公共団体におけるサイバーセキュリティに関する支援策

及び実効性確保の検討に係るワーキンググループ

目　次

１．はじめに

（サイバー攻撃の現状）

○　国民の社会生活、企業・行政の活動などの様々な場面においてデジタルの活用が浸透するにつれて、サイバー攻撃は、その手法のバリエーションと規模を絶えず拡大させながら深刻な脅威となっている。世界中の攻撃者は常に新たな技術を取り入れ、従来の防御策を回避しようとしている状況にある。

○　ランサムウェア攻撃は依然として最も深刻な脅威の一つであり、その被害は増加の一途をたどっている。特に、サプライチェーンを通じて複数の組織に被害が拡大するケースも多くなっており、甚大な経済的・社会的損失を与えている。

○　また、生成 AI 含む AI 技術の進化は、サイバー攻撃のあり方を根本的に変えつつある。攻撃者は AI を活用して、より巧妙で自動化された攻撃キャンペーンを展開している。例えば、AI は標的の組織に関する情報を自動で収集・分析し、効果的なフィッシングメールの文面を生成したり、脆弱性を効率的に探索したりすることに利用されている。防御側も AI による検知システムを導入しているが、攻撃側も AI でそれを欺く戦術を開発しており、攻防の高度化・自動化が急速に進んでいる。

○　さらに、IoT 機器の爆発的な増加は、新たな攻撃対象領域を生み出している。家庭用ルーターからスマート家電、産業用制御システムに至るまで、インターネットに接続される機器は増え続けているが、その多くはセキュリティ対策が不十分なまま運用されていることが多い。攻撃者はこれらの脆弱な IoT 機器を乗っ取り、ボットネット（乗っ取られた機器のネットワーク）を構築して、大規模な DDoS 攻撃（サービス不能攻撃）の踏み台として悪用している。

○　これらの要因が複合的に絡み合い、サイバー攻撃全体の増加に繋がっている。国立研究開発法人情報通信研究機構（NICT）による国内の観測データを見ても、不審な攻撃パケット数は年々増加傾向にあり、日本のネットワーク環境全体に対する脅威レベルは上昇し続けている。攻撃の自動化・効率化が進んだ結果、これまで以上に多くの攻撃が、より低いコストで実行可能となっており、全ての組織・個人が常にサイバー脅威にさらされている。

○　このことは、地方公共団体においても例外ではなく、委託先の事業者がサイバー攻撃を受けたために保有する住民情報が漏洩したり、ネットワークに対する不正アクセスを受けたりしており、いつ重大なインシデントが発生してもおかしくない状況にある。

（サイバーセキュリティ対策の確実な実施の必要性）

○　地方公共団体が管理する住民情報や税務データといった機密情報が流出した場合、住民生活に対する甚大な被害だけでなく、行政全体への信頼失墜を招く。また、水道、電力、交通、医療といった重要インフラに関わるシステムが攻撃を受けた場合、地域社会の機能停止という最悪の事態を引き起こしかねない。

○　こうした懸念を踏まえると、住民の生活を支える基盤である地方公共団体におけるサイバーセキュリティ対策の強化は、待ったなしの喫緊の課題である。

○　また、従来の「境界型防御」のみに依拠しないゼロトラストアーキテクチャの考え方の導入が検討されているが、これを導入する前提・前段階として、基本的なサイバーセキュリティ対策の徹底が必要となる。特に OS やソフトウェアの脆弱性管理、認証の強化、職員の教育など多岐にわたる項目で対策の底上げが必要となる。

○　さらに、令和７年の通常国会では、サイバー対処能力強化法[1]、同整備法[2]が成立し、地方公共団体についても官民連携協議会、通信情報の利用の枠組みへの参加等を通じ、社会全体のサイバーセキュリティ向上に一定の役割を果たすことが期待されている。また、同時に改正されたサイバーセキュリティ基本法において、サイバーセキュリティ戦略本部の所掌事務に、重要インフラ事業者等のサイバーセキュリティの確保に関する所管省庁の施策について、基準を作成すること等が追加されている。今後、改正サイバーセキュリティ基本法に基づき、総務省においても、「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。）」

---

[1] 重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第 42 号）

[2] 重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（令和７年法律第 43 号）

の改定や、重要インフラ事業者等たる地方公共団体のサイバーセキュリティの実効性確保等、基準の策定・変更を契機として、必要な施策を機動的に推進する必要がある。

２．地方公共団体におけるサイバーセキュリティ対策の現状と課題

○　地方公共団体におけるサイバーセキュリティ対策については、これまで総務省がガイドラインを示し、各団体はこれを参照して情報セキュリティポリシーを策定し、物理的・人的・技術的な対策を行ってきた。その結果、ガイドラインで示した多くの項目については、各団体において概ね実施されている状況にある。

○　具体的には、組織運営の要となる CISO（最高情報セキュリティ責任者）の設置[3]をはじめとする組織体制の整備や、全てのセキュリティ対策の起点となる情報セキュリティポリシーの策定[4]など、ガバナンスの根幹を成す基本的な規程類の整備はほぼ全ての地方公共団体において実施済みである。これらに加え、サーバー室の入退室管理[5]やサーバー等の停電対策・免振対策等[6]といった物理的セキュリティ対策、また、定期的なセキュリティ研修の受講[7]を通じたリテラシー向上や緊急時の迅速な庁内連絡体制の構築[8]といった人的セキュリティ対策についても、多くの団体において実施されている状況にある。さらに、許可されていないソフトウェアのインストール制限[9]やウィルス対策ソフトのパターンファイルの最新化[10]といった基礎的な技術的セキュリティ

---

[3] 「CISO の任命」を実施していると回答した団体　95.8%（「地方公共団体における情報セキュリティ対策に関する調査結果（令和 7 年 10 月末時点）」より。以下同じ。）

[4] 情報セキュリティポリシー（基本方針）を策定済みの団体　98.9%

[5] サーバー室等の重要区域への入退室管理を実施している団体　95.3%

[6] サーバー等の停電対策・免振対策等を実施している団体　90.4%

[7] 情報セキュリティ研修を実施している団体　90.7%

[8] 庁内の関係部署に伝達するための連絡体制を整備している団体　90.3%

[9] 許可されていないソフトウェアのインストール制限を実施している団体　88.7%

[10] ウィルス対策ソフトのパターンファイルの最新化を実施している団体　84.5%

対策に関しても、規模の大小を問わずほとんどの地方公共団体において実装が完了している。

こうした長年にわたる多角的かつ継続的な取組により、住民の機密情報を扱う「マイナンバー利用事務系」や、行政ネットワークの基幹である「LGWAN接続系」等の重要な情報システムにおいては、外部からのサイバー攻撃によって、行政サービスが長期停止するような深刻なシステム障害や、大規模な情報漏洩が発生した事案は、現在のネットワーク・システム構成となって以降、確認されていない。

○　また、令和6年の地方自治法改正により、地方公共団体はサイバーセキュリティを確保するための方針を策定等するとともに、サイバーセキュリティの確保のために必要な措置を講じることが法律上の義務となり、より制度的な対応が強化されている。

○　一方で、ガイドラインに記載されているサイバーセキュリティ上重要な対策項目の中には、依然として実施率が低い、あるいは対策が不十分な項目が存在している[11]。例えば、詳細なログ管理が実施されていない場合には、攻撃者等の不正なアクセスの兆候を検知できず、被害の封じ込めが遅れ、二次被害を拡大させるなど深刻な影響が発生したり、フォレンジックで詳細な解析ができず原因究明が困難となり、効果的な再発防止策の策定に影響したりする。また、未知の不正プログラム対策を含む高度な防御・検知・対処の一連の対策が確実になされていない場合には、「ゼロデイ攻撃等の昨今の巧妙なサイバー攻撃」に対して無防備となるとともに、「潜伏活動」による被害が深刻化し、結果として基幹システムの長期停止や大規模な情報漏洩など深刻な社会的混乱を引き起こすリスクが考えられる。

---

[11] ・機密性の高いデータの暗号化保存を実施している団体　25.0%
・機密性2以上の情報資産を扱う業務システムのアクセスログ収集と定期的な不正アクセスの確認を実施している団体　49.0%
・端末への未知の不正プログラム対策の導入を実施している団体　43.6%
・CSIRTの構築、整備を実施している団体　77.5%
・情報セキュリティインシデント対応訓練を実施している団体　44.3%
・脆弱性診断を過去3年以内に実施している団体　20.2%
・団体外の組織に委託する外部監査を実施している団体　19.7%

○　以上のように、地方公共団体においては、基幹系システムを中心にネットワーク分離と境界防御による多層防御が構築されており、これまで深刻なインシデントの発生は抑制されてきた。しかし、サイバー攻撃の高度化により「侵入を完全に防ぐことは困難」という前提に立てば、侵入後の被害拡大を最小化する応急対応や、有事における迅速な意思決定フローの確立・運用など、サイバーレジリエンスの実効性確保には課題が残されている。

○　また、依然として、メール誤送信や電磁的記録媒体の紛失など人的なミスによる情報漏洩や、委託先事業者がサイバー攻撃を受けたために情報が漏洩する事案も数多く報告されており、これらは地方公共団体における個々の職員に対するセキュリティ意識の徹底不足や、委託先事業者の管理が不十分であることが一因となっている。

○　さらに、近年、グローバルなサプライチェーン・リスクが深刻化する中、国家安全保障の観点から IT 製品等の信頼性を担保する調達リスク対策の重要性が、かつてないほど高まっている。この点、政府機関においては「IT 調達に係る国等の物品等又は役務の調達の安全性等の確保に関する申し合わせ」に基づき、実効性のある調達リスク対策が講じられている。一方で、地方公共団体においては、サプライチェーン・リスク対策への意識醸成が途上であるとともに、最新のインテリジェンスや高度な情報網を駆使してリスクを的確に判断し、実効的な調達管理を行う体制が多くの団体で整っていないことが喫緊の課題となっている[12]。

○　こうした重要かつ基本的な対策の実施状況のばらつきは、地域間の財政基盤やセキュリティ専門人材の偏在、あるいはセキュリティ対策の必要性に関する理解度の違いといった構造的な問題に起因するものあり、単に「ガイドラインを示す」という形式的な対応に留まらず、実際に機能する実効的な対策を講じるといった一段上の施策が求められる。

[12] 機器等の選定基準に関する運用規程を整備している団体　11.6%

３．施策の方向性

○　今後、全ての地方公共団体において、一定水準のサイバーセキュリティを確保し、向上させる観点から、以下の三つの方向性で実効性確保に向けた取組を推進していく必要がある。

①国等による支援

地方公共団体単独では導入・運用が困難な高度なセキュリティ基盤や専門的サービスについては、国が主導して提供する枠組みが必要である。特に、セキュリティに優位性があるガバメントクラウドの活用や、標準化・共通化されたシステムの認定・提供、高度な監視・分析機能の提供など、国が一括して行うことのメリットを十分に享受できる分野において積極的な支援を行うことが考えられる。

②改正地方自治法に基づき地方公共団体が講ずべきサイバーセキュリティ対策の細目化

サイバーセキュリティ対策の確実な実施を担保するため、改正地方自治法に基づき、地方公共団体が講ずべきサイバーセキュリティ対策を細目化し、一貫性のある明確な基準として示すこととすべきである。

③対策実施状況のフォローアップと評価

対策が確実に実行されているかを把握し、改善を促すための仕組みを構築することが不可欠である。特に、地方公共団体による自己点検だけでなく、総務省や外部機関による定期的な監査やセキュリティ評価を導入し、客観的な評価を実施すること、実施状況の調査とフィードバックを的確に行うことが考えられる。

○　これら「一段上の施策」を通じて、地方公共団体におけるサイバーセキュリティ対策を形式から実質へと深化させ、住民が安心してデジタルサービスを利用できる基盤を整えていく必要がある。以下、３つの方向性について、それぞれ具体的なあり方を提言する。

（1）方向性①「国等による支援」

ア　国等による支援

a 現在の国の支援

○　現在、国等においては、地方公共団体のサイバーセキュリティ強化のため、ASM の基盤整備や LGWAN の整備・運用等の共通基盤の整備、ガイドラインや法制度等の制度整備を行っている。

・ASM の基盤整備

ASM(Attack Surface Management)は、インターネットを通じて組織の外部からアクセスすることができる IT 資産（サーバー、クラウドサービス、ネットワーク機器等）について、攻撃者の視点で継続的に発見・監視し、潜在的な脆弱性や設定ミスなどのリスクを評価・管理するプロセス。

全ての地方公共団体が利用可能な「地方版 ASM システム」を国が一括で構築し、各地方公共団体が個別に専門人材を確保することなく、自組織の外部からの攻撃リスクを効率的に把握・対処できる仕組みを整備することとしている（令和 8 年度に構築・実証、令和 9 年度から全国展開）。

なお、政府機関においては、すでに ASM システムを構築し運用を開始しているため、地方版 ASM システムの具体的な検討の際には、政府機関の取組との調整をしながら構築を行うべきである。また、脆弱性が発見された場合の対応について、ルール化しておくことも必要である。

・ペネトレーションテストの実施

地方公共団体の情報システム、ネットワークに対して、疑似的な攻撃を仕掛けることにより、脆弱性を診断するテストを実施（令和 7 年度に 7 団体を対象として実施）。テストの結果、他の地方公共団体においても対応すべき事項があれば、全国に周知をして対策を促すこととしている。

・LGWAN の整備・運用（地方公共団体情報システム機構（J-LIS）実施）

総合行政ネットワーク（LGWAN）は、全国の地方公共団体間、地方公共団体と国の行政機関との間で、機密性の高い情報を含む行政情報を安全にやり取りするために構築された、行政専用の閉域ネットワーク。LGWAN は、インターネットとは直接通信が出来ないように分離されており、外部からの不正アクセスやサイバー攻撃のリスクを低減している点が最大のセキュリティ上の特徴。住民情報や税務情報といった重要な個人情報について、インターネット経由では困難なレベルで保護しながら情報連携することが可能となっている。

・自治体情報セキュリティ向上プラットフォームの整備（J-LIS 運用）

主に閉域系のコンピュータ端末に対し、OS やウィルス対策ソフトウェアの更新プログラム等を LGWAN 環境内で安全に提供する仕組み。各地方公共団体が個別にインターネット経由で更新プログラムを取得・適用する際のセキュリティリスクを排除しつつ、全地方公共団体のセキュリティレベルの均質化・底上げを図っている。

併せて、インターネット上に存在することが前提となっている業務アプリケーションの認証機能を増強することとしており、セキュリティを確保しながら利便性の向上に資する機能の提供も行う予定としている。

・自治体情報セキュリティクラウドの更新に対する補助

自治体情報セキュリティクラウドは、各都道府県が中心となり、その区域内の市区町村のインターネット接続を集約し、共同で高度なセキュリティ対策を実施・運用するために構築しているもの。具体的には、ファイアウォールや IDS/IPS（侵入検知・防御システム）、ログ分析基盤等といった複数のセキュリティ対策機能をクラウド上に集約して一元管理し、全ての通信をそこで監視・防御する体制を構築している。これにより、各地方公共団体が個別に高度な機器や専門人材を確保する必要がなくなり、コスト効率良く、かつ均一的で高いレベルのセキュリティ監視体制を実現している。

総務省は、自治体情報セキュリティクラウドの更新に対して、補助（1/2）を実施している。

・自治体 CSIRT 協議会の運営（J-LIS 実施）

「自治体 CSIRT 協議会」は、地方公共団体における CSIRT（Computer Security Incident Response Team：コンピュータセキュリティインシデント対応チーム）間の連携強化と、実践的なインシデント対応能力の維持・向上を目的として設立された組織。全国の都道府県及び市区町村を会員とし、J-LIS が事務局を運営している。主な活動内容は、インシデント対応策に関するノウハウの交換、共同での訓練の実施支援等であり、各地方公共団体が単独では対応困難な高度なサイバー攻撃の脅威に対し、組織的な防御体制を構築するための支援プラットフォームとしての役割を担っている。

また、有識者によるセキュリティ対策に資する講演等を実施する総会の開催や、実際に各地域に赴き、担当者間での意見交換等を通じてリアルな接点を確保しながら顔の見える関係を構築しているほか、CSIRT を立ち上げる支援等も行っている。総務省も積極的に活動に関与・支援しつつ、これらの活動の更なる充実が期待される。

・実践的サイバー防御演習（CYDER）の実施（NICT 実施）

実践的サイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）は、総務省の補助事業として NICT が実施する、国の機関、地方公共団体、重要インフラ事業者等の情報システム担当者を主な対象とした体験型演習。この演習は、実際に発生したサイバー攻撃事例に基づき、地方公共団体等の LAN 環境を再現した仮想演習環境において、受講者が攻撃の検知から初動対応、被害の拡大防止、システム復旧までの一連のインシデントハンドリングを実践的に学ぶことを目的としている。座学だけでなく、自ら手を動かし攻撃への対処方法を体得できるため、組織のセキュリティ人材育成とインシデント対応能力の向上に大きく貢献している。

・ガイドライン、ICT-BCP ガイドラインの策定

ガイドラインでは、地方公共団体が統一的かつ体系的なセキュリティ対策を構築・運用するための枠組み（基本方針や対策基準）を示している。また、「地方公共団体における ICT 部門の業務継続計画（BCP）策定に関するガイドライン」（ICT-BCP ガイドライン）では、地震を中心とした大規模災害における非常事態発生時においても、情報システムやネットワークを維持・回復し、行政サービスを継続・再開するための具体的な手順や体制づくりについての指針を示している。総務省は、これらガイドライン等を通じて、全国の地方公共団体における情報管理体制の標準化と、セキュリティレベル及び危機管理対応能力の底上げを図っている。

・サイバーセキュリティ対策に係る地方財政措置の拡充

令和 6 年改正の地方自治法に基づき、令和 8 年度から、地方公共団体においてサイバーセキュリティを確保するための方針を策定し、方針に基づき必要な措置を講じることとされている。

そのため、地方公共団体が望ましいセキュリティ対策を講じることができるよう、地方財政措置を講じることとしている。具体的には、地方公共団体が実施するペネトレーションテストやリスクアセスメント、各職員の端末等における各種脅威への対応の強化、地方公共団体におけるセキュリティ人材の確保・育成のための研修・訓練の実施、情報セキュリティポリシーの改定に要する経費について、地方交付税措置を講じることとしている。また、サイバーセキュリティ対策の強化のための業務端末やシステムへの不正アクセスを常時監視するシステムの導入に要する経費について、デジタル活用推進事業債の対象とすることとしている。

なお、本報告書で提言する地方公共団体が講ずべき措置の実施に支障が生じないよう、今後とも、適切な地方財政措置を講じるべきである。

b 今後実施すべき国の支援

○　以上のような既存の支援・仕組みに加え、今後、改正地方自治法に基づく必要な措置を細目化していくに当たって、各地方公共団体が細目化項目を確実に実施することができるよう、国は切れ目のない継続的な支援を実施する必要がある。特に、専門人材や予算が限られる中小規模の団体が、細目化基準を遵守できるよう、機械的な一律の対応ではなく、各地方公共団体の現状やリソースの状況に即した、きめ細やかな支援メニューを提供すべきである。

○　アンケートの結果からは、地方公共団体がサイバーセキュリティ対策を進める上で、特に人材面の不足と財政面の負担という二つの課題を抱えていることが浮き彫りとなった[13]。このような現状を踏まえ、国においては、これまでの支援策に加えて以下の項目の実施について検討すべきである。

＜基盤整備、制度整備＞

・重大インシデントレスポンス専門家チームの派遣の制度化

地方公共団体におけるインシデント対応の第一義的な責任は当該団体にあるが、自らの技術力では対応が困難な深刻な事態においては、国が積極的に支援する必要がある。

そのため、地方公共団体において重大なサイバーセキュリティインシデントが発生した場合に、被害の拡大防止や復旧を支援するため、専門チームを派遣して技術的支援を行う仕組みを構築すべきである。支援に当たって、総務省は、国家サイバー統括室（NCO）等の関係機関と連携して対応し、政府等が有する高度な情報を基にした全体像を把握しつつ、同種の事

---

[13] 地方公共団体がサイバーセキュリティ対策に関して課題と感じ、対応に苦慮している事項と当該事項に当てはまると回答した団体の割合（上位５つ）

・セキュリティ対策に必要な人員が不足している　71.2%
・システム担当者の人事異動により、職員間での引継ぎが難しい　65.0%
・製品やソリューションの導入や維持にコストがかかる　61.6%
・職員の情報セキュリティやネットワークスキルが不足している　61.5%
・情報セキュリティ監査や教育・訓練等、外部に委託する場合のコスト負担が大きい　52.3%

態が他の地方公共団体において発生しないよう情報共有を行うことも有効である。

・サプライチェーン・リスク対策も含めた地方公共団体からの相談を受け付ける総合窓口の設置

地方公共団体が直面するサプライチェーン・リスクを含む多様なセキュリティ上の課題に対し、一元的な相談窓口を設置すべきである。相談対象の事案としては、主に個別の市町村から相談を受けた都道府県では対応が困難な高度な専門性が必要なものとし、技術的な助言、外部専門家によるサプライチェーン特有のリスク評価支援などを提供することが考えられる。

また、この相談窓口を通じて得られた国の支援ノウハウや具体的な対応策を都道府県にフィードバックし、都道府県（又はより広域的な連携）ごとの対応体制を強化していくことも検討すべき。

寄せられた相談事例や最新の脅威情報を集約・分析し、Q&A データベースの整備・公開やアラート情報の迅速な配信といった予防啓発機能も併せ持つことも考えられる。以上の取組により、地方公共団体は専門家の知見を容易に得ることが可能となり、全国的な対策レベルの向上と、地域格差のない堅牢なセキュリティ環境の実現が期待される。

・個別団体の課題解決に資する専門人材を派遣する事業の活用促進

地方公共団体金融機構が実施している地方公共団体の経営・財務マネジメント強化事業においては、地方公共団体の要望に応じて DX 等も含めた専門家を派遣し、知識・ノウハウの不足を補う効果的な事業を展開している。今後これらの事業をサイバーセキュリティの強化にも有効に活用するため、セキュリティ専門家のアサインを加速し、各団体のサイバーセキュリティに関する個別ニーズに的確に対応することができる専門家の派遣を増加させるべきである。

・共通システムの積極的な活用促進

デジタル庁では、政府・地方公共団体が共通で利用することができる「公共 SaaS」について、その利用を促進するための制度的な枠組みを整備し

ている。公共 SaaS は、必要なセキュリティ水準も併せて確保されているため、利用を促進することにより、各団体で個別に対策を行うよりも効率的かつ確実にセキュリティ水準を確保することが可能となる。

・人事ローテーション上の工夫等の人事制度面での取組

地方公共団体の職員の定期的な異動慣行がある一方で、サイバーセキュリティ対策の実務を担う専門人材の育成・確保は喫緊の課題であり、職員の専門性を維持・向上させるための取組が必要である。

そのため、セキュリティ専門人材の異動サイクルについて、その専門性を踏まえた適切なサイクルへと見直すことが有効である。この際、必要に応じ人材育成基本方針を策定・改正することが考えられる。また、職員に対する資格取得支援のための補助制度を設けてスキルアップを奨励することも有効であり、こうした取組を拡大していくことも重要。専門人材のエンゲージメント向上のため、情報システムやサイバーセキュリティ対策に関わる職員が団体内でキャリアを積み、役職・ポジションを段階的に上げていくことができるキャリアパスを明確に示すことも有効である。当該団体のみで適切なキャリアパスを確立することができない場合は、近隣団体との相互交流等を組み合わせることも考えられる。

＜情報共有等＞

・脆弱性情報等に関する地方公共団体と事業者の情報共有の促進

総務省において整備する地方版 ASM システムにおいて把握した脆弱性情報等を個別団体に共有し、当該団体における対処の過程において事業者に対して情報を提供することが考えられ、このような一連の取組をシームレスに行うことにより、脆弱性情報や最新の攻撃動向が迅速かつ円滑に伝達される体制の構築を促進する。

また、サイバー対処能力強化法に基づく協議会等に地方公共団体が参画することで、総務省、事業者、地方公共団体の間における脆弱性情報や攻撃事例の共有が円滑に進むことが期待される。協議会に参加しない地方公共団体等についても、提供可能な情報を適時に共有することが考えられる。

・整備すべき規定類のひな形の提示

専門知識を持つ職員が不足している地方公共団体にとって、調達基準、インシデント対応手順書等をゼロから作成するのは大きな負担となる。そのため、地方公共団体の負担を軽減しつつ、一定水準以上の対策の実施を確実にするため、サイバーセキュリティ対策に関する各種規定類の「ひな形」（標準テンプレート）を総務省において作成し、示すべきである。

・対策事項の意義・背景等に関する理解醸成

ASM、ログ監査、個別の様々な対策、決められたプロセス等について、現場においてなぜそれを行う必要があるのか、その本来の目的が浸透していない。対策の細目化を行い、地方公共団体に示していく際には、単なるルールとして示すのみではなく、なぜその対策が必要なのか、万が一の事態にどのように住民の情報を守る盾となるのかという背景や意義を丁寧に伝えることが必要である。こうしたことによって、現場が納得感をもって主体的に取り組むことができる意識を醸成し、実効性の高いセキュリティ対策の実施につなげていくべきである。

＜研修・訓練等の機会の提供、人材確保＞

・研修・訓練の戦略的な拡充

研修や訓練の拡充をより実効的なものとするため、地方公共団体における研修・訓練に関するニーズを整理することが不可欠である。その上で、把握されたニーズに対し、関係する多様な主体が提供する最新の知見や実践的なプログラムを戦略的にマッチングさせ、最適な研修・訓練機会を確保することが重要である。

この点、まず情報セキュリティインシデントは、日常業務における些細な操作ミスや不審なメールの開封、メールの誤送付等に起因することが多いため、全ての職員の最低限のリテラシー向上が不可欠である【A】。次に、情報システム部門の職員を中心に、ネットワークの監視、インシデントの際の対応といった高度な専門知識の獲得が必要である【B】。さらに、組織全体を俯瞰して指揮を執るマネジメント人材も重要であり、技術的な理解とともに、インシデント発生時における社会的影響の把握、限られたリ

ソースの配分判断、法務・広報を含む全部局間の調整を統括できるマネジメント人材の能力開発も必要である【C】。

今後、自治大学校等をはじめとした関係機関の提供する研修・訓練について、以上のようなニーズにマッチする形で充実させることにより、戦略的な研修・訓練の拡充を図るべきである。

《自治大学校における特別研修・訓練の実施》（B、C に対応）

将来の地方公共団体幹部職員や実務担当者を育成する自治大学校において、サイバーセキュリティ対策に関する基本的な事項を網羅的に学ぶとともに、初歩的な実践訓練を受けることができる講座を新たに設けるべきである。この講座では、最新の法令改正の動向、脅威情報、技術的な対策等の基本原則から、万が一のインシデント発生時の初動対応や組織内の体制構築に至るまで、職員として必須となる実践的な知識を体系的に提供する。また、インシデント発生時を想定した机上演習等の訓練も実施する。こうした講座を総務省が開設することにより、全国の地方公共団体において、セキュリティ意識の高い人材を計画的に育成し、組織全体のセキュリティマネジメント能力の向上に資することが期待される。

《J-LIS 等が実施する教育訓練の活用推進・強化》

J-LIS においては、多角的な一般職員向け研修プログラムを提供しているため、総務省においても各地方公共団体に対して受講の徹底を周知するとともに、都道府県に対しても管内市町村への受講勧奨を要請し、全ての職員が年に 1 回は基礎的なセキュリティ講座を履修するよう取り組むべきである。（A に対応）また、J-LIS が主催する「インシデント発生時 CSIRT 訓練」は、想定される主要な脅威を対象として地方公共団体の実務に即した訓練を行うことができる非常に有用な取組である。今後は、その実効性をさらに高めるべく、未参加団体への普及を通じた参加母数の拡大や、最新のサイバー脅威を反映した訓練内容の不断の進化、さらには NICT との密接な連携による高度な実践演習の実現など、組織や機関の枠を超えた取組の抜本的な強化を推進すべきである。総務省は、こ

うした取組を実現すべく、予算措置等を含めて全面的なバックアップをすべきである。（B に対応）

独立行政法人情報処理推進機構（IPA）の産業サイバーセキュリティセンターにおいては、経営層と現場担当者をつなぐ人材（中核人材）を対象とした育成プログラム、組織を守るためのスキルを短期間で習得することを目的とした責任者向けの短期プログラムを提供している。こうしたセキュリティ研修事業についても、地方公共団体が活用できるよう、総務省において関係省庁と調整するなど、関係するあらゆる機関の事業を可能な限り活用できるよう、取り組むべきである。（A、B、C に対応）

・人的支援の施策のあり方の検討

市町村等に対する人的支援に関して、現地の複雑なネットワーク構成や特有の運用フロー等を十分に把握しないまま専門家を単に派遣する手法では、現場のニーズと支援内容に乖離が生じ、真に実効性のある対策を講じることは困難である。

また、近年の監査ニーズの増加により、多くの監査法人のリソースは逼迫しており、地方公共団体のセキュリティ監査を担う高度専門人材の確保は全国的に困難となりつつある。

これらを踏まえると、現場に深く入り込んだ「伴走型」の支援体制を強化すべきであり、地域固有の実情やリソースの限界を十分に勘案した上で、官民連携による広域的な人材融通や育成モデルの確立を含め、持続可能な専門人材確保支援のあり方を抜本的に再構築（リデザイン）することが求められる。

○　上記の支援策を実行に移すため、今後、総務省において必要な予算・体制の確保等に着手すべきである。また、示された支援策の具体的な実施内容の精査を進めると同時に、現場の実態・ニーズとの乖離が生じないよう、地方公共団体の意見やフィードバックを定期的に収集すべきである。これらの取組により、総務省は基準遵守を求めるだけでなく、現場に寄り添った柔軟かつ継続的な支援策のアップデートを行い、全国の地方公共団体におけるサイバーセキュリティレベルの確実な向上に繋げるべきである。

イ　都道府県による支援

○　現在、都道府県は主に次の事項について、市町村のサイバーセキュリティ確保に係る支援施策を実施している。

・専門人材の育成、確保

都道府県が市町村と連携した DX 推進体制を構築し、市町村が求める人材プール機能の確保する取組が全国的に進んでいる。

例えば、広島県においては、県内の自治体における DX 推進の鍵となる専門人材の確保に向け、「DXShip ひろしま」を中核とした戦略的な取組を展開しており、県が市町のニーズを積極的に把握し、県と市町でデジタル専門人材を一括採用し、希望する市町へ派遣・シェアしている。こうした取組によって、中小規模団体の人材不足の解消を図り、県全体として行政 DX を加速させている。他の都道府県においても、地域の実情に応じた人材プール機能の確保や活用が行われることが期待される。

・自治体情報セキュリティクラウド

自治体情報セキュリティクラウドは、都道府県が中心となって仕様調整、調達を行うとともに、構築後の運用・改修も行っており、小規模団体含めた市町村のサイバーセキュリティの確保に大きな役割を果たしている。

また、東北 6 県と新潟県では、自治体情報セキュリティクラウドを共同調達し、「割り勘効果」で財政負担を軽減するとともに、各参加団体のセキュリティレベルを均質化、向上させることが実現している。

・都道府県 WAN

都道府県 WAN（Wide Area Network）は、都道府県庁と域内の各市町村などの関係機関を相互に接続する広域通信ネットワーク基盤であり、セキュアで信頼性の高い行政情報通信を実現するための不可欠なインフラとなっている。

都道府県及び市町村を結ぶとともに、民間にも開放され、公共面だけではなく、地域住民の生活向上、地域産業の活性化に寄与する基盤として整備されている場合もある。

○　また、調査結果からは、多くの都道府県において

・サイバーセキュリティ対策に係る市町村からの相談対応

・サイバーセキュリティ対策に係る情報提供や市町村を集めた勉強会、研修の実施

・サイバーセキュリティの専門人材の派遣等の人的な支援

を行っている実態がわかった。

さらに、少数ながら、次のような施策を行っている団体もある。

・補助金等の財政支援[14]

・共同調達（自治体情報セキュリティクラウド除く）の実施[15]

・首長部局以外を対象とした監査ガイドライン・自己点検チェックリスト等の提示

○　以上のように、都道府県は実際に広域団体として基礎自治体の支援をしてきたという経緯があり、引き続き、国による直接支援だけではなく、市町村に近く地域の実情に応じた伴走支援を行うことができる都道府県が、自立を後押ししていくという意味で実効的なサポートをすることは理解を得られるところであると考えられる。

---

[14] 大分県では、市町村が作成した仕様書を基に、即戦力となる外部デジタル人材を派遣するベンダー等を県が選定。選定されたベンダーから支援員を市町村の派遣してもらい、庁内ネットワークのβ'モデルへの移行に関する技術的支援、セキュリティポリシーの概要作成、情報セキュリティ研修等を実施。支援員の派遣費用に対して、県が補助を行っている。

[15] ・県が事務局を務めている「ふくおか電子自治体共同運営協議会」にて、市町村がガバメントクラウドへの接続を共同調達。自治体クラウドサービスのオプション機能として、ローカルブレイクアウト（α'モデル）を提供予定（令和８年度稼働予定)。(福岡県)・県と市町村が、オンラインストレージサービスを共同調達。サービスの中で暗号化や無害化処理を実施。(徳島県)

・都道府県と市町村が、単一の仕様書に基づき、単一の事業者からβ'モデル環境及びテレワーク環境を実現するネットワーク基盤を共同調達（令和８年度構築予定)。

・都道府県と市町村が、ファイル無害化サービスを共同調達。

ウ　国と都道府県による重層的な支援

○　個人情報保護委員会が選択的に実施している地方公共団体に対する立ち入り検査等においては、サイバーセキュリティに関する課題も認められており、特に小規模な団体では指摘事項が多い傾向にある。また、全ての地方公共団体を対象として実施している番号法[16]に基づく定期報告においても、小規模団体において安全管理措置の未実施項目が多い傾向にある。

特に、小規模団体の対応状況の改善に関しては、都道府県の支援も重要である。一方で、総務省は、都道府県に対し支援を求めるだけではなく、個人情報保護委員会と連携して、都道府県の対応をサポートすることも必要である。例えば、個人情報保護委員会が実施している研修等について、総務省からも都道府県に対して積極的な参加を求めることなどが考えられる。この他にも、総務省と個人情報保護委員会とで密に連携を行い、都道府県の市町村支援の取組をサポートすべきである。

○　また今後、都道府県においては、共同調達や財政的な支援のほか、デジタル人材の確保・育成に関する支援の中で、サイバーセキュリティ人材についてもプール機能を拡充し、より一層、市町村を後押しする役割を担っていくことが期待される。さらに、人材を共同で確保する取組も一部の地方公共団体で行われており、こうした工夫についても地域の実情に応じた実施が期待される。特に町村のサイバーセキュリティを支えるリソースは脆弱であり、人材面等での支援をシステマチックに行っていくことが重要である。

○　総務省は、先進事例を積極的に横展開すべきであり、その際、先行団体における具体的な手法の紹介など、市町村支援の実務を進める上で役に立つような情報を都道府県に示すようにすべきである。

また、都道府県が市町村を支援する際には、ある程度アウトソーシングによる対応を行うことも考えられる。その際、適切な守秘義務のあり方について、総務省がベストプラクティスを共有する取組についても効果があると考えられる。

さらに、サイバーセキュリティに関しては、弱いところから狙われるというのが常識であり、町村等の小規模団体についても、一定程度以上の水準の

---

[16] 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（平成25年法律第27号）

セキュリティ対策を求めていかざるを得ない。そうであるが故に、都道府県の市町村支援を国が財政面や制度面でサポートすることも必要であり、都道府県と国において、重層的に市町村を支援する体制等を整えるべきである。

（２）方向性②「改正地方自治法に基づき地方公共団体が講ずべきサイバーセキュリティ対策の細目化」

○　令和６年改正の地方自治法において、サイバーセキュリティに係る必要な措置の実施が義務付けられたが、重要なサイバーセキュリティ対策に関して主に中小規模の団体においては実施率が低い項目がある。一方で、対策を確実に実施している団体もあり、地方公共団体の実施している対策の内容にばらつきがある状況である。

○　ランサムウェア攻撃の巧妙化やサプライチェーン・リスク対策の必要性などサイバーセキュリティ対策の重要性が増大している現状等を踏まえると、単にサイバーセキュリティ対策実施の義務がかかっているというだけでは全体的な対策の水準を確保するには不十分であり、改正地方自治法に基づき、地方公共団体が「どのような措置を」講じる必要があるかをより解像度を上げて示すべきである。

ア　国・地方関係を踏まえた考察

○　地方公共団体の事務・事業の実施は、デジタル社会の進展によりテクノロジーの活用が前提となっている。デジタルは、インターネットを通じた同質性が強く働くため、地域的な統治団体である地方公共団体のみで規律することが難しい部分がある。こうした事情・理由により、基幹的特性をもった国家が、地方のあり方について規律をすることは、必ずしも地方自治に反するわけではない。

○　また、本来地方公共団体は、その自立のあり方・意思決定のあり方のアプトプットについて、国の関与を受けないものであり、地方分権改革においてもそれが国と地方の関係の整理、関与の法定主義等の形で進められてきた。

一方で、憲法第 92 条は、「地方公共団体の組織及び運営に関する事項は、地方自治の本旨に基いて、法律でこれを定める。」と規定しており、デジタル化以前においても、地方公共団体の意思決定のプロセスやガバナンスの仕組みについて国が一定の責任を持つことを想定している。さらに、地方自治法第１条の２第２項においては、国は、全国的に統一して定めることが望ましい国民の諸活動・地方自治に関する基本的な準則に関する事務、全国的な規模・全国的な視点に立って行わなければならない施策の実施等、国が本来果たすべき役割を重点的に担うこととされている。

特に、サイバーセキュリティという分野においては、ネットワーク外部性によりセキュリティリスクが著しく増大することに対応するため、一律の手続き・水準の確保が強く要請される。

今後、サイバーセキュリティは、地方公共団体の意思決定のプロセスの中で重要性を増していくものと考えられるが、地方公共団体が自らのガバナンスを確立し、自治の主体として能力を高めていく方向に向かうよう国がサポートすること、また、方向性や考え方の参照先を示していくことも重要であり、その一環として国がサイバーセキュリティに関して基本的な部分を規律していくことも方法のあり方として許容されるものと考えられる。

○　この点、過去累次の地方制度調査会及び研究会等においても、デジタルの特性を踏まえた提言がなされている[17]。

---

[17] ・　第 32 次地方制度調査会「2040 年頃から逆算し顕在化する諸課題に対応するために必要な地方行財政のあり方等に関する答申（令和２年６月）」においては、デジタル化を進める際の前提として、セキュリティの確保や個人情報の保護に留意する必要があるとした上で、地方公共団体の事務の標準化・統一化の必要性や地方公共団体の総意工夫が期待される程度に応じて、国は適切な手法を採るべきであり、多くの法定事務におけるデジタル化は、地方公共団体が創意工夫を発揮する余地が比較的小さく、標準化等の必要性が高いため、地方公共団体の情報システムや事務処理の実態を踏まえながら、一定の拘束力のある手法で国が関わることが適当としている。

・　「デジタル時代の地方自治のあり方に関する研究会（総務省自治行政局）」報告書（令和４年３月）においては、デジタル技術は一般的に、統一化・共通化・効率化を志向する傾向にあり、デジタル社会の進展に対応するためには、これまで地方公共団体が自らの責任で実施していた事務についても、国が担う役割が増大する可能性がある。このような特性を持つデジタル技術を、個々の地方公共団体の自主性・自立性・多様性を尊重する地方自治にどのように取り込んでいくかが課題となると指摘している。これに

イ　方式について

○　従前の地方公共団体のサイバーセキュリティに関する法体系としては、サイバーセキュリティ基本法第５条において、サイバーセキュリティに関する自主的な施策の策定及び実行の責務が規定されているのみであった。

その後、ネットワークの相互接続の進展により、一つの地方公共団体のセキュリティ対策の不備が、他の団体や国のサイバーセキュリティに対する脅威となり、その安全性や信頼性に影響を与える蓋然性が高くなることが想定されるため、地方公共団体のサイバーセキュリティ対策を強化するべく、令和６年の地方自治法改正によって「情報システム」の章が新設されている。「情報システム」の章中、第 244 条の５第２項においては、「普通地方公共団体は、その事務処理に係る情報システムの利用に当たつて、サイバーセキュリティ（中略）の確保、個人情報の保護その他の当該情報システムの適

関し、地方公共団体が実施する事務について、その処理方法、即ち「how to do（どのようにするか）」について国が法令で義務付けを行ったり関与を強めたりすることは、地方公共団体の自主性・自立性を制約することになりうるものであるが、地方自治の中核が「what to do（何をするか）」であるならば、「how to do（どのようにするか）」は一定程度制約されてもやむを得ないのではないかとの意見があると指摘している。

・　第 33 次地方制度調査会「ポストコロナの経済社会に対応する地方制度のあり方に関する答申（令和５年 12 月）」においては、今後、国・地方公共団体・民間企業・住民のネットワークを通じた相互接続がますます進展することに伴い、一つの地方公共団体のセキュリティ対策の不備や不適切なシステム利用が、他の地方公共団体や国の機関等の情報セキュリティにも脅威となり、その安全性や信頼性に影響を与える蓋然性が高くなることが想定される。こうした状況を踏まえ、地方公共団体が講ずべき情報セキュリティ対策に係る指針を国が示すとともに、地方公共団体に対し、情報セキュリティ対策の方針の策定義務及びその方針に基づく措置の実施義務を課すこととすべきであるとしている。

・　「国・地方デジタル共通基盤の整備・運用に関する基本方針（令和６年６月デジタル行財政改革会議決定）」においては、国・地方デジタル共通基盤の整備は、地方分権改革前の国と地方公共団体の関係を復活させるものではない。国による共通化や標準化の支援は、地方分権改革により明確化された国と地方公共団体との役割分担の下で、地方公共団体の事務を技術的に下支えし、負担が軽減された分、これまで手の届かなかった地域特有の課題への対処や住民へのよりきめ細かなサービスの提供などを可能とするものであると指摘している。

正な利用を図るために必要な措置を講じなければならない」とし、地方公共団体の義務を規定している。

上記規定の追加後も国においては、サイバー対処能力強化法が制定され、国全体としてサイバー安全保障を確保する施策が推進されている。また、同整備法によりサイバーセキュリティ基本法が改正され、重要インフラ等たる地方公共団体のサイバーセキュリティ確保について、より一層の対策実施が求められるとともに、これら国における法制度の整備・対策の進展と呼応して地方公共団体のサイバーセキュリティに関してもガイドラインが改定され、改定されたガイドラインに基づく対策の実践も進みつつある。

したがって、地方公共団体の組織・運営に関する制度の企画・立案を所掌する総務省は、地方公共団体のサイバーセキュリティの水準の確保に、よりコミットすべき流れとなっており、また、セキュリティ水準確保の方法（措置義務の果たし方）についても、相当程度定型化が進展している。これらを踏まえると、地方自治法に規定されているサイバーセキュリティ確保に係る必要な措置の実施義務の内容について、地方公共団体がその義務を適切に果たすことができるよう、総務省において、その実現の方法を細目として示すことが適当である。

○　この点、地方公共団体以外の重要インフラ事業者においては、サイバーセキュリティ確保の義務が法律で課せられ、具体的な措置の内容が各業界のガイドラインで示されている。一方、地方公共団体に関しては、ガイドライン（技術的助言）による関与ではなく、地方自治法に基づく義務付けの内容を省令によって細目化することが、目的達成のためにより直截であり、かつ、国・地方関係を規律する法形式としてふさわしいものと考えられる。

そのために総務省が講じる措置として、地方自治法第 244 条の 5 第 2 項の「必要な措置」について、実施の細目を定める実施命令を整備することも有効かつ必要なことと言うことができる。

○　なお、今後、サイバーセキュリティ基本法、サイバー対処能力強化法、経済安全保障推進法等のサイバーセキュリティに関する法制において、サイバーセキュリティ確保のための諸活動に関する規律の密度が高まる等、国全体の制度・施策のステージが一段上がる状況となるような場合などには、地方制度調査会における議論等も踏まえつつ、地方自治法においても、サイバーセキュリティ確保に関する規律を体系的に整理・整備し、併せてその中

でより詳細なサイバーセキュリティ対策について規定を整備することも検討すべきである。

ウ　実施命令の内容についての考え方

○　国家行政組織法第 12 条第 1 項[18]に基づき、各省大臣は、主任の行政事務について法律等を施行するため、その機関の命令として実施命令を制定することができることとされている。ただし、実施命令においては、その法律を実施するために必要な細目的事項を規定することができるにとどまり、新たに権利を制限し、義務を課することとなる事項を規定することはできない。今般制定する実施命令については、法律上の義務の解釈として自ずと導かれるものについて規定するものであり、新たに創設的な義務を規定するものではない。

現在、地方公共団体においては、政府統一基準に準拠して策定されているガイドラインを参照して現にサイバーセキュリティ対策を実践しているところであり、実施命令の内容は、ガイドラインの内容に準拠して定めることが適当である。具体的には、ガイドライン対策基準に規定する事項において、法律上の義務の解釈として自ずと導かれるものを仕分け・選定すると、サイバーセキュリティ対策の根幹かつ基本的な事項である大項目・中項目で掲げている内容を中心に規定することが妥当と判断できる。

一方、ガイドライン対策基準の小項目で定めているような個別的な基準や手法については、個々の団体のシステム・ネットワーク構成の技術的な特性に応じた各者各様の対策内容を示すものであるとともに、脅威に対応する技術の著しい変化を逐次最新の対策という形で反映していることに鑑みれば、法律上の義務の解釈として自ずと導かれる内容とまでは言えないことから、地方公共団体が参照すべきガイドラインという形式で示すのが適当である。

---

[18] 国家行政組織法（昭和 23 年法律第 120 号）

第 12 条　各省大臣は、主任の行政事務について、法律若しくは政令を施行するため、又は法律若しくは政令の特別の委任に基づいて、それぞれその機関の命令として省令を発することができる。

２、３　（略）

○　実際に細目化項目を策定・変更するに当たっては、地方公共団体に対する意見照会を行う等、丁寧な対話のプロセスを踏むことが国・地方関係の観点からも重要である。

エ　経済安全保障対策（サプライチェーン・リスク対策）

○　近年「政府統一基準群」において、サプライチェーン・リスク対策に関する改定がなされ、これに準拠しているガイドラインにもサプライチェーン・リスク対策が明記されている。また、経済安全保障推進法[19]に基づき、地方公共団体が運営する大規模な水道事業者等を含めた「基幹インフラ」について、特定重要設備の導入・更新に当たって事前の届出・審査が行われるなど、特に重要な社会基盤について、サプライチェーン・リスク対策（調達リスク対策）を徹底する法制度の整備が進んでいる。

○　また、政府機関においては、「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続きに関する申合せ」に基づき、機密性の高い情報を扱う等の重要な情報システムの導入に際して、NCO による必要な措置に関する助言を実施することとなっており、こうした施策を通じて、政府機関全体におけるサプライチェーン・リスク対策の確実な実施が担保されている。国と地方公共団体の情報システムは、ネットワークを通じて相互接続しており、万が一、地方公共団体の情報システムのサプライチェーン上の脆弱性を突いたインシデントが発生した場合、その被害が政府機関へと波及する蓋然性は高い。そのため、政府機関と同様に公的な統治団体である地方公共団体においても、政府機関と歩調を合わせたサプライチェーン・リスク対策の実施が必要である。

ガイドラインにおいては、これまでも各地方公共団体に対し、サプライチェーン・リスク対策の実施を求めており、各団体においてガイドラインを踏まえた対策の実施が進んでいる。

したがって、細目化項目の中に、サプライチェーン・リスク対策に係る事項を取り込んで定めることによって、地方公共団体における経済安全保障対策の実施を徹底すべきである。

---

[19] 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和 4 年法律第 43 号）

○　地方公共団体のサプライチェーン・リスク対策に関しては、地方公共団体にとってわかりやすく、実行可能性のあるものとすることが必要であり、細目化項目の制定と併せて、その合理的な実施方法について、ガイドライン、通知等において、可能な限り詳細な事項を示すべきである。

○　また、細目化項目に調達リスク対策を位置づけるだけではなく、実際に地方公共団体が適切な調達を行うことができるよう総務省が支援するとともに、履行状況についてのチェックを行い、関係省庁とも連携して、サプライチェーン・リスクに対応するための包括的なメカニズムを構築すべきである。

　具体的には、調達リスクに関する地方公共団体からの照会を受け付ける等、事前チェック機能も担う総合窓口の設置（「国等による支援」の項目を参照）、調達した製品に関する調査の実施等が考えられる。また、地方公共団体が、実際の調達に当たって経済安保上懸念のある製品を納入しないことを契約先の事業者に保証・宣言を求めるとともに、契約違反の際の制裁措置等についてもセットで準備をしておく等の対応も考えられる。

オ　細目化項目

○　以上の考え方を基に選定した細目化項目は、「別紙」のとおりである。なお、現行ガイドラインの「情報システム全体の強靭性の向上」に関しては、「デジタル社会の実現に向けた重点計画（令和５年６月９日閣議決定）」においては、「現行のいわゆる「三層の対策」について、地方公共団体の意見も聞きながら、抜本的な見直しを行う」とされている。現在デジタル庁において、実証事業が実施されるとともに、総務省・デジタル庁において見直しに向けた検討がなされており、見直しの方向性が固まった段階で細目化項目として示すこととすべきである。

カ　適用範囲（一部事務組合・広域連合・地方独立行政法人）

○　ガイドラインは、普通地方公共団体及び特別区の首長部局への適用を念頭に置いて策定されているものであるが、細目化項目について、普通地方公共団体及び特別区以外の主体（一部事務組合、広域連合、地方独立行政法人）への適用をどう考えるべきかが論点となる。

この点、地方自治法第 244 条の 5 第 2 項に規定する必要な措置の実施義務が及ぶ範囲は、普通地方公共団体、特別区、一部事務組合及び広域連合並びに地方独立行政法人となっており[20]、全ての主体が細目化項目に基づき、必要な措置を講じる必要があるのが原則である。一方で、一部事務組合等の中には、総合行政を担う普通地方公共団体と比較して扱う情報資産の量が著しく少ない又は全国的なネットワークに接続していない組合等もある。このような組合等においては、ネットワークを通じて他団体へ及ぼす影響や当該組合等の情報資産の質・量等の実態を踏まえて、適用の範囲を画定できるようにすべきである。

今日、地方公共団体は、ネットワークの相互接続を通じて、住民情報等の機密性の高い情報を保有し、取り扱うとともに、住民生活にとって不可欠な行政サービスを運営している。そのため、主体（普通地方公共団体か、特別地方公共団体か、地方独立行政法人か）の別にかかわらず、機密性の高い情報のやり取りに利用され、他の地方公共団体・国等の重要情報や重要な情報システムに影響を及ぼす可能性があるネットワーク（LGWAN 等）に接続している団体については、適用範囲とすべきである。ただし、重要なネットワークに接続していなくても、構成団体と同程度の量の機密性の高い情報を保有している団体があれば、当該団体も対象とすべきである。

○　なお、公立大学については、設立団体と同様の情報システム、ネットワークを活用しているかどうかといった実態に即してよく調整の上判断すべきである。学生に関しても、具体的な適用関係については、議員とパラレルに考えられる部分もあるものと考えられる。

キ　適用範囲（議会・長以外の執行機関）

○　団体内の長以外の執行機関、議会への適用についても論点となる。この点、地方自治法のサイバーセキュリティに関する規定では、サイバーセキュリティを確保するための方針の策定について、議会及び長その他の執行機関ご

[20] 特別区は地方自治法第 283 条第 1 項の規定に基づき、一部事務組合及び広域連合は同法第 292 条の規定に基づき、地方独立行政法人は地方独立行政法人法第 24 条の 2 の規定に基づき、地方自治法第 244 条の 5 第 2 項の規定がそれぞれ準用される。

とに行うこととされており、細目化項目の適用についてもその趣旨に鑑みれば同様に解するべきというのが原則である。

一方、議会、その他執行機関が首長部局と同様の情報システム、ネットワーク等を利用している場合、そのサイバーセキュリティ対策の内容が異なるということは、通常考えられない。そのため、このような場合には、当該議会、当該執行機関についても、細目化項目を適用するのが適当と考えられる。

○　なお、議会に関して、より具体的には次のとおりと考えられるが、さらに現場の実態を踏まえた内容とするよう、総務省は、議長会等の関係機関との調整を綿密に重ねるべきである。

・　議会事務局は LGWAN 接続端末を利用する等、ネットワークや保有情報資産の実態が首長部局とほぼ同様であり、このような場合には、適用範囲に含めるのが適当である。

・　議員に関しては、地方公共団体の情報資産（貸与タブレットや、非公開の行政情報等）の保有・利用があれば、当該情報資産に関して、適用範囲と解するのが適当である。（BYOD についても、当該団体の情報システムやネットワークに接続され、行政情報の参照やシステム環境に影響を及ぼす場合には、適用範囲と解するのが適当。）

○　首長部局とは異なる独自のネットワークを有する等の実態や、サイバーセキュリティ対策を所管省庁の個別ガイドラインによって講じているという事情がある執行機関に関しては、所管省庁の示した基準等により対策基準を策定している場合がある。そのため、こうした執行機関に関しては、関係省庁との調整の上、個別に対象範囲とするか否かを判断すべきである。ただし、地方自治法第 244 条の 6 第 3 項に基づく同法施行令第 173 条の 7 において、大臣指針の対象から公安委員会を除外したのは、所管省庁の法令の体系の中でセキュリティを確実に担保しているためであり、そのため、公安委員会に匹敵するような担保がとれる執行機関ではない場合は、地方自治法の体系の中で規律をかけていくべきである。

○　小・中・高校といった教育機関については、生徒の情報がインターネットを通じて事業者のクラウドにつながるなど、首長部局と比べると特殊なシステム構成、ネットワーク構成をとっている。教育機関のサイバーセキュリティについては、文部科学省が「教育情報セキュリティポリシーに関するガ

イドライン」を示して対策を行っているが、首長部局のセキュリティ水準に合わせた対策の実施についても、引き続き関係省庁と調整を図るべきである。

ク　他法令との関係等

○　個人情報やマイナンバーなど、情報の種類によっては、個人情報保護法[21]、番号法の措置の適用となる場合がある。その他にも、標準準拠システムについては、標準化法に基づく省令（非機能要件）が適用になるものと考えられるため、必要に応じて関係法令との適用関係の整理を行い、適宜地方公共団体に示していくことも検討すべきである。

○　また、地方公共団体には、まだ紙媒体での業務が多く残っているため、地方自治法が求める「サイバーセキュリティ対策」でカバーできない部分を埋める必要がある。紙媒体も含む「情報セキュリティ」については、引き続きガイドライン等において、サイバーセキュリティ対策に準ずる形で実施していくべきである。

（3）方向性③「対策実施状況のフォローアップと評価」

○　地方公共団体におけるサイバーセキュリティ対策が確実に実施されているかを国が的確に把握し、必要な支援や改善につなげていくことは、日本全体のサイバーセキュリティ向上の観点から極めて重要である。

○　そのため、総務省は、地方公共団体の事務負担を軽減しつつ、調査実施等のフォローアップを適切に行うべきである。総務省によるフォローアップを実効的かつ効率的に行うための具体的な方策としては、以下の点が考えられる。

・調査手法のシステム化と機能の充実

現在、多くの行政調査で散見される Excel ファイルによる調査は、地方公共団体の職員にとって入力の手間やバージョンの管理負担が大きく、集

[21] 個人情報の保護に関する法律（平成 15 年法律第 57 号）

計作業も非効率である。これを解決するため、専用の Web システムを構築するなど、システム上での回答・提出を可能にすべきである。

システム化に際しては、以下の機能実装が考えられるが、具体的な内容については、今後総務省において検討すべきである。

＜回答負担の軽減機能＞

- 過去の回答の自動反映: 前年度や前回の調査結果をシステムが自動的に呼び出し、初期値として表示する機能。これにより、変更点や進捗のあった箇所のみを修正すれば済むようになり、地方公共団体の入力負担を大幅に軽減できる。
- 進捗管理機能: 回答状況の保存や、担当者間での共有・確認を容易にする機能。

＜振り返り支援機能＞

- 経年比較・ダッシュボード: 過去数年の自組織の対策レベルの変遷を視覚的に確認できる機能。これにより、対策の進捗状況や課題を客観的に把握し、次年度の計画立案に役立てることができる。

・国の同種調査の効率的な活用

サイバーセキュリティに関する国の調査は、総務省だけでなく、NCO や個人情報保護委員会など、複数の省庁によって実施されており、これらの調査項目には同様の内容のものが含まれることがある。

そのため、各省庁が実施する同種の調査内容を精査し、可能な限り質問項目や定義を共通化・標準化することを検討すべきである。また、ある調査で回答した内容が、他の府省庁による類似の調査でも自動的に活用（データ連携）されるような仕組みについても検討し、重複入力を根本的に解消することも考えられる。

○　以上に示したようなシステム化による調査の効率化によって、地方公共団体の負担を軽減し、本来のセキュリティ対策の実務に集中できるようにするとともに、総務省はより正確な実施状況をタイムリーに把握するよう努めるべきである。

○　国による地方公共団体のサイバーセキュリティ対策の調査は、現状把握に留まらず、実効性のある対策推進のための重要な起点となる。この調査結果

を総務省が的確に分析し、全国的な対策状況をフィードバックすることは、各地方公共団体が自らのセキュリティ施策を見直し、次のアクションへ繋げる上で必要不可欠である。同時に、総務省もまた、全国的な傾向や共通の課題を集約し、それを国の施策へと効果的に反映させるべきである。国と地方公共団体が連携し、「調査」「フィードバック」「施策への反映」という一連のプロセスを通じて適切な PDCA サイクルを継続的に回すことが、地方公共団体全体のセキュリティレベルを着実に向上させる鍵となる。

４．おわりに

地方公共団体のサイバーセキュリティ対策における実効性の確保は、我が国全体のデジタル基盤の信頼性を左右する重要な課題である。そして、サイバー攻撃が巧妙化・複雑化し、地域を問わず深刻な脅威にさらされている現状において、各地方公共団体の自助努力に委ねるだけでなく、総務省が対策の底上げを支援することが不可欠である。

セキュリティ対策に「終わり」はなく、脅威は常に変化し続けている。総務省においては、本報告書の提言を具現化するため、制度面・予算面での支援のみならず、各団体が迷うことなくセキュリティを確保することができるよう取り組むべきである。またその際は、地方公共団体の実情に合わせ、納得をもってサイバーセキュリティ対策を推進できるよう、国と地方公共団体において丁寧な対話のプロセスを経ながら進めていくことが不可欠である。

国と地方公共団体が足並みを揃え、住民の安全な暮らしを支えるセキュリティ基盤の強靭化を推し進めていくことこそが、デジタル社会の安全を担保する唯一の道であり、地方公共団体の組織・運営に関する基本的な制度を所管する総務省が先頭に立って、積極的かつ的確な施策を講じることを期待する。

（別紙）

細目化項目

・組織体制

　責任者の設置、各責任者への適切な責任の配分等の全庁的な組織体制の整備、その他組織体制の整備。

・情報資産の分類と管理

　保有する情報資産を適切に分類し、当該分類に基づき必要な取扱い制限を講じる、情報資産を適切に管理する、その他適切な情報資産の分類と管理の実施。

・物理的セキュリティ

　サーバ等の適切な管理、管理区域の適切な管理、通信回線及び通信回線装置の適切な管理、職員等の利用する端末や電磁的記録媒体等の適切な管理その他適切な物理的セキュリティ対策の実施。

・人的セキュリティ

　職員等の遵守事項の履行等のための適切な措置の実施、研修・訓練の実施、情報セキュリティインシデントの適切な報告、ID 及びパスワード等の適切な管理その他適切な人的セキュリティ対策の実施。

・技術的セキュリティ

　コンピュータ及びネットワークの適切な管理、アクセス制御の適切な実施、システム・機器等の開発、導入及び保守の適切な実施、不正プログラム対策の適切な実施、不正アクセス対策の適切な実施、セキュリティ情報の収集その他適切な技術的セキュリティ対策の実施。

・運用

　情報システムの監視の適切な実施、サイバーセキュリティを確保するための方針の遵守状況の確認、侵害時の適切な対応その他サイバーセキュリティ対策の適切な運用の実施。

・業務委託と外部サービス（クラウドサービス）の利用

　適切な業務委託の実施、情報システムに関する適切な業務委託の実施、外部サービス（クラウドサービス）の適切な利用。

・評価・見直し

　監査及び自己点検の実施、サイバーセキュリティを確保するための方針及び関係規程等の見直しその他サイバーセキュリティ対策の適切な評価・見直しの実施。