

前回の構成員意見について



総務省

令和 8 年 9 月 9 日
自治行政局 住民制度課
サイバーセキュリティ対策室

今年度のガイドライン改定における論点

論点①

- 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」におけるゼロトラストアーキテクチャの検証結果等をもとに検討した電磁的記録媒体を使用しないデータ連携のモデルに対しリスクアセスメントを行い、その結果を踏まえ、必要となるセキュリティ対策と遵守すべき基準等をガイドラインに示すことで、自治体におけるセキュリティの向上とDXの推進を両立して進めることができるのではないかな。

論点②

- 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（以下、「重要インフラ統一基準」）等の施行を見据え、新たに「組織統治」、「識別」、「防御」、「検知」、「対応及び復旧」を軸としたサイバーセキュリティ対策の重要性について「基本方針」及び「対策基準」に明記することで、レジリエンス（回復力）があり、業務継続が可能な仕組みの構築につながるのではないかな。

論点③

- AI性能の高度化に伴う地方自治体の対応に関しては、その活用によるサイバー対処能力の向上とサイバー攻撃への悪用の懸念の双方を念頭に、リスクに応じた対応方針を検討するとともに、基本的なセキュリティ対策を確実に実施することが喫緊の課題である。
- このため、委託先管理や構成管理・脆弱性管理等の基本的対策について、短期及び中長期の視点から計画的に推進する必要があるのではないかな。

前回いただいたご意見（論点①）

前回の検討会では、電磁的記録媒体を利用しないデータ連携モデルを検討するため「リスクアセスメント」を実施することについて承認をいただいた。また、ゼロトラストアーキテクチャの考え方を採用するにあたり、共同化・集約化の検討に関するご意見をいただいた。

検討項目	視点	発言要旨
電磁的記録媒体 を使用しないデータ 連携モデルの検討	1.リスクアセスメントの 内容等	・ リスクアセスメントの結果において、複数のモデル案が提示されてしまうと混乱が生じる恐れがある。<u>自治体に分かり易いように提示</u>すべきではないか。 ・ リスクアセスメントの結果に基づき必要とされる対策やモデルについては、<u>推奨・非推奨を示す</u>ことが重要ではないか。 ・ 特定のソリューションを導入すれば良いという誤解が生じないようリスクアセスメントの結果を整理すべきではないか。
	2.2030年頃の将来像 について	・ 人材不足やコスト増を踏まえた持続可能性の確保に留意し、<u>共同化・集約化といった運用モデルについても検討</u>するべきではないか。 ・ ゼロトラストアーキテクチャの考え方を採用すると脆弱性管理がより重要となる。また、デバイス管理等の運用負担も生じる。まずは、必要となる基本的な対策や措置から<u>段階的に進めていくといった方針の検討も必要</u>ではないか。 ・ <u>自治体の現状等を踏まえた検討が必要</u>ではないか。 ・ ベンダーや職員のセキュリティに対する意識や考え方についても同時に高めていく必要があるのではないか。

前回いただいたご意見（論点②）

前回の検討会では、重要インフラ分野等におけるサイバーセキュリティ対策のための統一基準に関するガイドラインへの反映において、特に業務継続の観点から、全庁的な連携体制等の必要性についてご意見をいただいた。

検討項目	視点	発言要旨
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	1.業務継続に対する 考え方	重要インフラのサイバーセキュリティ対策は、ICT部門に限らず関係部門を含めた全庁的な連携体制の構築が必要となる。業務継続を行う上で、目的や重要な情報資産に対する優先的な保護の在り方を全庁的に共有できる仕組みも必要となるのではないかな。
	2.その他	- 国家安全保障の観点から、サイバーセキュリティ対策の国内の対応力強化のため、国産ツールの導入を促進し、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のではないかな。 - 基本的なセキュリティ対策を確実に実施している団体の優良事例などを紹介したり、表彰するなどの仕組みも必要ではないかな。

前回いただいたご意見（論点③）

前回の検討会では、AI性能の高度化を踏まえたサイバーセキュリティ対策について、政府の動向の紹介と合わせて自治体に対する取り組みの方向性について説明をおこなった。即効性のある対策の検討の必要性などのご意見をいただいた。

検討項目	視点	発言要旨
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	1.今後の対応	- 人材育成による対応は、即効性というより継続的な取り組みにより効果が発揮されるのではないかと。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検討が必要ではないかと。 - AI性能の高度化を踏まえるとセキュリティ・バイ・デザインだけでは対応しきれないリスクの検討も必要となるのではないかと。