

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23回）
議事概要 要旨版

開催日時：令和8年9月9日（水）13:00～15:00

開催場所：Teams による遠隔会議

○：構成員 ●：総務省（事務局）

資料1 前回の構成員意見について

資料2 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結果について

資料3 ゼロトラスト基盤にかかるWGの設置について

資料4 今年度の改定方針について

資料5 高性能AIに係る自己点検シートのフィードバックについて

資料1・資料2

- AIが発達し、脆弱性を利用して攻撃に至るまでの期間が短くなっているほか、脆弱性そのものを発見する能力も上がっているため、厳格な脆弱性対策が必要になることを明確にした方がよい。
- 指摘のとおりである。日々脅威が高まり、脆弱性を突いた攻撃がより深刻化していると認識している。自治体が今後ゼロトラストアーキテクチャを実装する場合、組織的に脆弱性の管理を徹底した上で、適切な設計・運用が重要となると考えている。

- ネットワークアーキテクチャだけでなく、データをどのようにコントロールするかも重要である。クラウドにデータがあることを前提に運用する以上、端末へダウンロードさせない仕組み等も考えなければならない。ネットワークアーキテクチャとしてのゼロトラストアーキテクチャと、それに伴うデータ管理・データガバナンスの必要性を明記しなければ、「ゼロトラストアーキテクチャなら全て安全であり、そこへ向かえばよい」と誤解されるおそれがある。
- 重要なデータをどのように統制するかという視点が重要である。技術的に制御する部分、運用で補う部分、組織が各データをどのように扱うかという前提・方針を含め、整理していく。

- 利便性を重視するあまり、インターネット上のサービスに何でも接続してよいととらえられる懸念がある。マイナンバー利用事務系のデータを取り扱う場合やそれらを外部関係者と共有するかによっても自治体における責任の度合いや管理方法が異なるのではないかと。自治体に対して誤解を生まないよう整理してほしい。
- ご指摘のとおり特定通信であれば何でも接続できるという誤解が生じてはならない。自治体とも意

見交換しながら、必要な対応を分かりやすくまとめたい。

- オンライン申請ではファイルの添付を求めるケースが多く、様々な形式のファイルが送付されるため、リスクが高い。また、インターネット上のサービスである外部サービスは攻撃対象になり易いので、申請システムのアプリケーションだけでなく、構成する OS やミドルウェアの脆弱性管理も十分であるかを、自治体が利用前に確認することを徹底する旨を明記する必要があるのではないか。
- 外部サービスの見極めや信頼性をどのように測るかは難しいが、非常に重要な観点であり、利用前にセキュリティ対策の確認を行うことを自治体に徹底することを求めている。
- ゼロトラストアーキテクチャの考え方を採用する場合、認証基盤におけるセキュリティ対策や自治体における ID 管理が非常に重要になる。昨今は、正規の ID・パスワードを利用して組織へ侵入し、長期間潜伏した後に攻撃する事例が多い。認証情報の漏えい対策に加え、今後は、AI エージェントなどのノンヒューマン ID (NHI) の管理も必要となる。
- ID・パスワード以外の方式としてパスキーや生体認証等を活用したり、ID のライフサイクル管理も徹底する必要がある。AI エージェントの利便性を享受するならば、厳密な NHI の管理の徹底を自治体の責任において実施することが求められる。このことを自治体にどのように理解してもらい、運用を徹底してもらえるかが今後の検討課題である。
- 2030 年に向けて三層を前提としないゼロトラストアーキテクチャのモデルへ移行する場合、技術的な対応だけでなく、サイバー攻撃を受けてもすぐに検知し、感染拡大を防ぎ、迅速に復旧できるような高度な対応が可能となるよう、組織全体の対応力を高めることが求められる。
- 技術だけでなく、人と組織の対応力が必要であることは十分に認識している。必要となる技術的な基準・要件だけでなく、人・組織が必要となるレベル感や成熟度を今後自治体に示していくことが重要である。自治体が一定の組織レベルに達していなければ、ゼロトラストアーキテクチャの考え方を採用し運用することが難しいことを説明していく。
- 「2030 年にはゼロトラストアーキテクチャの世界になり、境界型防御や三層分離の時代は終わる」といった誤解が生まれないよう、将来像と合わせてどのように段階的に進めていくのか自治体に分かりやすく明確に説明する必要がある。
- ガイドラインに自治体が目指す将来像及び段階的なモデルを示した上で、具体的な運用方法や移行方法については、ワーキンググループで検討していく。

資料 3

- ゼロトラスト基盤について、県単位の共同運用や国・県・市の連携が強調されているが、マイナンバー利用事務は広域連合や一部事務組合でも行われている。これらの特別地方公共団体もワーキンググループの射程に含むのか。それとも当面、三層対策を継続する扱いなのか。
- 特別地方公共団体も議論の対象に含める予定である。運用主体についても県単位で運用するのか、

それ以外の単位で運用するのかについて議論を行う予定である。

- ゼロトラストアーキテクチャへ移行する前提に立つ場合、現在の自治体情報セキュリティクラウドのあり方も合わせて議論されるのか。
- 自治体情報セキュリティクラウドのあり方も検討対象に含む。事務局としては、県単位で運用する場合、既存のセキュリティクラウドをクラウドリフトし、改良して活用することが合理的な選択肢と考えている。

資料4

- ガイドラインの構成を見直し、第四編を第二編・第三編へ統合する方針は評価する。第四編を溶け込ませる場合も、クラウド利用を前提とした書きぶりにし、ボリュームを増やさない工夫を検討してほしい。
- ガイドラインが重厚長大になっていることは理解している。概要資料も作成するなど分かりやすく理解できるようにしていきたい。
- 自治体機密性3B やマイナンバー利用事務系の情報資産に対する、AI を含むクラウドサービスの利用方法や外部関係者等との共有可否等については、自治体に誤解が生じないように整理すべきではないか。
- インターネット上のサービスを利用するためのルールについて整理して提示することを検討していきたい。外部事業者と機密性の高い情報を共有する場合、どのようなリスクがあるかを分かりやすく明示する必要がある。その上で、リスクを受容するのか、低減するのか、回避するのかといった対応の考え方も示しながら、方向性を検討したい。

資料5

- AI セキュリティだけでなく AI セーフティも検討してほしい。現在の生成 AI にはハルシネーションが多く、誤った内容が政策や行政文書に反映されれば、自治体の権威・信頼や政策そのものに問題が波及する。今回または今後の検討で扱ってほしい。
- 自治体行政局の別部署から自治体向け AI 活用ガイドブックを公表しており、ハルシネーション、入力情報を学習させない設定、生成 AI 利用時の内部規程とそのひな形等を示している。自治体職員が安全かつ積極的に生成 AI を活用できるよう支援している。
- そのガイドブックを本ガイドラインから参照できるようにしてほしい。
- 金融庁が生成 AI に関して示した短期的対応の9項目のうち4項目がパッチに関するものであり、パッチを非常に重く見ている。パッチ適用人材という人的リソースを確保することまで求めている。これと横並びで考えると、パッチ適用者を決定することは必須である。人的リソースが不足している自治体ではパッチ適用者をベンダ担当者にするものの可否も検討しておくべき課題である。

またパッチ適用作業に伴う停止はやむを得ないというメッセージも必要である。

- 金融庁の短期対応では、パッチ以外にも経営課題やリーダーシップ、リスクの優先順位付けが重要と理解している。総務省も総務大臣書簡を通じて首長にリーダーシップを求めている。今回の自己点検で、まず情報資産に関する適正な脆弱性管理の状況の把握を行い、その結果を踏まえて対応を要請する。

システムを止めたくないという事情もあるため、ベンダを含め、リスクに応じた対応ができるよう継続的に要請したい。契約や費用の問題についても、今後の検討に反映する。

- ゼロトラストアーキテクチャの移行や総務大臣書簡に関連して申し上げる。地方自治法改正により、議会は首長部局から区別して法的義務の対象とされた。それにもかかわらず、改正後に議会への言及やフォローが十分でない状況は、法改正の趣旨から問題がある。法で明確に対象とした以上、議会へのフォローもお願いしたい。

- 議長会等から直接問い合わせを受けるなど、コミュニケーションを取っている。引き続きフォローする。

- 今回の調査結果については、調査期間等の制約により把握に至らなかったシステムがある可能性も踏まえ、引き続き実態の把握に努めることが重要である。

また、パッチ適用については、自治体と事業者が連携し、それぞれの役割を適切に果たすことが求められる。自治体職員向けの情報システム調達研修では、SLA 等にパッチ適用に関する事項を盛り込み、自治体と事業者との間で対応方法や役割分担をあらかじめ整理する考え方が示されることが多い。実際の運用においても、脆弱性のリスクやシステムへの影響等を踏まえ、関係者間で十分に調整した上で、適時に対応できる体制を整えることが重要である。

- 今回の調査結果については、御指摘のとおり、調査期間内に把握に至らなかったシステムがある可能性も考慮する必要があると認識している。今後も、各自治体において情報資産の把握と適切な脆弱性管理が進むよう、必要なフォローアップを行っていききたい。

また、今後作成する調達の手引きにおいて、SLA へのパッチ適用に関する事項の盛り込み方も含め、自治体とベンダの役割分担や、脆弱性のリスク、システムへの影響等を踏まえてパッチ適用を判断する際の考え方について整理していききたい。

総務大臣書簡を受け、大分市のように CISO アドバイザーを設置し、今後脆弱性対応や適用・サイクルの見直しなどを進めようとする自治体もある。こうした取組も参考にしながら、自治体が関係事業者と連携し、主体的に脆弱性管理を進められるよう支援していききたい。

今後の流れ

- 本日の資料2および資料5には、公表すると支障のある内容が含まれているため、事務局と調整の上、非公開としたい。
- 次回の検討会は、令和8年12月中旬頃から令和9年1月中旬頃を目途に開催する予定である。日程は改めて事務局から連絡する。

以上