参考

仕様書

1　件名

地域包括支援センター業務支援システムの運用保守業務委託

2　契約期間

令和８年４月１日から令和９年３月３１日まで

3　委託内容

「地域包括支援センター業務支援システム」の運用保守業務

4　履行場所

中野区指定か所

・受託者事務所
・中野区役所（中野区中野四丁目 11 番 19 号）
・南中野地域包括支援センター（中野区弥生町五丁目 11 番 26 号）
・本町地域包括支援センター（中野区本町五丁目 10 番 4 号）
・東中野地域包括支援センター（中野区東中野一丁目 5 番 1 号）
・中野地域包括支援センター（中野区中央三丁目 19 番 1 号）
・中野北地域包括支援センター（中野区松が丘一丁目 32 番 10 号）
・江古田地域包括支援センター（中野区江古田四丁目 31 番 10 号）
・鷺宮地域包括支援センター（中野区若宮三丁目 58 番 10 号）
・上鷺宮地域包括支援センター（中野区上鷺宮三丁目 17 番 4 号）

5　運用保守要件

（１）運用業務要件

地域包括支援センター業務支援システム（以下「本システム」という。）の通常運用に関する要件を以下に示す。

業務名	業務詳細
①セキュリティ管理	・本システムのセキュリティ対策、インシデント対応等
②作業管理	・ジョブ実行管理
③システム監視	・システム環境を継続的に安定して稼働させるため、各機器、ネットワークの挙動を監視すること。 ・アプリケーションのプロセス監視ができること。
④バックアップ	・オンライン処理及びバッチ処理終了時等を利用して、データベースのバックアップを取得し、ハードウェア障害やソフトウェア障害等によるデータの破損を防止すること。 ・定期的にアプリケーションプログラム等のバックアップを取

業務名	業務詳細
	得することにより、ハードウェア障害やソフトウェア障害等によるアプリケーションプログラムの破損を防止すること。 ・OS等の設定情報をはじめとする情報に関しても定期的にバックアップすること。

（２）保守業務要件

本システムの保守に関する要件を以下に示す。

業務名	業務詳細
①システム保守 （ソフトウェア）	・ソフトウェアの設定変更、更新プログラム適用及び検証等 ・ソフトウェア、ファームウェアのバージョンアップ対応
②構成管理 （ハードウェア、ソフトウェア）	・運用・保守においてプログラムの変更等を実施した場合、設計書等の関連資料の更新 ・各種マニュアル・手順書・研修テキストの更新及び区への引継ぎ
③変更管理	・瑕疵対応（バグ対応） ・運用管理方式の変更対応（パラメータ設定変更等） ・連携システムの改修に伴う影響調査（改修内容の相談等）
④パッチ・パターンファイル等の適用	・サーバ及に対する各種セキュリティパッチ、ウイルスパターンファイルの適用作業の実施とセキュリティパッチ適用

（３）障害対応要件

本システムの障害対応に関する要件を以下に示す。

業務名	業務詳細
①障害一次切り分け	・障害が発生した際には、障害箇所及び原因を調査し、障害の一次切り分けを行い、速やかに区に連絡すること。
②障害復旧作業	・障害等に対応する場合は、緊急度に応じて対応マニュアル等を作成し、区に障害内容、影響範囲、障害原因、復旧対応方針等を報告し、早急に本システムの復旧を行うこと。なお、障害の復旧に時間が掛かると見込まれる場合は、事前に区と協議すること。
③復旧後の報告	・障害復旧後、復旧対応結果等を記載した障害対応連絡票を作成し、区に提出すること。
④原因究明・再発防止策の検討	・障害発生時のシステムリソース（CPU、メモリ、ディスク等）の使用状況や障害ログの解析を行い、障害原因を究明すること。 ・同一事象の再発防止及び類似事象の発生予防のため、障害

参考

業務名	業務詳細
	の根本的な原因を究明し、区と協議の上、対応策の検討・実施、再発防止策の検討・実施等を行うこと。

（４）管理者ヘルプデスクの設置

区職員からの問合せ窓口を設置し、問合せに対応すること。（障害の一次受付や保守依頼）

※問合せがあった場合には迅速かつ的確な対応を行うこと。また、問合せ履歴はすべて蓄積の上、定期的に区へ報告すること。

（５）運用保守状況報告

ア　定例運用報告書等の作成（月次）

定例作業結果、障害管理状況、問い合わせ一覧を記載すること。

なお、報告資料は電子データで提供すること。

イ　運用保守定例会議等への出席

運用保守定例会議の開催は、月１回を原則とする。

なお、区との協議により、Web 開催や書面開催も可能とする。

（６）運用保守体制

運用保守担当者については、スキルを証明する書面を区に提出すること。

運用保守担当の変更を実施するにあたっては、変更後の要員のスキルが前任者と同等以上であることを証する書面を区に提出の上、必ず事前に区の了承を得ること。

（７）運用保守受付・回答方法

運用保守の受付及び回答の対応窓口として電話及び受付用メールアドレスを用意して、契約後速やかに区に提示すること。

（８）運用保守時間

８:３０～１７：００

ただし、緊急時障害については対象外とする。

６　支払方法

各月検査合格の後、正当な請求のあった日から３０日以内に当該月分を支払う。

７　情報資産の保護・機密保持

委託業務の遂行上、知り得た個人情報及びその他機密情報の取扱いについては、別添１「情報資産を取り扱う業務委託契約事項」によること。

個人情報の保護に関する法律等を遵守し、個人情報の管理及び保護を図るための必要かつ適切な措置を講じること。

参考

8　情報システムに関する安全対策

本仕様の履行にあたっての情報システムの安全対策については別添２「情報システムに関する業務委託契約事項」によること。セキュリティ確保のため、保守サポートが得られない基盤・ソフトウェア等の利用を行わないこと。

9　知的財産権

（１）プログラムの権利

業務プログラムの著作権

本件サービスにおいて受託者が使用する業務プログラムにおける一切の知的所有権に関して、著作権法第２１条から第２８条までに定める権利を含む全ての著作権は、受託者に留保する。受託者は本件サービスにおいて中野区が利用できるように利用許諾し、これについて著作者人格権を行使しない。

（２）成果物の著作権

本業務における成果物のうち、納品された各ドキュメントにおける一切の知的所有権に関して、著作権法第２１条から第２８条までに定める権利を含む全ての著作権は、パッケージ標準に付加されるマニュアル等の原本を除き、中野区に帰属する。また、中野区によりサービス稼働時に移行またはサービス利用期間中に蓄積されたデータは、中野区に帰属する。

成果物に第三者が権利を有する著作物が含まれている場合、受託者は当該著作権の使用に関する負担を含む一切の手続を行い、第三者の著作権その他の権利を侵害していないこと。

10 その他

① 本契約の履行に当たって自動車を使用し、又は使用させる場合は、都民の健康　と安全を確保する環境に関する条例（平成 12 年東京都条例第 215 号）他、各県条例に規定する、ディーゼル車規制に適合する自動車とすること。また、自動車から排出される窒素酸化物及び粒子状物質の特定地域における総量の削減等に関する特別措置法（平成 4 年法律第 70 号）の対策地域内で登録可能な自動車利用に努めること。中野区が取り組みを進めている電気自動車等の導入の趣旨に基づき、環境負荷の少ない自動車（電気自動車、燃料電池車、プラグインハイブリッド車、ハイブリッド車）の利用に努めること。

② 本契約の履行に当たっては、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。

③ 本契約の履行に当たって発生する交通費等の諸経費は委託料に含むこと。

④ 本仕様書に記載のない事項及び解釈について疑義が生じた場合は、区と受託者双方の協議により定める。

別添１　参考

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、必要に応じて情報システム監査又は検査を行う際に、受託者は、区の情報システム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。

別添２　参考

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、記録（ログ等）が保護（改ざん防止等）の対応をすること。

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	