

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の
改定等に係る検討会（第22回）
議事概要 要旨版

開催日時：令和8年6月8日（月）14:00～16:00

開催場所：Teams による遠隔会議

議 事：

1. 今年度の検討内容について
2. 総務省の取組について

○：構成員 ●：総務省（事務局）◎：デジタル庁

1. 今年度の検討内容について

#資料1 今年度の検討内容について#

#資料2 デジタル庁 令和7年度 国・地方ネットワークの将来像の実現に向けた検証事業について#

#資料3 電磁的記録媒体を利用しないデータ連携におけるリスクアセスメントの実施について#

#資料4 重要インフラのサイバーセキュリティ対策のための統一基準への対応について#

#資料5 AI性能の高度化を踏まえたサイバーセキュリティ対策の強化について#

#資料5 【別紙】自己点検シートについて#

- 自治体の IT 予算増大やセキュリティ水準の向上による専門人材不足を背景に、コストと人材の両面から持続可能性の確保が重要であり、ゼロトラストなどの技術選定や役割分担についても持続可能性を踏まえて検討する必要がある。共同化・集約化といった新たな運用モデルの検討も重要である。
- 持続可能性確保の重要性は認識しており、ガイドラインの改定と並行してワーキンググループにて自治体における実装に関する手順等も検討し、小規模自治体を含めたセキュリティ水準の向上の実現を図る方針である。
- ゼロトラストアーキテクチャの導入を含めた将来像の実現を 2030 年目途とすると自治体は次期の調達から意識する必要があるため、進行の見通しを伺いたい。
- ゼロトラストアーキテクチャの導入について必要性は理解するが、進展する AI のリスクを踏まえ、脆弱性の発見及び対応の高度化が必要となり、特にデバイス管理の負担増大の懸念がある。まず安全の確保を前提として、境界防御の見直しを段階的に進める方針とすることが望ましい。
- ◎ 既存の境界防御を維持しつつ、適用可能な領域からゼロトラストアーキテクチャに移行する、または、既存対策と重層的に組み合わせて導入することが現実的な進め方であると認識しており、検討を進める。

- アセスメントの結果、ゼロトラストアーキテクチャには特定のソリューションが必要であるという印象を与える可能性がある。なぜ当該ソリューションの導入が適切なのかを理解・整理したうえで、結果を提示するようにしていただきたい。
 - 自治体の採用できるモデルを複数パターン提示することにより「どれでもよい」という誤解が生じているため、結果の示し方を工夫し、誤解を招かないようにしていただきたい。
 - 高度化する AI のリスクを踏まえると自治体には喫緊のセキュリティ対策が必要であり、特に、実践的サイバー防御演習（CYDER）の活用を進めるべきだが、有償の B・C コースについても無償化などの国の支援があれば、より多くの自治体で対策が進むのではないかと。
 - データ受け渡しの必要性については、セキュリティ対策及び業務生産性の観点から分析し結果を提示する方針とする。
 - 本リスクアセスメントのモデルはあくまで仮想的なモデルであることを強調し、情報取扱に留意しつつ、自治体への発信を行う方針とする。
 - リスクアセスメントの結果を踏まえ、各モデルの適用条件、必要な対策、残余リスク等を自治体が読み取りやすいよう整理し、必要に応じて推奨・非推奨の考え方を分かりやすく提示する。一般的な市町村においては、庁舎内で保有又は管理する情報資産に加え、セキュリティ機能についても対象とする趣旨で記載している。資料の読み取りに誤解が生じないように修正し整合性を確保する。
 - CYDER の有償コース支援は課題として関係部門と検討する。
-
- 地方自治法改正に伴い各機関がサイバーセキュリティ方針を策定する中で、水道など重要インフラに該当する分野では複数のガイドラインが適用されるため、関係省庁との連携や役割分担の整理が重要である。
 - 人材育成は重要だが即効性はなく、継続的な取り組みが必要である。一方で、AI の急速な進展に対応するため、即効性のある対策も並行して進める必要がある。
 - 地方自治法に基づき、全ての地方公共団体の執行機関や議会には基本的なサイバーセキュリティ方針を定める必要がある。総務省ガイドラインは広く適用されるが、水道・病院・警察などは各所管省庁のガイドラインに従う整理である。
 - 高度化する AI への対応では、短期的には脆弱性対応やパッチ適用の迅速化が重要であり、NCO（国家サイバー統括室）との議論も踏まえ、自己点検シートの早期提供と説明会によるフォローを通じて、未適用パッチの速やかな適用など基本対策を推進する方針である。
-
- ゼロトラストが唯一の正解という風潮があるが、境界防御も含め各自治体の実情に応じてネットワーク構成を検討すべきであり、コスト面も踏まえ慎重な検討を求めたい。
 - 重要インフラのサイバーセキュリティ対策の検討では、ICT 部門だけでなく防災など他部門との連携が必要である。また、現場の混乱を避けるために、NIST が公表する Cybersecurity Framework 2.0（CSF 2.0）に加え、目的や保護の在り方を整理し全庁的に共有できる仕組みの導入を検討することが望ましい。
 - 「境界内は安全である」という認識を自治体職員だけでなく、委託事業者も改める必要がある。

る。また、人材育成の観点から人事異動サイクルの見直しや内製化の促進も重要である。

- ゼロトラスト導入については期限ありきではなく、各自治体の実態に応じて柔軟に進めることを求めたい。
- ◎ ゼロトラストは唯一の解ではなく、状況に応じた適切な対策の積み上げの結果と位置づけられると認識している。ゼロトラストアーキテクチャの考え方の導入に向け、自治体の実情に応じた複数の選択肢を提示する方針である。現在想定しているゼロトラスト移行時期については一斉移行を強制せず、各自治体に応じて段階的にセキュリティ向上を図る方針である。
- 重要インフラのサイバーセキュリティ対策では ICT 部門と防災部門の連携不足が課題であり、幹部の判断・関与が重要と認識している。今後は組織連携や人材配置をガイドラインに反映し、あわせて委託事業者を含む「境界は安全」という認識の見直しや啓発を強化していく方針である。
- リスクアセスメントの結果、自治体の採用できるモデルが増えすぎことは望ましくなく、分析結果に基づいて推奨・非推奨を明確に示すことが重要と考える。
- いずれのモデルを採用してもリスクは残るため適切な対策の検討が必要となる認識である。DX 推進の観点も踏まえて有効なモデルを分かりやすく整理し、結果を次回検討会で報告する。
- 地方自治体のサイバーセキュリティ対策について、国家安全保障の観点からも国内での対応力強化が重要であるため、国産のツール導入を促進する政策を取り込み、侵入時のデータ分析が海外依存とならないよう配慮することが望ましい。
- 是非検討させていただきたい。
- 小規模自治体では基本的なセキュリティ対策の実施状況に懸念があり、自治体の要請に応じて低コストで点検を受けられる仕組みの構築が望まれる。また、努力している自治体を表彰し、優良事例を共有する仕組みも検討いただきたい。
- 自己点検シートは総務省が内製でコストを抑えて提供しているが、自治体側でベンダー委託時にコストが発生する可能性があり、さらなる工夫を検討する。また、優良事例の評価・共有についても検討する。
- 資料 3 のリスクアセスメントの進め方に問題ない旨を確認できたため、記載のとおりに進める方針とする。

2. 総務省の取組について

#資料 6 地方公共団体が講ずべきサイバーセキュリティ対策の細目化について #

#資料 7 ペネトレーションテスト事業の結果について #

- 地方公共団体におけるペネトレーションテストやリスクアセスメント等に要する経費につい

て、地方交付税措置を実施するとのことだが、これは導入だけでなく運用に関する経費にも適用されるのか確認したい。

- 地方交付税措置は導入と運用の両方に適用される方針である。特にエンドポイント対策についてはデジタル活用推進事業債が活用できるように措置する。
- 本日議論した国・地方ネットワークの将来像、重要インフラ統一基準への対応、AI 性能の高度化を踏まえたサイバーセキュリティ対策強化はいずれも今年度のガイドライン改定に向けた重要論点であり、事務局は意見を踏まえてリスク評価の進め方やガイドライン反映方針、自己点検や自治体支援の具体化をさらに検討する。次回は 9 月下旬を目途に開催予定で、日程は改めて連絡する。

以上