参考資料２

ICT サイバーセキュリティ政策分科会（第６回）議事要旨

１．日　時）令和６年４月 26 日（金）13：00～15：00

２．場　所）WEB 開催

３．出席者）
【構成員】
後藤主査、上原構成員、栗原構成員、小山構成員、蔦構成員、盛合構成員

【オブザーバー】
内閣官房内閣サイバーセキュリティセンター、内閣官房サイバー安全保障体制整備準備室、デジタル庁、経済産業省、地方公共団体情報システム機構

【総務省】
山内サイバーセキュリティ統括官、豊嶋大臣官房審議官（国際技術、サイバーセキュリティ担当）、小川サイバーセキュリティ統括官室参事官（総括担当）酒井サイバーセキュリティ統括官室参事官（政策担当）、佐藤サイバーセキュリティ統括官室企画官、道方サイバーセキュリティ統括官室企画官、牧野サイバーセキュリティ統括官室統括補佐、井上サイバーセキュリティ統括官室参事官補佐、名越自治行政局住民制度課デジタル基盤推進室長、堀島自治行政局住民制度課デジタル基盤推進室課長補佐

【発表者】
髙橋邦夫（合同会社 KU コンサルティング）、菅原泰治（地方公共団体情報システム機構（J-LIS））、
吉本明平（一般社団法人全国地域情報化推進協議会（APPLIC））

４．配布資料
資料６－１　地方公共団体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方針（総務省自治行政局）
資料６－２　地方自治体情報セキュリティの現状（KU コンサルティング）（一部非公開資料）
資料６－３　J-LIS における地方公共団体への情報セキュリティ対策支援・教育研修に関する取組について（J-LIS）
資料６－４　自治体情報システム標準化時代の現状（APPLIC）
資料６－５　スマートシティセキュリティガイドラインの改定について（事務局）
参考資料１　スマートシティセキュリティガイドライン（第 3.0 版）（案）
参考資料２　実践的サイバー防御演習「CYDER」2024 年度開催予定
参考資料３　ICT サイバーセキュリティ政策分科会第４回　議事要旨

５．議事概要
（１）開会

（２）議題
◆議題「自治体におけるサイバーセキュリティ対策の取組について」、堀島課長補佐より資料６－１、KU コンサルティング髙橋氏より資料６－２を説明。

◆構成員の意見・コメント
後藤主査）
資料６－２の最後の２ページで示されているまとめは納得感があった。これまでコンサルティングされている中で、こういった話は自治体の方にうまく伝わるか。

KU コンサルティング 髙橋氏）
自治体では DX への機運が高まってきており、セキュリティの講師よりも DX の講師として呼ばれることが増えている。DX の話を行う際は「セキュリティと DX はセット」ということを必ず盛り込むようにしており、DX やデジタル化していこうという気持ちを上手く活用し、セキュリティのレベルも向上していただこうと考えている。

蔦構成員）
人がやることには限界があるといった点は強く共感した。PoC の設置に関して、PoC を掲載している自治体とそうでない自治体があるが、各自治体で PoC を掲示すべきなのか、あるいは J-LIS など、統一の窓口のようなもの

があったほうがよいのかついて御意見をいただきたい。実際に統一的な窓口があるかもあわせて伺いたい。

KU コンサルティング 髙橋氏）
特定の自治体に対して気づいたことを連絡するという点では、統一的な PoC より、自治体各自で PoC を設けている方がより早く対策に踏み切れると考えている。PoC という名前でないため検索のクローラーには引っかからない場合もあるが、約 8 割の自治体が CSIRT を立ち上げており、PoC を意識していると思う。他方、住民にどのように周知するかは今後、工夫が必要な点だと考えている。

盛合構成員）
PoC について、組織外からの通報には善意のものと悪意のものとがあり、的確な判断を行うことがとても重要だと思うので、組織の中において窓口の重要性の認識を広げていただきたい。CSIRT の立ち上げ後も人事異動などがある中で、各自治体だけで最新の動向を学ぶことは難しいと思うが、例えば日本シーサート協会のような他の CSIRT との意見交換や連携体制についての現状を教えていただきたい。もし障害や困難な点があればあわせて教えていただきたい。

KU コンサルティング 髙橋氏）
後ほど J-LIS からの発表もあると思うが、自治体の CSIRT が加盟する自治体 CSIRT 協議会のコーディネーターを務めており、協議会で開催される訓練のコーディネーターも担っている。自治体だけで訓練するのは難しいので、年度替わりには新しい CSIRT のメンバーに J-LIS の訓練に参加してもらい、そこで体験したものを自団体の中に取り込んでいってもらっている。

後藤主査）
一般的な相談窓口ではなく、セキュリティの PoC として示していることで、意見の集まり具合など現状どのような効果があったか。

KU コンサルティング 髙橋氏）
自治体における PoC の役割は大きく 2 つあり、外からの窓口としての機能についてはまだまだ周知されておらず、善意の方やセキュリティに関心のある方については PoC を探して連絡してくれるが、多くの住民は何かあっても全て広報へ連絡しているのが現状である。一方で、自治体内部や自治体に関係する団体からの連絡については、PoC をしっかりと周知することで、例えば自治体内部でシステムの不具合があった際の相談先が分かるといった点で非常に大きな役割を持っており、今後も重要視されると思う。

上原構成員）
情報セキュリティポリシーガイドラインに携っているほか、芦屋市で CIO 補佐官を務め、様々な現場を見ているが、セキュリティに関する規模感が千差万別の中で、ガイドラインを改定しセキュリティ対策を適切に講じなければいけないという全体の流れがあると同時に、クラウドサービスなどを使った DX を進めることでこれまでの境界型防衛が難しくなってきているという意見を聞く。先ほど堀島様から α モデルから β モデルへの移行が進まないという話があったが、私の現場感では、β モデルの 1 番の問題点は、β モデルを採用することで、境界で防御されないため、各端末が守られているかを確認し、有事の際にはすぐ動くといったインシデントレスポンスの体制を構築する必要があり、運用負荷が高くなってしまう。それを踏まえると、β モデルに移行できない規模の自治体は相当数残ると思われる。また、都道府県では β モデルが採用が進んでいるが市町村の多くは移行していないという話があったが、それは基礎自治体では多くの個人情報等の重要な情報を保有しており、求められるセキュリティが都道府県と市町村では異なるためだと理解している。そのため、α モデルと β モデルを普及率という点で見ると、ややミスリーディングになりがちな印象があることを踏まえた上での評価を行うのが良い思う。

小山構成員）
中央省庁・都道府県・市町村の IT 環境を企業と同じように考えると、デジタル庁が提唱しているゼロトラストアーキテクチャをゴールに据え、全国ネットワークを構築していくことでセキュリティレベルが上がり、生産性の向上や高度化、コストダウンが図れると思う。ガイドライン案の最後にはゼロトラストアーキテクチャの言及があったが、α'やβ'モデルについてははその方向に向かっていくのか。デジタル庁が中心となって議論されているとのことだが、どういった方向感を持って議論されているのか教えていただきたい。

蔦構成員）
業務委託先の管理について、直接の委託先はある程度管理ができると思うが、その先の再委託、再々委託となった場合についてお伺いしたい。例えば、重要インフラのサイバーセキュリティに係る安全基準等策定指針では、一次委託先が再委託先、再々委託先といった事業者を対象にサプライチェーンリスクマネジメントを行うと読める記述がある。サプライチェーン全体を把握するには、直接の委託先だけではなく、その先の委託先まで管理しなければならないと思うが、セキュリティポリシーガイドラインではどのように規定しているのか、また、今後どうしていく予定か教えていただきたい。

堀島課長補佐）
小山構成員からの御質問について、デジタル庁が総務省の協力を得て開催している「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」において議論を行っており、現在は地方自治体の意見を聞き、報告書の取りまとめを行っているところ。その中で出されている考え方として、境界型防御に依拠しないゼロトラストアーキテクチャがあり、トラストゾーンを極小化し、境界に守られているから安全ということではないという意識を取り入れていく方向で、地方公共団体・国を含めて、ネットワークアーキテクチャを考えていくよう知らされている。実際にどのようなセキュリティ対策を行っていくのかについては、デジタル庁と総務省が実証事業などを経て、具体的な対策を検討していくという方向性となっている。今後もデジタル庁と協力し、どのようなセキュリティ対策行えばゼロトラストアーキテクチャの考え方を取り入れた境界型防御に依拠しない対策ができるかを検討できればと考えている。令和２年度に、インターネット環境に業務端末や重要な情報資産を置くためのセキュリティ対策群であるβ´モデルを提示しており、オンプレ型 M365 を使えなくなってしまう等の事情により LGWAN 接続系からブレイクアウトしなければならない場合についてα´モデルを示している。インターネット上の SaaS サービスの利用のため、既にα´モデルやβ´モデルを実装している自治体があることを前提に、更に境界型防御に依拠しないゼロトラストを行っていくといった方向性になると認識している。

名越室長）
境界型防御とゼロトラストアーキテクチャについて補足させていただく。三層の対策は基本として境界型防御という前提で、デジタル庁と総務省の検討会では、境界型防御のみに依拠している三層の対策を見直してゼロトラストの考え方を取り入れていくと報告書案に明確に記載されている。境界型防御とゼロトラストは互いに矛盾せず両立するものであり、ゼロトラストの考え方を導入するからといってすぐに境界型の部分を無くすことはないという点を補足させていただきたい。ゼロトラストの考え方を導入するにあたって具体的にどうしていくべきかについて、今後、デジタル庁と協議しながら総務省においても、調査研究や実証を通して整理を行い、「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」で議論していく予定。

小山構成員）
私も賛同しており、境界型防御かゼロトラストかではなく、ゼロトラストアーキテクチャ、言い換えれば ID ベストセキュリティが完成するまでは境界型防御で守らざるを得ない部分は残り続けると思う。そのため、境界防御型が残る今からゼロトラスト型に移行に向けた動作を始めないといけないので、そのビジョンを示すことが重要だと思いコメントさせていただいた。

堀島課長補佐）
蔦構成員からの御質問について、現在の最新のガイドラインにおいて再委託先の管理について対策を求めており、具体的には委託契約時に、再委託先に関する制限事項の遵守、つまり再委託を制限するよう規定している。あくまでガイドラインのため、直接的に地方公共団体が遵守するのは、自団体のセキュリティポリシーになるが、ガイドラインを踏まえて各地方公共団体のセキュリティポリシーでも再委託について適切に制限をかけ、契約時において制御をかけていると認識している。

後藤主査）
先ほど話のあったデジタル庁の検討会に私も出席しており、短期的なゼロトラストソリューションではなく、中長期的にゼロトラストの考え方をしっかり取り入れていくようにといった趣旨の発言をさせていただいている。

◆議題「自治体におけるサイバーセキュリティ対策の取組について」、J-LIS 菅原氏より資料６－３、APPLIC 吉本氏より資料６－４を説明。事務局より資料６－５を説明

◆構成員の意見・コメント
後藤主査）
吉本様から説明いただいた標準化に関しては課題が大きいと感じた。自治体にとってどのレベルの標準化が役立つと考えているか。例えばガバメントクラウド上に集約するのであればこういったクラウドサービスが便利だといったことや、DX の部分で標準的なものに揃えた方がよいといったことなどあればお伺いしたい。

APPLIC　吉本氏）
自治体は標準化に従う義務があり、現在基幹系システムについての機能と帳票が既に決まっているため、機能一覧にある機能の実装が必須であるが、一覧以上の機能は認められない。帳票に関しても証明書の種類やレイアウトが決まっているので、これまでは自治体ごとに証明書の形式が異なっていたが、今後はどこでも同じ形式で出力されるようになる。率直に言えば自治体には特段メリットはないが、自治体のメリットとなる点としては DX を推進するにあたり、自前での構築は困難となってきているので、例えば、デジタル庁にて全国なサービスを作成し、基幹系システムと連携・連動する必要がある際、基幹システムの標準機能や保有データが分かっているので、連携方法など具体的な指示、手順を示すことができるようになり、全国的なサービスへの対応や自治体 DX

の推進に取り組みやすくなることが期待される。

後藤主査）
J-LIS で提供する研修における NICT の研修の活用について、連携状況や改善点などはあるか。

J-LIS 菅原氏）
NISC の分野横断的演習のほか、NICT が実施している CYDER への自治体の参加を促している。J-LIS は様々なシステムの開発や運用を行っており、訓練や教育研修に割ける人的リソース、財源には限界はあるが、一方でニーズも高いため、オンライン研修に切り替えて、少ない人的リソースで多くの方に受講いただけるようにしている。また、研修内容についても J-LIS だけで全てを揃えることは難しいため、研修の講師等などで関係機関の協力を得て行っている。

上原構成員）
吉本様からの、地方自治と標準化が矛盾するという御指摘は非常に重いと思う。具体的には自治権の中で自治体が独自の政策を打ちたい場合でも、標準システムのカスタマイズが認められていないことで阻害されることを気にする自治体がある。そのため、上手くバランスをとりながら行うことが必要であるが、セキュリティの観点では標準システムに則って堅くシステムを構築する方がセキュリティは向上する。特に今後ガバメントクラウドのような仕組みになることで、三層分離でなくなりゼロトラストの世界に移行する際、そのシステムをカスタマイズするほど、安全ではなくなるという大きなジレンマがある。解決策の検討にあたっては技術に深く踏み込んだ上で、標準システムをこのように作るべきということを本来的には示さなければならないと思うが、残念なことに手が回っていない状況。力を入れていくべきといった方向性などをこの分科会から打ち出していくべきではないかと思う。

APPLIC 吉本氏）
御指摘のとおり地方自治とのバランス。極論では、地方自治体のセキュリティ対応を全て国で行う選択肢もありえると思う。セキュリティクラウドなどが近しい概念だと思う。例えば地方自治という権力・権利を行使するなら、ガバナンスを徹底するという義務を果たさなければならないはずであり、地方公共団体が義務を果たせていないが、地方自治という権利だけ行使できるのかといった概念も議論しなければならなくなるのではないかと思う。義務と責任と権利のバランスや、方法論とガバナンスなどの区分けや整理学が必要になるのではないかと考える。

（3）閉会

以上