＜表紙＞

北中城村多要素認証システム構築業務及び運用保守業務

仕様書

北中城村
令和７年６月

１．概要

本仕様書は、多要素認証システム（以下「システム」という。）構築業務及び運用保守業務実施するにあたり、北中城村（以下「本村」という。）が実施する公募型プロポーザルに参加しようとする受託者が熟知し、かつ、遵守しなければならない一般的事項を明らかにするものである。

２．目的

現在稼働している二要素認証システムの機器が導入から５年以上が経過し老朽化していること、また、基幹系システムが標準準拠システムへの移行を控えていることから、システムを再構築するものである。

３．履行期限

契約締結日の翌日（令和７年８月中旬予定）から令和７年１２月４日（金）まで（予定）

４．設置施設

北中城村役場庁舎内（出先機関を含む）

５．調達範囲と内容

多要素認証システム構成は下記の環境を想定する。

※　本仕様書において「多要素認証」とは、端末及び基幹系システムへのログイン時に求められるログインID及びパスワード（知識要素）及びそれ以外の要素による認証方法を指します。

	調達（作業）項目	概要
1	多要素認証システム ※生体認証に限る。	＜ハードウェア＞ クライアント用認証センサー（100 台） 管理用認証センサー（必要時） ＜ソフトウェア＞ 認証システム関連 （クライアント250ユーザー） ＜サポート＞ メーカーサポート関連
2	多要素認証システムに係る設計・構築・運用保守作業	・多要素認証システムの構築・設置作業 ・保守／運用支援

６．システム要件

多要素認証システムにおける要件は下記の環境を想定する。

項目	内容
認証装置	① 生体要素による認証を行う装置であること。 ② 標準準拠システム移行後の基幹系システム（行政システム）にログインするために必要な規格、要件を満たした装置であること。（端末で二要素認証を実施する。基幹系システムとは連携しない想定。） ③ 新規に設置する場合のほか、端末にあらかじめ備わっている機器（ウェブカメラ（内面）、指紋認証デバイスなど）を活用することも可とする。
認証 ソフトウェア	① 生体要素による認証を行うソフトウェアで、かつ、オンプレミス環境で動作するものであること。 ② 端末で二要素認証を実施する仕組みであること。（基幹系システムログイン時は別途ユーザーID、パスワードで認証を行い、基幹系システムとは連携しない想定。） ③ （任意）直前の認証成功者のユーザーID が多要素認証画面にプリセットされるなどの方法により、利用者のユーザーID 入力の手間を省く仕組みを持つこと。 ④ ソフトウェアの設定でなりすまし対策を行った場合でも、認証速度が低下しないこと。 ⑤ Windows ログオン及びPC ロック、スクリーンセーバーロックの解除時の認証に利用可能なこと。 ⑥ Windows ログオンに関しては、既存のActiveDirectory ドメインと連携して稼働可能なこと。 ⑦ 構築にあたり、既存のActiveDirectory ドメインサーバの変更が必要な場合、その変更内容は必要最小限のものとすること。 ⑧ Windows ログオン時及びロック解除時において、多要素認証だけでなく、WindowsID/パスワードの入力を含めた二要素認証に対応可能であること。 ⑨ 多要素認証とパスワード認証の組み合わせによる二要素認証は、すべての要素の認証を実施後に認証の成否を判断することにより、どの要素の認証がエラーだったのかを利用者が判断できない仕組みであること。

	⑩ 一つのWindows アカウントを、複数の多要素認証ユーザーに設定できること。 （複数人が一つのWindows アカウントを共用する想定） ⑪ 共用のWindows アカウントを設定しているメンバー間では、Windows ロック状態を他のメンバーにてロック解除できること。 ⑫ クライアントPC がネットワーク障害等で認証サーバと通信できない場合の回避策を用意していること。なお、本機能は、ドメイン環境・ワークグループ環境のどちらでも利用可能であること。 ⑫ 利用者が怪我等により多要素認証できない場合は、管理者が該当利用者に対して非常用パスワードを発行することにより、利用者はユーザーID と非常用パスワードの手入力にてログオン可能となること。 ⑬ 管理者が非常用パスワードを発行する際には、非常用パスワードの利用可能期間、失敗可能回数を設定することが可能であること。 ⑭ 管理者が非常用パスワードを発行する際、パスワードの最低文字数や文字種（半角英字、半角数字、記号）の指定が可能であること。 ⑮ 全ての認証端末において、管理者機能が使えること。 ※管理者機能とは、多要素認証情報・テキスト系情報の登録・更新処理や、多要素認証サーバへのテキスト系情報の一括更新などを指す。 ⑯ ログオン履歴および認証システムの管理操作履歴を取得する機能を有すること。 認証ログにより、いつ、誰が、どのクライアントで認証成功／認証失敗したか特定できること。 ⑰ 氏名、ユーザーID、パスワード等のユーザー情報を、CSV 形式にて一括登録／更新／削除が可能なこと。また、登録済みユーザー情報（パスワードを除く）はCSV 形式にて抽出可能なこと。 ⑱ 蓄積されたログの中から、WindowsID／多要素認証ID／コンピュータ名／期間／対象イベント（ログオン成功／ログオン失敗 等）などをキーとしてログを抽出できるツールを提供すること。

	⑲ （任意）多要素認証情報登録画面および多要素認証情報認証画面において、センサーが撮影している生体等情報を利用者がリアルタイムに確認できるようになっていること。 ⑳ 他の利用者によってWindows ロックされたまま放置されている場合に、強制的にログオフ（又はシャットダウン）を実行できる機能を有すること。 ㉑ ActiveDirectoryドメイン環境下に、多要素認証を行う端末と行わない端末が混在する場合でも、Windows パスワードの定期変更ポリシーを有効にしたまま運用を継続できること。 ㉒ Windows 管理者権限がなくても、多要素認証システムの管理者権限さえあれば、多要素認証システムの管理ツールを起動できること。 ※多要素認証システムの管理者権限と、Windows の管理者権限は分離できること。
認証サーバ	① 多要素認証情報等の認証情報は、多要素認証サーバにて保持すること。 ② 障害発生に備え、冗長化を図ること。また、障害発生時には縮退運転が可能であること。 ③ 最適と思われるディレクトリ又はデータベースソフトを提案すること。 ④ サーバは、新たに設置すること。ただし、サーバラックは電算室内に設置された既存のラックを使用すること。（参考：Schneider製42U／ラック正面外側幅700mm） ⑤サーバは下記の条件に対応していること。 OS：WindowsServer 2025（製品がWindowsServer2025 に対応していない場合は一旦WindowsServer2022を導入後、動作確認ができ次第WindowsServer2025にアップデートすること。この場合、アップデートに要する追加費用は受託者が負担すること。） CPU：Xeon E-2434程度（製品の推奨スペックを妨げない程度とする） メモリ：16GB程度 HDD：1.0TB程度／ミラーリング バックアップ：外付けHDD／SSD：3.0TB程度 ⑥ バックアップ装置は、最適と思われる機器や仕組みを提

	案すること。必要に応じて、管理用ソフトとともに納品すること。 ⑦ UPS は、新たに設置すること。ただし、サーバラックは電算室内に設置された既存のラックを使用すること。
その他	① 多要素認証システムの設計段階では当村と受託者による打合せを行うこと。その際の旅費等の諸費用については受託者の負担とすること。 ② 多要素認証システムの構築において、既存のネットワーク管理業者及び基幹系システムベンダと打合せすること。また、その際の旅費等の諸費用は受託者の負担とすること。

７．運用保守における留意事項

(1) 問合せ及び支援作業

職員が効果的に操作及び運用できるよう助言及び技術的支援を行うこと。

ア 対応方法

原則、メール又は電話等で対応し、必要な場合は現地での支援を行う。

イ 対応時間

原則として、法令等に定める祝日等（慰霊の日、年末年始の閉庁日を含む。以下同じ。）を除く、平日8時30分から17時30分までとし、問合せには速やかに対応すること。

ただし、選挙等法令に基づき土曜日及び日曜日並びに祝日等に業務を実施する場合は、事前に協議のうえ対応することとする。

(2) 障害時対応

障害発生時及び障害の疑いがあるときは、上記(1)の対応時間内に、速やかに対応すること。

なお、時間外に受付が行われた場合、保守作業は原則として翌日の保守時間帯（翌日が土曜日、日曜日、祝日等に該当する場合は、翌開庁日）に行うものとする。緊急を要する場合は、村と受託者で協議することとする。

ハードウェア・ソフトウェア・OS 等サポート窓口は可能な限り同一にし、本村からの連絡を受け付けてから概ね当日中に現地で本業務の復旧作業を行うこと。

※ 障害対応について協議を行える連絡体制を整えること。

(3) 職員研修

職員が効果的に操作及び運用できるよう、本稼働前に下記内容で職員研修を実施すること。

「システム管理者対象研修」　　内容：管理画面、静脈センサーの使い方等

(4) その他
運営にあたり本村に有益となる運営支援等があれば提案すること。

８．成果物
本業務の成果物は以下のとおりとし、紙媒体１部及びデータを保存した電子媒体１部として納品すること。
(1) 詳細設計書（ハードウェア、ソフトウェアの設定パラメータシート）
(2) 操作マニュアル
(3) 研修資料
※（2）と（3）は、日本語で記載されている場合、メーカー発行分で代用可
(4) 保守連絡体制
(5) 業務完了報告書

９．提案及び見積
本事業の提案においては、下記①及び②の見積書をそれぞれ作成すること。記載する額の単位は円とし、税抜き額と税込み額の併記又は税込み額により記載することとする。
① 導入時費用
(1) 導入時費用には、認証ソフトウェア及び認証装置、認証サーバー、バックアップ装置、UPS（以下「認証装置等ハードウェア」とする。）を導入する際に同時購入可能な保守費用（概ね５年）を含むものとする。
(2) WindowsServer2025（本事業で調達する）と接続するクライアント端末用CALは、別途調達予定のため、本見積には含めないこと。
② 運用保守費用
①に含まれない、導入事業者による運用保守に係る費用
(1) 導入後60か月（5年）分
(2) 導入後61か月目から72か月目まで（6年目）の12か月（1年）分
※(1)及び(2)について、保守内容の内訳、月額及び総額をそれぞれ記載し提案すること。
（例）問い合わせ対応　：年〇回×〇円
メンテナンス・アップデート対応：年〇回×〇円
障害発生時対応　：年〇回×〇円
：
（その他必要な項目）
：

＜参考＞本事業で使用するクライアントについて

項目	内容
１．クライアント端末数	100台（常時80台、臨時10台、予備10台）
２．クライアントユーザー数	最大250名（職員、会計年度任用職員）
３．クライアント端末の種類等	デスクトップ型、ラップトップ型が混在 Windows10 Pro、Windows11 Pro が混在
４．認証後アクセスするシステム数	１つ（基幹系システム（総合行政システム））※標準準拠対象外システムを含む。

10．個人情報の保護

本業務を通じて知り得た個人情報については、個人情報の保護に関する法律（平成15 年法律第57 号）その他法令、規則等に基づき、適正に管理し、取り扱うこと。

11．機密保持

本業務の実施時に知り得た全ての情報の取り扱いに注意し、漏えい等が行われないようにすること。また、本業務終了後も同様とする。

12．再委託

業務の全部又は一部を第三者に委託してはならない。ただし、あらかじめ書面により本村に承諾を得た場合は、この限りではない。

13．留意事項

(1) 本業務の履行にあたっては、関係法令を遵守すること。
(2) 本業務において不明な点や、本仕様書に定めのない事項については、本村と十分協議の上、決定すること。
(3) 仕様書の内容について、本村の指示または設備上重大な問題が生じるおそれがある場合は、協議の上変更可能とする。
(4) 本業務における成果品及び中間生成物に関する一切の権利は、本村に帰属するものとする。

（以下余白）