自治体におけるAIの利用に関するワーキンググループ（第４回）　議事概要

開催日時：令和７年５月16日（金）１３：００～１５：００
開催場所：中央合同庁舎２号館９階903会議室　※ＷＥＢ会議と併用
出席者：須藤座長、板倉構成員、大竹構成員、越智構成員、北村構成員、喜連川構成員、成原構成員、箱丸構成員、堀之内構成員、横田構成員
事務局：阿部自治行政局長、君塚行政経営支援室長ほか
オブザーバー：全国知事会、全国市長会、全国町村会、指定都市市長会、デジタル庁

【議事次第】
1. 開会
2. 生成 AI の利活用における要機密情報・個人情報の取扱いについて（資料１）
3. 個人情報保護法における規律について（資料２）
4. 意見交換
5. 行政通則法的観点からの AI 利活用調査研究会の検討状況について（資料３）
6. 報告書の構成（案）について（資料４）
7. 意見交換
8. 閉会

【議事概要】
事務局及び個人情報保護委員会事務局から資料に沿って説明。その後、意見交換を実施。

【資料１及び資料２について意見交換】
○　それ単体では特定の個人を識別できないような情報を、生成AIの学習に利用せず、かつ、データの保存先が国内サーバであるような仕様であれば、生成AIにそれ単体で個人を識別できる情報を入力しても問題ないと考える。デジタル庁が策定を予定する「行政の進化と革新のための生成AIの調達・利活用に係るガイドライン」も同様の考え方に立っていると認識している。

○　多くの自治体に参照されている「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」は、国の定める「政府機関の情報セキュリティ対策のための統一基準」の改定等を踏まえて改定されてきた経緯がある。そのため、同ガイドラインに、注意点を十分記載した上で、個人情報を生成AIに入力することもできるという旨を記載すべきであると考える。ガイドラインに記載することが難しいということであれば、本ワーキンググループの報告書に記載する対応も一案と考える。

○　本自治体では、AI の活用等に関する条例を制定しているが、セキュリティポリシーの上位の規定として制定したものではない。生成 AI を含む AI の利活用を推進する方針や、市長が安全性を認めた場合には要機密情報の生成 AI への入力を認める等の運用ルールを市民に示すことを意図したものである。国と同じ方向を向いていると認識しており、国の方針に対する違和感はない。

○　個人情報は、「政府機関等のサイバーセキュリティ対策のための統一基準」に照らすと機密性２に分類され、「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」に照らすと、自治体機密性３B・３C に分類される。国の基準で、機密性２情報に該当する情報は、自治体機密性３B・３C 情報及び自治体機密性２情報に分類されるため、自治体機密性２情報と、自治体機密性３B・３C 情報を分けて検討する必要があると考える。

○　個人情報が含まれているか否かは比較的判断がつきやすい一方で、自治体機密性２情報と自治体機密性１情報の区別について、判断に悩む自治体職員がいると考える。判断に悩む場合、安全側の選択肢を取り、生成 AI に入力できる情報の範囲を狭く捉えると見込まれる。その結果として、生成 AI の有用性が低く認識されることがあると考える。

○　行政機関は目的外に個人情報を利用することはできない。また、仮名加工情報や匿名加工情報の作成に係る個人情報保護法の規定が、行政機関等には適用されていない。AI の開発のためであれば、クローリングにより要配慮個人情報を収集しても問題ないのではないかという議論の結果が、行政機関が生成 AI に個人情報を入力して問題ないという結論に直接的にはつながらないと考える。

○　個人情報保護法の見直しに関する論点のうち、「統計情報等の作成にのみ利用されることの担保等を条件に本人同意なき個人データ等の第三者提供を可能としてはどうか」、「行政機関等の保有個人情報について、利用目的以外の目的のための提供に係る例外規定の対象を、AI 開発等を含む「統計情報等の作成」に拡大してはどうか」といった論点は AI モデルの開発に関する論点である。先進的な自治体が AI モデルを開発する等の話でない限り、自治体にはあまり関係がないと考える。

○　「個人情報取扱事業者等からデータ処理等の委託を受けた事業者に対する規律の在り方」は、自治体を含む行政機関等に関係の深い論点と考える。例えば、生成 AI の API を利用したサービスを展開する場合、ユーザーが契約するのは API の事業者であり、API の事業者と生成 AI 事業者の情報のやり取りを監督するのは困難ではないかという議論が想定される。

○　「政府機関等のサイバーセキュリティ対策のための統一基準」では、情報公開法の不開示情報をベースに、取扱いが制限される要機密情報の内容が定められている。情報公開法で、不開示情報が定められている理由は、国の安全に関する情報、法人の営業秘密等の秘密にすべき情報が、公開されないようにするためであり、個人情報も秘密にすべき情報に含まれるものである。一方で、個人情報保護法で個人情報の取扱いについてルールが定められている理由は、情報の秘密を守るだけではなく、予め個人情報の取扱いのルールを定めることで、個人の権利・利益が侵害されるリスクを予防するためであると理解されることが一般的である。生成 AI の利用に伴う個人情報の取扱いを検討する際には、なぜ個人情報を保護する必要があるのか、という観点から検討する必要があり、自治体における機密性の分類を検討する際にも、同様にどの情報をどの理由でどの程度保護するのかを検討する必要があると考える。

○　生成 AI 利活用時の要機密情報・個人情報の取扱いに関する留意点は、クラウド利用時の留意点と重複する点が多い。これは自治体が生成 AI サービスを利用する際にはクラウド上の生成 AI を利用することが多いことを踏まえると自然なことである。一方で、生成 AI 利用に伴う固有のリスクもある。そのため、生成 AI 固有の留意事項、クラウド上で AI を利用する際の留意事項、クラウド一般についての留意事項を整理する必要があると考える。また、自治体など組織内で生成 AI のサーバを構築する場面も想定されるため、生成 AI をクラウド上で利用する場合だけでなく、オンプレミスで利用する場合の留意事項についても検討する必要があると考える。

○　生成 AI モデルの開発に個人情報を用いる際に、統計的な情報として個人情報が処理される場合もあれば、個人が識別される形で情報が処理される場合もあると考える。例えば、年齢や性別に応じて一般的な健康リスクを回答させるように生成 AI を開発・利用する場合もあれば、特定の個人の健康リスクを回答させるように生成 AI を開発・利用する場合もあり得る。生成 AI モデルの開発時の個人情報の取扱いについて、どこまでを統計作成のための利用の範囲とし、どこからを個人の権利・利益を侵害するおそれのある利用の範囲とするか整理する必要があると考える。

○　教育機関が生成 AI サービスを利用する場合でも、サービス事業者が外国にある第三者に該当せず、かつ、生成 AI が入力された情報を学習しない場合には個人情報の取扱いの委託として、又は、当初からオンプレミスで生成 AI を開発、利用するような場合には、学習をしたとしても、そもそも個人情報の第三者への提供（委託を含む）が発生しないので、個別に学生から個人情報の利活用について同意を得る必要はないと考える。

○　最近の生成 AI では、回答の論拠となる情報を明示できるような仕様となっているものもある。今後、生成 AI のアプリケーションは、論拠の説明を根深く行おうとすると、最終的には個人情報が含まれる情報に行きつくような仕様に変容していくことが考えられる。生成 AI の進化の速度は速いため、現在の生成 AI の状況よりも将来を見据えて検討する必要がある。

○　医療の場面において、画像認識 AI を用いて適切なフィードバックを患者に行うには、膨大な症例を解析する必要がある。生成 AI の利活用に伴う情報の取扱いは、利用場面や分野ごとに異なるため、それに応じて検討する必要がある。

○　日本語の LLM の開発が進められている中で、今後は行政に特化した LLM の開発も見込まれる。行政に特化した LLM の開発にあたり、学習させる情報の中に個人情報が含まれている場合についての議論も必要になると考える。

○　今後、RAG の情報をどのように守るのかの議論も必要となると考える。プロンプトインジェクションによって、機密情報が漏洩することを防ぐ必要がある。地域コミュニティの重要性が高まっている中で、LLM に入力された情報を自治体単位でどのように保護するかが重要になると考える。

○　生成 AI の利活用に関するルールが未策定であると、自治体における生成 AI の利活用は進まない。どのようなルールやガイドラインを策定する必要があるかについては、本ワーキンググループに留まらず、行政通則法的観点からの AI 利活用調査研究会等とも連携して議論を深めていく必要があると考える。

【議事概要】
行政管理局及び事務局から資料に沿って説明。その後、意見交換を実施。

【資料３及び資料４について意見交換】
○　本ワーキンググループの報告書の構成案は、基本的には提示されたもので問題ないと考えるが、ガイドラインの見本や参考例を付すことで、より自治体が参考にしやすいものとなると考える。また、国民にとっても、今後、どのようなガイドラインができていくのか、わかりやすいと考える。

○　本自治体では、内製した文字起こしツールで、自治体機密性３B 及び自治体機密性３C に相当する情報を処理しても問題ないという見解で運用を進めている。一方で、自治体機密性３B・３C にあたる情報を、RAG で参照できるようにするために、クラウドサービ

スに格納することは現状認めていない。自治体での RAG の活用を広げるためにも、本ワーキンググループの報告書には個人情報等が含まれる情報の取扱いについて踏み込んだ表記が求められる。

○　本ワーキンググループの報告書の構成案は、自治体における生成 AI の利活用を推進する内容となっており、基本的に問題ないと考える。生成 AI 利用時の留意点等を記載する際には、難解な表現や留意点を多数列挙することは、生成 AI の利活用の推進につながらないため、なるべく避けるように留意いただきたい。令和６年度に DeepSeek が公開された際の総務省から発出された通知のように、留意すべき事項が出てきたら適宜通知を発出する等の対応も含めて、生成 AI の利活用を推進していただきたい。

○　RAG について、検索するデータベースをローカルネットワーク上とクラウド上のいずれに置くかという点や、クラウド上に置く場合であっても、クラウドが国外にあるのか国内にあるのかでセキュリティの対応が変わってくる。また他にも、LLM をダウンロードしてローカルネットワーク内で運用する場合や、LLM が既にスマホやパソコンなどの媒体に搭載されている場合のセキュリティの対応も検討する必要がある。全てのセキュリティ上の対応を本ワーキンググループの報告書に網羅的に記載することは現実的ではないが、体系的にわかりやすく説明できる内容が求められる。

（以上）