国・地方デジタル共通基盤推進連絡協議会ワーキングチームによる
関係府省庁ヒアリング

⑤地方版アタックサーフェスマネジメント（ＡＳＭ）システム　説明資料

総務省

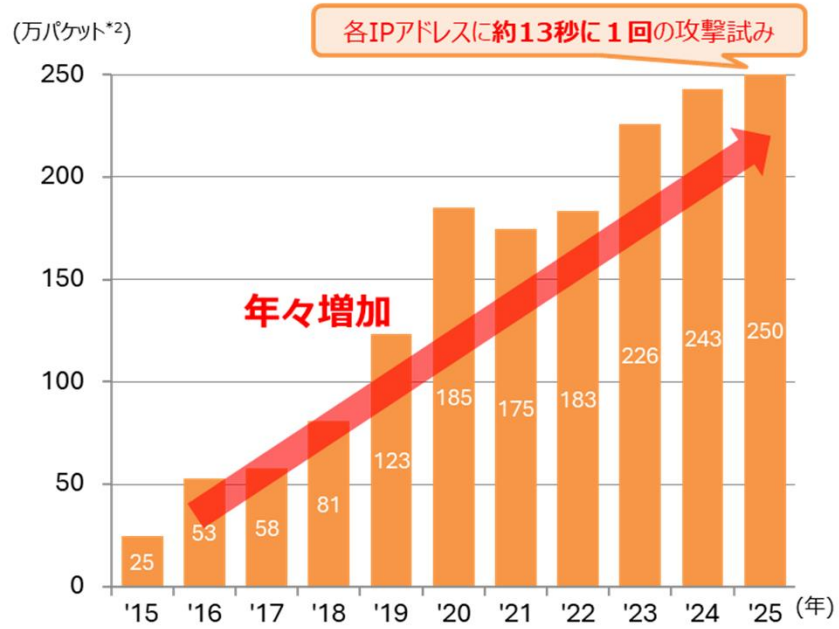
自治行政局住民制度課
サイバーセキュリティ対策室
7月27日（月）14:00～15:00

サイバー攻撃の変遷

○　ネットワーク外部性によりセキュリティリスクは著しく増大。サイバー攻撃関連通信数や被害数は増加傾向。
○　また、AIの高度化により、サイバー攻撃は今後さらに高速化・巧妙化。地方公共団体においても、資産管理、脆弱性対応等の基本的なセキュリティ対策を確実に実施することが必要。
○　一方で、地方公共団体は、専門人材の不足、財政負担の面でサイバーセキュリティ対策の実施が困難になりつつある状況。

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。

高性能AIの登場

Claude Mythosの性能

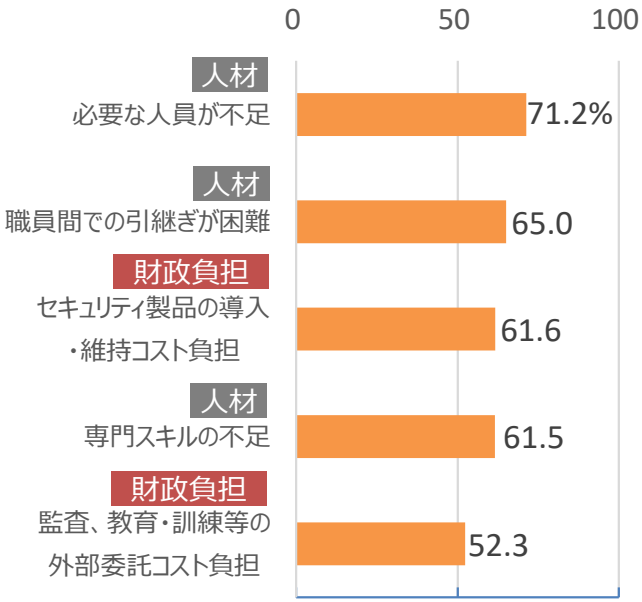
- Anthropicは、主要OS・主要ブラウザ等で数千件のゼロデイ脆弱性を特定し、その多くを自律的に発見したとしている。

GPT-5.5の性能

- OpenAIは、脆弱性発見ベンチマークで過去モデルを上回り、脆弱性発見・悪用関連の能力向上を示したとしている。

サイバーセキュリティ対策実施が困難

地方公共団体が課題と感じ、対応に苦慮している事項と当てはまると回答した団体の割合（上位５つ）



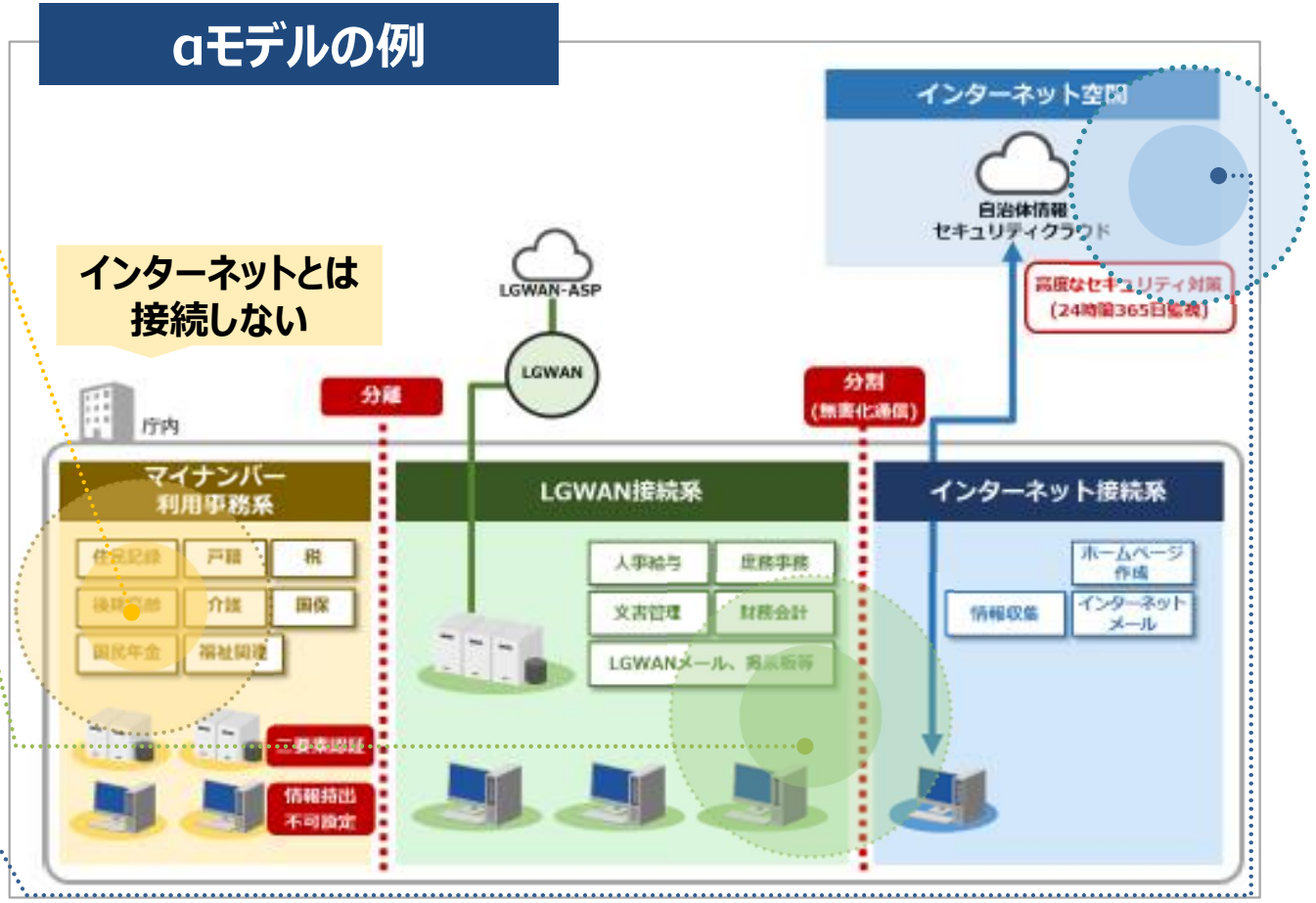
地方公共団体の情報システム全体像について

- 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

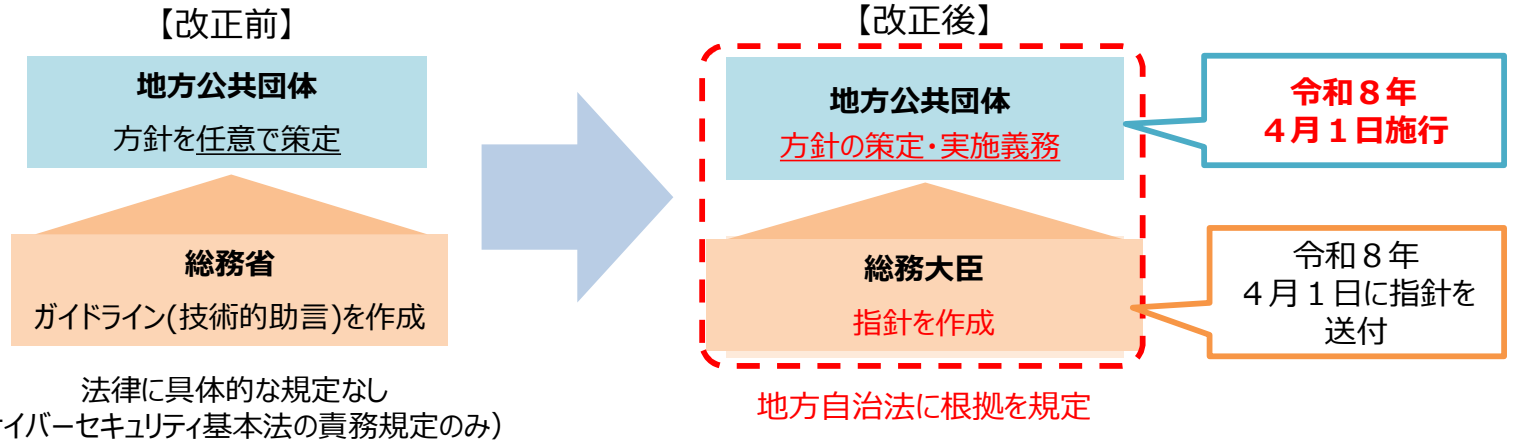
○　地方公共団体は、**事務の種類・内容に応じ**、**情報システムを有効に利用**するとともに、**他の地方公共団体又は国と協力**し、**その利用の最適化を図るよう努める**。

○　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＞



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

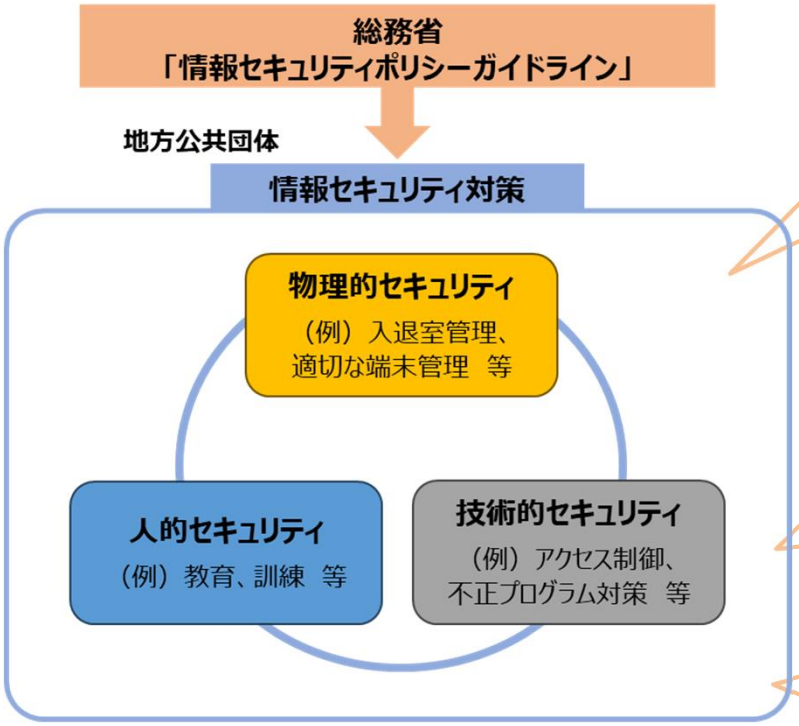
○ **R6地方自治法の改正**によって、**サイバーセキュリティに係る必要な措置の実施義務**と、**サイバーセキュリティを確保するための方針の策定義務**は措置済み。

○ 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）

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

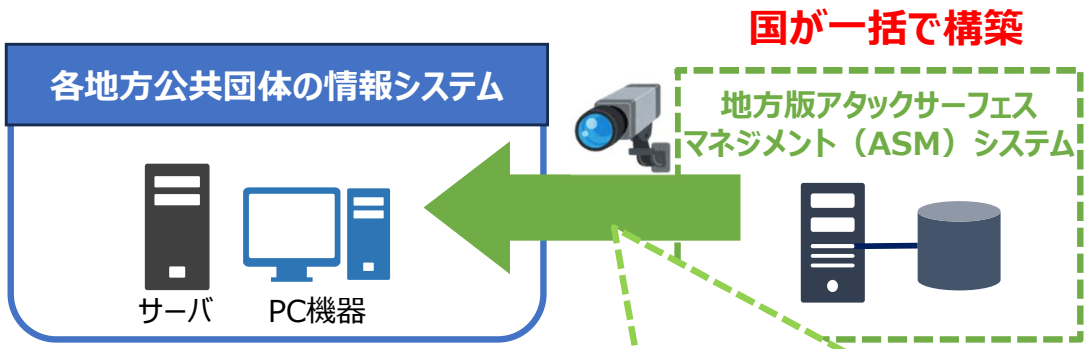
○　サイバー攻撃の対象が、外部からアクセス可能なIT資産に変化していることを踏まえ、**すべての地方公共団体が利用可能な地方版アタックサーフェスマネジメント（ASM）システム**を**令和８年度に構築**し、その**効果を実証**。

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（早ければ令和８年度中）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。

スケジュール

R8.4月～7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・選定。
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。
時期検討中	本格運用開始	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。