機密性２

令和８年度BIMソフトウェアライセンス調達及び設定業務

仕様書

独立行政法人都市再生機構

１．　調達概要

サブネットワークに接続する端末で利用するソフトウェア、及び既存のＵＲ－ＮＥＴ端末で利用するソフトウェアのライセンスの調達を実施するものである。

２．　調達内容

①ソフトウェアライセンスの種類及び数量

AEC Collection サブスクリプション シングルユーザー	更新/１年	13本
Autodesk Forma Data Management（旧 Autodesk Docs）	新規/１年	１本
	更新/１年	36本
Microsoft Entra ID Premium Plan1	新規/１年	50本

②Autodesk Forma Data Managementマニュアルの作成

Autodesk Forma Data Managementの管理者・利用者向けの作業マニュアルを作成する。

３．範囲

(1) サブネットワーク端末へインストールするAEC Collection サブスクリプションシングルユーザーライセンス調達

(2) ソフトウェアのユーザ登録、ライセンス権限の適用作業（※１）

(3) 設計業務受注者用Autodesk Forma Data Managementのライセンス適用作業代行、Autodesk Forma Data Managementプロジェクトへの設計業務受注者の招待作業代行

(4) Entra IDメンテナンス、環境設定（アカウントの新規作成、Autodesk SSO利用に必要となる属性情報作業、既存アカウントのパスワード変更等の軽微な設定修正。対応は令和９年６月までの１年間、頻度は月１回程度を想定）

※２：作業はリモートで行うこと

４．セキュリティーポリシー

別紙による

５．導入場所

２の調達物品を納入する拠点は、次に記載のとおりとする。

独立行政法人都市再生機構　本社

神奈川県横浜市中区本町　6-50-１ 横浜アイランドタワー

６．導入完了期限

２．調達内容①で定める本調達ソフトウェアの導入、及び更新作業の完了期限は 、令和８年６月21日とする。

７．契約期間

本調達ソフトウェア等のサブスクリプション期間は、令和９年６月21日とし、契約期間については、契約締結日の翌営業日から令和９年６月30日とする。

８．作業要件

・オートデスクアカウントの設定を行い、指定された Entra ID 上のアカウントと SSO 連携を行うこと。

・接続元 IP アドレスやデバイスなど、条件によりアクセスコントロールが可能な仕組みを導入すること。なお、ポリシーの設定については構築期間に別途機構と協議する。

・前提として、オンプレミスの Active Directory 環境との連携はせず、Entra ID 登録での構築となる。

・下記ソフトウェアの最新版および付属する日本仕様を指定の PC にインストール及び動作の確認をすること。

Revit, NavisWorks Manage, Civil 3D, InfraWorks, 3DS Max

・Autodesk Forma Data Management を利用するためのアカウントの登録を行うこと。

９．納品物

・パラメータシート、導入テスト計画および結果報告書、操作手順書

※：納品物については国等による環境物品等の調達の推進等に関する法律（平成 12 年法律第 100 号）に適合していること。

以　上

別　紙

セキュリティーポリシー

1.　インシデント対応

(1)　情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、受注者は、当該事項について速やかに機構に報告すること。

2.　クラウドサービスのセキュリティ要件

(1)　受注者が提案するクラウドサービスが具備しているべき条件については、以下の表のとおりとする。なお、提案時には、クラウドサービスの再販提供者として、条件の各項目について具体的な説明を行うこと。

○表

項番	区分	内容
1	資格・認証	ISO27017 を取得

(2)　受注者は、クラウドサービスで利用するアカウント管理に関する以下の措置を講ずること。

一　管理者権限を保有するクラウドサービス利用者に対する強固な認証技術を導入すること

二　クラウドサービス提供者が提供する主体認証情報の管理機能を利用して、以下の全てのパスワード要件が満たせるようにすること

イ　パスワード長を８文字以上とする

ロ　パスワードにはアルファベットの大文字及び小文字の両方を用い、数字又は記号を織り交ぜる

(3)　不正なアクセスを防止するための、以下を全て含む構築時におけるアクセス制御に係る基本方針は以下のとおりとする。

イ　クラウドサービスを利用する際に使用するネットワークに対するサービスごとのアクセス制御

ロ　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できることの確認及び適切なアクセス制御の実施

ハ　クラウドサービス利用者によるクラウドサービスに多大な影響を与える操作

の特定と誤操作の抑制

(4)　以下のクラウドサービスで利用するアカウント管理、アクセス制御、管理権限に関する情報セキュリティ対策を実施すること。

以下の管理者権限のアクセス管理と操作の確実な記録

一　クラウドサービスに対する管理者権限を持つ者の操作等の記録及び保存

二　人事異動等により管理者権限を必要とする者が交代する場合などにおける権限設定の変更

3.　情報システムのセキュリティ要件

(1)　受注者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、見直しが必要な場合には機構に提案すること。

4.　主体認証等の要件

(1)　受注者は、主体の識別及び主体認証を行う機能を設けること。なお、主体認証機能を設けるに当たっては、以下の主体認証方式を導入すること。

一　知識（パスワード等、利用者本人のみが知り得る情報）による認証

(2)　受注者は、機構外からリモートアクセス可能な主体及び管理者権限を有する主体に対する認証の強度として２つ以上の主体認証方式を組み合わせる多要素主体認証方式等の強固な認証技術を用いること。

(3)　受注者は、主体認証情報としてパスワードを使用し、主体認証情報を付与された主体自らがパスワードを設定することを可能とする場合には、辞書攻撃等によるパスワード解析への耐性を考慮し、強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用することを利用者に守らせる機能を設けること。

(4)　受注者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置として、以下の対策を講ずること。

一　主体認証情報の漏えい等による不正なアクセスを防止するため、以下を全て含む措置を講ずること。

イ　原則として、機器等において初期値として設定されている識別コードを使用しない。

ロ　不要な識別コードを無効にする。

二　主体認証情報が第三者に対して明らかにならないよう、以下を全て含む方法を用いて適切に管理すること。

イ　主体認証情報を送信又は保存する場合には、その内容を暗号化する。

ロ　主体認証情報に対するアクセス制限を設ける。

三　主体認証情報に対するアクセスに関するログを保存し、アクセスした主体を確認する。

(5)　受注者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与（発行、更新及び変更を含む。）し、管理するため、以下の措置を講ずること。

一　情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与すること。

二　識別コードの付与に当たっては、以下の措置を講ずること。

イ　単一の情報システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）を別の主体に対して付与することの禁止

ロ　主体への識別コードの付与に関する記録を消去する場合の機構からの事前の許可

三　主体以外の者が識別コード又は主体認証情報を設定する場合、主体以外の者が設定する主体認証情報は強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を設定し、主体へ安全な方法で主体認証情報を配布するよう、措置を講ずること。

(6)　受注者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するために、以下の措置を講ずること。

一　当該主体の識別コードを無効にする。

二　当該主体に交付した主体認証情報格納装置を返還させる。

三　無効化した識別コードを他の主体に新たに発行することを禁止する。

(7)　受注者は、主体の属性、アクセス対象の属性に基づき、以下のアクセス制御を実施すること。

一　利用時間や利用時間帯によるアクセス制御

二　同一主体による複数アクセスの制限

三　IP アドレスによる端末の制限

四　ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御

(8)　受注者は、以下のアクセス制御機能の実装を検討すること。

一　認証・認可の統合管理基盤を用いたアクセス制御

(9)　受注者は、主体から対象に対するアクセスの権限を必要最小限の範囲で適切に設定するよう、措置を講ずること。

また、初期値として利用可能な管理者権限を有する識別コード（Administrator、root、admin 等）には、管理者権限を付与しない又は無効化すること。

(10)　受注者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置として、以下の対策を講ずること。

一　以下のいずれかの措置を講ずること。

イ　業務上必要な場合に限定する

ロ　必要最小限の権限のみ付与する

ハ　管理者権限を行使できる端末をシステム管理者等の専用の端末とする

二　管理者権限を有する識別コードの利用は権限を必要とする業務に限定し、一般の業務として使用させないこと。

以　上