地方公共団体サイバーセキュリティ対策事業について
（補足説明資料）

総務省

令和８年６月30日
自治行政局住民制度課
サイバーセキュリティ対策室

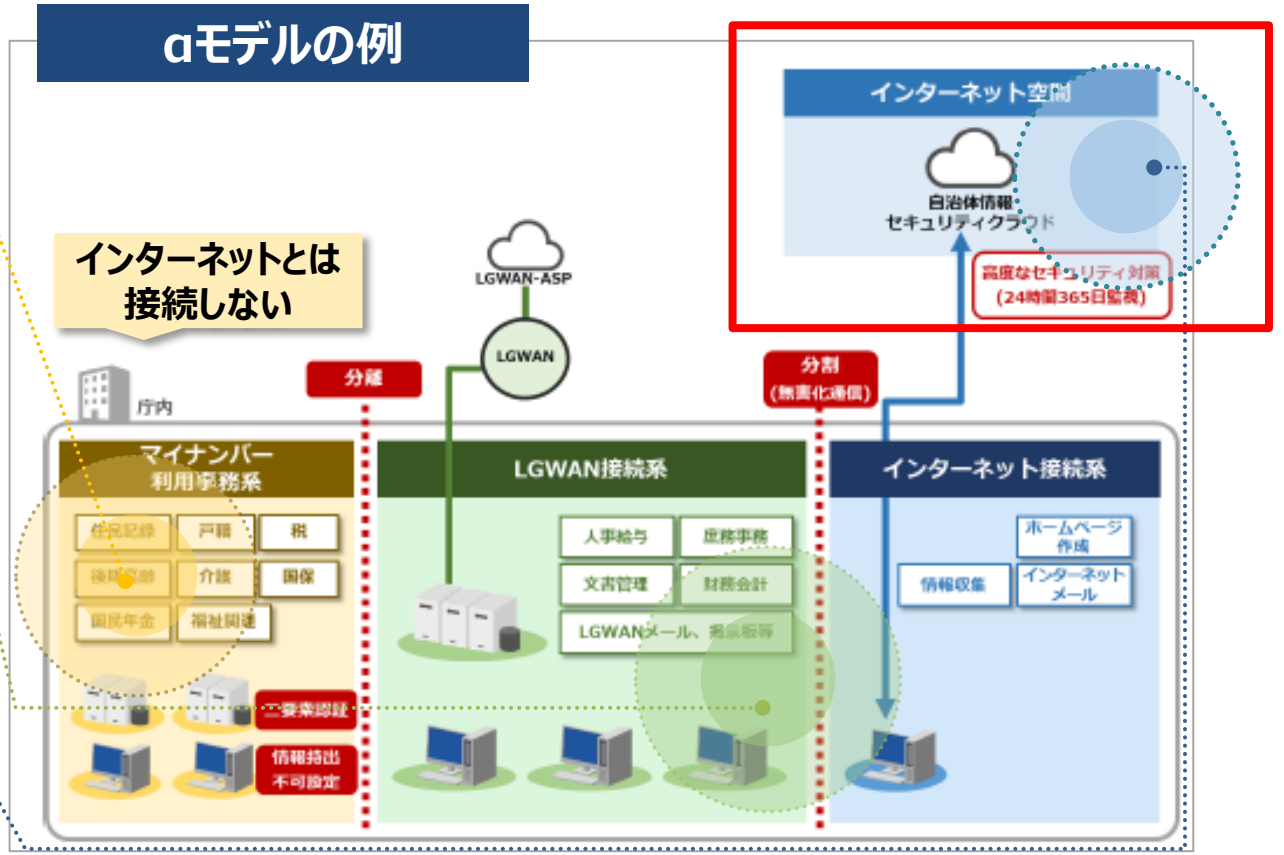
地方公共団体の情報システム全体像について

- 複雑・巧妙化しているサイバー攻撃の脅威により、地方公共団体の行政に重大な影響を与えるリスクが想定されるため、情報システムにおいては、機密性はもとより、可用性や完全性の確保にも十分配慮した、情報システム全体の強靭性の向上が求められる。
- 情報システム全体の強靭性の向上は、「三層対策」により実現。
- 平成29年７月、全ての都道府県において**インターネット接続系における高度な情報セキュリティ対策**として、都道府県及び市区町村のインターネットとの通信を集約した上で、**自治体情報セキュリティクラウドを構築・運用**。

1 マイナンバー利用事務系では、端末からの情報の持ち出し不可設定等を講じ、住民情報の流出を徹底して防止

2 LGWAN接続系とインターネット接続系を分割し、LGWAN環境のセキュリティを確保

3 都道府県と市区町村が協力して、自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を実施

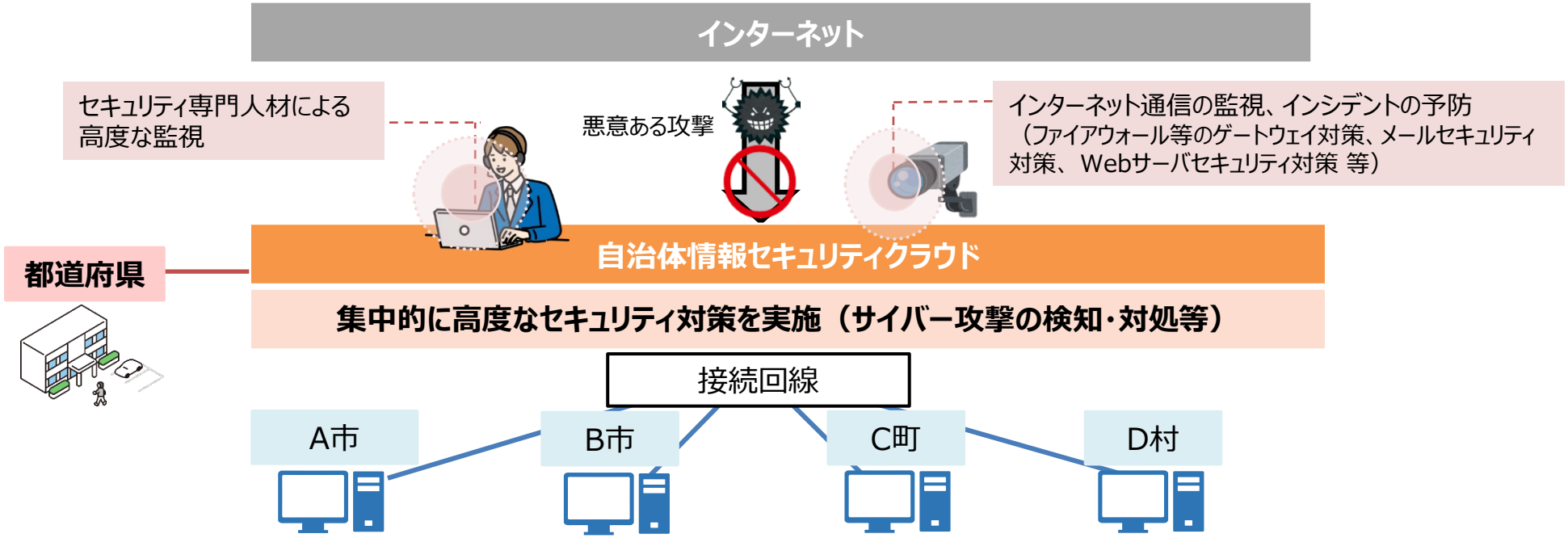


地方公共団体サイバーセキュリティ対策事業

○ 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、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の更新に要する経費について、国庫補助を行うことで、都道府県における円滑な更新を促進**（補助率２分の１）。

○ **概ね５年に１回、自治体情報セキュリティクラウドの更新を行う必要**があり、令和８年度及び令和９年度に全都道府県において更新完了予定。

○ 自治体情報セキュリティクラウドの活用により、これまで地方自治体のインターネット接続系の情報システムに係る**重大インシデントは発生していない。**



自治体情報セキュリティクラウドの効果

✓ **47都道府県すべてが**、現行の自治体情報セキュリティクラウドが**サイバー攻撃に対し効果があると回答。**

回答

- IPS(※1)、IDS (※2) 、WAF (※3)等のセキュリティ対策によって、**99%以上の日々のサイバー攻撃を遮断している**。なお、これらのセキュリティ対策を通過したものは、すぐにアラートが届き、危険度レベルに応じた迅速な対応が行われている。
- WAF (※3)で**1日あたりおおよそ500件の攻撃を検知・防御**できている。
- 毎月数百万件の攻撃通信やスパムメールが送付されているが、いずれも**セキュリティクラウドにより自治体のネットワークへの侵入は失敗**している。
- **スパムやフィッシングメールなど1日あたり1万件程度を検知・隔離**できている。
- **セキュリティクラウド更新時から現在に至るまでインシデントが発生していない**。
- メールにおいても、アンチウイルス機能やスパム対策機能により、**不審なメールの破棄、隔離等につき、相当件数の実績**がある。
- **悪意のある通信が自治体情報セキュリティクラウドにて防がれ**、庁内ネットワークに入らず防ぐことができた。
- SQLインジェクション(※4)等の**悪意ある攻撃を未然に防いでいることが確認できている**。また、**マルウェアを検知し、ブロックしている**実績がある。

A県の令和５年度実績

- インターネットからの不正なアクセスの遮断等： **ファイアウォール　15.1億セッション／月、IPS** (※1) **201万セッション／月**
- メール添付のマルウェアの削除： **6,988　件／月**
- スパムメール判定： **347万　件／月**
- 振る舞い検知機器による不審なファイル検知： **1,764　ファイル／月**
- URLフィルタによる不審なサイトへのアクセス遮断： **2,615万　セッション／月**

※1 IPS：ネットワーク上での不正アクセスや攻撃を検知し、防止するためのシステム。
※2 IDS：ネットワーク上での不正アクセスや攻撃を監視し、検知するためのシステム。
※3 WAF：Webアプリケーションの保護するためのセキュリティ製品。
※4 SQLインジェクション：不正なSQL（データベースを操作するためのプログラミング言語）文を利用し、データベースへアクセスし、情報の漏洩や改ざんを行う攻撃。

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。

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

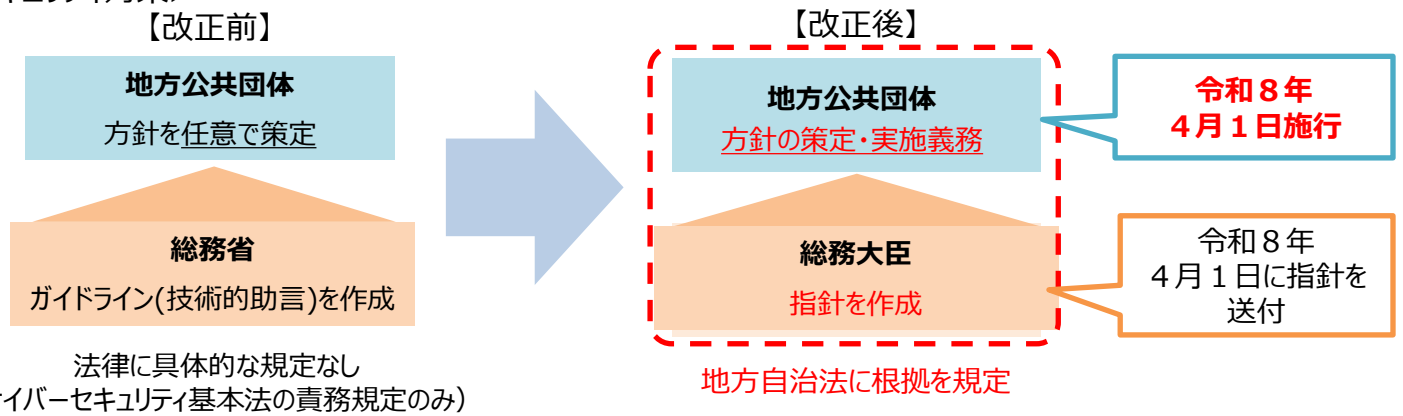
○　地方公共団体は、**事務の種類・内容に応じ**、**情報システムを有効に利用**するとともに、**他の地方公共団体又は国と協力**し、**その利用の最適化を図るよう努める**。

○　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＞



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**

○　NICTが開催している**実践的サイバー防御演習（CYDER）等の研修プログラム**について**受講を推奨**

○　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（特別交付税措置）

3. 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**

地方公共団体サイバーセキュリティ対策事業　活動目標・成果目標

○　本事業は、都道府県にて構築、運用を行っている自治体情報セキュリティクラウドについて、**令和８年度及び令和９年度に更新期限を迎える団体の円滑な更新を促進することを目的**とする。

○　自治体情報セキュリティクラウドの効果を測定するため、**サイバー攻撃に係る重大インシデント発生件数を０件とすることを短期アウトカムの成果目標**に設定。

○　本事業のみにとどまらず、地方自治体において物理的、人的、技術的セキュリティ対策等を総合的に適切に講じることで、**安全かつ持続的な行政サービスを提供できることを長期アウトカムの成果目標**に設定。

アクティビティ

自治体情報セキュリティクラウドの更新に要する経費に対する国庫補助（地方公共団体サイバーセキュリティ対策事業費補助金）の実施

アウトプット

（活動目標）

各都道府県における自治体情報セキュリティクラウドの更新に向けた支援を行うこと

（活動指標）

地方公共団体サイバーセキュリティ対策事業費補助金の交付団体数

＜目標値＞※累積値
26（R8）年度　30団体
27（R9）年度　47団体

短期アウトカム

（成果目標）

サイバー攻撃に係る重大インシデント発生件数を０件とすること

（成果指標）

各地方自治体から報告される重大インシデント報告件数

＜実績値＞
24（R6）年度　0件
25（R7）年度　0件

長期アウトカム

（成果目標）

地方自治体が、安全かつ持続的な行政サービスを提供できること

（成果指標）

地方自治体におけるサイバーセキュリティ対策の強化

（参考）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

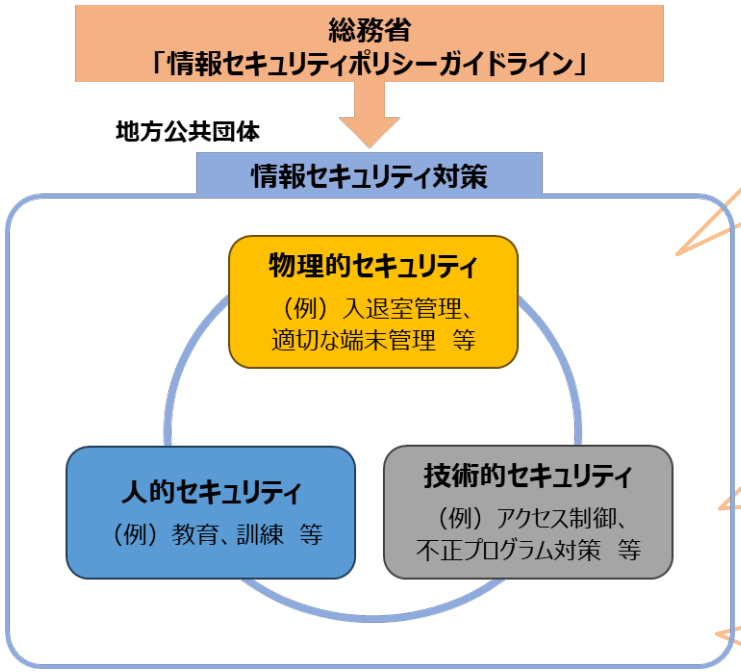
○ **R6地方自治法の改正**によって、**サイバーセキュリティに係る必要な措置の実施義務**と、**サイバーセキュリティを確保するための方針の策定義務**は措置済み。

○ 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

§244の５② 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**。

§244の６① 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。



現状・課題
（対策不足項目）
・脆弱性診断の実施

①対応の方向性　国による支援
地方公共団体が自ら講じるサイバーセキュリティ対策について、**効率化・強化の観点から国が基盤提供等の支援**を行う。

現状・課題
（対策不足項目）
・セキュリティ要件を踏まえた調達
・委託契約へのセキュリティ要件の盛り込み

②対応の方向性　対策内容の細目化
セキュリティ対策の確実な実施のため、**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**する。

現状・課題
（対策不足項目）
・セキュリティ監査
・リスクアセスメント

③対応の方向性　調査の実施
細目として示した対策について、**実行されているかどうかのフォローアップ**を行う。

・R8.4月
支援策及び実効性確保の方策等について検討会でとりまとめ

・R8.6月
対策内容を示す省令の制定・公布
(R9.7.1施行)

（参考）「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」報告書の概要

実効性確保に向けた３つの施策

① 団体単独では導入・運用が困難な**高度かつ専門的サービス**等、国等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、**積極的に支援**。

② 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について、細目化**。

③ 実施状況を**調査・評価**し、十分に**フォローアップ**する。

主な内容

【国等による支援】

- ✓ **重大インシデントレスポンス専門家チーム**の派遣制度化
- ✓ **サプライチェーン・リスク対策**も含めた相談を受け付ける**相談窓口の設置**
- ✓ **地方版脆弱性診断システム（ASM）の基盤整備**
- ✓ 自治大学校・J-LISにおける**教育訓練等の充実**
- ✓ サイバーセキュリティ対策に係る**地方財政措置の拡充**　　等

【都道府県による支援】

- ✓ 監査人等を含めた、サイバーセキュリティの**専門人材の確保・派遣等の人的な支援**

等

主な内容

- ✓ 地方自治法§244条の5②に規定する法律上の義務の解釈として自ずと導かれる**根幹かつ基本的な対策事項について、省令で規定**。

> §244条の５② 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**。

- ✓ 喫緊の課題である**サプライチェーン・リスク対策**についても、細目化と併せて**ガイドライン・通知等で可能な限り詳細な事項を示す**。

主な内容

- ✓ システム化による実施状況調査の効率化、地方公共団体の負担軽減。
- ✓ 実施状況の**フィードバック**を通じて、**セキュリティレベルの向上**につなげる。