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

総務省

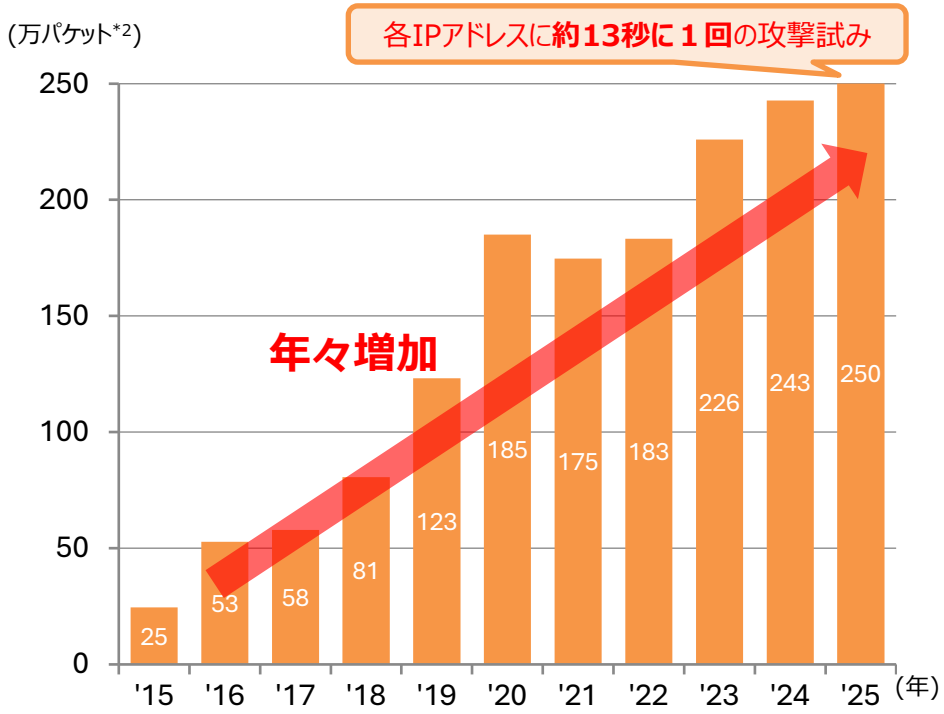
自治行政局住民制度課
サイバーセキュリティ対策室

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年米コロニア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）

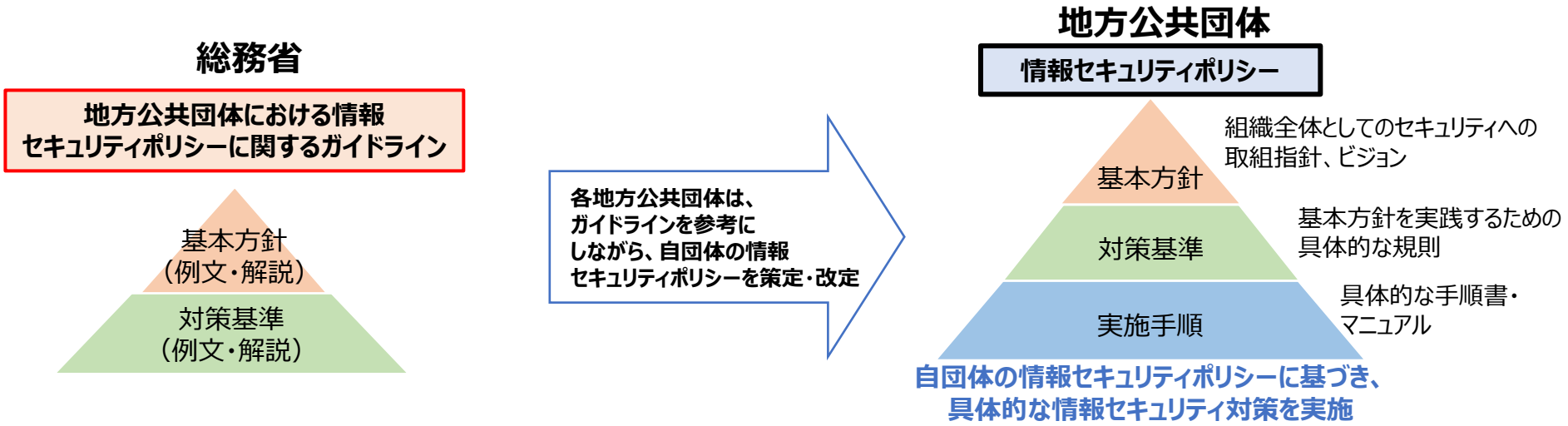
（例：2021~24年JAXAへの侵害、2023年NISCのメール窃取）

（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

1．概要

各自治体のセキュリティ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**。



※改正地方自治法に規定されている総務大臣の指針や各地方公共団体の方針は、上図の基本方針に相当。

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、地方公共団体が取り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８年３月	地方自治法の一部を改正する法律(令和６年法律第65号)により総務大臣が指針を示すこととされガイドラインとの重複箇所を一部見直すとともに、リユースを踏まえ機器の廃棄・データ消去に関する規定の見直しやUSBメモリ等の利用に関するリスクへの対処を反映

地方公共団体の情報システムにおけるサイバーセキュリティ対策の概要

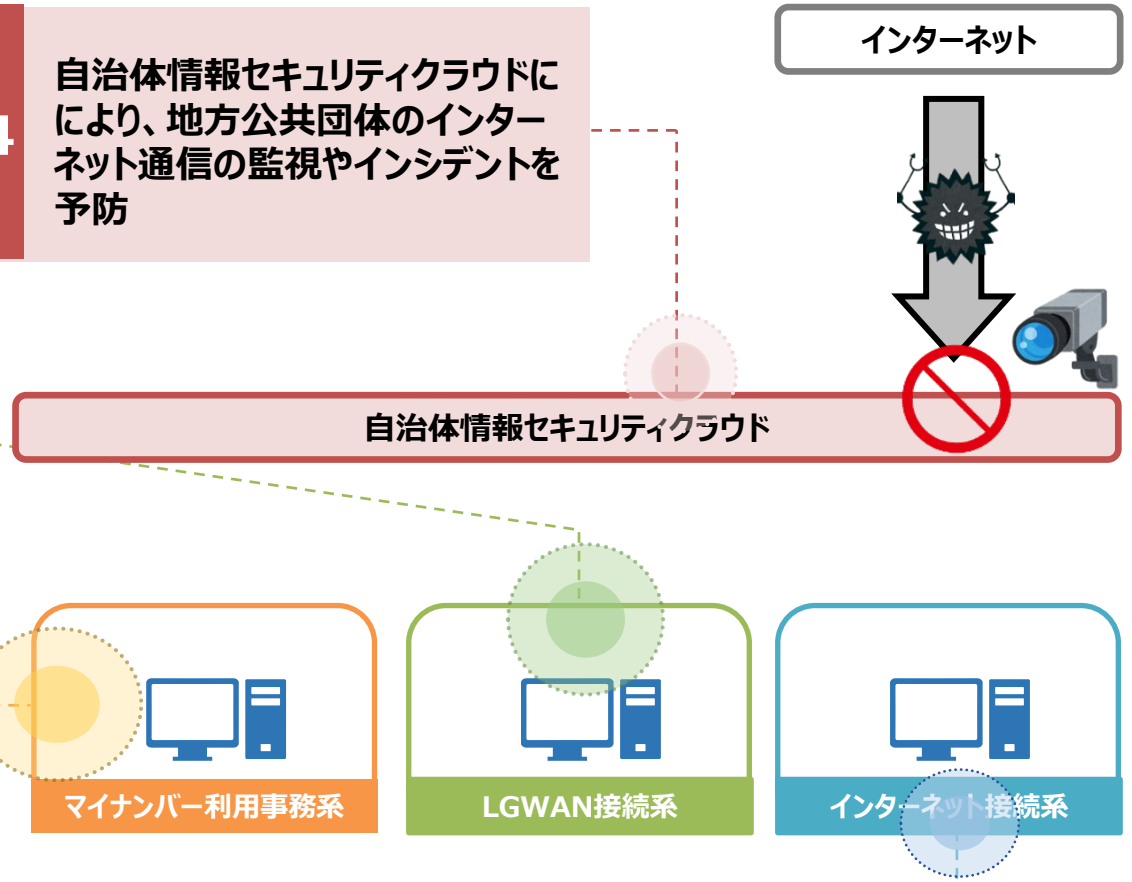
- 複雑・巧妙化しているサイバー攻撃の脅威により、地方公共団体の行政に重大な影響を与えるリスクが想定されるため、情報システムにおいては、機密性はもとより、可用性や完全性の確保にも十分配慮した、情報システム全体の強靭性の向上が求められる。
- 地方公共団体の情報システムをマイナンバー利用事務系、LGWAN接続系、インターネット接続系の３つに分けて防御を実施するとともに、都道府県が自治体情報セキュリティクラウドを構築して、インターネットからのサイバー攻撃の脅威等から効率的に防御。

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

4 自治体情報セキュリティクラウドにより、地方公共団体のインターネット通信の監視やインシデントを予防



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

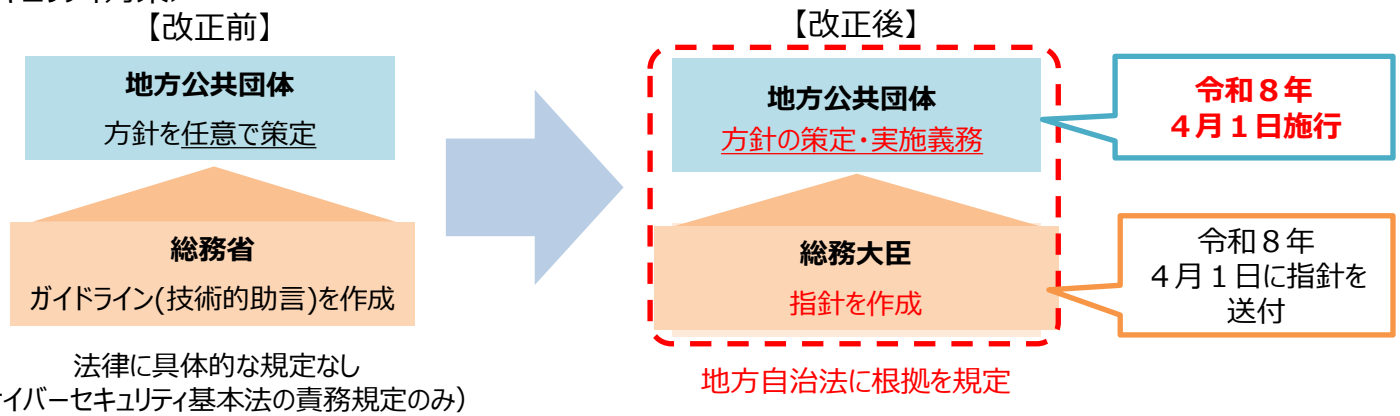
○　地方公共団体は、**事務の種類・内容に応じ**、**情報システムを有効に利用**するとともに、**他の地方公共団体又は国と協力**し、**その利用の最適化を図るよう努める**。

○　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＞



参照条文

サイバーセキュリティ基本法（平成26年法律第104号）

（地方公共団体の責務）

第５条　地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。

（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）

第14条　国は、重要社会基盤事業者等*におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。

＊電力、金融、通信等の重要な社会インフラ事業者。地方公共団体も含む。

地方自治法（昭和22年法律第67号）　**※令和６年地方自治法改正により、「情報システム」の章が追加。**

（情報システムの利用に係る基本原則）

第244条の5　（略）

２　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。

（サイバーセキュリティを確保するための方針等）

第244条の６　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。

２　（略）

３　総務大臣は、普通地方公共団体に対し、第一項の方針（政令で定める執行機関が定めるものを除く。）の策定又は変更について、指針を示すとともに、必要な助言を行うものとする。

４　（略）

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

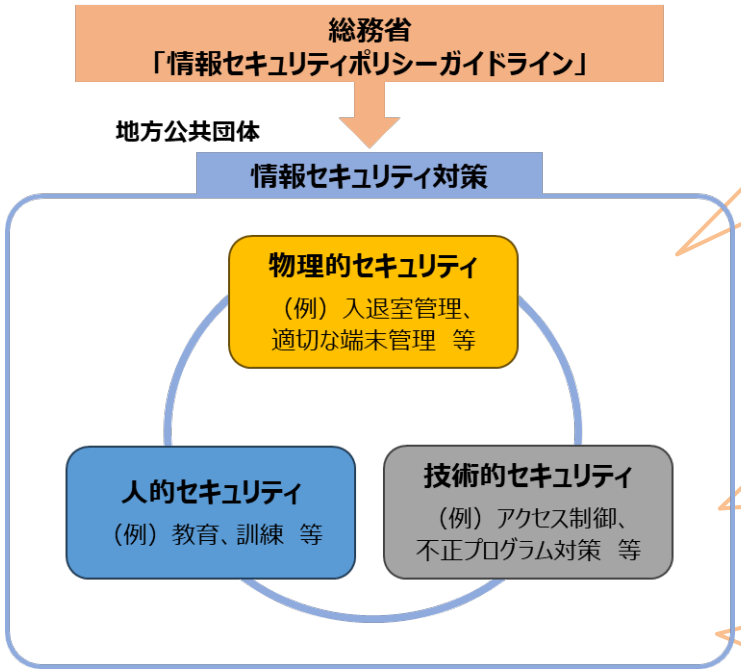
○ **R6地方自治法の改正**によって、**サイバーセキュリティに係る必要な措置の実施義務**と、**サイバーセキュリティを確保するための方針の策定義務**は措置済み。

○ 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.夏頃
対策内容を示す省令の制定
(R9.夏頃施行予定)

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WG報告書（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。

地方公共団体が調達するITシステム・機器等のサプライチェーン・リスク対策について

○ 地方公共団体に示す必要な措置の細目化に際しては、**サプライチェーン・リスク対策についても義務付け**を行う（①）。

○ また、総務省は細目化による義務付けだけではなく、**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支援する**（②）とともに、**履行状況についてのチェック**（③）を行うなど、関係省庁と連携して、**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**する。

【包括的なメカニズム案】

①	・ 改正地方自治法に基づき地方公共団体が講ずべき措置について、**省令により法令上細目化** → **R8年6月制定**、**R9年夏頃施行予定**
②	・ 総務省が**詳細な調達基準**や、調達実務に役立つ**チェックリスト等を提示**（ISMAP、JC-STAR等の活用） ・ 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**を**総務省に設置** ・ 地方公共団体は、事業者に対し**外部主体に該当しない旨の宣誓を求める**
③	・ **調達した製品に関する国による調査の実施**　等

8

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

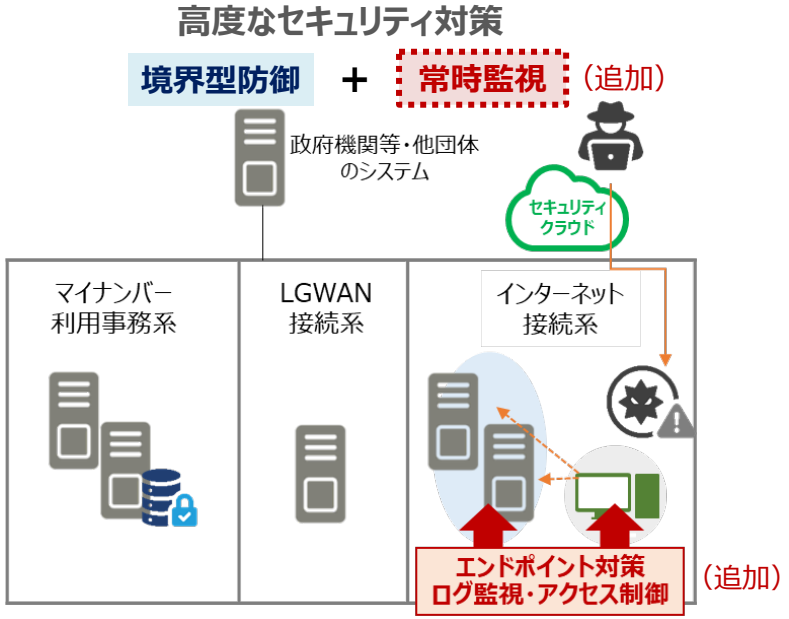
○ 地方公共団体の**サイバーセキュリティ対策の確保のために必要な情報システムの導入・改修**について、令和８年度より、新たに**デジタル活用推進事業債**（デジタル債）**の対象に追加**。

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**。

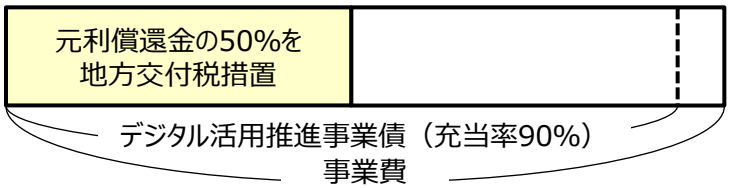


（参考）デジタル活用推進事業債の概要

【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。

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

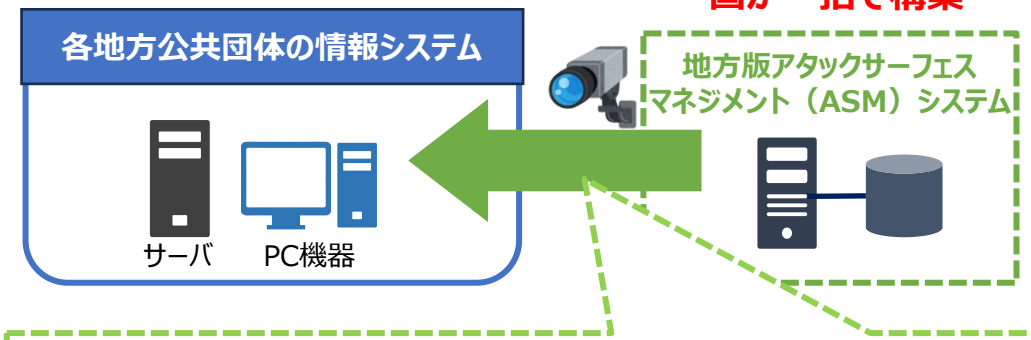
○ サイバー攻撃の対象が、外部からアクセス可能なIT資産に変化していることを踏まえ、**すべての地方公共団体が利用可能な地方版アタックサーフェスマネジメント（ASM）システム**を**令和８年度に構築**し、その**効果を実証**。

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。

地方版ASMシステムの構築・実証事業のスケジュール

○　令和９年度の地方版ASMシステムの本格運用に向けて、令和８年度において、以下のスケジュールのとおり、構築・実証事業を実施。
○　現在、全国の地方公共団体から実証事業の参加団体を公募中。

スケジュール

R8.4月～6月	実証団体の公募・選定	全国の地方公共団体から実証事業の参加団体を公募。
7月～10月	システム構築	地方版ASMシステムを構築。
10月～R9.1月	実証・とりまとめ	実証事業を実施し、運用面や体制面の課題を整理。
R9.1月～3月	運用手順検討	本格運用に向けて、運用ルールや運用手順書を作成。
R9年度中	運用開始	本格運用開始。地方公共団体情報システム機構（J-LIS）にて運用。

※　上記スケジュールは変更が生じる可能性があります。
※　構築・実証事業の具体的な内容は、決定次第、改めて周知いたします。

地方公共団体サイバーセキュリティ対策事業

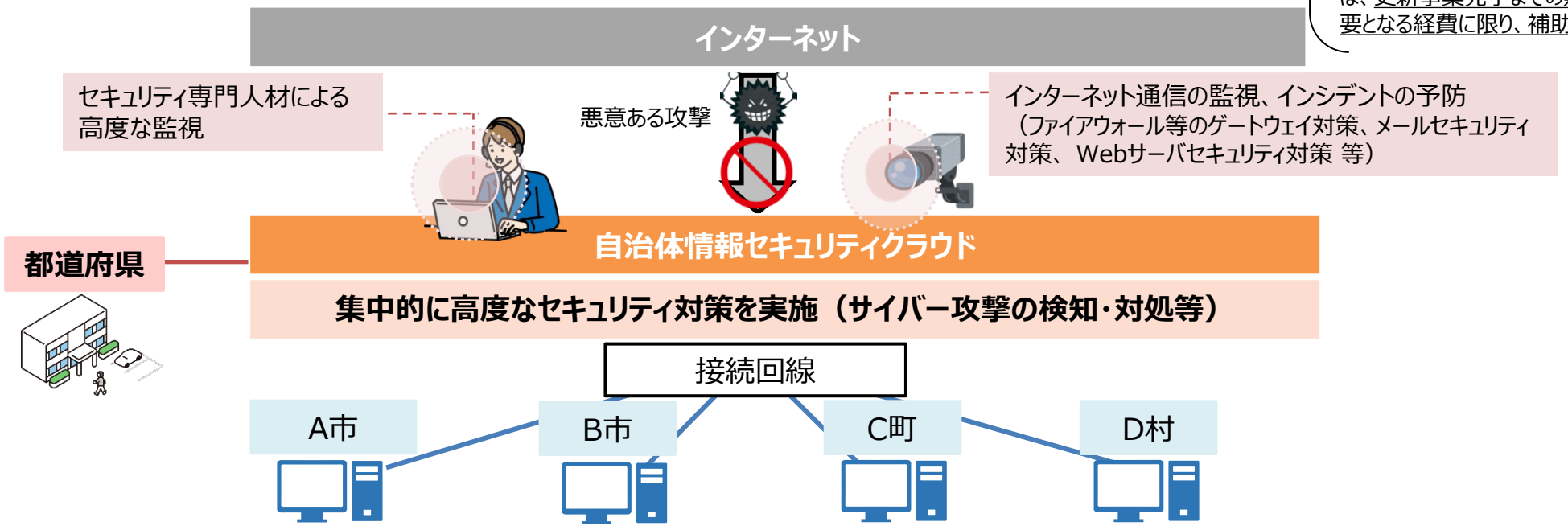
R7補正：29.4億円

○ 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。



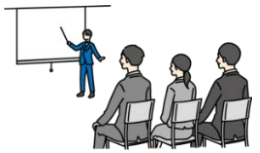
自治大学校における「サイバーセキュリティ人材育成研修」の新設について

○　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。

総務省サイバーセキュリティ統括官室作成資料

実践的サイバー防御演習「CYDER」（CYber Defense Exercise with Recurrence）

○ 総務省は、2017年度から、情報通信研究機構（NICT）において、**国の機関、指定法人、独立行政法人、地方公共団体**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」**（サイダー）を実施

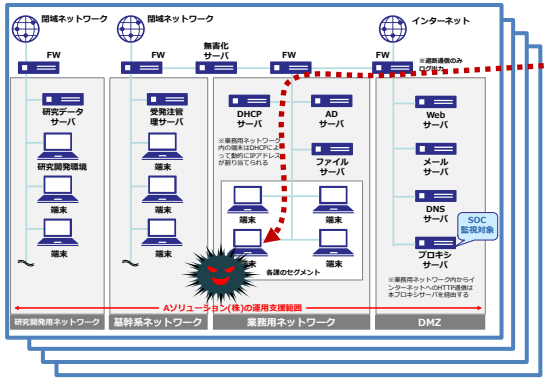
○ 受講者は、**チーム単位で演習に参加**。**組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って、**外部のセキュリティ事業者の支援を受けることを前提としてサイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験**

○ **全都道府県**において、年間**100回**の計**3,000名規模**で実施(集合コース)。2025年度は106回実施し、計**3,989名**が受講

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうるサイバー攻撃事例を再現した**最新の演習シナリオ**を用意。

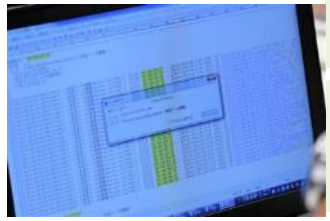
北陸StarBED技術センターの大規模高性能サーバ群を活用



擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**



専門指導員による補助

チーム内での議論を通じた相互理解

本番同様のデータを使用した演習

インシデント（事案）対処能力の向上

2025年度の実施状況

コース名		実施方法	レベル	受講想定者（習得内容）	受講想定組織	実施地	実施回数	実施期間
CYDER	A	集合形式	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	47都道府県	78回	7月～1月
	B-1		中級	システム管理者・運用者 (主体的な事案対応・ｾｷｭﾘﾃｨ管理)	地方公共団体	全国８地域	10回	10月～11月
	B-2				地方公共団体以外	東京・大阪・名古屋	13回	1月
	C		準上級	セキュリティ専門担当者 (初動分析を含む主体的な事案対応)	全組織共通	東京・大阪	5回	11月～1月
プレCYDER		オンライン形式	-	全ての情報システム担当者 (最低限必要となる知識の習得と最新化)	全組織共通	（受講者職場等）	-	1期：5月～8月 2期：9月～11月 3期：11月～1月