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（関係府省庁等ヒアリング）
議事要旨

１．日　時　令和８年７月 27 日（月）14:00～15:05
２．場　所　オンライン開催
３．出席者
(1)　ヒアリング対象者
中山　貴洋　　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長
松葉　勇志　　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課長補佐
岩尾　和樹　　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事務官
(2)　ワーキングチームメンバー
林　弘一郎　　山口県総合企画部デジタル推進局長
伊藤　正樹　　愛知県一宮市総務部長
藤田　恵二　　福岡県水巻町企画課長
（代理　福岡県水巻町企画課情報政策係　渡邊主任）
名越　一郎　　内閣官房デジタル行財政改革会議事務局参事官
折田　裕幸　　内閣官房デジタル行財政改革会議事務局参事官　併任　総務省行政管理局管理官
鈴木　優一　　内閣官房デジタル行財政改革会議事務局参事官
杉本　敬次　　内閣官房デジタル行財政改革会議事務局参事官
橘　清司　　デジタル庁統括官付参事官
糸　将之　　デジタル庁統括官付参事官
萩原　一博　　デジタル庁統括官付参事官付企画官
志賀　真幸　　総務省自治行政局地域情報化企画室長
（代理　総務省自治行政局地域情報化企画室　髙橋課長補佐）

４．議事概要
＜事前に送付した質問事項について、総務省より説明。＞
※「→」はワーキングチームメンバー発言

①地方公共団体におけるサイバーセキュリティ対策の現状と課題について、その概要をご教示ください。

・　近年、サイバー攻撃関連通信数や被害数が増加傾向にあり、また、高性能 AI が登場したことにより、サイバー攻撃が今後さらに高速化、巧妙化していく見込み。地方公共団体においても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と考えている。
・　一方、地方公共団体においては、財政面、人材面、技術面の３つが現在の大きな課題。
・　第 33 次地方制度調査会において、国と地方公共団体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、仮に地方公共団体のある団体のネットワークが攻撃を受けた場合、そこから国のネットワークにまで影響が及ぶ可能性もあること等を踏まえ、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必要性が答申され、令和６年に地方自治

法を改正した。地方自治法の改正前は、情報システムに関する規定を地方自治法には置いておらず、総務省が作成している技術的助言としてガイドラインを示し、各団体の個々の判断でセキュリティポリシーを作成していただいていた。地方自治法の改正後は、地方公共団体のサイバーセキュリティ確保に関する措置義務を規定するとともに、サイバーセキュリティの確保に関する方針の策定と実施を義務としている。

- 昨年 12 月 23 日に閣議決定された政府のサイバーセキュリティ戦略の中で、地方公共団体のサイバー対策強化の方向性を記載している。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支援、また、人材の確保・育成に対する支援、そして脆弱性を診断するシステムを構築し、脆弱性対処能力の向上を図ることとしている。こちらは地方版 ASM のことを指しているが、それ以外にも、適切な財政措置、必要な予算の確保など、更なる安全性の確保に向けた取組を実施・強化することとしている。
- 今年度の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取組は大きく 3 つあり、1 つ目は財政負担の軽減、2 つ目が人材の確保・育成、3 つ目が技術的な支援。1 つ目の財政負担の軽減については、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による支援を行っている。それ以外にも、ペネトレーションテストの実施経費などを地方交付税措置の対象として新たに追加するとともに、不正アクセスを常時監視するシステムの整備について、デジタル活用推進事業債の対象に追加している。2 つ目の人材の確保・育成については、今年度新たに自治大学校でサイバーセキュリティに特化した特別研修を 10 月と 12 月に開催する予定としている。あわせて、実践的サイバー防御演習（CYDER）や、都道府県単位での人材確保プールによる市町村支援などに取り組んでいる。3 つ目の技術的な支援については、今回の共通化の議題となっている地方版 ASM である。こちらを国が一括して構築し、効果を検証するということで、この 3 つの柱で取組を進めている。また高性能 AI の登場を受け、現在、7 月末までに全地方公共団体において脆弱性管理について自己点検をお願いしており、引き続き地方公共団体とも連携して対応していきたい。
- 地方公共団体における最低限のサイバーセキュリティ対策については、これまで実施していただいているが、重要な項目の中でも実施率が低い項目があることが課題。特に脆弱性診断の実施については、実施率が全団体の約 2 割ということで、まだ対策が不足している状況。高性能 AI の登場により、脆弱性管理についてはきちんと実施していかなければ非常に危険である。脆弱性管理に関する課題への対応という観点からも、地方版 ASM をしっかり活用していただきたい。また、令和 8 年 6 月 26 日に、改正地方自治法の確実な実施を図るため地方自治法施行規則を改正（施行は来年 7 月 1 日）し、地方公共団体が講ずべきセキュリティ対策の細目を省令で位置付けている。その省令の中に、サイバーセキュリティに関する情報の収集という規定があり、その一つの手法として、今回の地方版 ASM を活用した脆弱性診断を位置付けている。
- 全ての地方公共団体が利用可能な地方版 ASM システムを今年度構築し、効果の実証を行う。地方版 ASM システムを活用することで、各団体の IT 資産の脆弱性を攻撃者目線で評価することができる。また、国が一括して構築することにより、各団体が個別に実施するよりも低コスト・低負担で利用可能になることがメリット。あわせて、情報システムをスキャンした結果を国で集約・分析し、その情報を横展開することも、国が構築し共通化するメリ

ットと考えている。

・　主な機能としては、資産の把握、それから定期的なスキャン。また、ダッシュボードを作成し、リスクの評価、脆弱性情報の管理を行う。国やJ-LIS、都道府県による管理・助言も予定しており、各都道府県には域内市町村の管理画面を閲覧できるようにしたいと考えている。都道府県から域内市町村に対して様々な助言を行っていただくことも考えている。

・　運用のイメージであるが、まず地方公共団体から利用申込みを行っていただく。それを総務省及びJ-LISで受け付け、その後、地方公共団体にドメイン名を登録・入力していただく。毎週スキャンを実施し、脆弱性情報を地方公共団体へ提供していく。仮に脆弱性が見つかり、特に緊急性の高いものがあった場合には、保守事業者に対して、地方公共団体から連絡をしていただく。例えば、修正プログラムの適用を保守事業者に依頼していただき、その対応が完了した後に、その旨を報告していただくという流れである。利用する地方公共団体の立場からすると、独自にシステムを構築して実施するよりも非常に低負担で利用できる仕組みとしているため、その点でも効果があり、メリットがある。また、個別に実施するとシステム利用料が高額になるケースもあると聞いているが、今回、国が一括して整備することにより、コスト面についても非常に低く抑えることができる。そのため、低コストかつ低負担で地方公共団体に利用していただけることがメリットである。併せて、都道府県が域内市町村の管理画面を確認して支援を行うことや、国が総合窓口を設置して支援を行うことも可能である。そのため、人員不足などの課題を抱えている多くの地方公共団体の脆弱性管理の強化。ひいては、我が国全体のセキュリティ水準の向上につながると考えており、この辺りが本取組の効果ではないかと考えている。

→　地方自治法も改正され、法律に基づく施行規則も来年施行されるという話も伺った。さらに、地方版ASMという一つの共通システムを今後展開していくとのことであり、総務省もこれまでのスタンスから大きく一歩踏み出しているのではないかという印象を持った。もちろん、各地方公共団体の努力は当然必要であるが人材や経費負担の面で厳しい部分があることも事実。そのため、まとめて実施することで合理化を図り、全体のレベルを引き上げていくということについては、やはり進めていくべきであると考える。そして、その一つの象徴がこの地方版ASMになるのではないかと思っている。地方版ASMの進捗に期待しているし、その進展を契機として、地方公共団体においてサイバーセキュリティに関する問題意識や関心が高まり、実際のサイバーセキュリティレベルが向上していくことを期待する。高性能ＡＩのクロードミュトスの話もあったし、ランサムウェアによる攻撃もかなり増加していて、大企業でも情報が窃取されたり業務継続に支障が生じたりする事例も発生しており、機密性や可用性の観点から非常に問題のある状況が続いている。そのため、サイバーセキュリティ分野は極めて重要な仕事である。

→　先週にはOpenAI社の新しいAIが暴走し、勝手にスタートアップ企業を発見して攻撃してしまったという報道もあり、大変恐ろしいというのが率直な実感である。こうしたサイバー攻撃が巧妙化、高度化する中において、地方公共団体それぞれが個別に防御を行うことには限界があるように感じている。

→　ご説明にあった人材育成の面について、地方公共団体として積極的に活用していきたい。

・　現在、地方公共団体の職員向けの研修機関について、できるだけ内容の重複が生じないよ

う整理しながら、対象者のレベルに応じた研修体系の構築を進めていきたいと考えている。また、都道府県においても独自の研修機関を有している場合があるため、そうした都道府県の研修機関との連携についても視野に入れながら、人材育成に力を入れて取り組んでいきたい。

②政府機関でもアタックサーフェスマネジメント（ASM）を実施していますが、連携等を検討しているでしょうか。

・　国が構築している政府機関向け ASM は、NCO（国家サイバー統括室）が構築している。国 ASM との連携について申し上げると、今回、我々が地方版 ASM を構築するに当たっても NCO の皆様と意見交換を行いながら、機能の在り方についてこれまで検討を進めてきたところ。国 ASM は既に先行して構築されているため、その技術的知見を生かしていきたいと考えている。

・　また、国 ASM で収集した様々な脅威情報についても、地方版 ASM に提供いただき、各利用団体である地方公共団体に周知していきたいと考えている。逆に、我々が地方版 ASM を通じて地方公共団体から得た様々な脆弱性に関する情報については、国側で国 ASM を運用している NCO にも提供することとしており、相互に情報を交換・共有しながら取組を進めていきたいと考えている。

→　国は各省庁に分かれているとはいえ一つの組織体であるため、意思決定や調整が比較的迅速。そうした国の知見を活用させていただくことは非常に重要。一方で、地方公共団体には様々な実情や団体ごとの特性があると思う。そのため、地方公共団体側で得られた情報を国にフィードバックすることも、国にとって非常に有益ではないか。NCO との連携については、さらに一歩踏み込んで、しっかりと主導して進めていこうとする姿勢が感じられるところである。この点について、NCO とは既に協議や意見交換を行っているという理解でよろしいか。

・　地方版 ASM の機能の検討に当たり、できる限り国と同等の水準を地方公共団体にも提供できればよいと考え、NCO の ASM システム担当者と意見交換を重ねてきたところ。現在も月 1 回程度、意見交換を行いながら進めている。当初は、ある意味で国側の方が先行しており、国側の知見をいただきたいという思いが強かった。しかし、国側に話を伺うと、地方公共団体は数が非常に多く、そこで得られる様々な脆弱性情報は、NCO の立場から見ても非常に価値が高く、共有してほしいとの意見をいただいている。そのため、相互にメリットがあると考えている。すなわち、我が国全体としてサイバーセキュリティ水準を向上させるために、一緒に取り組んでいこうという趣旨の話をいただいているところである。今後も引き続き連携を深めていきたいと考えている。

③地方版アタックサーフェスマネジメント（ASM）システムの共通化を進めることによる効果をどのように見込まれていますか。

・　（再掲）地方版 ASM システムを活用することで、各団体の IT 資産の脆弱性を攻撃者目線で評価することができる。また、国が一括して構築することにより、各団体が個別に実施するよりも低コスト・低負担で利用可能になることがメリット。あわせて、情報システムを

スキャンした結果を国で集約、分析し、その情報を横展開することも、国が構築し共通化するメリットと考えている。

・　（再掲）都道府県が域内市町村の管理画面を確認して支援を行うことや、国が総合窓口を設置して支援を行うことも可能である。そのため、人員不足などの課題を抱えている多くの地方公共団体の脆弱性管理の強化。ひいては、我が国全体のセキュリティ水準の向上につながると考えており、これも本取組の効果ではないかと考えている。

→　財政的な部分が非常に重要と思っている。構築は総務省が対応されるとのことであるため、初期経費は総務省が予算を用いて構築し、ランニングコストは参加する地方公共団体に、ある程度頭割り、あるいは一定の傾斜はあると思うが、それぞれ負担していただくという考え方なのか。

・　お見込みのとおり。令和 7 年補正予算において 4.5 億円を総務省として国費で確保しており、構築は全額国費で実施するもの。その上で、本格運用の段階になった際には、利用する団体から利用料という形で負担いただき、運用を行っていきたいと考えている。各団体が個別に実施する場合には、かなり高額となり、1,000 万円程度の費用がかかるケースもあると聞いている。しかし、できるだけ多くの地方公共団体に活用・利用していただくよう働きかけることによって、いわゆるスケールメリットによるコスト低減効果も期待できると考えている。また、その利用料については、地方財政措置についても、財政当局と調整しながら検討していきたいと考えている。

→　県としても、規模の小さい団体については、様々な機会を通じて意見や状況を確認している。その中で、サイバーセキュリティ対策に十分な手が回らないという実態があると認識している。そのため、国が共通化して取りまとめていただけることは大変ありがたい。特に小規模市町村のサイバーセキュリティに関する状況を踏まえると、人材やノウハウが不足していることが想定される。そのため、研修や相談体制についても併せて構築していただけるとありがたい。また、イニシャルコストについては国のシステムとして負担いただけるとの説明があったが、実際に運用する際には、その業務に関わる人的負担も生じることになる。実際に導入し、業務へ落とし込んでいくに当たっては、地方公共団体側でも様々な検討が必要になると思われる。そのため、運用段階で必要となる人的負担や実施体制、具体的な対応内容について、できるだけ早い段階で見通しをご提示いただければ、本取組を推進することとなった場合には非常にありがたい。

　また、市町村へのフォローも県の役割として求められることになると思われる。その場合、どのような範囲までが県の役割として求められるのかという点が課題である。実際には地方公共団体ごとに組織が異なり、どの程度の運営体制やセキュリティ対策レベルを有しているのかについて十分に把握できているわけではない。そのため、市町村をフォローし、支援していく際の役割分担について、本プロジェクト全体のスキームやフレームワークの中で明確にしていただくことも必要ではないかと考えている。

・　研修については、まだ予算要求の検討段階ではあるが、例えば市町村アカデミー（JAMP）や国際文化研修所（JIAM）において、更に研修を実施することも検討している。また、J-LIS においても、情報セキュリティやサイバーセキュリティ関係の研修教材など様々なコンテンツがあるため、J-LIS との連携も進めていきたいと考えている。さらに、都道府県単位で人

材をプールする取組についても、各都道府県においてかなり進展してきているところであり、それをさらに充実できるよう取組を進めていきたいと考えている。加えて、スポット的なアドバイザー派遣、いわゆる専門家派遣については、地方公共団体金融機構によるアドバイザー派遣制度があり、これは無料で利用可能である。今回、サイバーセキュリティ対策もメニューに加わっているため、その周知も進めていきたい。また、相談体制についてであるが、ASM 自体の相談体制については、J-LIS と協力してしっかりと構築する予定である。併せて、総務省としても、来年度はサプライチェーンリスク対策を中心として、例えば高性能 AI への対応など、高度な技術的相談が今後増加すると考えている。そのため、国として総合相談窓口を設置していきたいと考えている。

次に経費負担については、できれば 8 月末から 9 月頃までには、地方公共団体の来年度予算編成に間に合うよう、利用料の設定を示したいと考えている。また、その利用料について地方交付税措置が活用できるよう、来年度の地方財政措置についても検討していきたいと考えている。

最後に、市町村のフォローや県の役割分担についてである。実証については 10 月から 1 月まで実施する予定である。この実証においては、県と県内市町村を組み合わせた形で、県と市町村が一体となったグループにより実施していきたいと考えている。その際、市町村支援において県がどのような役割を担うのか、また、地方版 ASM に関する国の相談窓口も設置されることから、国、県及び市町村の間で、どのような役割分担や運用体制が円滑であるのかについて、実証を通じて検証していきたいと考えている。運用手順についても、年明けの 1 月以降になるが、運用ルールや手順書を作成する予定である。当然ながら、地方公共団体においても担当者を配置して地方版 ASM を運用する以上、一定の業務負担が生じることになる。そのため、運用時の負担軽減にも努めていきたいと考えている。

→　サイバーセキュリティに関する取組は、かなり幅広く、かつ内容も高度になってきている。総務省におかれては、研修機関との連携として、先ほど JIAM や J-LIS の研修の話や、調達との関係では、サプライチェーン対策のための相談窓口を設けるという話もあった。しかし、そのような取組については、まだ十分に認識していない地方公共団体もあるように感じている。直ちにということではないが、総務省が研修機関や、NCO のような関係省庁と連携してどのような取組を進めているのかについて、全体像が見える形で示していただけるとよいのではないかと思う。また、その全体像の中の一つの取組として地方版 ASM が位置付けられていることが分かれば、地方公共団体側の理解もより進むのではないか。ご検討いただければありがたい。

・　今後はセキュリティ対策全体の方向性や全体像についても、しっかりと示しながら、人材育成も含めて着実に取り組んでいきたい。

→　小規模な市町村にとっては、人材の育成がなかなか難しい環境にある。来年度は研修等をかなり強化して実施いただけるとのことであり、ぜひその取組をお願いしたい。また、現在、情報システム関係の経費によって財政的にかなり厳しい状況にある。そのような中、低コスト・低負担で本取組を実施していただけるとのことであり、大変ありがたいと感じている。さらに、この費用に係る地方負担分については、地方交付税措置を強く求めていきたいとのご発言もあったため、その点についても併せてお願いしたいと考えている。

・　昨年、有識者会議を複数回開催し、そこに町村会の代表として広島県坂町に参加いただいて議論を行った。その際、最も強くおっしゃっていたのは、小規模な町であるため人材の確保が非常に難しいということであった。現在、役場の中でも DX を推進するという流れがあり、どちらかというと、デジタル技術を活用していかに業務を効率化するかということに重点が置かれている。そのため、なかなかセキュリティ対策まで十分に手が回らないという話を伺っている。その際、広島県では県が人材を確保し、各市町村を支援するアクセラレーターの取組を非常に積極的に活用しているとの発表もあった。まさに、各都道府県単位でセキュリティの専門家を配置することができれば、市町村にとっても非常に心強いものになるのではないかと考えている。

現在検討しているのは、自治大学校で実施する研修において、中級から上級程度のレベルを対象とし、都道府県や政令指定都市の職員を主な対象として実施することである。そして来年度からは、市町村アカデミーや全国市町村国際文化研修所（JIAM）において、初級から中級程度のサイバーセキュリティ人材を育成していくことを考えている。このように対象者ごとに役割を整理しながら研修を実施していきたいと考えている。さらに、将来的にはそこで蓄積した教材やノウハウを活用し、都道府県の研修所など、各地にある研修施設でも活用していただくことを考えている。また、NICT が実施している CYDER という実践的なサイバー防御演習についても、地方公共団体向けの受講枠を一層充実させることができるよう、総務省サイバーセキュリティ統括官室とも協議を進めているところ。

→　DX への対応もあるし、最近は AI が前面に出てきているため、それらに対応するだけでも大変な状況である。しかしながら、やはりセキュリティが全ての基盤にあると考えている。いわゆるセキュリティ・バイ・デザインという考え方であるが、何かを始める際には、最初からセキュリティを十分に考慮した上でサービスやシステムを設計していくことが重要。そのため、そのような問題意識や知識、能力をしっかりと高めていくことが必要である。先ほど、NICT の CYDER についての説明もあった。CYDER については非常に評価が高いと聞いており、地方公共団体の職員も多く参加しているところである。そのため、そのような取組についても拡充していく方向で、総務省全体としてはもちろんのこと、先ほど申し上げた NCO も含めて、国として地方公共団体をしっかり支援していただければありがたい。

→　地方公共団体に新たに発生する事務としては、基本的には利用申込みを行うこと程度であり、その後、脆弱性が発見された場合には当然ながら必要な対応が発生するものの、このシステムに関連して新規に発生する事務としては、それが主なものと考えてよいのか。というのも、おそらく NCO と各省との関係と同様に、今回は総務省、J-LIS と都道府県、市町村との関係になるものと理解している。お話を伺っている限りでは、特に業務の進め方のばらつきを是正したり、既存業務を平準化・標準化したりするといった対応は、特段必要ないようにも思われた。そこで、国における運用経験を踏まえた場合、そのような業務の平準化や標準化といった対応が必要となるのかどうかについて、確認させていただきたい。

・　地方公共団体側で利用団体として発生する事務は、まず利用申込み、それからドメイン名入力、この 2 つを事前の準備段階で行っていただくことになる。それを実施すると、それ以外については地方版 ASM 側でスキャンを実施し、脆弱性情報を提供していくこととなる。また、緊急度の高い脆弱性が発見された場合には、保守事業者に対して、脆弱性への対応依

頼を行う必要が生じる。そのため、全体としては低負担な仕組みであり、地方公共団体において新たに煩雑な事務が数多く発生するものではないと認識している。

④地方版アタックサーフェスマネジメント（ASM）システムの共通化を進める上で、どのような課題が考えられますか。

・　共通化を進める上での課題であるが、現在、大きく 3 つあると考えている。

・　1 つ目は、脆弱性診断、そもそもこの ASM システムそのものの理解促進と醸成をどのように行うかということである。おそらく地方公共団体の皆様からすると、このシステムが一体何のためにあるのかという点について、まだ十分に理解されていない面もあるのではないかと考えている。そのため、総務省としても、あらゆる機会を通じて、この脆弱性管理の重要性や、この診断の重要性、あるいは地方版 ASM を活用することの意義や効果といったものを丁寧に説明していきたいと考えている。

・　2 つ目は、セキュリティ成熟度への考慮であると考えている。当然ながら、大規模な団体になると、専門家や人材も多数おり、この地方版 ASM に求めるレベルも高くなってくると思われる。他方で、小規模な市町村になると、様々なサービスがあったとしても、そこまでの機能は過剰であり不要であるということもあるかもしれない。そのため、成熟度の異なる様々な団体が存在する中で、過剰感や不足感のないサービス提供を実現していくことも、1 つの大きな課題であると考えている。

・　3 つ目は、継続的な機能改善であると考えている。高性能 AI が登場しており、これが仮に悪用された場合には非常に大きな脅威になるという指摘がある。サイバーセキュリティをめぐる環境は刻一刻と変化しており、その変化のスピードも非常に速いことから、今年構築した機能が来年もそのままでよいということには、おそらくならないと考えている。そのため、NCO との連携も含めて、継続的に機能を改善していくことにも配慮していきたいと考えている。

→　本システムは全ての地方公共団体が利用できる仕組みとのことであるが、現時点ではあくまで利用可能という位置付けであると理解している。しかし、将来的には全ての地方公共団体に利用していただいた方が望ましい取組でもあると思う。そのため、今後、努力義務のような形で利用を促していく可能性があるのか。

・　地方自治法施行規則の改正によりサイバーセキュリティに関する情報収集を実施することを義務付けているが、この脆弱性診断について、地方版 ASM システムを利用しなければならないという義務を課しているわけではない。そのため、利用するかどうかはあくまでも各団体の裁量によるものである。しかしながら、個別に実施するよりも、低負担で共通的に利用できる本システムを活用する方が合理的であると考えているため、我々としてはあらゆる機会を通じて地方公共団体に対する周知・広報を行っていきたいと考えている。

→　脆弱性が判定された後の対応が重要であると考えている。地方公共団体や保守事業者においても、脆弱性が発見されれば、その都度パッチ適用等の対応を行わなければならず、運用管理に係る負担は非常に大きくなると思われる。そのため、ASM の利用料という入口部分に対する財政措置も重要であるが、それによって発見された脆弱性に対応するための地方公共団体側の取組についても、財政措置をしっかり考えていかなければならないのでは

ないかと思う。特に標準財政需要額の中で適切に評価していかなければ、今後その負担はかなり増加するのではないかと考えている。また、最終的には AI によって発見されたセキュリティ上の脆弱性に対応するためには、AI を活用して対処していく必要が生じる可能性もあり、どの水準まで対応するのかという議論にも関わってくると思う。

・　高性能 AI の活用によって脆弱性が大量かつ高速に発見される可能性がある。ただし、発見された脆弱性の全てに対応しなければならないというものではないと NCO からも聞いている。そのため、優先順位を付け、特にクリティカルなものや緊急性の高いものから順次対応していくことが重要であると考えている。そうした観点から、優先順位付けをしっかり行っていきたいと考えている。もっとも、脆弱性への対応に伴い、様々な費用が発生する可能性はある。その点については、地方交付税措置の対象とすることができるかどうかについて、自治財政局との調整を進めていきたい。

→　優先順位付けというのは、CVSS のことを指しているのだと思う。これは、全ての脆弱性に対応するというよりは、そのスコアリングシステムを活用し、重要度に応じて対応していくという考え方であると理解している。また、それ以外にも、既に悪用されている脆弱性であるのか、あるいは近い将来に悪用される可能性がどの程度あるのかといった情報もあると思う。そうした情報については、様々な機関が発信しているものもあると認識している。そのような情報まで含めて対応の優先順位を決めていくとなると、地方公共団体が単独で実施することは非常に難しい面もある。そのため、NCO とも連携しながら、総務省から必要な情報をしっかりと提供していただき、まず優先的に実施すべきことを着実に進めていくことが非常に重要であると考えている。

→　低コスト・低負担との説明があったが、AI 時代に対応したセキュリティ水準を確保していくことは非常に高度な取組であり、実際には相応のコストがかかっているはずである。そのため、持続可能な仕組としていくためには、「この取組によってどのような効果が得られたのか」を可視化していくことも重要ではないかと考えている。例えば、この仕組がなければ重大なサイバー攻撃によって大きな被害が発生していた可能性がある、といった効果についても、実証事業の中でしっかり検証していく必要があると思う。そして、その結果を地方公共団体に示し、「これがなければこのような事態になっていたかもしれない」ということを理解していただくことで、本取組の必要性を実感していただけるような取組を進めていくことが重要ではないか。

・　「評価レポート通知」として月 1 回程度、マンスリーレポートを提供することを考えている。具体的には、どのような脆弱性が発見されたのか、また、その脆弱性に対してパッチを適用することによってどのようなリスクを防止できたのかといった効果も含めて、地方版 ASM の価値や効果を全利用団体に発信していきたいと考えている。また、自団体で特に脆弱性が見つからなかったから問題ないということではなく、他団体においてどのような事例があったのか、どのようなリスクが確認されたのかといった情報についても共有していきたいと考えている。さらに、NCO から提供される脅威情報についても共有しながら、利用団体にとって有意義な仕組みとなるよう取り組んでいきたい

以上