

## 仕 様 書

### 1 件名

令和8年度オンライン通知管理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、当区から郵送している通知等について、アプリケーションを通じて、オンラインで区民に通知することで、区民の利便性向上、送付ミスの防止および郵便料等のコスト削減を図る。

### 5 想定通知種別数および想定通数

#### (1) 想定通知種別

7～10種類（令和9年度以降は増加予定）

#### (2) 想定通数

初年度5,000通（令和9年度以降は増加予定）

### 6 サービスの設計の要件

契約期間中、次の機能要件を満たしていること。

#### (1) 法令適合性

本調達範囲業務に関する関係法令（「処分通知等のデジタル化に関する基本的な考え方」）等に適合した処理ができること。

#### (2) ユーザビリティ

- ・シンプルな設計で誰でも使用できることシステムであること。また、簡単な操作でスムーズに運用ができること。
- ・メッセージにURL貼付や文字へのURLリンク作成が可能であること。

#### (3) 通知管理

- ・複数の電子通知について、電子署名を一括付与できること。
- ・処分通知データと通知宛先情報とを突合できること。
- ・突合したデータを専用のポータルサイトへ送信できること。
- ・送信した処分通知の開封状況がポータルサイトでリアルタイムに確認できること。

- ・処分通知等に関連する PDF を、宛先ごとに同一内容で一括送信すること、また宛先ごとに異なる内容（メッセージや添付 PDF）を設定して個別送信することもできること。

(4) 認証管理

- ・ユーザー ID およびパスワードによりシステム認証管理ができること。
- ・職員ごとに権限設定がカスタマイズ可能であること。

(5) テスト利用ができること。

(6) 通知物送付時の設定

- ・通知内容（通知物の説明文）、メール等の連絡方法の設定ができること。また、リマインドメール（再連絡）の設定ができること。
- ・ワンタイムパスワードやマジックリンク等、認証方法の設定ができること。

(7) 送付先リストおよび通知物の突合・分割機能

- ・通知物毎の送付先リスト（宛先名、メールアドレス、通知物情報等の CSV）が作成できること。
- ・通知物（PDF）と申請データ（オンライン申請で出力された CSV 等）との突合ができること。
- ・複数頁で作成された通知物 PDF を住民毎の単一 PDF に分割できること。

(8) 通知物の送付および管理機能

- ・通知物の送付および住民の開封状況が確認できること。
- ・未開封の住民に対して再連絡でき、連絡回数が確認できること。
- ・通知物毎に利用状況（送付数、添付資料、職責証明書発行数等）が確認できること。

## 7 システム環境および要件

(1) システム環境

システムの管理画面は、発注者が業務で使用する端末で利用できること。  
利用環境は次のとおり。

ア OS

- ・Microsoft Windows11 Enterprise

イ ブラウザ

- ・Microsoft Edge
- ・Google Chrome

(2) システム要件

ア 定期的にバージョンアップ（機能拡張）を図るシステムを L G W A N - A S P サービスで提供すること。

イ 使用する機能は、L G W A N - A S P サービスで提供すること。また、データ通信は、原則 S S L により暗号化すること。

ウ J - L I S（地方公共団体情報システム機構）の認定を受け、電子署名済みの文書（PDF ファイル）を L G W A N 環境下にダウンロードしても電子

署名が破損しないこと。

(3) セキュリティ対策

ア サーバとクライアント間の通信がT L S により暗号化されていること。なお、T L Sはバージョン1.2 以上とし、これに欠陥が見つかり安全でなくなった場合は、より新しいバージョンを使用すること。

イ 事業者が管理するサーバ等の運用基盤として、以下の要件を満たすこと。

- ・データセンターの安全性の確認基準が、ティア3 以上またはそれと同等の仕様を満たすこと。
- ・データセンター事業者がISO／IEC27001 等情報セキュリティにかかる付与認定を受けていること。

ウ 24 時間365日のシステム監視を行い、厳格なルールでシステムを運用していること。

エ セキュリティ情報を確認し、定期的にセキュリティパッチの適用をしていること。

オ I S M Sクラウドセキュリティ認証の取得またはプライバシーマーク付与認定を受けている事業者による保守運用がされているシステムであること。

カ サーバへ侵入しての情報の盗聴、情報の不正コピー、改ざん、破壊、不正な削除など不正アクセスに対して防衛と検知等の対策をとること。

キ S Q Lインジェクションによる情報窃取や改ざんを防ぐ対策がされていること。

ク 旧来の既知のものおよび最新のウイルス・マルウェア等に対して対策をとること。

ケ D D o S攻撃・S Q Lインジェクション・クロスサイトスクリプティング(X S S)・クロスサイトリクエストフォージェリ(C S R F) 等を検知し、ブロックする、W e bアプリケーションファイアウォール等のセキュリティ対策をとること。

コ サーバ内のデータやネットワーク経由でやり取りするデータについて、情報漏洩を防ぐ対策を十分にとること。

サ サービスを通じて登録し保存された回答データは、電子政府推奨暗号リストに記載された暗号方式で暗号化されていること。

シ データを閲覧可能とすることについて、特定のユーザアカウントに限定できること。

ス 情報漏洩事案発生時等、インシデント発生時の対応手順が整備されていること。

セ クラウドサービス（ウェブアプリケーション）における脆弱性について、システム面・運用面で対策を行っていること。脆弱性の詳細については、情報処理推進機構（I P A）の「安全なウェブサイトの作り方(\*)」等を参考にするこ

と。

(\*) <https://www.ipa.go.jp/security/vuln/websecurity.html>

## 8 委託内容

練馬区（以下「甲」という。）において、オンライン通知管理サービスを維持・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、オンライン通知管理サービスを利用できる環境を整備すること。

### (2) 製品の提供

- ・乙は、甲に「オンライン通知管理サービス」の提供を行う。
- ・乙は、サービス導入における法的支援および技術的支援を行う。

### (3) 運用・保守・サポート

#### ア 問合せ対応

- ・乙は、契約期間を通じて、技術的な支援や助言、製品のバージョンアップ、問合せ対応などを提供すること。
- ・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。
- ・乙は、甲からの使用方法等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営業日以内に一次回答、回答は3営業日以内に行うこと。

※土・日曜、祝休日、年末年始（12/29～1/3）を除く。

※問合せ内容によって、回答に時間を要する場合は協議可能とする。

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。

- ・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こと。
- ・問い合わせは、回数に制限なくできること。

#### イ アカウント管理

乙は、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。

#### ウ マニュアルの提供

事業者はサービスに関する操作マニュアル等を作成し、区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 研修の実施

乙は、次の職員向けオンライン通知管理活用研修およびオンライン通知管理サービスの説明会を行う。

- ・導入直後にオンライン通知管理サービス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。この研修では、サービスの利用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甲が行う。

- ・オンライン通知管理サービスについての説明会を実施する。この説明会では、次年度以降利用希望者を募るためのサービス説明会で、サービスの内容紹介、導入・活用事例、導入効果等を説明すること。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。
- ・上記研修を契約期間内で最低1回ずつ実施する。また、実施はリアルタイムで行い、録画を可能とすること。
- ・上記研修に用いた資料を区へ電子データで提供すること。

#### オ 適用業務拡大支援

甲がオンライン通知適用業務を拡大するにあたって、以下の支援を行うこと。

- ・ビジョンや実施計画、成果指標の策定支援
- ・運用ルールや規定、ガイドライン等の策定支援
- ・広報施策案の提供、広報施策の実施支援
- ・利用希望アンケート調査の調査項目案の提供
- ・アンケート調査の集計、結果資料の作成支援
- ・通知選定における原課ヒアリングへの同席（年3回程度）
- ・ヒアリング項目案の提供

### 9 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。

### 10 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1「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) 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。
- (3) 調達の実施における個人情報等の取扱いについては、個人情報保護の重要性を十分認識し、個人の権利、利権を侵害することのないよう必要な措置を講じること。
- (4) 事業者の責任者および担当者一覧を作成すること。
- (5) 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。

### 11 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
電 話	03 (3825) 0211
E-mail	JOKAN02@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。