

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について



総務省

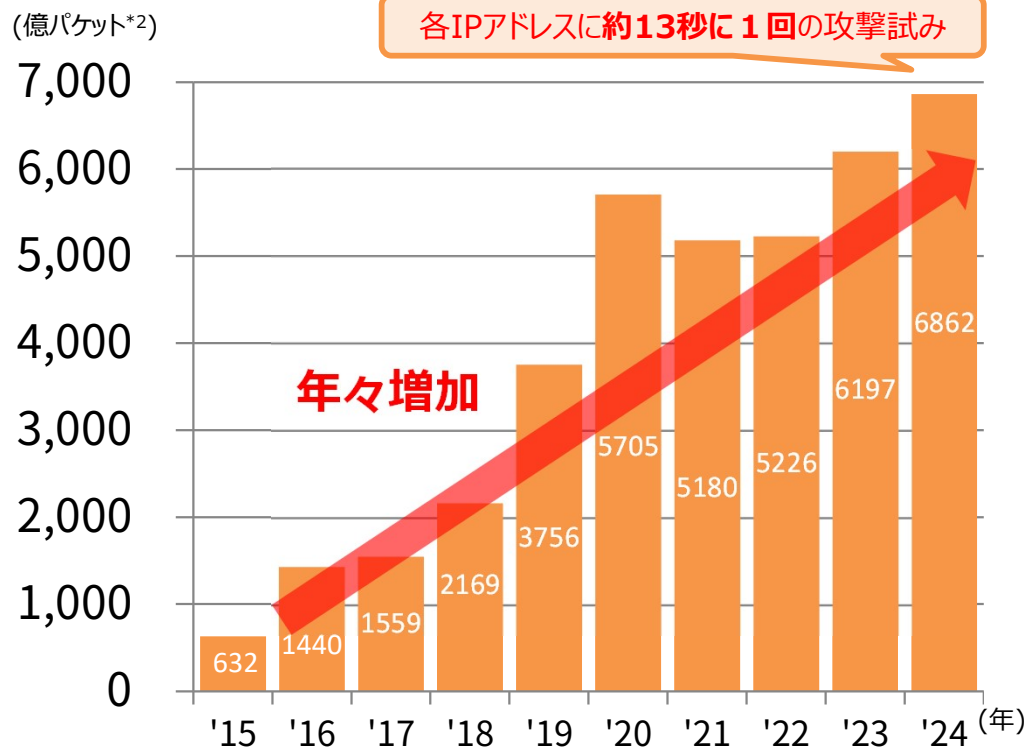
令和8年1月23日
自治行政局住民制度課
サイバーセキュリティ対策室

近年のサイバー攻撃の巧妙化・深刻化について

- サイバー攻撃は巧妙化・深刻化するとともに、サイバー攻撃関連通信数や被害数は増加傾向にあり、**質・量両面でサイバー攻撃の脅威は増大**している。

サイバー攻撃関連通信や被害の量

NICT^{*1}が観測したサイバー攻撃関連通信数の推移



*1 国立研究開発法人 情報通信研究機構

(National Institute of Information and Communications Technology) の略。

*2 1度に届くデータの塊のこと。センサーがデータを受信した回数と同義。

サイバー攻撃の巧妙化・深刻化

サイバー安全保障に関わる攻撃例

IT系システムの侵害

(暗号化・システム障害、身代金要求)

(例: 2021年米コロナルパイプライン業務停止、2022年大阪急性期・総合医療センターの業務停止、2023年名古屋港業務停止)



有事に備えた重要インフラ等への侵入

(高度な侵入・潜伏能力)

(例: 2014年クリミア併合、2022年ウクライナ侵略、2023年VoltTyphoonによるグアム等にある米軍施設や政府機関、重要インフラへの侵害)



機微情報の窃取

(アクセス権限の獲得)

(例: 2021~24年JAXAへの侵害、2023年NISCのメール窃取)

(出典: 国家サイバー統括室(NCO))

地方公共団体に関する情報セキュリティインシデント事案の主な例

サイバー攻撃

① テレワークシステム（VDI）への不正アクセス

ある地方公共団体において、テレワークシステム（仮想デスクトップ（VDI）方式で庁内ネットワークに接続し、業務を行うもの）が脆弱性を突く攻撃を受け、攻撃者が職員3名のアカウントになりすましてVDIにログインする不正アクセスが行われた。テレワークシステムのログに、不正アクセス時に外部のオンラインストレージ等にアクセスしてデータのアップロードが行われた形跡があり、情報漏えいが発覚。

② 一部団体の対策不備によるLGWANを通じた国のネットワークへの不正アクセス

複数団体が利用しているシステムに脆弱性があり、A町のファイルサーバに侵入され、A町のファイルサーバ経由でLGWANからG-Net（国のネットワーク）へ不正アクセスが発生。G-Netにおいて不正な通信を検知した。

③ 卒業アルバムを印刷する印刷会社（再委託先）へのサイバー攻撃

全国の自治体の学校が委託した写真館等から卒業アルバムの印刷を請け負った事業者（再委託先）の情報システムに対して、ランサムウェアによるサイバー攻撃が行われ、全国の自治体の学校が保有する約17万件の児童・生徒の情報（氏名や写真）が漏えいしたおそれ。

④ 通信大手事業者へのサイバー攻撃

全国の自治体や民間企業に対して、メールサーバやセキュリティ機能のサービスを提供する事業者の設備に対して、ランサムウェアによるサイバー攻撃が行われ、全国の自治体を含むサービス利用者約400万人の情報（メールアドレスや管理用パスワードなど）が漏えいしたおそれ。

情報漏えい

① USBメモリの紛失による個人情報の漏えい

住民税非課税世帯等に対する臨時特別給付金の支給事務の受託者の、再々委託先の従業員が、個人情報を含むUSBメモリを紛失。

【流出した個人情報】

- ・ 全市民の住民基本台帳の情報（46万517人分）
- ・ 住民税に係る税情報（36万573件）
- ・ 非課税世帯等臨時特別給付金の対象世帯情報（R3年度分 7万4,767世帯分、R4年度分 7,949世帯分）
- ・ 生活保護受給世帯と児童手当受給世帯の口座情報（生保 1万6,765件、児手 6万9,261件）

② メールの誤送信による個人情報の漏えい

ある地方公共団体において、職員がメールの宛先を誤って送信し、第三者に個人情報の漏えい事案が発生（漏えい人数：約6,000人）。

地方自治法改正の概要（サイバーセキュリティ関係）

- 地制調答申において、これまでの地方自治を基盤としつつ、事務の種類に応じて、他の地方公共団体や国等と連携・協力し、デジタル技術を最適化された形で効果的に活用することが重要であるとともに、**国・地方公共団体等のネットワークを通じた相互接続がますます進展する中で、地方公共団体のサイバーセキュリティ対策の実効性を担保することが必要**との提言があったことを踏まえ、以下の改正を行った。（令和6年通常国会成立）

改正前

- 現在の地方自治法には、情報システムについての規定は置かれていない。
- サイバーセキュリティについては、総務省において技術的助言として「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」を示すとともに、各地方公共団体はこれを踏まえ、個々の判断でセキュリティポリシーを定めている。

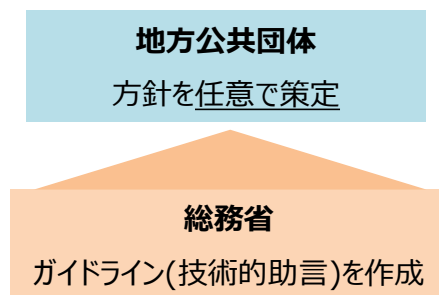
改正後

- 地方公共団体は、事務の種類・内容に応じ、情報システムを有効に利用するとともに、他の地方公共団体又は国と協力し、その利用の最適化を図るよう努める。
- 地方公共団体は、サイバーセキュリティの確保、個人情報の保護※など、情報システムの適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。
- サイバーセキュリティの確保について、地方公共団体の議会及び長その他の執行機関は、方針を定め、必要な措置を講じる。
総務大臣は、方針の策定等について指針を示す。

※ 個人情報については、漏えい防止等の安全管理措置を講じるなど、引き続き、個人情報保護法に基づき適切に対応することが求められる。

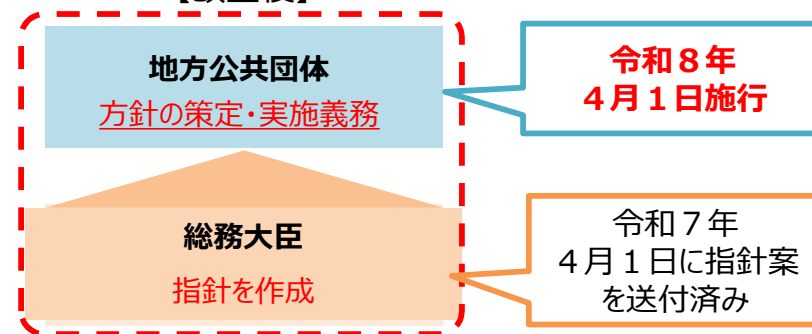
＜地方公共団体におけるサイバーセキュリティ対策＞

【改正前】



法律に具体的な規定なし
(サイバーセキュリティ基本法の責務規定のみ)

【改正後】



地方自治法に根拠を規定

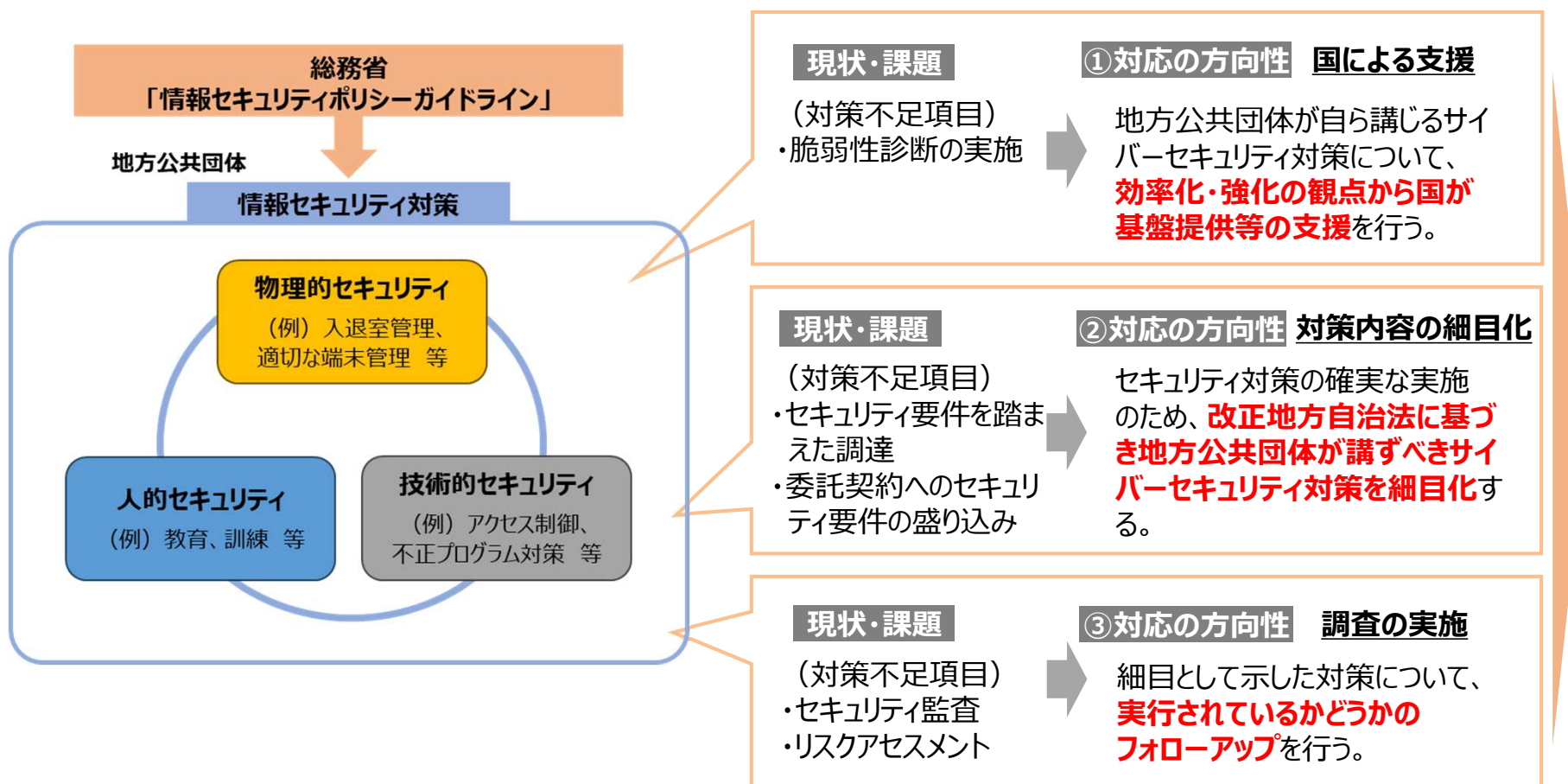
地方公共団体のサイバーセキュリティ対策に係る現状・課題、対応の方向性

- R6地方自治法の改正によって、サイバーセキュリティに係る必要な措置の実施義務と、サイバーセキュリティを確保するための方針の策定義務は措置済み。
- 現在、総務省は技術的助言としてガイドラインを示し、各地方公共団体においては、最低限のサイバーセキュリティ対策は実施済み。一方で、重要な事項でも実施率が低い項目がある状況。

【参考】地方自治法

第二百四十四条の五 普通地方公共団体は、その事務の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（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。

第二百四十四条の六 普通地方公共団体の議会及び長その他の執行機関は、それぞれその管理する情報システムの利用に当たつてのサイバーセキュリティを確保するための方針を定め、及びこれに基づき必要な措置を講じなければならない。



今後の予定

- ・ R8.春頃
検討会を開催し、支援策及び実効性確保の方策等についてとりまとめ
- ・ R8.夏頃
対策内容を示す省令・告示等の制定 (R9.4施行予定)

新たなサイバーセキュリティ戦略について【地方公共団体関係部分】

- 新たなサイバーセキュリティ戦略（令和7年12月23日閣議決定）において、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に向けた方向性を明記。

Ⅲ. 目的達成のための施策

2. 幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

（2）重要インフラ事業者・地方公共団体等におけるサイバーセキュリティ対策の強化

② 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

地方公共団体が、個人情報等の多数の機微な情報を保有し、国民生活や地方の経済活動に密接に関係する基礎的なサービスを提供していることに鑑み、国は、地方公共団体において適切にサイバーセキュリティ対策が実行されるよう、国と地方の役割分担を踏まえつつ必要な支援を実施する。

2024年に改正された地方自治法に基づき、地方公共団体は2026年度から、サイバーセキュリティを確保するための方針の策定が義務付けられることから、国は、当該方針に基づく対策の実効性を確保するため、新たに策定される重要インフラ統一基準も踏まえ、**地方公共団体のセキュリティ基盤の強化のための更なる取組**を進める。

具体的には、**自治体情報セキュリティクラウドの円滑な更新に向けた財政的な支援やデジタル人材の確保・育成に対する支援及び人員体制構築に必要な実践的サイバー防御演習（CYDER）等の研修プログラム、地方公共団体情報システム機構（J-LIS）が運営する自治体CSIRT協議会の活用推進を図るとともに、地方公共団体の情報システムに内在する脆弱性等を診断するシステムを構築し、地方公共団体の脆弱性対処能力の向上を図るなど、更なる安全性の確保に向けた取組を実施する。**また、**各地方公共団体が情報セキュリティ監査等を実施できるよう、適切な財政措置を講ずるとともに、サイバーセキュリティ対策の実施に必要な予算や人員の確保に向けた取組を強化する。**

さらに、全ての地方公共団体が確実に**サプライチェーン・リスク対策を含むサイバーセキュリティ対策を実施できるような新たな仕組みの構築を検討する。**

併せて、「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」に基づく対策が適切に実施されるよう、国は引き続き、地方公共団体の取組を支援する。

国民生活・国民の個人情報と密接に関わるマイナンバーについても、引き続き、国は利便性とセキュリティの調和を考慮して対策を強化し、安全・安心な利用を促進する。

令和8年度における地方公共団体のサイバーセキュリティ対策の強化について

- 令和8年度においては、改正地方自治法等を踏まえ、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に向けて、以下の施策を展開。

① 地方財政措置、国費支援の拡充

- ペネトレーションテストやリスクアセスメント、業務端末等のセキュリティ対策に要する経費について新たに地方交付税措置
- 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に必要なシステム（業務端末・システムへの不正アクセスを常時監視するシステム）の整備をデジタル活用推進事業債の対象事業に追加
- 自治体情報セキュリティクラウドの改修経費について国費支援（補助率1/2、地方負担分は普通交付税措置）

② セキュリティ基盤の強化

- 地方公共団体の外部からアクセス可能なIT資産の脆弱性を診断するために、すべての地方公共団体が利用可能な脆弱性診断システム（地方版ASMシステム）を国が一括で構築し、その効果を実証

③ セキュリティ人材の確保・育成

- 自治大学校においてサイバーセキュリティ人材の育成に関する特別研修を新設
- J-LISが開催している情報セキュリティ対策に関する各種研修について受講を推奨
- 都道府県がセキュリティ人材を含む外部デジタル人材を確保・プールし、市町村を支援する事業を推進

地方公共団体のサイバーセキュリティ対策に関する地方交付税措置の拡充について

- 改正地方自治法を踏まえた地方公共団体のサイバーセキュリティ対策の強化に要する経費について、令和8年度より地方交付税措置を拡充し、約0.1兆円規模を確保。

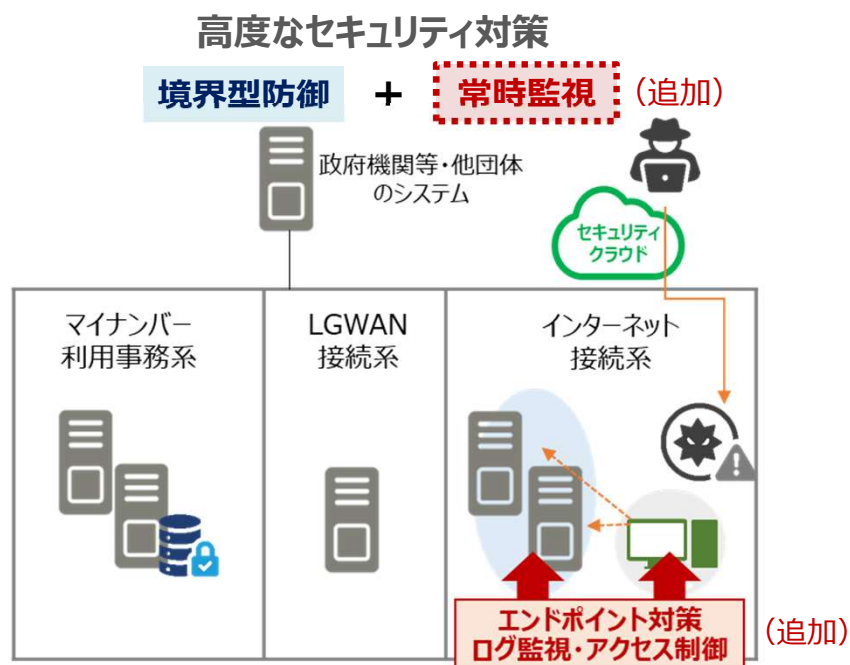
	経費内容	概要
既存	セキュリティモデルの運用 (いわゆる「三層」の対策)	地方公共団体におけるセキュリティモデルの運用に要する経費
	自治体情報セキュリティクラウドの運用	都道府県単位で運用している自治体情報セキュリティクラウドに要する経費
	セキュリティ機器等（FW等）の活用	地方公共団体が活用するセキュリティ機器等に要する経費
	情報セキュリティ監査の実施	情報セキュリティ監査（外部監査）の実施等に要する経費
	情報セキュリティポリシーの改定等	地方公共団体の情報セキュリティポリシーの改定等に要する経費
	セキュリティ対策の研修・訓練	地方公共団体が実施するセキュリティ対策の研修・訓練に要する経費
新規	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に対して疑似的な攻撃を実施することによって、当該システムへの侵入可否を検証するペネトレーションテストの実施等に要する経費
	リスクアセスメントの実施	情報システムにとって脅威となる事象が発生する可能性の高さや負の影響についての分類、リスク基準の決定及び当該リスクの回避等の方法について検討するリスクアセスメントの実施に要する経費
	業務端末等のセキュリティ対策	地方公共団体が保有するPCやモバイル端末等（エンドポイント）におけるウイルスやマルウェア等の検知、マルウェアに感染したエンドポイントの隔離等の各脅威への対応の実施に要する経費

地方公共団体のサイバーセキュリティ対策に関するデジタル活用推進事業債の拡充について

- 地方公共団体のサイバーセキュリティ対策の強化に必要なシステムの整備について、令和８年度より、新たにデジタル活用推進事業債（デジタル債）の対象に追加。

拡充内容

- 担い手不足が急速に深刻化するおそれがある中、デジタル技術を活用した行政運営の効率化・地域の課題解決等に向けた取組をしていくため、令和７年度にデジタル活用推進事業債を創設（地方財政法第５条の特例）。
- 昨今の複雑化・巧妙化するサイバー攻撃により、地方公共団体が保有するシステムに深刻かつ致命的な被害を生じさせるリスクが一層高まっており、**従来の境界型防御に加えて、より高度なセキュリティ対策を実施する必要**。
- そのため、各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に必要なシステム（業務端末・システムへの不正アクセスを常時監視するシステム）の整備を**対象事業に追加**。



(参考) デジタル活用推進事業債の概要

【事業期間】 令和７年度～令和１１年度（５年間）

【対象事業】 ・ 行政運営の効率化・住民の利便性向上を図る自治体ＤＸ
・ 地域の課題解決を図る地域社会ＤＸ
の推進のためのシステム・情報通信機器の整備

【事業費】 令和８年度： １，５００億円

元利償還金の５０％を
地方交付税措置

デジタル活用推進事業債（充当率
事業費

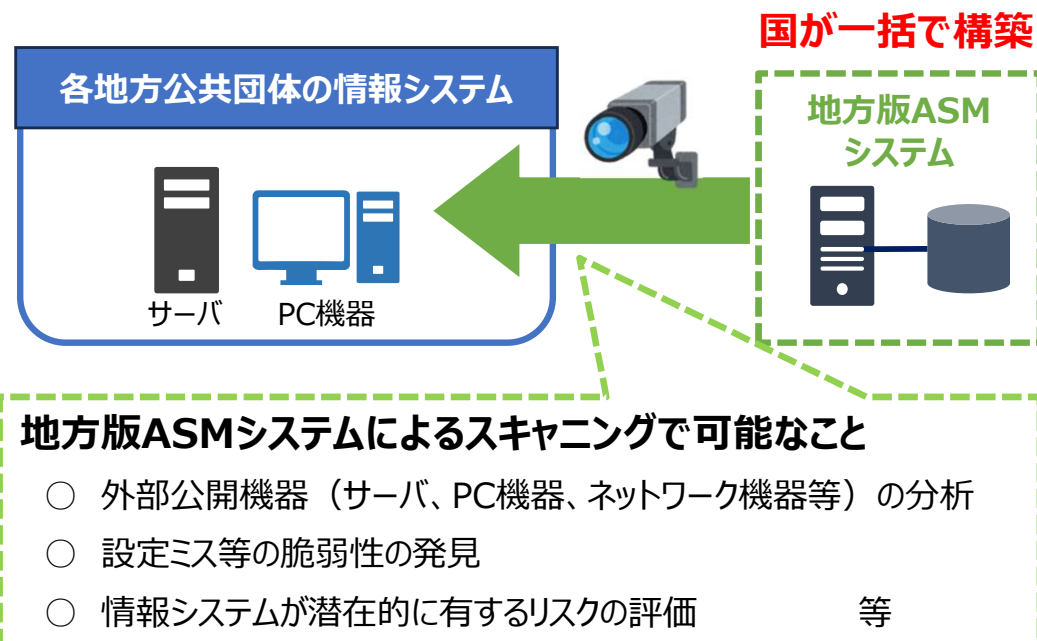
- サイバー攻撃の対象が、外部からアクセス可能なIT資産に変化していることを踏まえ、**すべての地方公共団体が利用可能な脆弱性診断システム**（地方版ASMシステム）を**令和8年度に構築**し、その**効果を実証**。

事業イメージ

- ◆ 地方版ASMシステムを用いて、**各地方公共団体の情報システムの脆弱性を評価**することで、攻撃者目線でのリスク評価・是正管理を効率的・効果的に推進。
- ◆ **国が一括で構築**することで、各団体のシステムに内在する各種の**脅威情報を集約**することが可能となり、これらの情報をもとに、各地方公共団体が潜在的に有する**リスク影響を横断的に把握**し、サイバーセキュリティ対策の強化に活用。

地方公共団体の情報システムをスキャン

集約した情報分析及び事例の横展開



スキャン結果の分析



リスク回避策の検討



- ✓ 地方版ASMシステムによるスキャン結果は、地方公共団体あてに共有され、それぞれの団体において、スキャン結果を分析し、**リスク回避策を検討**する。また、国・J-LISにおいて適切なフォローを行う。

自治大学校における「サイバーセキュリティ人材育成研修」の新設について

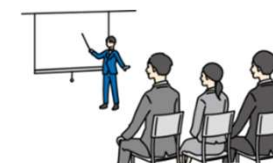
- 高度化・巧妙化するサイバー攻撃等への脅威から地方公共団体の情報システムを防御するため、**サイバーセキュリティ人材の育成が急務**であり、その**中核を担う職員を主な対象**に、**基本的な事項の講義**や**実践的な演習**等を実施。

日時

第1回：令和8年10月19日（月）～10月30日（金）

第2回：令和8年12月7日（月）～12月18日（金）

※講義内容は第1回・第2回いずれも同じ内容となります。ご都合のつくいずれか片方の日程でご参加ください。
※土日祝除く2週間で研修を実施いたします。



科目

①講義形式

【総論】 サイバーセキュリティ対策概論、昨今の法令改正、セキュリティ対策におけるPDCAサイクル 等
【各論】 情報セキュリティポリシーの運用、技術的セキュリティ対策、人的・物理的セキュリティ対策、
情報セキュリティ監査の重要性、インシデント発生時の対応 等

②演習形式

事例演習（インシデント発生時の対応）、グループ討議（地方公共団体における効率的・効果的な
防御）、研修成果の個別発表 等



対象

【対象】セキュリティ対策の企画立案を担う都道府県・市区町村の職員

【定員】第1回・第2回ともに約50名

※積極的な学習意欲と高い企画立案能力を有し、将来当該団体のサイバーセキュリティ対策の中核を担うことが期待できる者であれば、
年齢・役職等問わず歓迎します。

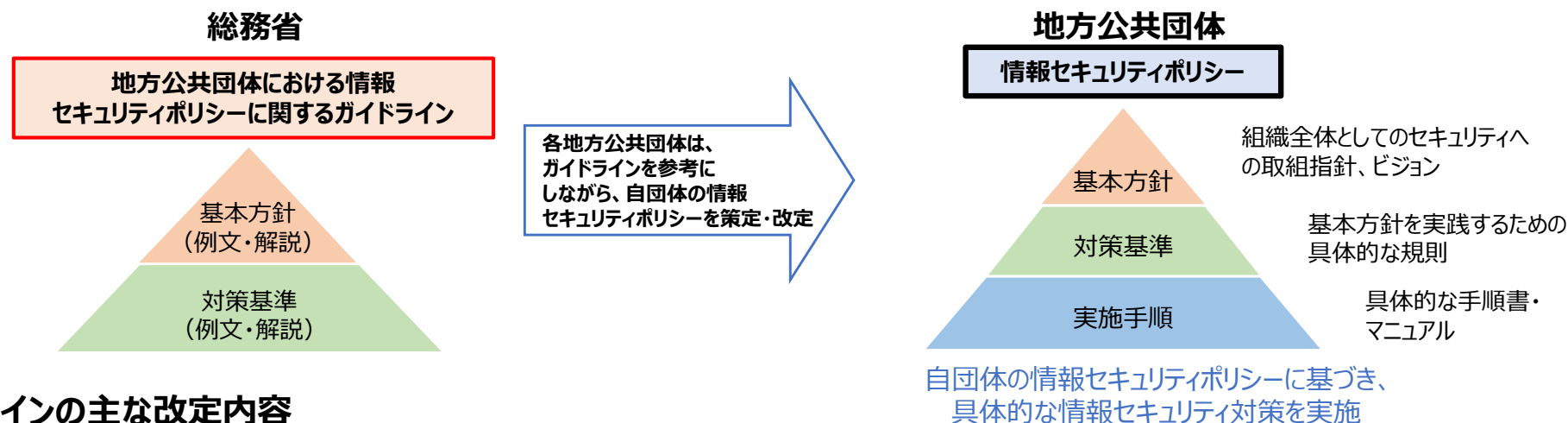
參考資料

「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」について

地方公共団体の業務システムの標準化・共通化やサイバー攻撃の高度化・巧妙化を踏まえ、新たな自治体情報セキュリティ対策の在り方について調査研究を行い、「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」に反映する。

1. 概要

各自治体のセキュリティー対策の指針として総務省が策定し助言。国における情報セキュリティ対策の動向やデジタル化の動向等を踏まえながら、有識者検討会での議論を経て、**年度ごとに改定を実施**。昨年6月の地方自治法改正等を踏まえ、最新のセキュリティ動向に合わせた技術的な知見に加え、自治体の業務に即した対策を検討することが重要。



2. ガイドラインの主な改定内容

改定時期	改定内容
平成30年9月	平成27年の日本年金機構における情報流出事案を受け、総務省から地方公共団体へ要請を行った「三層の対策」等の情報セキュリティの抜本的強化策の内容を反映
令和2年12月	「三層の対策」の効果や課題、新たな時代の要請を踏まえ、セキュリティの確保と効率性・利便性向上の両立の観点から、高度なセキュリティ対策を実施することを条件に、インターネット接続系に業務端末を配置するモデルを提示するなど新たな対応策を追加
令和4年3月	令和3年7月の「政府機関等の情報セキュリティ対策のための統一基準群」の改定や、地方公共団体のデジタル化の動向を踏まえた内容を反映
令和5年3月	標準準拠システム等のクラウドサービスの利用を想定し、クラウドサービスを利用する際の具体的な情報セキュリティ対策の内容を第4編（特則）に反映
令和6年10月	Web会議等の目的で、業務端末からインターネット経由で、特定のクラウドサービスを安全に利用するための対策や、政府統一基準の改定内容に沿った業務委託時における対策、地方公共団体が扱う個人情報の重要性を鑑みて、個人情報を自治体機密性3分類に分類することを追加
令和7年3月	令和6年6月の「国・地方ネットワークの将来像及び実現シナリオに関する検討会報告書」を踏まえたマイナンバー利用事務系に係る画面転送の方式やLGWAN接続系・マイナンバー利用事務系における無線LAN利用の要件等について新たに規定

令和 7 年 3 月のガイドライン改定のポイントについて



1. マイナンバー利用事務系に係る画面転送の方式について

- 「国・地方ネットワークの将来像及び実現シナリオに関する検討会報告書」（2024年 6 月）において「一人一台端末」の考え方が示されたことを受けて、ガイドラインの別紙として、現在のガイドラインに規定している対策や製品の動向を踏まえた方式を示す。
- 総論として、各団体の状況に応じ、利便性とコスト、リスク、セキュリティ等を総合的に勘案して、本別紙で規定している画面転送の方式の採用について判断することなどを規定。



2. 無線LAN利用の要件について

- 令和 6 年地方分権改革に関する提案を踏まえ、LGWAN接続系やマイナンバー利用事務系における無線LAN利用の要件について規定。
- マイナンバー利用事務系については、LGWAN接続系における対策に加え、番号法に基づく特定個人情報に関する安全管理措置の実施のための対策を追加で規定。



3. 機器等の調達について

- 「政府機関等のサイバーセキュリティ対策のための統一基準群」の改定に合わせ、インターネットプロトコルを使用する通信機能を持つ製品の調達について、「IoT製品に対するセキュリティ適合性評価制度構築方針」（令和 6 年 8 月）に基づき構築されたセキュリティ要件適合評価及びラベリング制度（JC-STAR）上の、適合ラベルの取得状況が参考になること等を規定。



4. インシデントの対応について

- 機器の脆弱性により不正アクセスがあった事案を踏まえ、再発防止のためのパッチ適用の判断、相談先の確保について規定。

1. 策定の主体

執行機関等ごとに策定。具体的には次のとおり。

- ・普通地方公共団体、特別区、一部事務組合及び広域連合の議会
- ・〃〃の長（地方公営企業の管理者を含む）
- ・〃〃の委員会及び委員
- ・地方独立行政法人

2. 策定を要する自治法上の方針等

- **すでに情報セキュリティポリシーを策定している場合**

既存の情報セキュリティポリシーの基本方針について、総務大臣指針を十分に踏まえて必要に応じて見直したものの策定をもって、自治法上の方針に位置付けることも可能。

- ## ○ 情報セキュリティポリシーを未策定の場合

改正法施行日（令和８年４月１日）までに情報セキュリティポリシー（少なくとも基本方針）を策定し、基本方針をもって自治法上の方針とする等の対応が必要。

- 自治法上の方針を策定又は変更した際は、公表が必要。

- 必要となる情報セキュリティ対策が概ね同様のものとなるなど別個の自治法上の方針を定めることが非効率となるような場合に、一つの方針を複数の執行機関で共同で策定することも可能。

【具体的な方策の例】

- ・ 委員会及び委員は、長の補助機関に委任（地方自治法180条の7）
- ・ その他の執行機関及び議会は、長との連名で共同策定 など

3. 自治法上の方針に規定すべき項目

○ 自治法上の方針に規定すべき項目については、次のとおり。

（総務大臣指針（案）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」も参照のこと）

1. 方針の目的
2. 定義
3. 対象とする脅威
4. 適用範囲
5. 職員等の順守義務
6. 組織体制の確立、情報資産の分類・管理、物理的・人的・技術的セキュリティ対策をはじめとした情報セキュリティ対策
7. 情報セキュリティ監査・自己点検の実施
8. 情報セキュリティポリシーの見直し
9. 情報セキュリティ対策基準・実施手順の策定（※）

※各執行機関等の情報システムの状況等にもよるため推奨事項とするが、対策基準・実施手順を策定する場合は、方針に規定すること。

4. 今後のスケジュール

- 改正法施行日（令和8年4月1日）に、各執行機関において自治法上の方針を策定。
大臣指針（案）は（案）から正式なものに。
- 自治法上の方針（案）の策定に向けた取組状況については、フォローアップ調査を実施

地方公共団体におけるサイバーセキュリティの実効性を確保するための取組の例

- 改正地方自治法により策定される「方針」等に基づき講じられる各地方公共団体のサイバーセキュリティの実効性を確保するための取組（例：情報セキュリティポリシーの改定、研修・訓練、監査、ペネトレーションテスト、リスクアセスメント、業務端末等のセキュリティ確保等）に対して、普通交付税措置。

P

地方自治法上の「方針」の策定

地方公共団体

方針の策定・公表、実施義務

総務大臣

指針を作成

「方針」を踏まえて改定

情報セキュリティポリシーの改定

※R8年度中に改定

情報セキュリティポリシー

組織全体としてのセキュリティへの取組指針、ビジョン
基本方針
基本方針を实践するための具体的な規則
対策基準
具体的な手順書・マニュアル
実施手順

D

情報システムのセキュリティ確保等



自治体情報セキュリティクラウド



マイナンバー
利用事務系

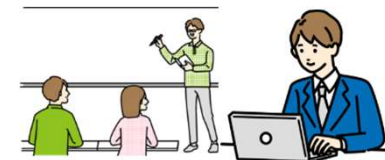


LGWAN
接続系



インターネット
接続系

セキュリティ対策研修・訓練



セキュリティモデルによる各団体の情報システムのセキュリティの確保や、職員等に対する研修や訓練の実施等により、サイバーセキュリティの確保の実効性を高める

A

リスクアセスメントの実施



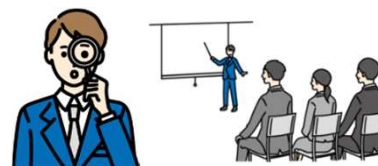
業務端末等のセキュリティ確保



情報セキュリティ監査やペネトレーションテストの結果を踏まえてリスクアセスメントを実施するとともに、地方公共団体においてサイバーセキュリティ対策に適切に対応できるように、物理的・人的・技術的セキュリティの充実を図る

C

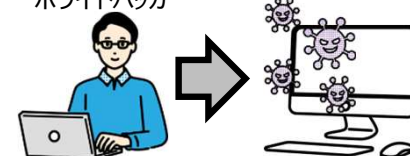
情報セキュリティ監査の実施



国の行政機関等における情報セキュリティ監査やペネトレーションテストの実施にない、地方公共団体においても、情報セキュリティ監査やペネトレーションテストを実施し、サイバーセキュリティ対策の不断の見直しを実施する

ペネトレーションテストの実施

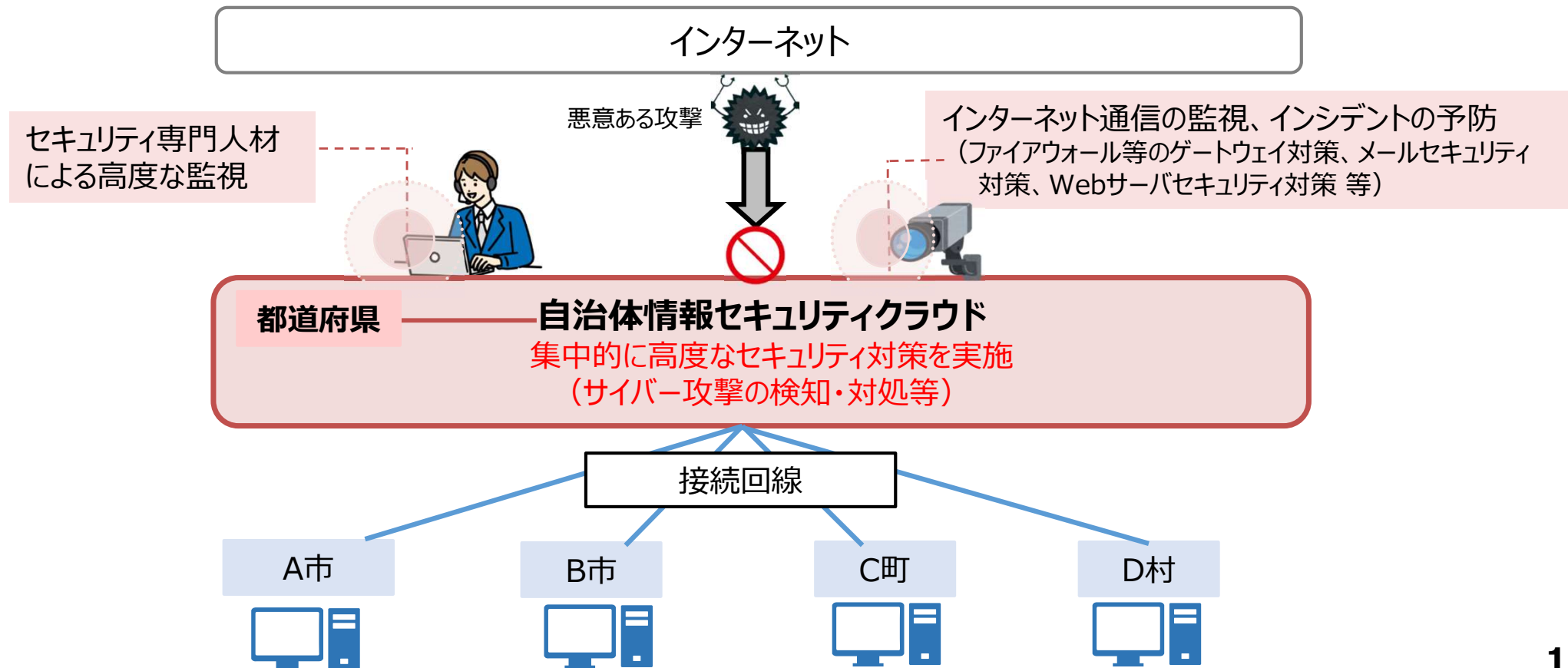
ホワイトハッカー



- インターネットからのサイバー攻撃の脅威等から地方公共団体の情報システムを防御するため、マイナンバー制度の開始に合わせ**都道府県が域内市町村のWebサーバ等をカバーする形で構築した自治体情報セキュリティクラウドを改修**。

事業イメージ

- ◆ 総務省が示す最低限満たすべき要件（必須要件）を満たすことを前提に、**自治体情報セキュリティクラウドの更新に要する経費**（設計、設定、テスト等に要する経費）について**都道府県に対して国庫補助を実施** ※概ね5年に1回
- ◆ 自治体情報セキュリティクラウドの活用により、これまで**99%以上のサイバー攻撃を防御**。国庫補助の実施により、**都道府県における円滑な更新を促進**する。 ※国庫補助率2分の1、地方負担分は普通交付税措置



自治体DX推進を担うデジタル人材育成のための段階的なレベルに合わせた研修を実施し、一般職員の底上げとリーダーとなる「中核人材」の育成を強化していく

オンライン研修

動画研修・ライブ研修の録画を学習管理システムに登録し、**自治体職員が受講しやすい環境を提供**
政策立案者を含む自治体DX推進の中核を担う職員向けの**充実したカリキュラムを提供**

動画研修

(事前に講義を収録して配信する研修)

- ・情報セキュリティの基礎セミナー
- ・業務に潜むリスクの管理・対策セミナー
- ・インシデント対応セミナー
- ・情報セキュリティ対策セミナー ・ゼロトラストセミナー
- ・CIO・CISO・情報セキュリティ責任者向けセミナー 他

※令和7年度研修より抜粋

ライブ研修

(Web会議システムを利用して双方向で実施する研修)

- ・情報セキュリティマネジメント基礎セミナー
- ・情報セキュリティマネジメントシステム企画解説セミナー
- ・情報セキュリティ監査セミナー 他

※令和7年度研修より抜粋

リモートラーニングによるデジタル人材育成のための基礎研修

全ての自治体職員に必要なデジタルリテラシー入門、デジタルリテラシー（ITパスポート相当）、**情報セキュリティ**、個人情報保護の4コースを実施

全地方公共団体無料 4コース
募集定員上限なし

情報化研修支援

職員研修用テキスト
の提供

セミナーの専門講師の
紹介

都道府県等が市町村を取りまとめて開催する集合研修への必要経費の助成等、支援

都道府県等における市町村支援のためのデジタル人材の確保に要する職員の人件費等に係る特別交付税措置【拡充】

- デジタル人材が逼迫する中で、特に小規模市町村において人材確保が進んでいないこと等を踏まえ、都道府県等が市町村支援のためのデジタル人材の確保に要する経費に係る特別交付税措置を引き続き措置。
- 対象経費は、**非常勤のアクセラレータの人件費、民間事業者への業務委託、アクセラレータ（常勤・非常勤）の募集経費** 等。
- 今後数年間で集中的にアクセラレータの確保に取り組むことができるよう、**令和7年度から令和9年度までの間、募集経費に係る対象経費の上限額を1団体あたり300万円に引き上げ**。
- また、令和8年度から、人件費相当額に係る対象経費の上限額を**1人あたり2,100万円に引き上げ**。

特別交付税措置の概要

対象団体	対象経費	措置額	対象経費の上限額	対象期間
都道府県 市町村	<ul style="list-style-type: none"> ○ <u>都道府県（連携中枢都市等含む）による市町村支援のためのデジタル人材の確保に要する非常勤のアクセラレータ等の人件費、民間事業者への委託費、募集経費</u> 等 ○ 上記の経費の一部につき市町村の負担金が生じる場合の当該負担金 	対象経費の合計額に 0.7 を乗じて得た額	人件費相当額： 2,100万円/人 募集経費： 100万円/団体 → 300万円/団体	R11年度まで 拡充期間は R9年度まで

市町村支援業務の想定事例

- ・ DX・情報化計画／デジタル人材確保・育成方針等の策定・見直し案の作成
- ・ 標準化・クラウド化に向けた助言・仕様調整
- ・ デジタル技術等も活用した業務見直し（BPR）、システム発注支援
- ・ データ利活用に関する助言
- ・ 人材育成（研修企画・講師等）
- ・ セキュリティ研修・監査支援 等

<都道府県による市町村支援（イメージ）>



※ 普通交付税措置の対象となる常勤のアクセラレータの人件費については、特別交付税措置対象外。

留意点

- 主な所掌事務が市町村支援業務でないデジタル人材に係る経費は、対象外。
- 民間事業者への委託の場合、デジタル人材の人件費以外（交通費、通信運搬費等）に要した経費は、対象外。ただし、事業運営経費等のうち募集経費に相当する経費は、措置の対象。