

仕様書（プロポーザル公募時提示用案）

- 1 件名
令和 8 年度練馬区事務改善監査等支援業務委託
- 2 履行期間
契約締結日の翌日から令和 9 年 3 月 31 日
- 3 履行場所
区の指定する場所
- 4 委託の目的
区では、平成 30 年度より「ヒューマンエラーのリスク低減」と「業務の効率化」を図るため、業務フローに着目した改善提言を行う事務改善監査事業を実施している。
また、令和 6 年度から、事務の事故リスクの把握から改善対応までを一元的に管理する「係事務最適化シート」の導入や、他自治体を含めた事故事例と対応策を集約した「事務のリスクデータベース」の展開等の取組を行っている。
本業務は、これら全庁的な事務のリスクマネジメントの取組を一層強化するため、内部統制、業務プロセス分析、情報セキュリティ等の専門的知見に基づく分析および改善策の提案を得ることを目的とする。
- 5 委託内容
 - (1) 事務改善監査支援
 - ア 監査の観点
 - ① 業務上のリスク（書類の誤交付等）を適切に把握し、対応するルールを明文化しているか。
 - ② 実際の業務は、定められたルールに基づき行われているか。
 - ③ より妥当で効率的な事務の手法はないか。
 - イ 監査対象事務
区が選定した組織が指定する事務。対象事務の詳細は、契約締結後速やかに区が受託者に提示する。年間 3 事務とする。
なお、区は以下の基準のもと対象組織を選定する。
 - ① 前年度個人情報に係る情報セキュリティ事故が発生した課
 - ② 前年度事務処理ミスにより、個人情報に係らない事故※が発生した課※ ただし、個人情報の取扱いがある事務に限定する。
 - ウ 体制
 - ① 区の体制
監査員として、総務課、情報政策課、情報公開課の職員を配置する。
 - ② 受託者の体制
主任監査員 1 名、主任監査員を補佐するサポートスタッフを配置する。サポートスタッフの人数は、受託者が設定する。

主任監査員は、内部監査または業務監査に係る実務 5 年以上、地方公共団体またはそれに準ずる公的部門の内部統制・情報セキュリティ監査の実績を有すること。サポートスタッフは、当該分野の知識・経験を有すること。

エ 区が想定する監査の進め方

①計画（目的・範囲・基準、手続、サンプリング）②実査（文書レビュー、ヒアリング・観察、証跡収集、所見のファクト確認）③報告（重大度、原因・影響、是正提案）④フォローアップ（是正の実施確認）を最低手順として実施すること。

①ー 1 プロジェクト計画【契約締結後 2 週間以内】

監査の実施スケジュール、監査実施順序、個別監査計画の作成方針等、事務改善監査支援全体の進行管理に関する事項をとりまとめたプロジェクト計画案を作成すること。個別監査計画の作成方針は、区の「情報セキュリティマネジメント運営計画」および「練馬区事務改善実施方針」に沿った内容とする。

プロジェクト計画案は、契約締結後 2 週間以内に区へ提出すること。

なお、監査の日程は、契約締結後速やかに区から受託者に候補日を複数提示し、候補日の中から区と受託者の協議のうえ決定するものとする。

①ー 2 個別監査計画【契約締結後～各監査実施 1 か月前まで】

受託者は、区から提供を受けた監査対象事務に関する資料を読み込み、業務内容・関連法令・内部規定等を十分に把握したうえで、対象事務ごとに個別監査計画案を作成すること。個別監査計画案には、監査項目、確認資料等を記載するものとし、区の「情報セキュリティマネジメント運営計画」および「練馬区事務改善実施方針」に沿った内容とする。

個別監査計画案は、各監査実施 1 か月前までに区へ提出すること。

個別監査計画確定後、計画に沿って監査当日に向けた準備を進めること。

② 実査（監査当日）【9～11 月】

対象組織等を訪問し、半日程度でヒアリング、現場視察を行う。当日の進行は、主任監査員が務めるものとする。

ヒアリングおよび現場視察後、主任監査員および監査員で意見形成を行い、提言の方向性を整理する。そのうえで、提言内容の概要を示す監査結果概要報告書を作成する。

終わりに、監査結果概要報告書をもとに、主任監査員が対象組織に対して監査結果の総括を説明すること。

③ 報告【監査終了後 1 か月以内】

監査の実施結果を集計・分析し、監査結果報告書を作成すること。このとき、監査により把握したリスクや業務上の改善余地について、その分析結果や対応策を明確に記載し、今後の改善に資する内容とすること。

また、監査結果概要報告書に示した内容と整合が取れるよう、構成や記述を整理するものとする。

④ フォローアップ【令和 8 年度内（令和 9 年 3 月 31 日）まで】

監査終了後、対象組織の是正状況について、区が確認できるよう支援するとともに、是正状況の分析および解決案の提示を行うこと。

(2) 事務のリスクマネジメントの取組に係る支援

区が実施している事務のリスクマネジメントの取組に関連して、受託者が提案した業務を行うこと。受託者はこの結果として得られた分析内容、示唆、改善策等を整理、必要に応じて文書として取りまとめ、業務報告書に含めて区に提出するものとする。

提案業務は、事務改善監査支援業務の概ね 1 / 3 程度の工数を見込んでいる。

提案業務の主たる担当者は、主任監査委員と兼ねることを妨げない。

提案の例は、以下のとおりとする。なお、提案内容は例示したものに限らず、委託の目的に資する内容であれば差し支えない。

ア 「事務のリスクマネジメントの取組」に係る令和 9 年度以降を見据えた課題整理および今後の方向性に関する検討

イ 「リスク情報シート」に基づく全庁的な事故・ヒヤリハット情報の分析によるリスク傾向の抽出・改善に関する助言

ウ 「係事務最適化シート」の分析によるリスク傾向の抽出・改善に関する助言

エ 「事務のリスクデータベース」への新規事例・再発防止策の登録支援

(3) その他

区からの事務のリスクマネジメントの取組に係る相談に対して、適宜助言等対応すること。

6 成果物

(1) 成果物の内容

成果物は、原則として直接印刷が可能なデータ形式（MS-Word、MS-Excel、MS-PowerPoint 等）で、区の電子メールアドレスあてに電子データで納品する。

ア 計画書（プロジェクト計画・全 3 回分の個別監査計画）

イ 監査結果概要報告書（全 3 回分）

ウ 監査結果報告書（全 3 回分）

エ 5（2）で作成した文書

オ 業務報告書（本業務で作成したすべての資料を整理し、まとめたもの）

(2) 成果物の帰属関係

本委託業務の履行により受託者が作成し、区に納入した作成物の所有権・著作権（著作権法第 27 条および第 28 条の権利を含む）は、区に帰属するものとする。受託者は、著作者人格権の行使をしないこと。

作成等にあたり、第三者の著作権等の権利に抵触した場合は、受託者の責任と費用をもって適正に処理すること。作成物とは、受託者が区との協議の上に作成する一切の著作物等をいう。

7 再委託の取扱い

受託者は、この契約に係る履行の全部または主要な部分を一括して第三者に委託してはならない。

業務の一部について再委託する場合は、あらかじめ、再委託契約を締結する前に、区に対し再委託承認手続きを行うこと。

8 契約金額

契約金額には、交通費等本委託にかかるすべての費用を含む。

9 検査および支払い方法

履行終了後、受託者の適法な請求を受けてから速やかに一括して支払う。

10 その他

- (1) 本業務を履行するにあたり、別紙「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) 本業務を履行するにあたり、本仕様書に記載のない事項については、区と受託者で協議の上、決定する。

11 担当

練馬区総務部総務課適正事務推進係 小池・柳川

電話 03-5984-2439 FAX 03-3993-1195

電子メールアドレス SOMU15@city.nerima.tokyo.jp

【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9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。

5 この特記事項において「クラウドサービス」とは、ネットワークを通じて事業者が区に提供するコンピューティングサービスで、つぎのいずれかに該当するものをいう。

IaaS型

PaaS型

SaaS型

(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。

再々委託等を行うことについて、甲の承認を得ること。

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。

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。

情報の授受は、管理責任者および従事者に限定すること。

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。

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。

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。

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。

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。

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。

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。

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。

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。

情報を乙の情報システムにおいて取り扱う場合は、以下の措置を講じること。

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。

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。

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。

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。

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(クラウドサービス)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 乙は、クラウド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。

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。

海外への機密情報の流出リスクを考慮し、クラウド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。

クラウド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。

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。

クラウドサービス提供者が、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。

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、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、判断可能なこと。

クラウド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。

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、クラウド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 乙は、利用するクラウドサービスについて、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。

不正なアクセスを防止するためのアイデンティティ管理(アカウントの発行から利用停止・削除等までの一連の管理・メンテナンス)ができること。

クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御(クラウドサービスに保存される情報やクラウド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。

クラウド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。

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、乙はクラウドサービスで取得可能なログの種類、範囲を確認すること。

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。

暗号化に関し、クラウド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。SaaSの場合は、対象外とする。

利用するクラウド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

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。

利用するクラウド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、クラウド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。

クラウドサービスの利用終了時に、クラウドサービスで取り扱った本契約に関わる全ての情報がクラウド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。これらについてクラウド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、または確実に削除されることが文書で確認できること。

クラウド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 乙が甲に対しクラウド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、当該クラウド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、乙が他のクラウド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(クラウドサービス)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クラウドサービスで取り扱う場合は、利用するクラウドサービスの約款、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、または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、乙がクラウド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、乙がクラウド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。

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。

当該事故等の原因を分析すること。

当該事故等の再発防止策を実施すること。

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が生じたとき、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)

	情報の管理や処理をクラウド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。
	クラウド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。
	クラウド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。
	不特定多数の利用者の情報やプログラムを一つのクラウド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。
	サーバ等機器の整備環境がクラウド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。
	クラウドサービスに保存された情報をクラウド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。
	情報が改ざんされた場合でも、クラウドサービス提供者が一切の責任を負わない場合がある。
	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。
	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、クラウド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。
	約款や利用規約の内容が、クラウド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。
	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。
	利用上の不都合、不利益等が発生しても、クラウド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。