参考資料

サプライチェーン・リスク対策等を通じた地方公共団体のサイバーセキュリティ対策の抜本的強化

○　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、人材・ノウハウ・基盤等の共有化・集団的対応を実施。



１．サイバーセキュリティ対策総合相談窓口の創設

サプライチェーン・リスク対策を含む多様なセキュリティ上の課題に対する、相談窓口として、総務省に**「サイバーセキュリティ対策総合相談窓口」を設置**する。

２．重大インシデントレスポンス専門家チーム派遣制度の創設

重大インシデント発生時に、国から地方公共団体等へセキュリティ専門家を派遣する仕組みを創設し、地方公共団体全体のインシデント対応力の強化を図る。

３．サイバーセキュリティ人材の育成

地方公共団体における専門職員の不足等を踏まえ、各団体で**中核となるサイバーセキュリティ人材を効果的、効率的に育成**する。

４．ゼロトラストアーキテクチャの考え方の共同実装に向けた検証

複数の地方公共団体において**ゼロトラストアーキテクチャ基盤を構築した上で、コスト低減効果、運用方法、セキュリティの有効性等について検証**を行う。

５．自治体情報セキュリティクラウドの更新

都道府県が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する。

令和９年度要求額　55.4億円（うち、「強く豊かな日本」投資枠　54.3億円）
（令和８年度予算額　81百万円、令和７年度補正予算額　40.3億円）

地方版アタックサーフェスマネジメント（ASM）システムの構築・実証事業

R7補正：4.5億円

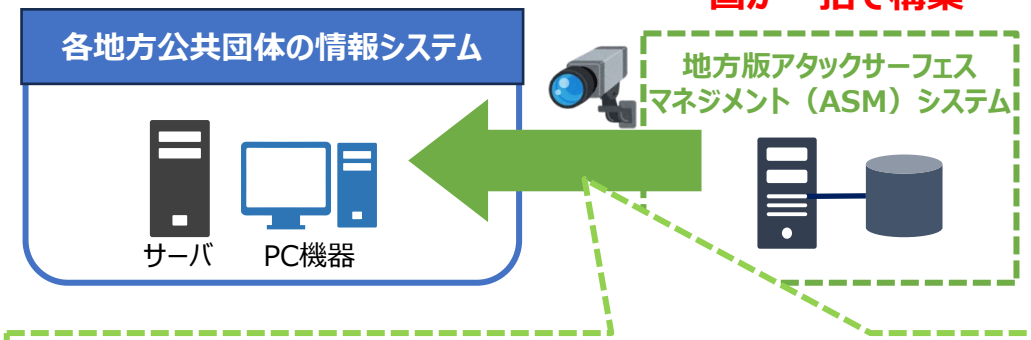
○ サイバー攻撃の対象が、外部からアクセス可能なIT資産に変化していることを踏まえ、**すべての地方公共団体が利用可能な地方版アタックサーフェスマネジメント（ASM）システム**を**令和８年度に構築**し、その**効果を実証。令和９年度から本格運用開始。**

事業イメージ

○ 地方版アタックサーフェスマネジメント（ASM）システムを用いて、**各地方公共団体のIT資産の脆弱性を攻撃者目線で評価**することで、リスク対策を効率的・効果的に推進。

○ **国が一括で構築**することで、各団体のIT資産の脆弱性**情報を収集**可能となり、これらの情報をもとに、各地方公共団体の**リスクを把握**し、国及び都道府県がサイバーセキュリティ対策の支援のための情報として活用。

地方公共団体の情報システムをスキャニング　→　**集約した情報の分析及び事例の横展開**



スキャン結果の分析



リスク対策の検討



地方版アタックサーフェスマネジメント（ASM）システムで対応可能なこと

- ○ 未把握のIT資産（サーバ、PC機器、ネットワーク機器等）の発見
- ○ 脆弱性や設定ミス等の検出
- ○ IT資産が有する脆弱性の評価　　等

- 地方版ASMシステムによる収集結果は、地方公共団体あてに共有され、それぞれの団体において、収集結果を分析し、リスク対策を検討する。また、自治体の対応について、適切なフォローを行う。

地方公共団体サイバーセキュリティ対策事業

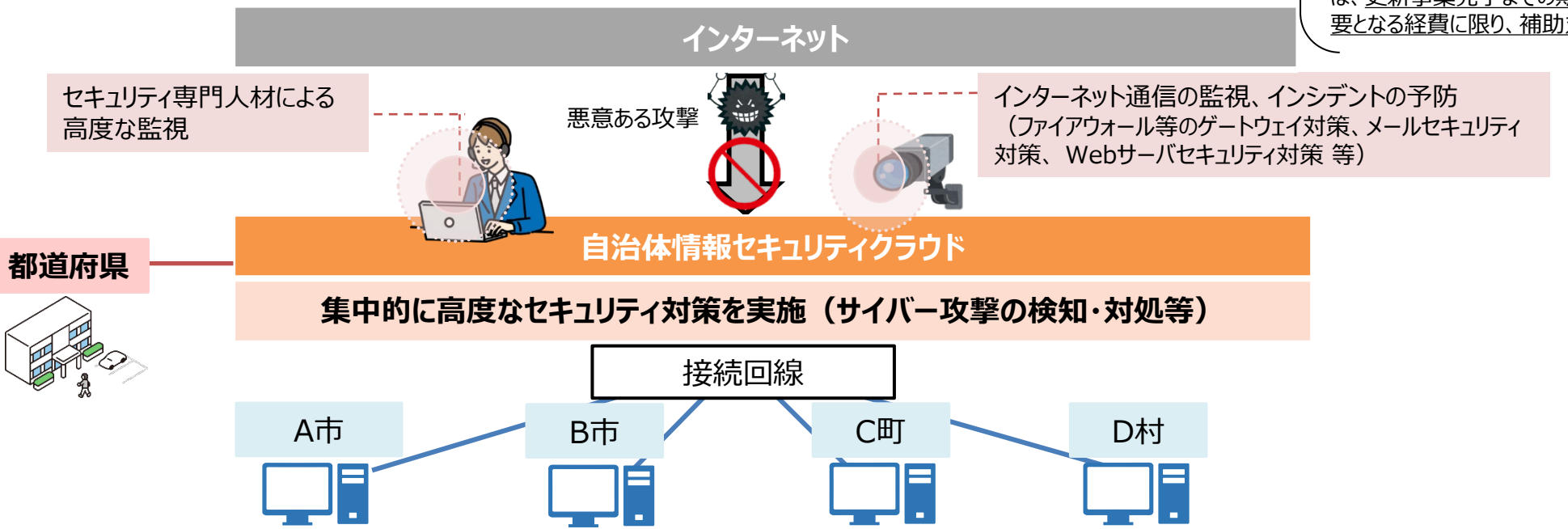
R7補正：29.4億円

○ 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。**

施策概要

- ✓ 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**
- ✓ 補助対象経費（１）作業に要する経費（設計、環境構築、テスト、更新の一連の工程に係る経費。）
  （２） ハードウェア購入に要する経費（端末購入にかかる経費を除く。）
  （３） ソフトウェア購入に要する経費（ライセンス費を含む。）

※（２）及び（３）については、第２期においてオンプレ型を採用していた団体が、第３期においても引き続きオンプレ型を採用せざるを得ない場合に限り、補助対象。
※ソフトウェアのライセンス費については、更新事業完了までの期間に必要となる経費に限り、補助対象。



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

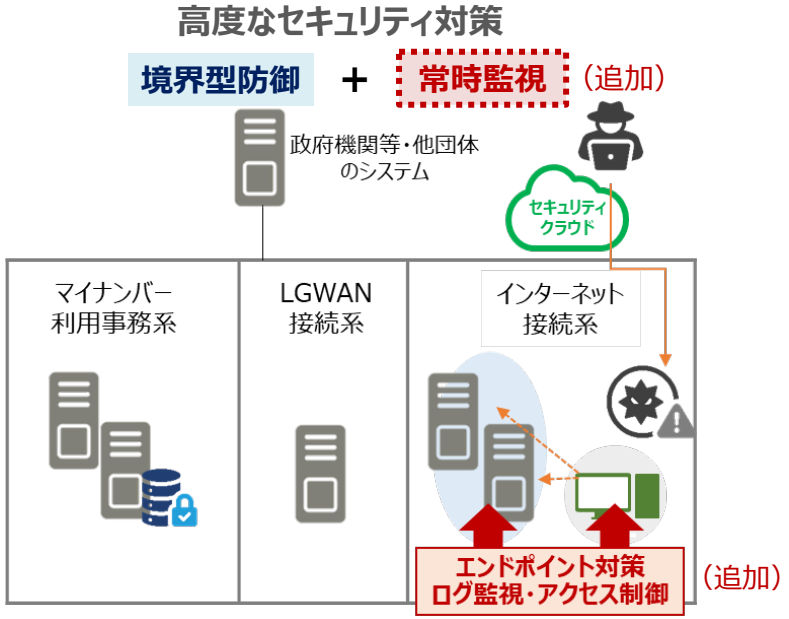
○ 地方公共団体の**サイバーセキュリティ対策の確保のために必要な情報システムの導入・改修**について、令和８年度より、新たに**デジタル活用推進事業債**（デジタル債）**の対象に追加**。

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**。

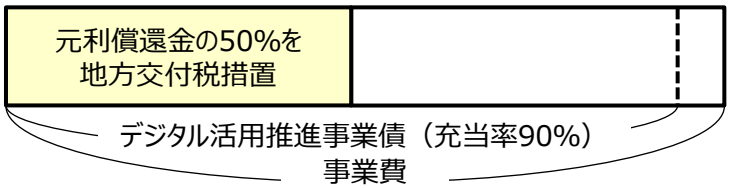


（参考）デジタル活用推進事業債の概要

【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



令和８年４月１日付け 自治行政局住民制度課サイバーセキュリティ対策室長通知について

「地方公共団体におけるサイバーセキュリティ対策の実効性の確保にあたっての留意事項について」（令和８年総行サ第16号）

○ 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）の対象となる「**サイバーセキュリティの確保のために必要な情報システムの導入・改修**」の具体的な**事業内容を記載**。

①エンドポイント対策のためのソフトウェア・機器の導入

- 従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）を示す異常な挙動の端末を監視・検出・特定するもの。
- 異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施するもの。
- インシデント発生要因の詳細な調査を実施するもの。
- ネットワーク、メール、クラウド等の各情報を収集し、AI等を用いた高度な検知・分析とインシデントへの対応を支援するもの。

②アクセス制御のためのソフトウェア・機器の導入、業務システムの改修

- 不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認証・認可に基づき、アクセスの許可または拒否を行うもの。
- 情報資産の機密性レベルに応じて業務システム単位でのアクセス制御を行うもの。

③ログ監視のためのソフトウェア・機器の導入、業務システムの改修

- インシデントの兆候検知やインシデント発生後の調査に使用するため、業務システムのログの収集、分析、保管を実施するもの。

総務省自治大学校 特別研修「サイバーセキュリティ人材育成研修」の実施

○　高度化・巧妙化するサイバー攻撃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、**制度面・技術面の講義**や**実践的な演習**を実施。

○　R6改正地方自治法に基づく地方公共団体が講ずべきサイバーセキュリティ対策、**サプライチェーン・リスク対策**、**高性能AIへの対応を盛り込んだ研修**を実施。

研修日程

第１回：　令和８年10月19日（月）～ 10月23日（金）
第２回：　令和８年10月26日（月）～ 10月30日（金）
第３回：　令和８年12月　7日（月）～ 12月11日（金）
第４回：　令和８年12月14日（月）～ 12月18日（金）

研修計画

①講義形式

サイバーセキュリティ対策概論　近年のサイバー脅威　昨今の法令改正
セキュリティマネジメント **サプライチェーン・リスク対策**　**高性能AIへの対応**　等

②演習形式

模擬環境を用いたセキュリティ**インシデント対応**
演習内容を踏まえた**グループ討議**　研修成果の個別発表



研修対象

セキュリティ対策を担う都道府県・市区町村の職員
（１回あたり20名程度）