

仕 様 書

1 件名

令和 8 年度練馬区生成 AI サービス導入運用委託

2 履行期間

契約確定日の翌日から令和 9 年 3 月 31 日まで

サービスの提供開始は契約確定日の翌日から概ね 1 か月以内とする。

3 履行場所

練馬区役所中村北分館（練馬区中村北 1 - 6 - 7）ほか、区が指定する場所

4 目的

区民視点の行政サービスの実現およびデジタル技術の活用による行政運営の効率化のため、生成 AI を活用し、職員の事務処理負担の削減、生産性向上、庁内業務の効率化に取り組んできた。文書の要約やアイデア出しなどに活用しているが、インターネット上の情報などをもとに質問への回答を生成するため、区独自の事務への活用には限界があった。この課題を解消し、更なる業務の効率化を図るため、生成 AI と RAG (Retrieval-Augmented Generation: 検索拡張生成) を活用できる環境を整備する。

5 生成 AI サービスの設計の要件

- (1) 生成 AI と RAG を活用し、各部門で保持している文書を連携させ、情報検索や定型業務の効率化を行えること。
- (2) 各部門の職員が自主的に RAG の構築と改善を行い、部門ごとの業務に最適化することで、継続的な生産性向上を実現できること（区役所での RAG 構築と改善の内製化実現）。
- (3) システムとして LGWAN（総合行政ネットワーク）（以下「LGWAN」という。）環境から利用可能なクラウドサービスであること。
- (4) その他生成 AI サービスの仕様・セキュリティ対策
別紙 1 「生成 AI サービスの仕様・セキュリティ対策等」のとおり

6 委託内容

練馬区（以下「甲」という。）において、生成 AI サービスを維持・運用するに当たり、つぎの作業を委託する。

- (1) システム環境の整備

受託者（以下「乙」という。）は、生成 AI サービスを利用できる環境を整備する。

(2) 製品の提供

乙は、甲に「生成 AI サービス」の提供を行う。

(3) 運用・保守・サポート

ア 体制

生成 AI アプリ作成を支援できる体制が確保されていること。

区との連絡窓口を明確化し、即時に対応できる運用体制が構築されていること。

イ 問合せ対応

乙は、甲からの使用方法に関する問い合わせに対し、電話等による対応を行うこと。

サポートの範囲は、技術的な問題や操作方法等に関する問い合わせとし、窓口の時間は、平日午前 9 時から午後 5 時までとする。

問い合わせに対し、2 営業日以内に一次対応、回答は 3 営業日以内に行うこと。なお、天災等によりこれが困難となる場合は別途協議とする。

※土・日曜、祝休日、年末年始（12/29～1/3）を除く。

操作方法や簡易な問い合わせについて、24 時間 365 日、メールまたは Web 上の問い合わせフォームにより受付できる。なお、問い合わせは、回数に制限なく行うこと。

ウ 操作マニュアル等

乙は、サービスに関する操作マニュアル等を作成し、甲へ最新版を提供すること。提供方法に「ヘルプページ等サービス内での公開」を含めるが、公開した場合、周知すること。

エ アカウント管理

1,500 アカウント以上の利用が可能であること。また 100 アカウント以上の同時接続が可能であること。

また、乙は、甲が行うアカウントの初期登録および職員の異動等に伴う変更管理を支援すること。

オ プロンプトの随時作成

乙は、甲の業務に適応可能なプロンプトを甲からの要望に応じ作成すること。

※頻度は、月 1～2 回、年間 20 件程度を想定。

カ データ連携機能の管理・支援

乙は、次のデータ連携機能の利用に必要な管理業務を行う。

- ・データフォルダの作成

- ・データフォルダのアクセス権限の設定
 - ・データフォルダへのファイルアップロード
- なお、ファイルアップロードについては、甲が行うことを基本とするが、エラー発生時等、アップロードに必要なデータ修正等のアドバイスや支援を行うこと。

キ バージョンアップ版が公開された場合、事前に区と協議の上、無償でバージョンアップすること。

ク 研修の実施

乙は、次の職員向け生成 AI 活用研修および生成 AI・RAG についての技術研修を行う。

- ・導入直後に生成 AI の活用方法と基本操作、効果的な使用について学ぶための研修を実施すること。この研修では、ツールの利用方法と効果的なプロンプト（指示文）の作成方法、生成精度を向上させるための方法等を学べるようにすること。参加対象は全職員とするが、希望者を募る形式とし、全職員が必ず参加することを前提としない。研修実施方法は対面・オンライン問わない。なお、研修参加者の調整は区が行う。
- ・生成 AI・RAG の技術研修を実施する。この研修では、RAG の改善などに必要な知識や今後の技術トレンド、活用事例などを学べること。また、グループワーク等を実施し、生成 AI サービスの利用促進を目指すこと。参加対象は全職員とするが、希望者を募る形式とし、全職員が必ず参加することを前提としない。研修実施方法は対面とする。研修会場の収容人数（最大 100 名程度）を考慮し、参加希望人数が収容人数を超える場合は、複数回に分けて実施すること。なお、研修参加者の調整は区が行う。
- ・上記研修を契約期間内でそれぞれ 1 回以上実施すること。ただし、参加希望者が多い場合は、1 回の研修を複数回に分けて実施することを認める。また、研修はリアルタイムで行い、録画を可能とすること。
- ・上記研修資料を電子データで提供すること。

7 支払方法

毎月 1 日から月末までの月払いとし、適法な支払請求を受けてから速やかに支払う。

8 その他

- (1) 業務を履行するに当たり知りえた区の情報の取扱いについては、別紙 2「情報の保護および管理に関する特記事項」を遵守すること。

- (2) 常に高性能かつ革新的な AI ソリューションを提供し、業務生産性向上を持続的に実現するため、乙は、生成 AI・LLM についての最新技術の研究開発に精通する組織を有し、研究結果を製品開発・アップデートへ適用する仕組みを保有すること。
- (3) 行政データの処理においてセキュリティを重要視し、安全かつ信頼性の高い行政サービスを提供するため、乙は、安全性と透明性を重視すること。
- (4) 仕様書に定めのない事項または疑義が生じた場合は、甲と協議のうえ決定すること。

9 担当および連絡先

所 属	練馬区企画部情報政策課 DX 推進担当係
担当者	瀬口
Tel	03 (3825) 0211/03-5984-4529
E-mail	JOKAN02@city.nerima.tokyo.jp

生成 AI サービスの仕様・セキュリティ対策等

1 サービス仕様

- (1) LGWAN にて利用可能であること。
- (2) 庁内の文書や規程等のデータを取り込み、RAG（検索拡張生成）技術（以下「RAG」という。）を用いてその内容を基にした生成を行うデータ連携機能を有すること。
 - ア RAG データ連携として登録が可能なファイル形式は以下とすること。
 - ・テキスト、Word、PDF、PowerPoint、Excel、CSV
 - イ 管理者により、随時庁内データの追加、削除が可能であること。また、特定の一般ユーザーにも権限を付与することが可能であること。
 - ウ データをアップロードするデータフォルダごとの閲覧について、管理者および管理者に許可された者が管理できるようにすること。
 - エ 回答の根拠となる情報源を文書レベルで特定し、リンクを提供すること。
 - ・この際に提供された文書のページ数も示すこと。
 - ・リンクを開いた際には、該当ページを表示すること。
- (3) 前項(2)で規定する RAG 機能について、各部門の職員が自主的かつ容易に構築・カスタマイズできる機能を有すること。具体的には以下を満たすこと。
 - ア 専門的な技術知識を要さず、簡易な操作で RAG の構築が可能であること。
 - イ 甲が部門固有の文書や規程を随時追加・更新・削除できる機能を有すること。
 - ウ ア・イがユーザー画面から操作できること。
- (4) 乙は、常に甲の利用に適した RAG のパラメータ設定に改善すること。
- (5) 少なくとも 1 種の LLM は国内リージョンに対応した最新のモデルを使用できること。
- (6) アカウントごとの利用履歴等を個別に管理できること。
- (7) どのユーザーが、いつ、どのような操作を行ったか管理者が履歴を確認できること。
- (8) プロンプト入力時にファイル形式のデータを用いて利用できること。使用可能なファイル形式は以下とすること。
 - ・Text、Word、CSV、PDF、PowerPoint、Excel、PNG、JPG
- (9) 過去のチャット履歴の参照、チャット新規開始を選択できる機能を有すること。
- (10) 乙は、サービスに関する操作マニュアル等を作成し、甲へ最新版を提供すること。
 - ・提供方法に「ヘルプページ等サービス内での公開」を含めるが、公開した場合、周知すること。
- (11) 資料のデータは 1,500GB 以上蓄積可能であること。または、1 アカウント 1,000 ファイル以上のデータを登録可能であること。

2 セキュリティ対策

- (1) 本サービスで使用するサーバおよびデータの保管場所は、日本国内に限ること。
- (2) 入力した情報が、本区利用外の環境における学習に利用されないこと。
- (3) 利用するデータは閉鎖領域で管理され、外部に漏れないこと。
- (4) 契約終了時には、管理されたデータは全て消去し、契約終了後 30 日以内に消去証明書を提出すること。

3 利用料金体系

- (1) サービスは固定料金体系で提供すること。この固定料金に委託内容、生成 AI サービスの仕様、セキュリティ対策の内容が含まれる。
- (2) 有料 LLM の利用文字数の上限を設ける場合は、1 アカウント 1 か月あたり 5 万文字以上または 5 万トークン以上（全体管理ならば 5,000 万文字以上または 5,000 万トークン以上）とし、利用文字数（トークン数）がそれを超える場合は GPT-4 等の無償利用に自動的に切り替わり継続利用が可能であること。

別紙2
【委託契約等用】

情報の保護および管理に関する特記事項

(目的)

第1条 この特記事項は、本契約の受託者(以下「乙」という。)が委託者(以下「甲」という。)から受託した業務を履行するに当たり、本契約で取り扱う情報の機密性を確保するために、受託契約と併せて乙が遵守すべき事項を定める。

(定義)

第2条 この特記事項において「情報」とは、甲または乙が管理する情報システム、当該情報システムから出力された印刷物および情報システムから出力されたか否かを問わず重要情報を含む文書等で取り扱われる甲の情報をいう。

2 この特記事項において「重要情報」とは、前項に規定する情報のうち、個人情報およびその情報が脅威にさらされることにより区政運営または本契約に重大な影響を及ぼす情報をいう。

3 前項に規定する重要情報のうち、特定個人情報(行政手続における特定の個人を識別するための番号の利用等に関する法律(平成25年法律第27号)第2条第8項に規定する特定個人情報をいう。以下同じ。)を本契約で取り扱う場合は、別に定める「特定個人情報の保護および管理に関する特記事項」を併せて適用する。

4 この特記事項において「外部サービス」とは、情報システムのうち、クラウドサービス等、外部の者が一般向けに情報システムの一部または全部の機能を提供するものをいう。ただし、当該機能において本契約に係る情報が取り扱われる場合に限る。

(基本的事項)

第3条 乙は、本契約の履行に当たっては、個人の権利利益を侵害することのないよう情報を適切に取り扱わなければならない。

(注意義務)

第4条 乙は、情報の取扱いに当たっては、善良なる管理者の注意をもって、情報の機密性の確保に必要な措置を講じなければならない。

(情報セキュリティの確保)

第5条 乙は、本契約の履行に当たり重要情報を取り扱う場合は、甲の定める手順等を遵守するとともに、この特記事項と同等またはそれ以上のセキュリティ水準を保障する対策等を定めた規程を設ける等、情報セキュリティの確保を図るための必要な措置を講じなければならない。

(管理体制等)

第6条 乙は、本契約の履行に当たり個人情報を取り扱う場合は、受託業務に従事する者(以下「従事者」という。)から個人情報の管理に責任を持つ者(以下「管理責任者」という。)を選任し、指定する書面により甲に提出しなければならない。これによりがたい場合は、乙は甲の許可を得た上で、従事者以外から管理責任者を選任できる。

第7条 乙は、本契約の履行に当たり個人情報を取り扱う場合は、従事者の氏名、所属および受託業務への従事期間(開始日および終了予定日)を記録し、甲に書面で提出しなければならない。

第8条 乙は第6条および前条の規定により提出した書面の内容に変更があったときは、変更内容について、速やかに甲に書面で提出しなければならない。

第9条 乙は、管理責任者および従事者に対し、この特記事項の内容を周知徹底すること。なお、本契約の履行に当たり個人情報を取り扱う場合は、特記事項の内容を遵守するために必要となる教育を行うとともに、実施結果について指定する書面により甲に提出しなければならない。

第10条 乙は、甲がこの特記事項の遵守に必要となる教育を実施するときは、これを受けなければならない。

(知り得た情報の保持の義務)

第11条 乙は、本契約の履行に当たり、知り得た情報を第三者に漏らしてはならない。本契約が終了し、または解除された後においても同様とする。

(収集の制限)

第12条 乙は、本契約の履行のために個人情報を収集するときは、当該契約の履行を達成するために必要な範囲内で、適法かつ公正な手段により、行わなければならない。

(目的外使用の禁止)

第13条 乙は、情報を他の用途に使用してはならない。

(第三者への提供の禁止)

第14条 乙は、情報を第三者に提供してはならない。ただし、甲が必要と認めた場合には、重要情報を除く情報について、第三者に提供することができる。

(再委託の制限)

第15条 乙は、受託業務について、第三者に再委託してはならない。ただし、甲が認めた場合は、この限りでない。

2 乙は、前項ただし書の規定により、甲へ申請する再委託の業務内容に個人情報の取扱いが含まれる場合は、再委託先となる予定の者において、この特記事項に規定する安全管理措置が講じられることを再委託契約の締結前にあらかじめ確認し、指定する書面により甲に提出しなければならない。

3 再委託先がさらに第三者に再委託する場合(それ以降の委託も含む。以下「再々委託等」という。)で、かつ、当該再々委託等の業務内容に個人情報の取扱いが含まれる場合は、再々委託等を行う者は、以下の事項を遵守しなければならない。

(1) 再々委託等を行うことについて、甲の承認を得ること。

(2) 再々委託等の契約の締結前に当該契約の受託者となる予定の者において、この特記事項に規定する安全管理措置が講じられることをあらかじめ確認し、指定する書面により甲に提出すること。

(3) 前2号の承認申請を行ったことについて、再々委託等の元となる契約(再々委託の場合にお

ける再委託など)の委託者に通知すること。

第16条 前条の規定により再委託を行う場合は、乙は、この特記事項と同等以上の規定を当該再委託契約に定めなければならない。

2 乙は、再委託先に、本契約における一切の義務を遵守させるとともに、その履行状況を監督しなければならない。

3 前2項の規定は、個人情報を取り扱う再々委託等を行う場合についても準用する。

(情報の授受)

第17条 乙は、情報の授受に当たり、つぎに掲げる事項を実施しなければならない。

- (1) 情報の授受は、管理責任者および従事者に限定すること。
- (2) 情報を格納した記録媒体(情報システム機器のハードディスクを含む。以下同じ。)を郵送等により送付するときは、ファイルにパスワードを設定する等によりデータを暗号化すること。
- (3) 重要情報を格納した記録媒体を郵送するときは、特定記録郵便等の追跡可能な移送手段を用いること。
- (4) 情報の格納の有無にかかわらず、受託業務で利用する記録媒体を郵送するときは、送付の記録を管理簿により管理すること。
- (5) 情報をFAXにより送信するときは、必要最小限の範囲に留め、送信宛先の誤りに十分注意すること。
- (6) 重要情報をインターネットメールにより送信するときは、添付ファイルとし、ファイルにパスワードを設定する等によりデータを暗号化すること。
- (7) 重要情報を含む印刷物、文書を郵送するときは、特定記録郵便による送付または親展表示による送付をすること。

(情報の管理)

第18条 乙は、情報の管理に当たり、つぎに掲げる事項を実施しなければならない。

- (1) 重要情報を甲が指定する履行場所から持ち出さないこと。ただし、甲が必要と認めた場合は、この限りではない。
- (2) 情報の格納の有無にかかわらず、受託業務で利用する記録媒体を持ち出すときは、格納情報、持ち出し日時、持ち出した者、承認者、用途、持ち出し先、返却日時、返却確認者等について、管理簿により記録・管理すること。
- (3) 前号の場合において、前条第2号の規定と同様の措置を講じること。
- (4) 情報を乙の情報システムにおいて取り扱う場合は、下記の措置をとること。
 - ア 従事者が正当なアクセス権を有する者であることを認識するため、IDとパスワード等による認証を実施すること。
 - イ インターネットに接続された環境において重要情報を取り扱う場合は、標的型攻撃等の不正アクセスによる重要情報の漏えい等が生じないよう適切な措置を講じること。
 - ウ イの場合において、重要情報は、容易に解読することができないようにパスワードを設定する等によりデータを暗号化すること。

- エ 情報システム機器にウィルス対策ソフトウェアの導入および最新のウィルスパターンファイルの更新を行うこと。
 - オ 情報システム機器を構成するOS、ソフトウェア、ミドルウェア等に定期的に修正プログラムを適用すること。
 - カ 情報の保管または処理に当たり、従事者の私物等、許可されていない情報システム機器および記録媒体を用いないこと。また、これらを業務で利用する甲および乙の情報システム機器に接続しないこと。
 - キ 記録媒体を甲および乙の情報システム機器に接続する場合は、ウィルスチェックを行うこと。
 - ク 情報をWinny、Share等のファイル交換ソフトがインストールされた情報システム機器で処理しないこと。また、許可されていないソフトウェアを甲および乙の情報システム機器にインストールしないこと。
- (5) 重要情報を本契約の履行以外の目的のため、複写または複製してはならない。ただし、甲が必要と認めた場合は、この限りでない。
 - (6) 重要情報を含む印刷物、文書および情報の格納の有無にかかわらず、受託業務で利用する記録媒体は、管理責任者および従事者以外の者が利用できないよう、施錠管理すること。
 - (7) 重要情報を含む印刷物、文書および情報の格納の有無にかかわらず、受託業務で利用する記録媒体を廃棄する場合は、データを復元できないよう物理的に破壊し、または漏えいを来さない方法でデータ消去を行うこと。受託業務で利用する記録媒体を廃棄する場合は、その記録を管理簿により管理すること。
 - (8) 情報を記録媒体に格納し保管するときは、管理責任者および従事者以外の者が情報にアクセスできないよう、アクセス管理を行うこと。

(重要情報を取り扱う外部サービスの利用)

第19条 乙は、本契約の履行に当たり、重要情報を外部サービスで取り扱う場合は、つぎに掲げる事項を遵守しなければならない。ただし、電気通信サービス、郵便、運送サービスおよび金融機関が提供する外部サービスならびに甲または国等の公的機関より利用を求められる外部サービスを除く。

- 2 外部サービス提供者について、つぎに掲げる事項を満たす事業者を選定しなければならない。
 - (1) 日本の法令の範囲内で運用できるサービスであること。また、日本国内の裁判所を合意管轄裁判所に指定できること。
 - (2) 海外への機密情報の流出リスクを考慮し、外部サービスを提供するリージョン(国・地域)を国内に指定できること。利用者のデータが、海外に保存されないこと。
 - (3) 外部サービスの終了または変更時における事前の通知等の取り決めや、情報資産の移行方法を契約に規定できること。特に事前の通知については、事前通知の方法・期限についての条項を盛り込んだ契約が締結可能なこと。
 - (4) 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(改善、追完、損害賠償等)について、契約またはサービスレベル契約(SLA)に定められること。

- (5) 外部サービス提供者が、情報資産へ目的外のアクセスや利用を行わないように、契約に定められること。
 - (6) 外部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および管理体制について、公開資料や監査報告書(または内部監査報告書・事業者の報告資料)、各種の認定・認証制度の適用状況から、外部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、判断可能なこと。
 - (7) 外部サービス提供者もしくはその従業員、再委託先またはその他の者によって、乙の意図しない変更が加えられないための管理体制について、公開資料や監査報告書(または内部監査報告書・事業者の報告資料)の内容を確認できること。
 - (8) 情報セキュリティインシデント(情報セキュリティ事故およびその兆候)への対処方法について、外部サービス提供者との責任分担や連絡方法を取り決め、契約またはサービスレベル契約(SLA)に定められること。
- 3 利用する外部サービスについて、つぎに掲げる事項を満たすものを選定しなければならない。
- (1) 外部サービス上に保存する情報や外部サービスの機能に対してアクセス制御(外部サービスに保存される情報や外部サービスの機能ごとにアクセスする権限のない者がアクセスできないように制限すること)ができること。
 - (2) 外部サービス内および通信経路全般において暗号化処理が行われていること。この際、利用される暗号化方式は、「電子政府推奨暗号リスト」に記載された方式であること。
 - (3) 必要となる各種ログの取得機能を実装していること。また、乙は外部サービスで取得可能なログの種類、範囲を確認すること。
 - (4) 取得するログの時刻、タイムゾーンが統一されること。また、乙は時刻同期方法について確認すること。
 - (5) 暗号化に関し、外部サービス提供者が提供する鍵管理機能を利用する場合、鍵の生成から廃棄に至るまでのライフサイクルにおける仕組みに関する内容等が確認できること。また、乙は、その内容にリスク(鍵が窃取される可能性や鍵生成アルゴリズムが危険にさらされる可能性等)がないことを確認すること。
 - (6) 利用する外部サービスのネットワーク基盤内において乙が利用するネットワークが、他の利用者のネットワークや通信と分離され、論理的に独立していること。SaaSの場合は、他の利用者が本契約で取り扱うデータにアクセスできないよう確実な制御を行っていること。
 - (7) 利用する外部サービスの仮想マシンのネットワークが他の利用者のネットワークと分離されていることを、外部サービス提供者の開示している情報等で確認できること。SaaSの場合は、他の利用者が本契約で取り扱うデータにアクセスできないよう確実な制御を行っていること。
 - (8) 外部サービスの利用終了時に、外部サービスで取り扱った本契約に関わる全ての情報が外部サービス基盤上から漏えいを来さない方法で確実に削除されること。なお、削除する対象はバックアップ等により複製されたものも含むこと。これらについて外部サービスの利用終了時に、乙に情報の廃棄の実施報告書を提出できること。

(9) 外部サービス利用者の各アカウント以外に特殊なアカウント(ストレージアカウントなど)がある場合は、関連情報(資格情報等)を含めて廃棄可能であること。

4 乙が甲に対し外部サービスを提供する場合は、第2項および第3項の規定のほか、当該外部サービスのセキュリティ要件等について、甲の定める仕様を遵守すること。

5 前項の規定において、乙が他の外部サービスを用いて甲にサービスを提供する場合は、乙が利用するサービスにおいても甲の仕様およびこの特記事項の内容を遵守できるサービスを選定しなければならない。

(重要情報を取り扱わない外部サービスの利用)

第20条 乙は、本契約の履行に当たり、重要情報以外の情報を外部サービスで取り扱う場合は、利用する外部サービスの約款、その他の提供条件等から、別表に定める利用に係るリスクが許容できることを確認した上で利用しなければならない。

(受託業務に必要な物品等の持ち込みの禁止)

第21条 乙は、甲の許可なく受託業務に必要な物品等を履行場所へ持ち込んで서는ならない。

(情報の返還および処分)

第22条 乙は、本契約が終了し、または解除されたときは、情報を甲の定めるところにより返還し、または漏えいを来さない方法で確実に処分しなければならない。

2 乙は、情報の返還または処分を完了したときは、甲にこれを証明する書類を提出しなければならない。

3 前項は、契約期間中において、乙が情報の廃棄を外部へ委託する場合も同様とする。ただし、外部へ委託することについて、あらかじめ甲の承認を得なければならない。

(報告および立入検査)

第23条 甲は、必要と認めるときは、乙の情報の取扱いの状況について、実地に調査し、また乙に対して説明もしくは報告を求め、改善の指示を与えることができる。

2 前項の規定において、乙が外部サービス提供者である場合で、セキュリティ上の理由から甲による実地調査が困難な区域等があるときは、甲の求めるところにより、第三者の監査人が発行する証明書や監査報告書を提出すること。

3 甲は、第15条および第16条の規定により、再委託または再々委託等が行われる場合は、その受託者における遵守状況について、乙に対して報告または説明を求め、改善の指示を与えることができる。

(情報セキュリティに関する監査への協力)

第24条 乙は、本契約の履行に関連する業務について、「練馬区情報セキュリティに関する要綱」に基づく監査が実施されるときは、その実施に協力しなければならない。

2 前項の規定において、乙が外部サービス提供者である場合で、セキュリティ上の理由から甲による監査の実施が困難な区域等があるときは、甲が実施する監査に代えて、甲の求めるところにより、第三者の監査人が発行する証明書や監査報告書を提出すること。

(事故等発生時の対応および公表)

第25条 乙は、情報の漏えい、破壊、改ざん、消去等の事故もしくはそのおそれが生じた場合またはこの特記事項や、その他の関係法令等への違反もしくはその兆候を把握した場合（以下「事故等」という。）は、つぎに掲げる事項を実施しなければならない。

- (1) 直ちに被害を最小限に抑えるための措置または被害を生じさせないための措置を講じるとともに、甲に報告すること。
- (2) 当該事故等の原因を分析すること。
- (3) 当該事故等の再発防止策を実施すること。
- (4) 当該事故等の記録を文書で提出すること。

2 乙は、第15条および第16条の規定により、再委託または再々委託等が行われる場合は、その受託者において前項各号に規定する事項が遵守されるよう監督しなければならない。この場合において、再委託先または再々委託等の受託者からの事故等の報告先は甲および乙とすること。

3 乙は、事故等が起きた場合を想定し、対応手順について定期的に確認または訓練を行わなければならない。

第26条 甲は、必要があると認めるときは、当該事故等の内容（乙の名称を含む。）について、公表することができる。

（損害賠償）

第27条 乙は、乙、再委託先または再々委託等の受託者がこの特記事項に定める義務に違反し、甲に損害を与えたときは、損害賠償の責任を負う。

（契約解除）

第28条 甲は、乙が前各条に違反した場合は、契約を解除することができる。

（疑義の決定）

第29条 この特記事項の解釈について疑義を生じたとき、またはこの特記事項に定めのない事項については、甲乙協議の上、定めるものとする。

別表（第20条関係）

①	情報の管理や処理を外部サービス提供者に委ねるため、その情報の適正な取扱いの確認が容易ではなくなる。
②	外部サービス提供者の運用詳細等が公開されない場合は、利用者が情報セキュリティ対策を行うことが困難となる。
③	外部サービスで取り扱われる情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用され、現地の政府等による検閲や接收を受ける等のリスクが存在する。
④	不特定多数の利用者の情報やプログラムを一つの外部サービス基盤で共用することとなるため、情報漏えいのリスクが存在する。
⑤	サーバ等機器の整備環境が外部サービス提供者の都合で急変する場合、サプライチェーンリスクへの対策の確認が容易ではない。

⑥	外部サービスに保存された情報を外部サービス提供者が自由に利用することや、利用者から収集した種々の情報を分析し、利用者の関心事項を把握し得る立場にあることを約款や利用規約等に明示していない場合がある。
⑦	情報が改ざんされた場合でも、外部サービス提供者が一切の責任を負わない場合がある。
⑧	突然サービス停止に陥ることがある。その際に預けた情報の取扱いは保証されず、損害賠償も行われない場合がある。また、サービスの復旧についても保証されない場合が多い。
⑨	保存された情報が誤って消去または破壊されてしまった場合に、サービス提供者が情報の復元に応じない可能性がある。また、復元に応じる場合でも時間を要することがある。
⑩	約款や利用規約の内容が、外部サービス提供者側の都合で事前通知等なく一方的に変更されることがある。
⑪	情報の取扱いが保証されず、一旦記録された情報の確実な消去は困難である。
⑫	利用上の不都合、不利益等が発生しても、サービス提供者が個別の対応には応じない場合が多く、対応を承諾された場合でも、解決まで時間を要することがある。