仕　様　書

１　件　　名　中野区＿＿＿地域包括支援センター事業運営委託

２　履行場所　中野区＿＿＿＿＿＿

※なお、施設の状況により契約期間中に施設の設置場所（履行場所）が変更になる場合がある。

３　契約期間　令和９年４月１日から令和１０年３月３１日まで

４　業務内容

介護保険法に基づく包括的支援事業、高齢者虐待の防止、高齢者の養護者に対する支援等に関する法律第１７条に基づく業務、中野区地域包括支援センター事業実施要綱第５条及び中野区高齢者実態把握事業実施要綱第７条に定める事業、第１号介護予防支援事業、その他区が必要と認める事業

※ 詳細は別添の「中野区地域包括支援センター運営方針」のとおり

（１）基本業務

ア　総合相談支援業務（介護保険法第１１５条の４５第２項第１号）

イ　権利擁護業務（介護保険法第１１５条の４５第２項第２号）

ウ　包括的・継続的ケアマネジメント支援業務
（介護保険法第１１５条の４５第２項第３号）

エ　介護予防ケアマネジメント（介護保険法第１１５条の４５第１項第１号ニ）
「中野区介護予防ケアマネジメント実施要綱」に基づく介護予防ケアマネジメント業務

（２）関連業務

ア　認知症の人及び家族への支援業務

イ　在宅療養者への支援

ウ　生活支援コーディネーター業務

（３）指定介護予防支援

（４）その他業務

ア　養護者による高齢者虐待の防止、養護者に対する支援等の業務

イ　在宅福祉事業事務

５　支払方法

（１）前記４（１）エ　介護予防ケアマネジメント及び（３）指定介護予防支援以外の委託料
区は、受託者に対し、受託者からの正当な請求に基づき、その請求を受理した日から３０日以内に支払う。年２回の前金払いとする。

（２）前記４（１）エ　介護予防ケアマネジメント及び（３）指定介護予防支援の委託料

受託者は、毎月の実績を翌月１０日までに東京都国民健康保険団体連合会へ請求すること。なお、介護予防ケアマネジメントの請求方法についての詳細は「介護予防ケアマネジメントの手引き」を参照の上、対応すること。

6　個人情報保護及び情報セキュリティの遵守

（１）受託者は業務で必要な保健福祉サービス情報のうち、受給情報及び受給の可否に係る情報に限っては区に問合せをすることができる。ただし、本人同意のうえ、月曜日から金曜日（祝休日年末年始を除く）までの午前８時３０分から午後５時００分までに行うこと。

（２）個人情報保護法等を遵守すること。詳細は別紙１及び別紙２を参照のこと。

7　職員確保

受託者は業務を実施するため、中野区地域包括支援センターの職員及び運営に関する基準を定める条例で定めた最低人員を配置するほか運営に必要な職員を確保しなければならない。

8　業務従事者の健康管理

（１）受託者は、業務従事者に対して感染症予防及びメンタルヘルス等の的確な健康管理の措置を講じるとともに、本事業の執行に支障を来さぬ人的体制をとること。

（２）受託者は、学校保健安全法施行規則第１８条に定める感染症にり患した業務従事者、又はり患の疑いがある業務従事者（以下「り患者等」という。）を確認した場合、直ちに次の措置を講ずること。

ア　り患者等について、他者への感染可能性がなくなるまでの期間は本事業に従事させないこと。

イ　当該り患者等の氏名、他者へ感染させる可能性のある期間内に接触した事業利用者氏名及び接触日時等を区に対して報告すること。受託者における確認が夜間又は休日であった場合も同様とする。

9　貸与物品

（１）区は、財産の交換、譲与、無償貸付等に関する条例（昭和３９年条例第７号）第９条の規定に基づき、事務室内の備品等を、受託者に無償貸与する。

（２）受託者は、使用者を、予め区に書面で届け出なければならない。使用者の範囲は、地域包括支援センター職員、介護予防・生活支援サービス事業担当者、指定介護予防支援事業に従事する管理者及び従業者、及び給付管理業務など事務的な業務を処理する事務職員とする。

（３）受託者は、貸与物品を善良な管理者の注意をもって、維持管理しなければならない。これに係る必要経費、有益費その他の費用は、区が負担する。ただし、消耗品費及び受託者の故意又は過失によって生じた費用は、受託者が負担する。

（４）この契約期間が満了したとき、又は契約が解除されたときは、受託者は、貸与物品を区に返還しなければならない。

10　事業計画

受託者は、この契約締結後、速やかに事業計画書を作成し、区に提出しなければならない。

11　報告等

（１）受託者は、実績報告書を月単位で作成する。毎月、当該月の終了後速やかに実績報告書を区へ提出すること。ただし、３月分については、３月３１日までに区に提出すること。

（２）受託者は、この契約期間満了後３か月以内もしくは当該年度法人決算後速やかに、事業実績報告書及び会計経理決算報告書、運営委託費確認書を区に提出しなければならない。

（３）受託者は、災害その他の事故があったとき又はそのおそれがあるときは、応急措置を行い、直ちにその状況を区に報告し、その指示を受けなければならない。

（４）受託者は、本委託業務を翌年度も引き続き受託する意向があるか否かについて、４月３０日までに報告すること。

12　調　査

区は、受託者に対し、必要に応じて委託業務の実施状況について、報告を求め、又は調査を行うことができる。

区は、前条の規定に基づく報告又は前項の調査の結果、必要と認めるときは、受託者に対し是正措置を命ずることができる。

13　契約解除

区は、約款に該当する場合のほか、法令の改正等により業務を委託する必要がなくなったときは、この契約を解除することができる。

14　障害を理由とする差別の解消の推進

本契約の履行にあたり、障害を理由として障害者でない者と不当な差別的取扱いをすることにより、障害者の権利利益を侵害しないこと。また、障害者から現に社会的障壁の除去を必要としている旨の意思の表明があった場合において、その実施に伴う負担が過重でないときは、障害者の権利利益を侵害することとならないよう、当該障害者の性別、年齢及び障害の状態に応じて、社会的障壁の除去の実施について必要かつ合理的な配慮をすること。

15　法令の遵守等

受託者は、この契約書の定めによるほか、中野区地域包括支援センターの職員及び運営に関する基準を定める条例、中野区地域包括支援センター事業実施要綱の規定に基づいて、契約を誠実に履行しなければならない。

受託者は、この契約条項に明示されていない事項であっても、受託業務の性質上必要なもの及び別途運営方針に定めるものについては、区の指示に従い実施しなければならない。

16　災害時における協力体制

中野区地域防災計画に基づく災害時における応急対策活動について協力すること。

協力内容については別途、契約締結後に協議書を締結する。

17　その他

この仕様書に定めのない事項については双方協議の上定める。

担当　地域支えあい推進部地域包括ケア推進課

中山、伊勢崎

電話　　０３（３２２８）５７８５

別紙１

情報資産を取り扱う業務委託契約事項

１　情報セキュリティ体制の整備

以下を整備し、区へ関係する文書を提出すること。

（１）受託者は、区に対して本契約の履行に関しての責任者、監督者及び作業従事者の名簿を届け出ること。

区が作業従事者に身分証明書の提示を求めた際は、速やかに提示ができるようにすること。

（２）受託者は、情報セキュリティ事故等発生時の連絡体制、対応方法（対処手順、責任分界点、対処体制等）について明示すること。

（３）区の情報セキュリティポリシー及び情報セキュリティ実施手順を遵守すること。

（４）受託者は、作業従事者に対し情報セキュリティ対策について教育を行うこと。区が求めた場合は、教育の記録を提示すること。

（５）受託者は、区と協議のうえ、作業従事者ごとの作業場所、業務、情報資産等のアクセス制限を定めること。

（６）受託者は、第三者が提供するサービスを利用している場合、サービスレベルの達成状況及びセキュリティ上の要求事項が適切に実行されていることを監査または検査などで確認し、区に報告すること。

（７）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を取り決めること。

２　情報資産の取り扱い

（１）取り扱い

受託者は、区が決定した情報資産の分類に基づき、区と同様に情報資産の取り扱いを行うこと。

ア　情報資産の漏えい、紛失、改ざん及び破損を防止すること。

イ　業務上必要のない情報資産を作成しないこと。

ウ　情報資産を必要以上に複製及び配布しないこと。

エ　業務以外の目的に情報資産を利用しないこと。

オ　区が決定した情報資産分類の価値が高い情報資産は、施錠できる場所での保管又はアクセス制御を行うなど、許可されていないものに対して、情報資産を使用不可又は非公開にする措置を講じること。その他の情報資産は、必要に応じて施錠できる場所での保管又はアクセス制御を行うなど、許可されていないものに対して、情報資産を使用不可又は非公開にする措置を講じること。

カ　個人情報漏えい防止のための技術的安全管理措置を講じること。

（２）搬出入

受託者は、区が提供した情報資産の搬出入が必要な時には、事前に区の承認を得ること。また、情報資産の暗号化等の技術を活用し、盗難、不正コピー等の防止を厳重に実施すること。

（３）記録

区が提供した情報資産の内容及び交換・持ち出し等の履歴に関しては記録すること。

（４）記録媒体の制限

受託者は、区が提供した情報資産の不正な持ち出しや不適切な情報の混入を防止するため、業務に使用する記録媒体を制限すること。

（５）区が提供した情報資産の返還・廃棄

受託者は、区が提供した情報資産等について本契約終了後、速やかに区に返却するか、消去又は廃棄してその旨を書面で報告すること。

（６）記録媒体等の修理・廃棄

受託者は、区が提供した情報資産が含まれる記録媒体を有する機器を修理・廃棄する必要が生じた場合は、事前に内容を消去できる場合を除き修理又は廃棄事業者と機密保持義務を設けるとともに、廃棄時は情報資産の磁気破壊装置や消去専用ソフトによる消去、または物理的破壊等を行い、その旨を書面で報告すること。

（７）情報機器の持ち込み

受託者は、業務履行のため受託者が所有する業務用パソコン等の情報機器を区の機密区域及び業務区域に持ち込む必要がある場合は、文書をもって区の承認を受けること。また、持ち込み機器を区の機器もしくはネットワークと接続する必要がある場合については、区の情報セキュリティ対策に準じた対策を図り、その対策内容を提出して承認を得ること。

３　守秘義務

受託者は、本契約に基づき業務上知り得た情報について、第三者に開示・提供・漏えいしてはならない。なお、本契約終了後も同様とする。

４　区による監査・検査

区が、受託者に対して本契約内容における情報セキュリティ対策が遵守されていることを確認するため、必要に応じて情報セキュリティ監査又は検査を行う際に、受託者は、区の情報セキュリティ監査又は検査が円滑に遂行できるよう協力すること。

５　情報セキュリティインシデント発生時の対応

受託者は、個人情報の漏えい、紛失、盗難、誤送信等の事故が発生し、又はそれらの疑いがあるときは、適切な措置を取るとともに、至急、区に報告すること。また、区が情報セキュリティインシデントについて公表する際は協力すること。

なお、事前に情報セキュリティインシデントの状況を追跡する仕組みも構築しておくこと。

別紙２

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	