霧島市二要素（静脈）認証システム構築業務委託及び運用保守事業

仕様書

霧島市

令和５年８月

1　概要

本仕様書は、二要素（静脈）認証システム構築業務委託及び運用保守事業を実施するにあたり、霧島市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

本市では、セキュリティ強化のため国の示す「自治体情報システム強靭性向上モデル」に基づき、個人番号利用事務系ネットワークに接続しているパソコンに対し、静脈認証を利用した二要素認証システムを導入し、セキュリティ強化を図っている。

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、安定した運用・管理を行うことが難しくなり、機器の保守サービスも終了することから新たにシステムを再構築するものである。

3　納入期限

契約締結日から令和５年 12 月 15 日（金）まで

4　設置施設

霧島市役所庁舎内（総合支所、出先機関を含む）

5　調達範囲と内容

二要素（静脈）認証システム構成は下記の環境を想定する。

	調達（作業）項目	概要
1	二要素（静脈）認証システム	＜ハードウェア＞ 認証センサー（100 台） ＜ソフトウェア＞ 認証システム関連（クライアント 600 ユーザー） ＜サポート＞ メーカーサポート関連
2	二要素（静脈）認証システムに係る設計・構築・運用保守作業	・二要素（静脈）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

項目	内容
認証装置	①　既存センサーを使用可能であること。(型番：FAT13SLD01)
認証ソフトウェア	①　１：１認証方式に対応していること。 ②　直前の認証成功者のユーザーID が静脈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。 ③　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。 ④　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。 ⑤　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。 ⑥　構築にあたり、既存の ActiveDirectory ドメインサーバを変更しないこと。(ソフトウェア等をインストールしたり、静脈認証情報を保存したりしないこと) ⑦　＜標準的な二要素認証設定＞ Windows ログオン時及びロック解除時において、静脈認証だけでなく、Windows 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。 なお、WindowsID は静脈認証サーバから取り出した値を利用し、利用者による手入力は許さないこと。 ⑧　＜簡易的な二要素認証設定＞ Windows ログオン時及びロック解除時において、静脈認証だけでなく、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。 なお、直前に静脈認証に成功した人が入力した WindowsID を画面上にプリセットすることにより、WindowsID の入力を省略する仕組みがあること。 ⑨　静脈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、複数の静脈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ことを想定。) 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は、以下の回避策を用意していること。 → 同一端末において直近でログオンしていた 50 人分のログオン情報をキャッシュしておき、キャッシュ情報を使った静脈認証によりセキュアにログオンできること。更に、キャッシュには有効期限（日数）を設定できること。 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。 ⑬　利用者が怪我等により静脈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。 ⑭　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。 ⑮　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。 ⑯　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、静脈情報・テキスト系情報の登録・更新処理や、静脈認証サーバへのテキスト系情報の一括更新などを指す。

	⑰　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。 ⑱　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。 ⑲　蓄積されたログの中から、WindowsID／静脈認証 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。 ⑳　静脈情報登録画面および静脈情報認証画面において、センサーが撮影している静脈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。 ㉑　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。 ㉒　認証クライアントに、接続先認証サーバのプライマリ・セカンダリの設定が可能であること。 ㉓　AD ドメイン環境下に、静脈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。 ㉔　Windows 管理者権限がなくても、静脈認証システムの管理者権限さえあれば、静脈認証システムの管理ツールを起動できること。 ※静脈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。 ㉕　ユニバーサルデザインの一環として、静脈認証の成功/失敗を設定によって音を鳴らせるようにできること。 ㉖　システム全体の管理者とは別に、各部門単位に管理者（以降、部門管理者と呼ぶ）を設定して、運用管理できること。 　なお、部門管理者は各自が所属する部門のユーザーのみを閲覧／更新／新規追加／静脈登録させる運用が可能であること。
認証サーバ	①　静脈情報等の認証情報は、静脈認証サーバにて保持すること。 ②　静脈認証サーバは、仮想環境にて構築可能なこと。 ③　サーバ２台での冗長化、負荷分散の構成とすること。障害発生時には縮退運転が可能であること。 ④　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。 ⑤　霧島市電算室に設置済みの仮想化基盤サーバ上の仮想マシンに組み込むこと。 ⑥　サーバ OS は WindowsServer2022 に対応していること。 ⑦　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。 ⑧　UPS は、霧島市電算室に設置済みの仮想化基盤サーバ用を使用すること。
その他	①　二要素（静脈）認証システムの設計段階では霧島市と受託者による打合せを行い、それに係る諸経費については受託者の負担とすること。 ②　二要素（静脈）認証システムの構築において、既存の仮想化基盤サーバの設置業者と打合せすること。また、その際の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、年末年始(12 月 29 日から翌年１月３日まで)を除く、平日 8 時 15 分から 17 時 00 分までとし、問合せには速やかに対応すること。

(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、祝祭日に該当する場合は、翌開庁日）に行うものとする。

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、本市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。

「情報政策課対象研修」

内容：管理画面、静脈センサーの使い方等

(4) その他

運営にあたり本市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

(4) 保守連絡体制

(5) 業務完了報告書

9　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)に基づき、適正に管理し、取り扱うこと。

10　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。本業務終了後も同様とする。

11　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、あらかじめ本市に承諾を得た場合は、この限りではない。

12　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、本市と十分協議の上、決定すること。

(3) 仕様書の内容について、本市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及び成果物の所有権、著作権(著作権法第 27 条及び第 28 条に定められた権利を含む)は、本市に帰属するものとする。

(5) 受託者は、本業務の履行にあたり必要となる人件費、出張旅費及び諸手当等の費用を全て負担すること。