情報システムに関する業務委託契約事項

１　操作手順

情報システム等の操作手順は文書化し、最新の状態を維持すること。また、その手順は、必要とする全ての利用者に対して利用可能とすること。

２　不正プログラム対策

（1）受託者は、利用するパソコンやサーバ等に不正プログラム対策ソフトウェアの最新バージョン及び定義ファイルを維持管理し、不正プログラムを検出する措置を行うこと。不正プログラムが検知された場合は速やかに検知された不正プログラムは自動的に隔離し駆除するとともに、区に報告すること。またネットワークから遮断し、改ざんが確認された場合は、区と相談の上、正しい内容に復元すること。

（2）インターネットに接続している情報システムでは、不正な攻撃を防止するための検知機能を有すること。

（3）クラウドサービスを提供する場合は、不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）の確認と定期的な報告をすること。

３　脆弱性対策

（1）受託者は、本契約の履行に際し、開発、運用、保守の際の情報セキュリティ上問題となりうる機器およびソフトウェアを使用しないこと。

（2）受託者は、情報システムの脆弱性を突いて行われる攻撃等のリスクについて常に情報収集を行い、業務の重要度に応じた情報セキュリティ対策を提示し、実施すること。

（3）受託者は、システム障害を未然に防止するための措置、障害発生を早期発見するための措置及び障害発生時の拡大防止や迅速復旧のための措置について、業務の重要度に応じた対策を明示すること。

（4）ウェブアプリケーションではセキュリティを考慮した実装を行い、特にインターネットに接続する情報システムでは、「脆弱性一覧」を参考に脆弱性に対応すること。

（5）業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用しないこと。

（6）利用するクラウドサービスに影響し得る技術的脆弱性の管理内容、区の業務に対する影響や保有するデータへの影響、技術的脆弱性に対する脆弱性管理の手順について、区に報告すること。

４　構成管理

（1）情報システムを構成するハードウェアやソフトウェアの名称と版数を明らかにし、区に提示すること。

（2）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、関連文書を更新し、区に報告すること。

（3）利用するクラウドサービスの使用において必要な監視機能を適切に実施し、業務継続の上で必要となる容量・能力を予測し業務が維持できるようすること。

上記により、構成に変更があった場合も適宜報告すること。

5 ネットワークセキュリテイ

（1）機密性の高い情報資産をインターネットに接続しているサーバ等の公開領域に保管しないこと。また、データベースサーバ等は、ファイアウォール等でインターネットと分離されたセグメントに設置すること。

（2）受託者は、情報システムの利用中に一定の使用中断時間が経過したときには、そのセッションを遮断する機能を提供すること。

（3）受託者は、情報システムの認証方法（ID、パスワード、ICカード、認証鍵等）を区に提供すること。

（4）受託者は、特定の場所又は装置からの接続を認証する手段として、自動の識別装置を必要に応じて導入すること。

（5）インターネットを利用する情報システムでは、業務の重要度に応じて、https、VPN等により暗号化を行い、通信路での盗聴及び改ざんから保護する。また不要な通信はファイアウォール等により遮断すること。

6 情報システムのログや記録

ログオンやログアウトなどの利用者の活動状況や外部からの非定常的なアクセス等のセキュリティ事象を監視・記録し、区の求めに応じて提供すること。また、ログ等の記録は、改ざん防止等の適切な手段により保護すること。

7 時刻の同期

全ての情報システム内の時刻は、正確な時刻源と同期させること。

8 情報システム停止等

情報システムを停止する場合や運用制限がある場合は、区の了承を得ること。

9 変更管理

受託者が調達・管理する情報処理設備及び情報システムの変更において、区に影響を及ぼすものは、事前に区と協議を行うこと。また、情報システムの変更が行われた際には変更履歴を区に明示すること。約款による利用については、この限りでない。

10 データベース管理

委託先が調達・管理する情報システムにおいては、区に割り当てられる容量・能力の限界値を開示すること。また、区から要請があった場合は、資源の利用率などを明示すること。約款に

よる利用については、この限りでない。

11 ソースコード管理

（1） ソースコードが不正に変更・消去されることを防ぐために、ソースコードの管理を適切に行うこと。

（2） ソースコードを納入する場合は、区の本番環境以外の開発環境等に導入し、管理すること。また、その管理手順を区に提示し、区の承認を得ること。

12 品質管理

情報システムの開発工程において、区の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。

13 バックアップ

業務継続に支障が発生する恐れのあるデータは、定期的にバックアップをとること。その際に個人情報等の機密性の高い情報資産の保護を行うこと。また、区がバックアップ手順を策定する場合は情報を提供すること。

14 アクセス制御

(1)受託者は、情報システムのアクセス制御を適切に行うこと。また、区がアクセス制御等の状況を確認できるようにすること。

(2)区が定めた情報セキュリティポリシーにおけるアクセス制御（パスワードや認証情報を含む）に関する事項が、実現できるようにすること。

(3)クラウドサービスを利用する際に、受託者に管理権限が与えられた場合、多要素認証を用いて認証した上で、クラウドサービスにアクセスすること。

(4)不正アクセス対策として、ユーティリティプログラムについてはクラウドサービスのシステムやアプリケーション設定を変更するものは原則として使用を禁止する。これらのうち、利用が必須なものは情報セキュリティの責任者の承認を取得し、利用を管理した上で使用すること。

15 開発及び運用

(1)開発及び運用において、運用環境とテスト環境を分離する。運用内容を変更する際には、テスト実施及び検証結果を事前に区へ報告し、確認を得ること。

(2)受託者は、情報システムの変更を行う際には、変更履歴を区に明示すること。

(3)受託者は、情報システムの利用環境に変更が生じる場合は、あらかじめ区に通知し、了承を得ること。

16 情報セキュリティ

(1)情報セキュリティの観点から必要な試験がある場合には、試験項目及び試験方法を定め、これに基づいて試験を実施すること。

（2）情報セキュリティの観点から実施した試験の実施記録を保存すること。

17　インシデント対応準備

クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化すること。

（ア）サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

（イ）クラウドサービス利用の終了手順

（ウ）バックアップ及び復旧

18　クラウドサービス利用時の責任分界点について

デジタル庁提供の「ガバメントクラウド手続き概要（全編）」（2023/09/22 公開）の「3.5 責任分界点」に記載の図を参考に責任分界点（説明責任範囲も同様）を明確にし、区に提示すること。

19　テストデータの管理

テストをする際は、実施及び検証のテストデータに、個人情報及び一般に公表することを前提としていない情報資産の実在データが含まれていないようにすること。個人情報及び一般に公表することを前提としていない情報資産の実在データが含まれている場合は、区が管理する区域内にテスト環境をつくり、都度許可を得ること。また、テストの完了後は、適切に削除すること。

20　入退域管理

受託者は、運用、機器の搬出入で区のサーバ室等機密区域へ入退域する場合は、入退域管理簿の記入等、区の定めた手続に従うこと。定期的に入退域しなければならない受託者は作業従事者ごとに担当する作業内容を明記した名簿を提出すること。

21　監視

データセンター等機密性及び完全性の高い情報資産を保管する場所では、カメラ監視や入退出管理等による不審者の監視が可能な状態にすること。

脆弱性一覧

本システムに混入しないよう対処を求める主な脆弱性は次のとおり。

＜参考＞「脆弱性名称の定義に関する参照先」

(1)IPA『安全なウェブサイトの作り方 2021年3月改訂』

(2)CWE - Common Weakness Enumeration

(3)IPA『ウェブ健康診断仕様』

No	脆弱性名称	
1	SQL インジェクション	
2	OS コマンド・インジェクション	
3	ディレクトリ・トラバーサル脆弱性	
4	「ログイン機能」の不備	推測可能なセッション ID
		URL 埋め込みのセッション ID の外部への漏えい
		クッキーのセキュア属性不備
		セッション ID の固定化
5	クロスサイト・スクリプティング(XSS)	
6	利用者の意図に反した実行の防止機能の不備	クロスサイト・リクエスト・フォージェリ(CSRF)
		クリックジャッキング
7	メールヘッダ・インジェクション脆弱性	
8	「アクセス制御」と「認可処理」の不備	アクセス制御
		認可処理
9	HTTP ヘッダ・インジェクション	
10	eval インジェクション	
11	競合状態の脆弱性	
12	意図しないファイル公開	
13	アップロードファイルによるサーバ側スクリプト実行	
14	秘密情報表示時のキャッシュ不停止	
15	オープンリダイレクタ脆弱性(意図しないリダイレクト)	
16	クローラへの耐性	