資料１

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）

事務局提出資料

令和７年５月
総務省

本ワーキンググループの進め方

1月 23日	第１回ＷＧ	・キックオフ（WGの目的、趣旨、進め方など）
3月 5日	第２回ＷＧ	・実際のユースケースや自治体への聞取り等を踏まえ、業務効率化等が見込める業務や導入・利用に当たっての課題等を議論
4月 18日	第３回ＷＧ	・政府におけるルール策定等の動向等を踏まえつつ、地方公共団体のAI利用に当たっての留意事項やリスク管理等を議論
5月 16日	第４回ＷＧ	・政府の取扱い等を踏まえた、AIを利用する上での要機密情報・個人情報の取扱いにおける留意点について議論 ・個人情報保護法における規律といわゆる３年ごと見直し規定に基づく検討状況について個人情報保護委員会から報告 ・「行政通則法的観点からのAI利活用調査研究会」の議論状況を行政管理局から報告
6月	第５回ＷＧ	・生成AI以外の従来型AI等を活用した自治体業務効率化について議論 ・第４回WGまでの議論を踏まえ、論点の整理や報告書の骨子など、報告書のとりまとめに向けて議論
7月	第６回ＷＧ	**報告書案について議論**

１．要機密情報（特に個人情報）の取扱いについて

政府が取り扱う情報の機密性の分類と個人情報の位置づけ

○ 「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（令和５年度版）」（以降、「統一基準」）において国の業務で取り扱う情報は、**機密性１～３情報の３段階に格付け**されている。

○ 個人情報は、不開示情報（**個人に関する情報で特定の個人を識別できるもの**等）に該当するため、**機密性２情報**となる。

「統一基準」（令和6年7月24日一部改定）を基に事務局において作成

分類	分類の基準又は例
機密性３	極秘文書：秘密保全の必要が高く、その漏えいが国の安全、利益に損害を与えるおそれのある情報を含む行政文書 秘文書：極秘文書に次ぐ程度の秘密であって、関係者以外には知らせてはならない情報を含む極秘文書以外の行政文書
機密性２	国の行政機関における業務で取り扱う情報のうち、行政機関の保有する情報の公開に関する法律（平成11年法律第42号。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報 情報公開法　第５条 行政機関の長は、開示請求があったときは、開示請求に係る行政文書に次の各号に掲げる情報（以下「不開示情報」という。）のいずれかが記録されている場合を除き、開示請求者に対し、当該行政文書を開示しなければならない。 一　**個人に関する情報**（事業を営む個人の当該事業に関する情報を除く。）**であって、当該情報に含まれる氏名、生年月日その他の記述等**（文書、図画若しくは電磁的記録に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項をいう。次条第二項において同じ。）**により特定の個人を識別することができるもの**（他の情報と照合することにより、特定の個人を識別することができることとなるものを含む。）又は特定の個人を識別することはできないが、公にすることにより、なお個人の権利利益を害するおそれがあるもの。ただし、次に掲げる情報を除く。
機密性１	国の行政機関における業務で取り扱う情報のうち、情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報

地方公共団体が取り扱う情報の機密性の分類と個人情報の位置づけ

「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」（令和7年3月28日改定） に基づき事務局作成

国	自治体	情報資産	パブリッククラウドサービスの範囲
機密性３	自治体機密性３Ａ	極秘文書：秘密保全の必要が高く、その漏えいが国の安全、利益に損害を与えるおそれのある情報を含む行政文書 秘文書：極秘文書に次ぐ程度の秘密であって、関係者以外には知らせてはならない情報を含む極秘文書以外の行政文書	「行政文書の管理に関するガイドライン」、統一基準の規定に則って取り扱うものとする（なお、上記ガイドラインにおいては、極秘文書について、インターネットに接続していない電子計算機又は媒体等に保存することが求められている
機密性２	自治体機密性３Ｂ	データベースや台帳形式になった**住民情報を含む個人情報ファイル**及びこれに準ずる情報（住民記録システム、税務システム、国民健康保険システム、生活保護システム、農業委員会台帳システム、貸付金償還システム等に保存される住民の個人情報）	**ISMAP登録サービスは利用可**（8.3で規定されるアクセス制御、機密性保護のための暗号化等が必要） ※統一基準改定に合わせて、8.3でクラウドサービスの利用について規定 注）自治体機密性３C情報については、情報資産単位でのアクセス制御、業務システムログ管理の実施等、β’モデルにおいてインターネット接続系に求められている対策を実施することで、インターネット接続系における取扱いが可能。
	自治体機密性３Ｃ	・**職員としての属性に基づく個人情報** ・オンライン申請の処理等により、システム処理上**一時的にインターネット上に保管されるデータ** ・文書管理システムの**決裁文書として保存されている個人情報** ・施設設計情報や入札予定価格など非公開情報	
	自治体機密性２	・政策検討に関する情報	可（8.3で規定されるアクセス制御、機密性保護のための暗号化等が必要）
機密性１	自治体機密性１	・公表された情報 ・将来公表する予定の文書（白書の案等）	可

地方公共団体における要機密情報の入力に係る考え方

○　「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」（以降、「セキュリティポリシーに関するガイドライン」）では、**自治体機密性２以上の情報を取り扱う場合のクラウドサービスの利用のルールとして、**取り扱う情報の格付け及び取扱制限を踏まえた検討・選定を求め、**セキュリティ対策・要件として目的外利用の禁止及び情報が保存される国・地域に言及**している。

○　また、**約款型クラウドサービスへの自治体機密性２以上の情報の取扱いを原則不可**としている。

「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」（令和7年3月28日改定）　抜粋

8.3. 外部サービス（クラウドサービス）の利用（**自治体機密性２以上の情報を取り扱う場合**）

＜情報セキュリティ対策基準（例文）＞

（３）クラウドサービスの選定

①情報セキュリティ責任者は、**取り扱う情報の格付及び取扱制限を踏まえ**、クラウドサービス利用判断基準に従って、**業務に係る影響度等を検討した上でクラウドサービスの利用を検討**しなければならない。

②情報セキュリティ責任者は、**クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ**、クラウドサービス提供者の選定基準に従って**クラウドサービス提供者を選定**すること。また、以下の内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件に含めなければならない。

（ア）クラウドサービスの利用を通じて本市が取り扱う情報のクラウドサービス提供者における**目的外利用の禁止**

～（略）～

④情報セキュリティ責任者は、クラウドサービスの利用を通じて本市が取り扱う**情報の格付等を勘案し、必要に応じて以下の内容をクラウドサービス提供者の選定条件に含めなければならない**。

（ア）情報セキュリティ監査の受入れ

（イ）サービスレベルの保証

～（略）～

次ページへ続く

地方公共団体における要機密情報の入力に係る考え方

⑦情報セキュリティ責任者は、**取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め**、クラウドサービスを選定しなくてはならない。また、クラウドサービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めなければならない。【推奨事項】

⑧情報セキュリティ責任者は、クラウドサービスの特性を考慮した上で、クラウドサービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、以下を全て含むセキュリティ要件を定めなければならない。

～（略）～

(イ)クラウドサービスで取り扱う**情報が保存される国・地域**及び廃棄の方法

～（略）～

8.3. 外部サービス（クラウドサービス）の利用（**自治体機密性２以上の情報を取り扱う場合**）

＜情報セキュリティ対策基準（解説）＞

【趣旨】

なお、事業者等が**不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となるクラウドサービス**（ただし、電気通信サービスや郵便、運送サービス等は除く）**では**、セキュリティ対策やデータの取扱いなどについて自組織への特別な扱いを求めることができない場合が多く、自治体機密性２以上の情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、**原則として自治体機密性２以上の情報を取り扱うことはできない。**

政府における生成AIの業務利用について

○　政府における生成AIの業務利用については、「ChatGPT等の生成AIの業務利用に関する申合せ」にて考え方を示した。また、自治体に対しても、「セキュリティポリシーに関するガイドライン」において、生成AIを含む外部サービスの利用について「統一基準」のクラウドサービスの選定・利用と同様の対応を求めている旨を通知したところ。

○　今般、上記申合せに代わるものとして、「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」を策定予定。

以下、事務局にて「ChatGPT等の生成AIの業務利用に関する申合せ（令和５年５月８日）」等の内容を抜粋

ChatGPT等の生成AIの業務利用に関する申合せ（令和５年５月８日）

（１）　約款型クラウドサービスによる生成AI の業務利用関係

・現在のChatGPTは約款型外部サービスに区分されるサービスであること
・約款型クラウドサービスでは、原則として要機密情報を取り扱うことはできないこと
・利用に当たっては、組織の規程に則り承認を得る手続きが必要であること
について職員等に対して周知

（２）　約款型クラウドサービスでない形態による生成AI の業務利用

・非約款型外部サービスの生成AI利用を検討する場合は、検討状況を「AI戦略チーム」に報告し、了解を得ること

ChatGPT 等の生成AI の業務利用に関する申合せ（第２版）（令和５年９月15日）

（２）　約款型クラウドサービスでない形態による生成AI の業務利用

関係省庁においては、
・サービスにおいて生成AI を利用していることの明示
・生成AI の出力結果を二次利用する場合の責任の明確化
・一般利用者を対象とする場合は検証段階であることの明示とテスト参加の同意の取得等について対応し、
「AI 戦略チーム」の了解及び組織規定上の利用承認を得たうえで一部の機密性２情報まで取り扱うことができる

※なお、第2.1版（令和７年３月25日）によって、報告先等が「AI戦略チーム」から「AI 戦略推進関係省庁会議幹事会」に変更された。

AI戦略チーム事務局への確認結果（令和５年11月13日）

○　機密性２情報の範囲については、機密性２情報のうち適切なリスク分析を行った情報であり、例えば、以下の業務等に利用することを想定。
- 将来の公表を予定している文書（想定問答、白書等）の下書きの作成
- 国際会議（公開されるもの）における情報収集、翻訳、提案の下書きの作成
- 自治体職員からの質問に対する回答案の作成
- 技術文書の作成、ソフトウェア開発運用保守、インフラ構成管理の支援

政府における生成AIと要機密情報・個人情報の取扱いルール

○　政府において検討している「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」（以降、「ガイドライン」）においては、以下のとおり記載されている。

「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群」、「IT調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」、「個人情報の保護に関する法律についてのガイドライン（行政機関等編）」等の政府情報システムに係るガイドラインを遵守することが必要である。

要機密情報を取り扱うクラウドサービスを調達する場合においては、政府情報システムのためのセキュリティ評価制度（ISMAP：Information system Security Management and Assessment Program）の原則利用の考え方に基づき、原則としてISMAPクラウドサービスリスト又はISMAP-LIUクラウドサービスリストから選定した上で、別途、本ガイドラインによる対応を行う必要がある。

○　また、ガイドライン案では、府省毎に生成AIの利活用ルールの策定を求め、ルールのひな形を示している。
　具体的には、**約款型では要機密情報を原則取り扱わない**ことや国外サーバの場合の留意点、**個人情報については利用目的のための必要最小限の利活用又は提供であることを確認**することなどが示されている。
○　さらに、「調達チェックシート」では、個人情報、プライバシー、知的財産を取り扱う場合は、「**生成AIシステムにおいて取得・処理・保存する個人情報について適切な取扱いが確保**されるとともに、知的財産とプライバシーが保護される状態としていること」が要求されている。

＜参考：上記のガイドラインの改定状況など＞
- 「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群」（令和５年度版）（令和５年７月４日　令和６年７月24日 一部改定）
- 「IT調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（平成30年12月10日関係省庁申合せ(令和７年４月１日一部改正が最新)）
- 「個人情報の保護に関する法律についてのガイドライン（行政機関等編）」（令和4年1月（令和7年4月一部改正））
- 政府情報システムのためのセキュリティ評価制度（ISMAP：Information system Security Management and Assessment Program）については、令和２年６月から運用が開始されたもの。

次ページへ続く

政府における生成AIと要機密情報・個人情報の取扱いルール

ガイドライン中の「〇〇省 生成AI システム利活用ルール（ひな形Ver1.0）（パブコメ開始時点(2025/3/28)版）」（抜粋）

（１）利活用前のルール

●**不特定多数の利用者に対して提供**され、かつ**定型約款や規約等への同意のみで利用可能となるクラウドサービス型の生成AIシステム**を業務で利活用する場合には、**原則として要機密情報を取り扱わない**こと。 ～（略）～ また、要機密情報を取り扱わない場合であっても、例えば、**国外にサーバ装置を設置している場合は、現地の法令が適用され、現地の政府等による検閲や接収を受ける可能性がある**ことに留意すること。

（２）利活用中のルール

① 入力データ又はプロンプトにおけるルール

●生成AIシステムに個人情報を含むプロンプトを入力する場合には、事前に当該生成AI システムへの入力の可否を確認の上、当該**個人情報の利用目的のための必要最小限の利活用又は提供であることを十分に確認**すること
（例：〇〇省のプライバシーポリシーや生成AI システムの提供者が定める利活用ルールを確認し、問題がないかを判断したうえで利活用、判断が付かない場合は個人情報を含まないプロンプトとする。）。

●行政機関等が、生成AI システムに保有個人情報を含むプロンプトを入力し、**当該保有個人情報が当該プロンプトに対する応答結果の出力以外の目的で取り扱われる場合、**当該行政機関等は個人情報保護法の規定に違反することとなる可能性がある。そのため、このようなプロンプトの入力を行う場合には、当該生成AIシステムを提供する**事業者が、当該保有個人情報を機械学習に利活用しないこと等を十分に確認**すること。

ガイドライン中の「調達チェックシート（パブコメ開始時点(2025/3/28)版）」（抜粋）

分類	評価・選定時の項目の分類	要求事項
生成AIシステムの基本機能要件	個人情報、プライバシー、知的財産を取り扱う場合は基本項目として適用	生成AIシステムにおいて取得・処理・保存する個人情報について適切な取扱いが確保されるとともに、知的財産とプライバシーが保護される状態としていること

地方公共団体における機密性分類及び生成AI活用の考え方(事例)

○　神戸市においては、「セキュリティポリシーに関するガイドライン」の令和６年10月２日改定による先述の５段階の**機密性分類基準の見直し**を受けて、「神戸市情報セキュリティ対策基準（第5.10版）」（令和7年4月1日施行）の改定が行われている。

「神戸市情報セキュリティ対策基準（第5.10版）」（令和7年4月1日施行）抜粋

4.1.1　機密性

分類	分類基準
自治体機密性3A	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成 23 年４月１日内閣総理大臣決定）に定める秘密文書に相当する。
自治体機密性3B	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産 （例えば下記のデータが考えられる。なお、次のデータだけではなくそれらが含まれる電磁的記録媒体、パーソナルコンピュータ、システム等も同様） ・特定個人情報に関するデータ ・保有個人情報に関するデータ（出版、報道等により公知の情報を除く。）
自治体機密性3C	行政事務で取り扱う情報資産のうち、自治体機密性 3B 以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産 （例えば下記のデータが考えられる。なお、次のデータだけではなくそれらが含まれる電磁的記録媒体、パーソナルコンピュータ、システム等も同様） ・法令の規定により秘密を守る義務を課されているデータ ・部外に知られることが適当でない法人その他団体に関するデータ ・部外に漏れた場合に行政の信頼を著しく害する可能性があるデータ ・公開することでセキュリティ侵害が生じる可能性があるデータ

地方公共団体における機密性分類及び生成AI活用の考え方(事例)

○　また、条例において、**安全性が確認された生成AIに対して、特別の定めをすることにより、要機密情報(個人情報含む)の入力を可能とする**規定を設けている。

○　現時点においては、要機密情報を入力できるとする「別に定める場合」はない。

神戸市におけるAIの活用等に関する条例

（生成AI等を活用する場合の責務）

第７条 市長は、**安全性が確認されたものとして別に定める場合を除き**、本市の機関等（ 本市又は本市の機関（ 議会を除く。） をいう。） の**職員が職務上知り得た情報のうち神戸市情報公開条例**（平成13年７月条例第29号）**第10条各号に掲げる情報を含む指令**を、**生成AIその他これに類するもの**（以下「生成AI等」という。）**に対して与えない**よう措置しなければならない。

○神戸市HPより（抜粋）

公開しないことができる情報

（神戸市情報公開条例第10条各号該当）

- **個人のプライバシーに関する情報**
- 法人等の正当な利益を害するおそれがある情報
- 人の生命、身体、健康の保護、生活の安全の確保に支障が生じると認められる情報
- 意思決定の中立性等が不当に損なわれるおそれがある情報
- 事務事業の適正な遂行に支障をおよぼすおそれがある情報
- 法令や条例により公開しないこととされている情報

本WGにおいて示されている要機密情報・個人情報の取扱いに係る意見

要機密情報・個人情報に係る制度改正について

○　個人情報については、その内容に応じた管理・共有の在り方を改めて検討する必要があると考える。特定の個人が不利益を被る事態は避けなければならないが、テクノロジーの発展や社会環境の変化が進んでいることを踏まえて、個人情報の取扱いを考え直す必要がある。個人情報保護法改正の話をこの研究会のアウトプットに入れるかどうかは別として、議論の前提として法律の課題があるということは取り上げる必要がある。

○　機密情報や個人情報の取扱いに慎重にならざるを得ないという議論があったが、アメリカにおいて、ケースワーカーを支援するシステムで個人情報を利用している事例がある。法規制や自治体の権限は日本とアメリカで異なるものの、機密性の高い情報の取り扱いを積極的に行う姿勢は参考になると考える。

個人情報の利用目的の整理について

○　個人情報の保護の目的は、単に個人情報の機密性を守るということではなく、その不適切な利用により、本人に不利益な判断や差別が生じないようにするためとも考えられる。こうした目的の理解の仕方により個人情報の保護の範囲が変わることを踏まえた上で、公益の観点から生成AIに個人情報を学習させることの可否について、検討する必要があるのではないか。

○　個人情報保護条例が個人情報保護法の行政基幹部分に移管されたことにより、条例でこれまで示されてこなかった解釈が、国により示すことができるようになった。目的規定の範囲外で、個人情報や機密性情報を含む可能性のある情報を生成AIに入力することについて、どこかで立法上の措置が必要か検討する必要がある。

○　当団体では、生成AIに個人情報を入力しないことを前提としているが、仮に先のような話になれば、所管を越えたデータベースを作成し、住民からの個別具体的な事案に係る相談について生成AIで適したサービス案を提示するなど、新たな活用が可能となる側面もあるかと思う。現状、個人情報を目的外利用するためのハードルが高いため、新たなルール作りがなされるのであればありがたい。

個人情報の匿名情報化について

○　令和２年の個人情報保護法の改正により、民間事業者については、仮名加工情報制度が創設されたことで、仮名加工した情報をマーケティング等に利用できることとなった。一方で、行政機関には仮名加工情報制度がない。行政情報の庁内における統計利用を進めるために、行政機関の仮名加工情報制度を創設してもよいのではないか。

個人情報保護委員会から現行法制について
（報告）

本WGにおける要機密情報・個人情報の取扱いに係る議論から考えられる論点

本WGにおける要機密情報・個人情報の取扱いに係る議論から考えられる論点

【論点①】 生成AIの利活用にあたり要機密情報・個人情報を扱うことについてどう考えるか。

要機密情報・個人情報を扱わない範囲でのAI活用について

○ 第３回検討会で示した「自治体における生成AI導入状況調査（速報版）（令和６年12月31日現在）」において
・利活用の実態として、あいさつ文の作成、議事録作成、企画書案の作成等の汎用的な利用が上位を占めている
・そうした利用においても、一定の定量的効果が確認されている

要機密情報・個人情報の扱いに係る不安について

○ 第３回検討会で示した自治体における生成AI導入状況調査（速報版）（令和６年12月31日現在）」において、生成AI導入における課題として「要機密情報流出の懸念がある」という回答が、前回に引き続き上位に挙げられている。

○ AIに入力できる機密情報について、自治体担当者は、国よりも厳格に捉えている実感がある。他方で、機密性２情報を入れないと仕事に使えない。それでも、個人情報を入れることは、はばかられる。

○ 本自治体では、データ処理が国内で完結する仕組みで生成AIを利用している。また、入力データは学習に利用されないようにするとともに、RAGが参照するデータベースは庁舎内のサーバに置いている。このように、万全のセキュリティ対策を講じている。一方で、機密性２以上の情報を生成AIに入力しても問題ないのかの判断がつかないため、機密性２以上の入力は禁止している。自治体でも共通のアドバイザリーボードに相談できるのが理想ではあるが、現実的には難しいため、庁内における体制も含めた生成AI利活用のルールのひな形を示していただきたい。

AI活用において要機密情報・個人情報を扱うことの有効性について

○ 氏名等を黒塗りにしても、元の情報を削除したわけではなく、明らかに元の情報と容易照合可能であって、個人情報に該当する。基礎自治体の持つ情報は、ほとんどが個人情報を含むものであり、また、個人情報の該当性は提供元で判断するため、個人情報を生成AIで取り扱うことを一律に禁止する場合、自治体は生成AIを十分に活用できない。

（考え方）

◆ 生成AIにおいて要機密情報・個人情報を入力することに伴う流出リスクへの懸念や不安があることを理由にAIそのものの導入や利用の検討を行わないことは行政効率化の機会を逃していると言えないか。

◆ 要機密情報・個人情報の扱いに係る不安や漏洩リスク等といった課題への対応を講じた上で、AIの恩恵を受けられるよう適切な活用を進めていくべきではないか。

本WGにおける要機密情報・個人情報の取扱いに係る議論から考えられる論点

【論点②】 生成AIの利活用にあたり要機密情報・個人情報を扱う際の留意点をどのように示していくべきか。

○ 生成AIを利用する際は、一般的に、海外の事業者の基盤モデルをAPI連携で利用することになる。これは、個人情報保護法において、個人情報の取扱いの委託として整理されるが、現に、個人情報を契約に基づいて委託先に渡す場合、実質的には委託先の監督ができていないという問題がある。既にこのことを前提として、委託事業者の選定などについて、セキュリティポリシーガイドラインに充実した記載がある。この考え方をベースにして、例えば、海外の生成AIのAPIなどの選び方を示すなど、安全管理措置を満たすような取組を提案することが現実的には必要なのではないか

○ 生成AIを国内事業者を介して国内サーバ上で利用し、入力データが学習に利用されない仕組みとしている場合においては、個人が特定されない個人情報を生成AIで取り扱うことを許容して良いと考える。一方で、「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、画一的な約款や規約等への同意のみで利用可能となる外部サービスでは、原則として機密性２以上の情報を取り扱うことはできない旨が示されている。「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」の記載内容を見直すか、本ワーキンググループの成果物で機密性２以上の情報を取り扱える旨を案内するかの対応が必要と考える。

（考え方）

◆ 独自に生成AIにおける要機密情報・個人情報の扱いについて条例を定めて対応する自治体も見られる一方で、全ての自治体において同様の対応がとられることは現実的ではないと考えられる。

◆ 「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」の外部サービスにおける機密情報の取扱いは、政府において、約款型サービスに関し、原則として要機密情報を取り扱うことはできない（※）ことを踏まえたもの。国と地方公共団体のネットワークがつながり多くの情報がやりとりされていることからも、政府と整合性のとれた対応を自治体に促すべきではないか。

※ 前述の「ChatGPT 等の生成 AI の業務利用に関する申合せ」、「DeepSeek 等の生成 AI の業務利用に関する注意喚起（事務連絡）」（令和７年２月６日デジタル社会推進会議幹事会事務局）、「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群」（令和5年度版）

◆ 今後総務省において策定するガイドラインにおいて、要機密情報・個人情報の扱いについても政府における取り扱いを踏まえ、自治体が参照できるよう考え方や事例を示すべきではないか。

本WGにおける要機密情報・個人情報の取扱いに係る議論から考えられる論点

【論点③】 生成AIの利活用にあたり要機密情報・個人情報を扱う際の留意点としてどのような点を示していくことが必要とが考えられるか。

要機密情報・個人情報を扱う上での調達における留意点について

○ 行政は、強制力を伴って個人情報を取得している側面があることに留意する必要はあるが、強制性に見合った安全保護措置が取られるのであれば、行政運営の改善のために個人情報を活用することが認められてもいいと考える。そのようなニーズの有無を確認し、検討を進める必要があると考える。

○ 個人情報を学習に用いず、国内サーバで処理する生成AIモデルであれば、個人情報を取扱って問題ないのではないか。

○ 生成AIで個人情報が取扱われるとしても、適切な防護措置により、情報漏洩や個人が特定され得る回答の出力を防ぐことができれば、問題は生じないと考える。個人情報について、機密であることを理由に使用をしないのではなく、職員の権利を守るという観点も含め、適切な防護措置のあり方を考えていく必要があると考える。

○ プライベートな領域に格納した庁内ナレッジに基づいて、回答を生成するような、要機密情報が外部に流出しない仕組みであれば、生成AIで個人情報を取扱っても問題は生じないと考える。

○ 非約款型で、入力データが学習に利用されず、十分なセキュリティ対策が講じられている生成AIであれば、機密性の高い情報の取扱いを可能とする余地もあると考える。法律上も、機密性２以上の情報の取扱いが禁止されているものではないと理解している。

○ 本団体では、要機密情報の生成AIへの入力ルールの緩和については、国の動向を注視しているところであり、国に先んじた対応をするところまでは進んでいない。高機能なLLMがオープンソースとして公開され、ローカル環境で完結する構成で生成AIを実装できるようになれば、検討を進められる可能性がある。ナレッジを共有できるプラットフォームが整備されると良いのではないか。

次ページへ続く

本WGにおける要機密情報・個人情報の取扱いに係る議論から考えられる論点

前ページからの続き

要機密情報・個人情報を扱う上での運用における留意点について

○ 個人情報の取扱いに対する市民の不安を解消することが課題であった。それらリスクや課題に対し、条例改正等の利用上のルール整理を早い段階で行うことで解決した。（第１回　会議資料「生成AIの導入における課題についての地方公共団体の意見」）

○ 福祉相談の相談記録表作成業務において、個人情報に当たる部分をマスキングし、生成AIに入力しないようにした上で、対面・電話による相談内容の要約などに活用。（第２回　会議資料「生成AIのユースケース例②」）

○ 情報セキュリティ対策の技術的対応として、個人情報と思われる情報を入力するとポップアップが表示される仕組みとなっている。（第２回　会議資料「生成AI導入団体へのヒアリング結果（利用に当たっての留意事項①）」）

○ 本団体では、安全性を確保した上で市長の許可で機密性２以上の入力を可能にする規定を置いている。

○ 本自治体では、生成AIガイドラインは策定していない。個人情報の入力の禁止や生成AIの生成物をそのまま利用しないこと等の留意事項をまとめた動画を視聴した職員のみに生成AIサービスのアカウントを配付する運用である。

○ 本団体では、生成AIへの個人情報の入力に係る安全性については、入力データの学習利用の有無、裁判所の管轄国、生成AIに入力されたデータの保存場所等技術的な要件を踏まえて、案件ごとに判断をしている。また、行政処分以外でリスクアセスメントの対象となる「その他市民生活に重大な影響を与えるおそれがあるもの」については、例えば具体的に申し上げると、要綱に基づく給付や、井戸水の水質検査、避難勧告等行政処分には該当しないものであっても、市民生活への影響が大きいものを想定している。

（考え方）

◆　生成AIの利活用における要機密情報・個人情報の扱いについては、「セキュリティポリシーに関するガイドライン」に沿った対応を前提として、政府における取り扱いを踏まえることになる。上記では、安全性の確保、国内サーバ、職員のリテラシーが挙げられるが、この他に、どのような留意点を示していく必要があるか。

参考資料

第３回WGにおける主な議論内容

① 自治体向けガイドライン作成の意義について

＜主な発言要旨＞

○ 各自治体において、生成AIの利用に関するガイドラインを策定しているが、その際に、どの自治体も類似する内容を検討しているように見受けられる。このことを踏まえると、政府が自治体向けに生成AIの利用に関するガイドラインのひな型を示すと良いと考える。

○ 自治体には、住民監査請求制度があるため、生成AIサービスを適正に利用しているかについて、住民から説明を求められる可能性がある。そのため、生成AIを利用する正当性をどのように説明するかのハウツー（基本的考え方及び実践例）を示す意義は大きいと考える。

② 生成AIの利用をより効率的に行うための留意点について

＜主な発言要旨＞

○ 各自治体が同じような検討をしなくても済むようにすべきである。中長期的に、生成AIサービスをガバメントクラウドの基本的な機能として搭載していくことを検討しても良いと考える。

○ 無料アカウントの数を増やすなど生成AIの利用環境を提供してもらえれば、より多くの職員が生成AIを利用できるようになると考える。

○ 省庁から発出される通知について、各自治体がデータベースに格納し、RAGを利用する前提で発出されると、自治体職員の負担はかなり軽減されると考えられる。

③ 生成AIの利用に伴うリスクへの理解について

＜主な発言要旨＞

○ 自治体が生成AIサービスを調達する際には、生成AIの利用に伴うリスクや責任の所在を明確にした上で調達することが重要であると考える。

④ ガバナンス確保のため体制構築について

＜主な発言要旨＞

○ 仮に自治体における生成AIの推進・ガバナンス体制図として、CAIOを設置するひな型が示されたとしても、小規模自治体では、誰かがCAIOを兼任する形になってしまうと考える。

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（令和５年度版）①

「統一基準」（令和6年7月24日一部改定）より抜粋

機密性についての格付の定義

格付の区分	分類の基準
機密性３情報	国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成 23 年４月１日内閣総理大臣決定。以下「文書管理ガイドライン」という。）に定める秘密文書としての取扱いを要する情報 独立行政法人及び指定法人における業務で取り扱う情報のうち、上記に準ずる情報
機密性２情報	国の行政機関における業務で取り扱う情報のうち、行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報 独立行政法人における業務で取り扱う情報のうち、独立行政法人等の保有する情報の公開に関する法律（平成 13 年法律第 140 号。以下「独法等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報。また、指定法人のうち、独法等情報公開法の別表第一に掲げる法人（以下「別表指定法人」という。）についても同様とする。 別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報
機密性１情報	国の行政機関における業務で取り扱う情報のうち、情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報

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（令和５年度版）②

「統一基準」（令和6年7月24日一部改定）より抜粋

4.2 クラウドサービス

4.2.1 クラウドサービスの選定（要機密情報を取り扱う場合）

目的・趣旨

（略）なお、民間事業者等が不特定多数の利用者に対して提供する、定型約款や規約等への同意のみで利用可能となるクラウドサービスでは、セキュリティ対策やデータの取扱いなどについて機関等への特別な扱いを求めることができない場合が多く、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として要機密情報を取り扱うことはできないため、4.2.3「クラウドサービスの選定・利用（要機密情報を取り扱わない場合）」の規定を遵守する必要がある。

「DeepSeek等の生成AIの業務利用に関する注意喚起」についての周知（令和７年２月6日）

■ 各政府機関等に対して、デジタル社会推進会議幹事会事務局より「DeepSeek等の生成AIの業務利用に関する注意喚起（事務連絡）」（令和７年２月６日デジタル社会推進会議幹事会事務局）のとおり注意喚起がなされたので周知。

「DeepSeek等の生成AIの業務利用に関する注意喚起（事務連絡）」の概要

令和７年２月３日付で個人情報保護委員会事務局より、DeepSeek 社による生成 AI サービスに関し、同社が公表するプライバシーポリシーについて中国語及び英語表記のみであることを踏まえ、以下の情報提供がされた。

① 当該サービスの利用に伴い DeepSeek 社が取得した個人情報を含むデータは、中華人民共和国に所在するサーバに保存されること

② 当該データについては、中華人民共和国の法令が適用されること

生成 AI の業務利用については、「ChatGPT 等の生成 AI の業務利用に関する申合せ」を行っている。

- 約款型サービスに関し、原則として要機密情報を取り扱うことはできない。
- 機密情報を取り扱わない場合であっても、リスクを考慮した上で利用可能な業務の範囲をあらかじめ特定し、個々の利用に当たっては、利用手続に従って、利用目的（業務内容）や利用者の範囲などの利用者からの申請内容を許可権限者が審査した上で利用の可否を決定し、その利用状況について管理することが必要

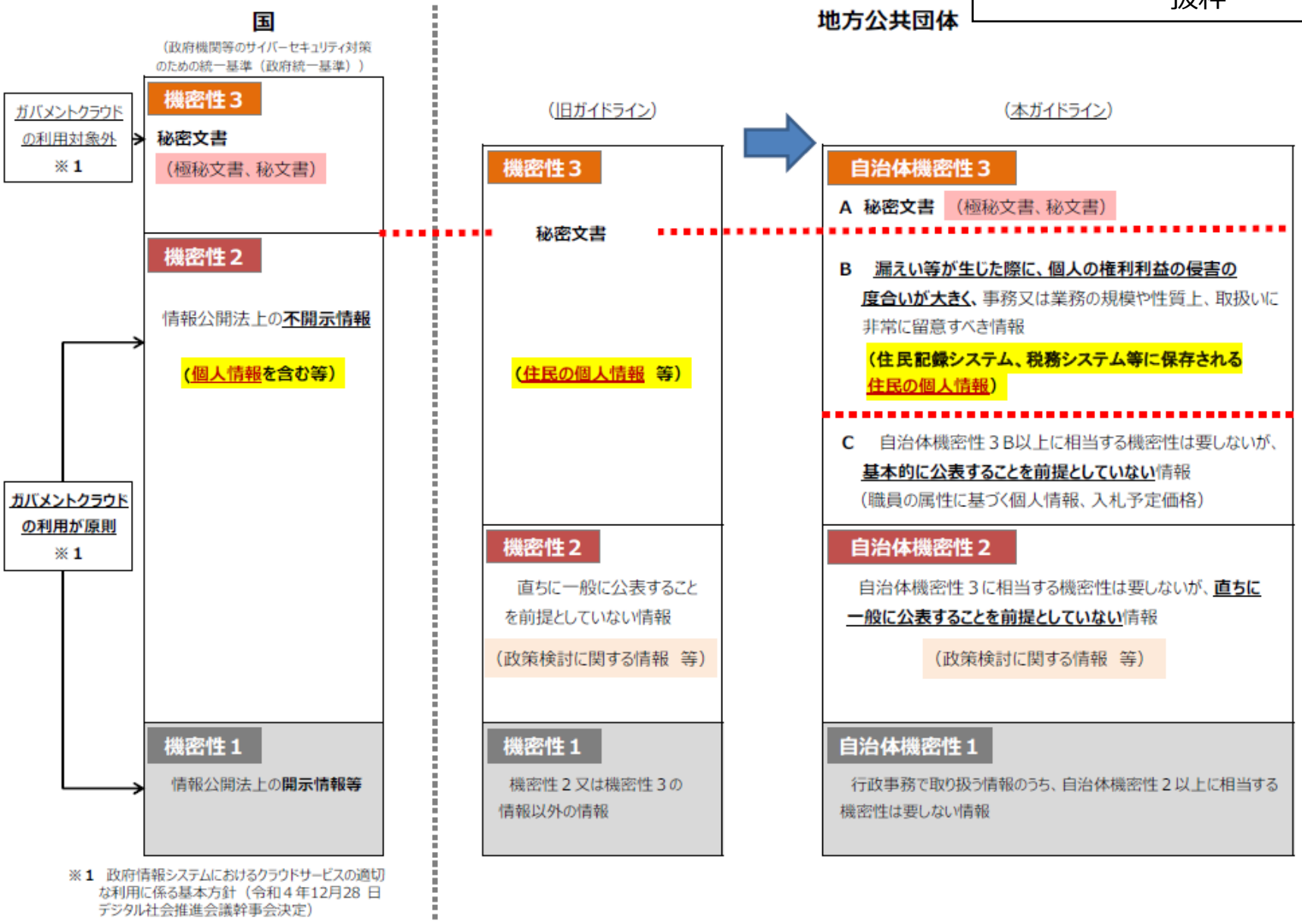
「政府機関等のサイバーセキュリティ対策のための統一基準群」においては、要機密情報を取り扱わない場合であっても、例えば、国外にサーバ装置を設置している場合は、現地の法令が適用され、現地の政府等による検閲や接収を受ける可能性があることなどが、利用の可否を判断する際に考慮すべきリスクとして例示

■ 「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」においても、外部サービス（クラウドサービス）の利用について「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」と同様の以下の対応を求めている。

- **画一的な約款等への同意のみで利用可能となるものでは機密性の高い情報を扱わない**こと
- **サービスによっては海外の法令等が適用され、現地の政府による検閲や接収を受けるリスクがある**ことに注意すること

地方公共団体における機密性の分類①

「セキュリティポリシーに関するガイドライン」（令和7年3月28日改定）より抜粋



図表 22　現行の政府機関とガイドラインの機密性分類の対応関係

地方公共団体における機密性の分類②

「セキュリティポリシーに関するガイドライン」（令和7年3月28日改定）より抜粋

機密性の分類、分類基準については、以下の情報資産の例、利用可能なパブリッククラウドサービスの範囲を参考とされたい。

機密性 高 → 低

分類	分類基準	情報資産	パブリッククラウドサービス（※１）の範囲
自治体機密性３A	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成23年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書	＜例＞ ・「行政文書の管理に関するガイドライン」上の極秘文書、秘文書に相当する文書（統一基準における機密性３情報に相当する情報） ・極秘文書：秘密保全の必要が高く、その漏えいが国の安全、利益に損害を与えるおそれのある情報を含む行政文書 秘文書：極秘文書に次ぐ程度の秘密であって、関係者以外には知らせてはならない情報を含む極秘文書以外の行政文書	「行政文書の管理に関するガイドライン」、統一基準の規定に則って取り扱うものとする（なお、上記ガイドラインにおいては、極秘文書について、インターネットに接続していない電子計算機又は媒体等に保存することが求められている（※２））
自治体機密性３B	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	＜例＞ ・データベースや台帳形式になった住民情報を含む個人情報ファイル及びこれに準ずる情報 （住民記録システム、税務システム、国民健康保険システム、生活保護システム、農業委員会台帳システム、貸付金償還システム等に保存される住民の個人情報）	ISMAP登録サービスは利用可（8.3で規定されるアクセス制御、機密性保護のための暗号化等が必要） ※統一基準改定に合わせて、8.3でクラウドサービスの利用について規定
自治体機密性３C	行政事務で取り扱う情報資産のうち、自治体機密性３B以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	＜例＞ ・職員としての属性に基づく個人情報 ・オンライン申請の処理等により、システム処理上一時的にインターネット上に保管されるデータ ・文書管理システムの決裁文書として保存されている個人情報 ・施設設計情報や入札予定価格など非公開情報	
自治体機密性２	行政事務で取り扱う情報資産のうち、自治体機密性３に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	＜例＞ ・政策検討に関する情報	可 （8.3で規定されるアクセス制御、機密性保護のための暗号化等が必要）
自治体機密性１	自治体機密性２又は機密性３の情報資産以外の情報資産	＜例＞ ・将来公表する予定の文書（白書の案等） ・公表された情報	可

注）自治体機密性３C情報については、情報資産単位でのアクセス制御、業務システムログ管理の実施等、βモデルにおいてインターネット接続系に求められている対策を実施することで、インターネット接続系における取扱いが可能。

※１　クラウド事業者が提供するサーバやネットワークなどのインフラを、仮想化技術により複数のユーザで共用し、個々のユーザが、システムの運用体系を完全に制御することが難しいサービスを想定している。

※２「行政文書の管理に関するガイドライン」（平成23年４月１日内閣総理大臣決定、令和４年２月7日 全部改定）第10 秘密文書等の管理

図表 23　機密性の分類、分類基準の例示

地方公共団体における生成AIサービスの調達仕様書の記載の例

○　国内サーバで、入力情報の学習がなく、情報の入力制限機能があるという要件の下、生成AIサービスが調達されている。

地方公共団体における調達仕様書の例

４生成AIサービスの仕様

(1) LGWAN-ASPで提供されるサービスであること。またインターネットからも利用することができること。インターネットからの利用時にIPアドレス制限が可能なこと。
(2) Microsoft Edge、Google Chromeで利用できるものであること。
(3) 原則24 時間365 日（計画停止は除く）利用できること。
(4) アカウントの利用数は無制限とする。
(5) アカウントの同時接続数は50以上とする。
(6) 利用する生成AIモデルは、日本国内リージョンでGPT3.5turbo、Gemini1.5 Flash、Claude3Haiku及びGPT-4oが利用できること。またユーザー側で生成AIモデルの切り替えが可能な仕組みであること。
(7) 管理者が管理画面から●●市の環境で利用する生成AIモデルを制限する設定ができること。
(8) GPT3.5 turbo、Gemini1.5 Flash、Claude3Haikuの利用は、文字数が無制限に利用できること。GPT-4oの利用文字数は1か月あたり500万文字以上とし、利用可能な上限設定が可能なこと。
(9) 利用可能な生成AIモデルで音声認識機能及び画像認識機能があること。

次ページへ続く

地方公共団体における生成AIサービスの調達仕様書の記載の例（続き）

地方公共団体における調達仕様書の例

(10) 利用可能な生成AIモデルで画像生成機能があること。
(11) 生成AIに入力した情報が学習に利用されないこと。
(12) 禁止ワードや機密情報の入力制限の機能を有し、入力のブロックができること。情報は、氏名や住所、電話番号などのカテゴリで設定できるとともに、禁止ワードを任意で設定ができること。
(13) Rag (Retrieval-Augmented Generation) により、データを取り込み、その内容をもとにした生成を行うデータ連携機能があること。
(14) テンプレートを作成でき、他の利用者と共有できること。
(15) 自治体向けのプロンプトのテンプレート機能を有していること
(16) ログイン時に、ユーザーアカウントとパスワードによるユーザー認証ができること。
(17) 管理者アカウントが、アカウントごとに利用状況を確認できる機能があり、CSV等でダウンロードできること。
(18) 利用者と管理者を分けて権限設定ができ、所属別などグループ分けが可能なこと。
(19) どのアカウントが、いつ、どのような操作を行ったか履歴を確認できること。

国家公務員法・地方公務員法における守秘義務について

○　国家公務員法第100条・地方公務員法第34条に基づき職員に課される秘密保持義務は、職員が職務に関連して知り得た全ての秘密であり、一般に**個人情報など外部に漏れると国や個人の利益を著しく侵害する事項**が該当する。

「懲戒処分の指針について（概要）」（職職－６８　人事院事務総長通知（最終改正令和２年４月１日））における標準例一覧より抜粋

事由	免職	停職	減給	戒告
（８）秘密の漏えい				
ア　故意の秘密漏えい	●	●		
自己の不正な利益を図る目的	●			
イ 情報セキュリティ対策のけ怠による秘密漏えい		●	●	●

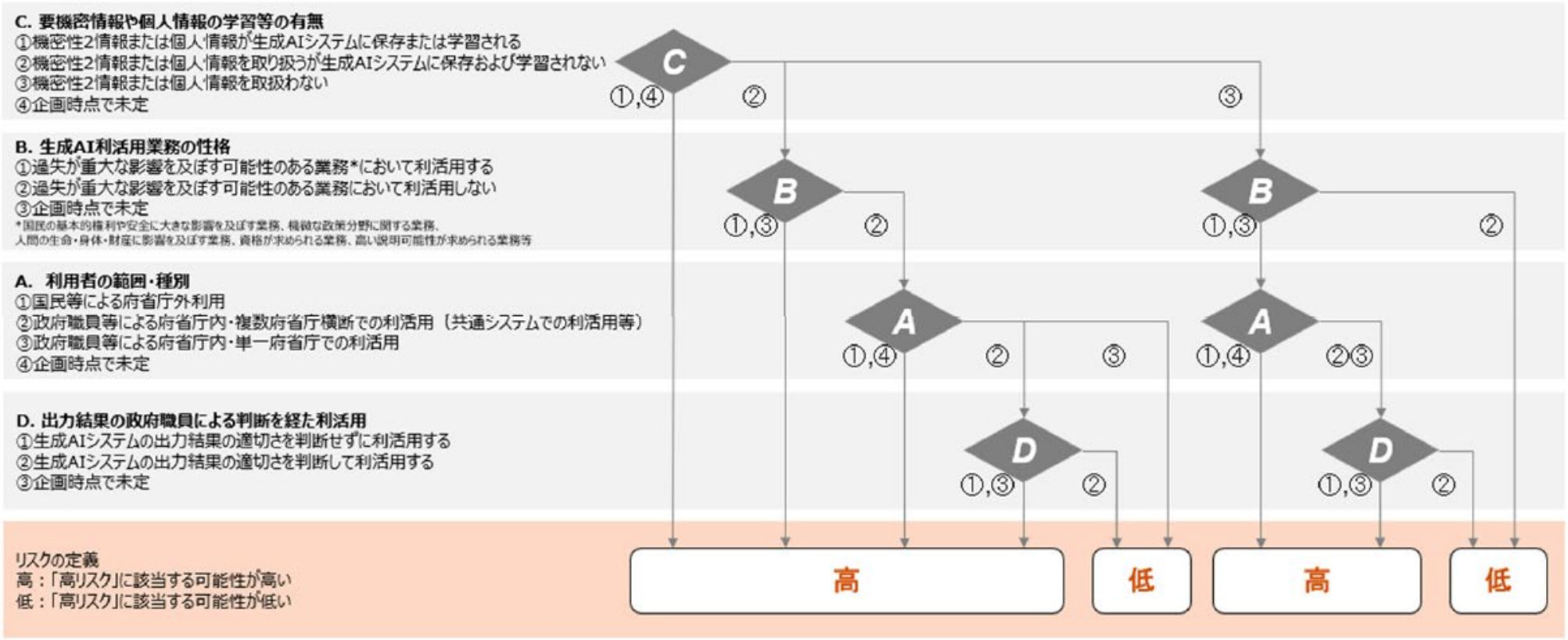
横浜市「懲戒処分の標準例　処分量定一覧」（令和６年１月16日）を基に事務局作成

事由	免職	停職	減給	戒告
イ　守秘義務違反			●	●
公務の運営に重大な支障を生じさせた場合	●	●		
具体的に命令又は注意喚起されたセキュリティ対策を怠った場合		●	●	●

<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（案）>
生成AIのリスク判断をするための高リスク判定シートにおけるリスク判定ロジック

『「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（案）」に対する意見募集について（令和7年3月28日）』公表資料（デジタル庁）より抜粋

「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３回事務局提出資料を再掲



「セキュリティポリシーに関するガイドライン」（令和7年3月28日改定）より抜粋

8.3外部サービス（クラウドサービス）の利用（自治体機密性２以上の情報を取り扱う場合）
（１）クラウドサービスの選定に係る運用規程の整備
統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱う場合、以下を含む外部サービス（クラウドサービス、以下「クラウドサービス」という。）の選定に関する規定を整備しなくてはならない。
①クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下8.3 節において「クラウドサービス利用判断基準」という。）
②クラウドサービス提供者の選定基準
③クラウドサービスの利用申請の許可権限者と利用手続
④クラウドサービス管理者の指名とクラウドサービスの利用状況の管理
（２）クラウドサービスの利用に係る運用規程の整備
統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱う場合、以下を含クラウドサービス（自治体機密性２以上の情報を取り扱う場合）の利用に関する規定を整備しなければならない。
①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。
②統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。
③統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。
(ア)クラウドサービスの利用終了時における対策
(イ)クラウドサービスで取り扱った情報の廃棄
(ウ)クラウドサービスの利用のために作成したアカウントの廃棄
（３）クラウドサービスの選定
①情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従って、業務に係る影響度等を検討した上でクラウドサービスの利用を検討しなければならない。
②情報セキュリティ責任者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス提供者の選定基準に従ってクラウドサービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件に含めなければならない。
（ア）クラウドサービスの利用を通じて本市が取り扱う情報のクラウドサービス提供者における目的外利用の禁止
（イ）クラウドサービス提供者における情報セキュリティ対策の実施内容及び管理体制
（ウ）クラウドサービスの提供に当たり、クラウドサービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制
（エ）クラウドサービス提供者の資本関係・役員等の情報、クラウドサービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定
（オ）情報セキュリティインシデントへの対処方法
（カ）情報セキュリティ対策その他の契約の履行状況の確認方法

「セキュリティポリシーに関するガイドライン」（令和7年3月28日改定）より抜粋

（キ）情報セキュリティ対策の履行が不十分な場合の対処方法
③情報セキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、クラウドサービス提供者の選定条件に含めなければならない。
④情報セキュリティ責任者は、クラウドサービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容をクラウドサービス提供者の選定条件に含めなければならない。
（ア）情報セキュリティ監査の受入れ
（イ）サービスレベルの保証
⑤情報セキュリティ責任者は、クラウドサービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価してクラウドサービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。
⑥情報セキュリティ責任者は、クラウドサービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、クラウドサービス提供者の選定条件で求める内容をクラウドサービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、クラウドサービス提供者の選定条件に含めなければならない。また、クラウドサービス利用判断基準及びクラウドサービス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。
⑦情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、クラウドサービスを選定しなくてはならない。また、クラウドサービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めなければならない。【推奨事項】
⑧情報セキュリティ責任者は、クラウドサービスの特性を考慮した上で、クラウドサービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、以下を全て含むセキュリティ要件を定めなければならない。
(ア)クラウドサービスに求める情報セキュリティ対策
(イ)クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法
(ウ)クラウドサービスに求めるサービスレベル
⑨統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス提供者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。
（４）クラウドサービスの利用に係る調達・契約
①情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。
②情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、利用承認を得なければならない。また、調達仕様の内容を契約に含めなければならない。
（５）クラウドサービスの利用承認
①情報セキュリティ責任者は、クラウドサービスを利用する場合には、利用申請の許可権限者へクラウドサービスの利用申請を行わなければならない。
②利用申請の許可権限者は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定しなければならない。
③利用申請の許可権限者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名しなければならない。

「セキュリティポリシーに関するガイドライン」（令和7年3月28日改定）より抜粋

（６）クラウドサービスを利用した情報システムの導入・構築時の対策
①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、以下を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。
（ア）不正なアクセスを防止するためのアクセス制御
（イ）取り扱う情報の機密性保護のための暗号化
（ウ）開発時におけるセキュリティ対策
（エ）設計・設定時の誤りの防止
②クラウドサービス管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載しなければならない。なお、情報システム台帳に記録又は記載した場合は、統括情報セキュリティ責任者へ報告しなければならない。
③クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。
（ア）クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順
（イ）クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順
（ウ）利用するクラウドサービスが停止又は利用できなくなった際の復旧手順
④クラウドサービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録しなければならない。
（７）クラウドサービスを利用した情報システムの運用・保守時の対策
①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。
（ア）クラウドサービス利用方針の規定
（イ）クラウドサービス利用に必要な教育
（ウ）取り扱う資産の管理
（エ）不正アクセスを防止するためのアクセス制御
（オ）取り扱う情報の機密性保護のための暗号化
（カ）クラウドサービス内の通信の制御
（キ）設計・設定時の誤りの防止
（ク）クラウドサービスを利用した情報システムの事業継続
②クラウドサービス管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正しなければならない。なお、情報システム台帳を更新又は修正した場合は、統括情報セキュリティ責任者へ報告しなければならない。
③クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。
④情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスで発生したインシデントを認知した際の対処手順を整備しなければならない。
⑤クラウドサービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録しなければならない。

「セキュリティポリシーに関するガイドライン」（令和7年3月28日改定）より抜粋

（８）クラウドサービスを利用した情報システムの更改・廃棄時の対策
①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスの利用を終了する際のセキュリティ対策を規定しなければならない。
（ア）クラウドサービスの利用終了時における対策
（イ）クラウドサービスで取り扱った情報の廃棄
（ウ）クラウドサービスの利用のために作成したアカウントの廃棄
②クラウドサービス管理者は、前項において定める規定に対し、クラウドサービスの利用終了時に実施状況を確認・記録しなければならない。