別紙１

那覇市二要素認証システム
更新・運用保守業務仕様書

令和８年４月

那覇市企画財務部情報政策課

目　　次

1　背景及び目的

1.1　調達件名

二要素認証システム更新・運用保守業務（以下「本業務」という。）

1.2　背景及び目的

本市では平成２８年度より基幹系ネットワークへのログインに IC カード認証を用いた二要素認証を行っている。現行システムの保守終了に伴う次期システム導入にあたり、昨今のセキュリティ脅威に対処するため、現行の IC カード認証のほか最新技術である顔認証の導入を検討し、堅牢性と迅速な認証処理を両立する最適解をプロポーザル方式により広く求め、個人情報の適正な管理の徹底と利便性向上による業務の最適化に資することを目的とする。

2　業務概要

2.1　業務概要

（1）　二要素認証システム導入業務

二要素認証システム導入に必要な設計、環境構築、テストを実施する。

（2）　二要素認証システム運用・保守業務

二要素認証システム（ハードウェアやソフトウェア等を含む）の運用・保守を行う。

2.2　業務期間

（1）　二要素認証システム導入業務

契約締結日から令和８年７月３１日まで

①　導入期間

契約締結日から令和８年７月３１日まで

②　テスト期間

令和８年６月中旬ごろから令和８年７月３１日まで

（2）　二要素認証システム運用保守業務

令和８年８月１日から令和 13 年９月 30 日まで（６２ヶ月）

2.3　業務履行場所

那覇市役所本庁舎（沖縄県那覇市泉崎１丁目１番１号）及び本市が指定する場所

2.4　前提となる環境

（1）　ネットワーク環境

本市のネットワークは次の系統に分類し、異なる系統間では通信できないように制御している。本業務で導入する二要素認証システムのサーバ及び対象となる端末は個人番号利用事務系に属する。

No.	系統	内容
1	個人番号利用事務系	・個人番号利用事務を中心とした基幹系システムを扱う端末やサーバ等で利用するネットワーク。 ・基本的に異なる系統への通信はできないよう制御されている。
2	LGWAN 系	・メールやグループウェア等の内部情報系システムを扱う端末やサーバ等で利用するネットワーク。
3	インターネット系	・インターネットに接続する端末やサーバ等で利用するネットワーク。

（2） クライアント端末環境

本業務で導入する二要素認証システムの対象となるクライアント端末は 1,700 台で、主な端末の仕様、ソフトウェア及びシステムは次のとおりである。

No.	構成	内容
1	CPU	AMD Ryzen 5 5600GE 4.0GHz
2	メモリ	16GB
3	ストレージ	SSD256GB
4	I/F	USB タイプ A
5	光学ドライブ	なし
6	OS	Microsoft Windows®11 Pro　64bit
7	ブラウザ	Edge、Chrome
8	Office	Microsoft Office2024Professional
9	ウイルス対策	Trend Micro Apex One

（3） 認証機器

IC カード認証または顔認証いずれの場合も、本市が用意する以下の機器を利用すること。

①カメラ（顔認証による提案の場合）

本業務で導入する二要素認証に利用するカメラは、「ロジクール HD ウェブカム C270n」を利用すること。

②IC カードリーダー（IC カード認証による提案の場合）

非接触 IC カードリーダー／ライター PaSoRi（パソリ）RC-S380 を利用すること。

※IC カードは FeliCa Standard 4K 及び FeliCa Standard 6K を使用する。

（4） その他環境

①WindowsServer2025CAL は本市が必要数を確保している。

②個人番号利用事務系専用端末には資産管理システムを導入している。

③二要素認証システムについては、AD による管理は行わないものとする。

３　システム導入要件

3.1　構成要件

（1）　共通要件

①　各職員の生体（顔）またはICカードの固有情報に基づき認証を行えること。

②　本調達仕様書に示す要件を満たすシステム構成（ハードウェア、ソフトウェア、ライセンス）とすること。

③　「2.4 前提となる環境」記載の環境で動作すること。

④　正常に動作するために必要な機器、備品（接続ケーブル、OAタップ等）、ソフトウェア、ライセンスが他にある場合は、仕様に含めること。

（2）　認証・管理サーバ

①　ハードウェア要件

(ア)　「2.2 業務期間」記載の期間を通じて保守・サポートの対応ができるものであること。

(イ)　同時に端末 1,700 台から認証要求があっても動作に影響がないよう二要素認証システムが快適かつ安定的に稼働する性能を有すること。

(ウ)　ユーザの属性、Windows 認証のための情報、パスワード、クライアント設定情報、認証ログなどを管理、格納でき、これらのデータを５年以上保持可能であること。

(エ)　障害発生時等において、サーバ機能及び業務が停止しない冗長化を行うこと。また、障害が発生した機器を交換する際は、システムを停止せずに交換可能であること。

(オ)　本市が指定する 19 インチサーバラック１基内（5U 以内、電源１００Ｖ、UPS 不要）に収納すること。

(カ)　機器管理に必要なサーバ切替機、コンソールユニットは本仕様に含め、上記（オ）のサーバの数に含めること。

(キ)　ハードウェアを監視し、その結果を通知する（死活監視）機能を有すること。

②　ソフトウェア要件

(ア)　ソフトウェアの選定にあたっては、各ソフトウェア相互の動作に支障をきたさないものとすること。

(イ)　「2.2 業務期間」記載の期間を通じて保守・サポートの対応ができるものであること。

(ウ)　インストール用の媒体を１セット以上提供すること。

(エ)　「2.2 業務期間」記載の期間を通じてライセンス契約に抵触しないものであること。

(オ)「2.2 業務期間」記載の期間を通じてウイルス対策を実施すること。また、定期的にウイルスの定義ファイルの更新を実施すること。なお、導入するウイルス対策ソフトが Trend Micro Apex One である場合、本市の配信サーバを利用することも可とする。

(カ)　二要素認証システムに関するデータのバックアップを自動的に保存する仕組みがあること。

(キ)　リモートアクセスにより、システムの管理が可能なこと。

（3）　二要素認証システムライセンス

対象端末 1,700 台、ユーザ 2,000 人が利用可能なライセンスとすること。

3.2　機能要件

（1）　認証機能

①　ユーザは認証成功後、認証・管理サーバからダウンロードされた設定情報により Windows 認証を自動で行うことができること。

②　1 人で複数の端末の利用や複数人で 1 つの端末利用ができること。

③　（任意機能）複数人で 1 つの端末を利用する場合であっても認証を行った利用者個人を特定できること。またクライアント端末からログオフすることなく、ログオン操作を行った利用者に代わり、他の利用者が自身の認証情報によりロックを解除し、業務を継続可能であること。

④　ログオン時に必要な認証情報は、各職員の IC カードの固有情報または生体（顔）とすること。

⑤　顔認証による提案の場合、マスク、眼鏡等を着用していても 95 パーセント以上の確率で認証できること。写真や動画などの偽造対策がされていること。

⑥　ネットワークに繋がっていない環境においても暗号化された期限付きキャッシュ設定等により、二要素認証によるログオン認証ができること。また、ログオンを許可しない設定もできること。

⑦　IC カードの紛失又は所持忘れ（顔認証の場合の認証不具合）のユーザに対する救済措置として、代替となるワンタイムパスワードを使用できること。ワンタイムパスワード利用可能回数等の制限が設定可能であること。

⑧　クライアント端末のメンテナンス時等、二要素認証を回避するパスワードを使用できること。当該パスワードは、有効期限を設定できること。

⑨　既定の認証方法で任意の回数を超えて認証に失敗した際に、認証方式をロックする機能を有すること。

（2）　ロック機能

①　認証装置から顔または IC カードを外してもロックしない設定が可能であること。

②　スクリーンセーバー時にロックする機能を有すること。

③　簡易な操作で端末をロックする機能を有すること。

（3）　登録機能

①　ユーザ情報を CSV ファイル等で取込むことでユーザ情報及び権限の一括登録・変更処理を行えること。

②　ユーザに変更権限が与えられた情報（パスワードなど）をユーザが変更した場合、クライアント端末から認証・管理サーバにアップロードを行い、常に認証・管理サーバに最新の情報を格納する機能を有すること。

③　利用者の認証情報の登録処理は端末の各設置拠点で行うことができ、登録処理に使用する管理者アカウントは複数発行可能なこと。
④　登録可能な認証情報に上限値はないこと。
⑤　認証情報を未登録なユーザを検索し表示できること。

（4）　ログ機能
①　クライアント端末の認証時やロック解除時のログを認証・管理サーバやクライアント端末に出力する機能を有すること。そのログは、いつ、だれが、どのクライアントでの認証の成否について特定が可能なこと。
②　認証ログを一覧化するビューアー機能を有すること。
③　その他運用保守管理する上で必要な情報を管理者が画面で確認でき、CSV 形式でのデータ保存やプリントアウトが可能なこと。

（5）　運用管理機能
①　ユーザ情報、IC カード設定、顔認証設定、認証パスワード、二要素認証ソフトウェア設定情報などを、登録・変更・削除する管理ツールを有すること。ユーザが設定したパスワードは、アスタリスク等で見えない状態にできること。
②　二要素認証システムの管理ツールは任意且つ複数の端末で簡易に操作でき、ユーザに応じた操作権限を設定できること。
③　管理ツールのログやクライアント端末から送信されたログを CSV 等の形式で出力できること。
④　IC カードを回収することなくユーザの設定変更が可能で、変更された値は次回ログオン時に変更が反映されること。
⑤　管理者により認証用パスワードのロック回数、変更ポリシー（文字種、文字数、変更履歴）管理や変更履歴管理が行えること。また期限が切れる前に変更を催促する機能を有し、ユーザによるパスワードの変更が可能であること。
⑥　認証情報は、データベース上、通信経路上ともに暗号化できること。
⑦　クライアント端末への二要素認証システムソフトウェアのインストールは本市の資産配付ツールや AD による一括配付が利用できること。その際はサイレント・インストールパラメータが用意されていること。
⑧　（任意機能）業務システムとの連携は本業務の対象外とするが、将来における業務システムとの連携を見込み、連携可能なインターフェース機能を有すること。そのインターフェースは特定のメーカーに依存した言語などで開発されたものでないこと。

3.3　作業内容
（1）　基本要件
①　本市庁舎等における作業等は、平日（土曜・日曜・祝日及び年末年始休業を除く日）の午前 8 時 30 分から午後 5 時 15 分までの間に行うこと。なお、夜間又は閉庁日に作業を実施する場合は、事前に協議するものとする。
②　本市の既設サーバ及びネットワークの停止を伴う作業等職員の業務に影響する作業を実施する場合は、夜間又は閉庁日の実施を前提にすること。
③　物品等の搬入時に発生した不要物（梱包材等）は速やかに回収し、受託者の責任、負

担において、安全に廃棄すること。

（2） プロジェクトの管理

① 本業務を確実に遂行する履行・支援体制を確保すること。

② 本業務におけるプロジェクト体制、スケジュール、作業概要、プロジェクト管理方法、会議、進捗・課題管理の方法等を記載した業務計画書を提出すること。

③ 業務計画書に基づき進捗管理を行うこと。作業に関する進捗を定期的に報告し、計画に遅延が生じた場合は、原因を調査し、要員の追加等体制の見直しを含む改善策を講じること。

④ 全ての納品物に対して、目的の品質が確保されているかを確認し、品質の確保が不十分な納品物や作業に対して適切な対応、改善策を講じること。

⑤ 進捗報告、課題の検討及び解決等の会議開催及び議事録の作成を行うこと。

（3） システム設計

① 導入するシステムに関して、本仕様書を踏まえ、本市に詳細な要件を確認し、要件を定義すること。

② 要件定義に基づき、ハードウェア、ソフトウェア、ネットワーク、システム、テスト、クライアント環境等の構成や各種設定を設計すること。

③ 本市の既存の機器やネットワークの設定変更を伴う場合、それらの変更を事前に本市と協議し、内容を定義すること。

④ システム運用（人事異動等時における登録情報更新方法等）に必要な設計を行うこと。

⑤ 障害、障害の予兆、データ容量制限値到達等を本市及び受託者の保守担当へ電子メール等で自動的に通知する仕組みを設計すること。

⑥ 導入ソフトウェア等の設定情報について，バックアップ及びリカバリの設計をすること。

⑦ 障害発生時に迅速な障害回復を行うことができるよう、障害切り分け手順及び調査フロー等の障害に対する運用設計を行うこと。

（4） システム機器設置

① 基本要件

(ア) 搬入作業に当たり、搬入作業予定前までに、搬入計画書（設置図面、作業体制図、スケジュール・手順書等）及び機器一覧を提出し、本市の承認を得ること。

(イ) 機器類の搬入時には必要に応じて交通誘導員を配置するなど、安全対策を十分に講じること。

(ウ) 機器類の搬入、設置に関連して起きた一切の事故や損害、諸設備の破損等については、本市の指示に従い、受託者の責任と負担において当該設備を迅速に修理、修復又は交換すること。

② 認証・管理サーバ

(ア) 受託者は、各種設定、設置レイアウト、設置ラック数、総重量（kg）、総電力（KVA）、配線等について本市と調整を行い、その結果を本市に提示し、設置までに本市の承認を得ること。

(イ) 本市が指定する 19 インチサーバラック 1 基内（5U 以内、電源 １００Ｖ、UPS

不要）に設置し、配線を行うこと。
(ウ) サーバ管理用にサーバ切替機とコンソールユニットを設置し、配線を行うこと。
(エ) 据付に伴う LAN 配線、電源作業その他必要な部材は全て受託者で用意すること。
(オ) 搭載する各機器に、機器名称、管理番号等のラベルを貼付すること。
(カ) ラックの電源の口の利用数は最低限とし可能な限り OA タップを利用すること。OA タップは受託者で用意すること。

③ 認証装置
(ア) IC カードによる提案の場合、本市が用意する「非接触 IC カードリーダー／ライター PaSoRi（パソリ）RC-S380」を利用し正常に動作すること。
(イ) IC カードによる提案の場合、本市が利用している IC カード「FeliCa Standard 4K 及び FeliCa Standard 6K」を利用し、正常に動作すること。
(ウ) 顔認証による提案の場合、本市が用意する 「ロジクール HD ウェブカム C270n」を利用し、正常に動作すること。
(エ) 設置については、情報政策課職員との連絡を密にとり事前打ち合わせを実施すること。

（5） 二要素認証システム環境構築
① 本仕様書に基づき、二要素認証システムに必要なハードウェアの環境設定、ソフトウェア（ドライバ等を含む）インストール、設定を行うこと。
② クライアントへの二要素認証ソフトウェアのインストールは本市の資産配付ツールや AD による配信を実施するための技術的支援を行うこと。
③ 二要素認証システムを稼働する上で必要となる本仕様書に含まない本市の機器又はソフトウェア等への各種設定について、技術的支援を行うこと。

（6） システム動作検証
① 構築した二要素認証システムのテスト実施方法を提出し、本市の承認後、正常に動作することを確認すること。
② テストの結果は全て報告書を提出すること。
③ テストにおいて指摘があった場合には、本市の指示に従い、適切な処置を施すこと。

（7） 職員研修
① 研修のスケジュールや内容について研修計画書を作成し、システム稼働前の適切な時期に提出すること。
② 管理者用、利用者用のシステム操作マニュアルを作成し、研修を実施すること。

（8） 稼働支援
IC カードまたは顔認証の認証情報を登録するために必要なユーザ情報等を登録すること。

4 システム運用保守業務要件

4.1 基本要件

（1） 運用・保守業務期間
「2.2(2) 二要素認証システム運用保守業務」記載の期間とする。

（2） 運用・保守体制

受託者は保守業務の実施に際し、事前に保守業務体制図を作成し、本市の承認を得ること。なお、保守業務体制図の作成にあたっては、責任者を明確にすること。

（3） 保守対象

保守対象は、「3.1 基本要件」に示す納入物品を含む二要素認証システム一式とする。

（4） 対応窓口の設置

① 受託者は、問合せ窓口を設置し、障害や動作に関する各種問合せに対応すること。

② 窓口対応時間は、土曜日、日曜日、国民の祝日に関する法律に規定する休日及び年末年始（１２月２９日から１月３日まで）を除く平日午前８時 30 分から午後６時までとする。

4.2 運用・保守作業

（1） 共通

① 契約期間中のハードウェア及びソフトウェアの保守を行うこと。

② 「4.1(3)保守対象」の機器には、契約期間満了日までの製造メーカーオンサイト保守を付すこと。

③ 作業等でリモート接続を行う際には本市の指定する端末で行うこと。

④ 契約期間中に機器を保守交換する場合、引き上げられた機器上に残置された情報については、個人情報保護の規定を遵守し適切な対応をとり、その処理結果を報告すること。

⑤ 故障対応、保守点検等の作業で生じる梱包等の廃棄物について、関係法令等に準拠した適切な処置を講じ、責任をもって処分すること。

（2） 報告

① システムを運用・保守する上で必要な報告を行うこと。

（3） 問い合わせ

① 問い合わせについては、「4.1(4)対応窓口の設置②」記載の期間、時間帯を原則とするが、緊急時や障害発生時は本市の業務に影響がでないよう必要な支援対応を行うこと。

② システムの稼働トラブル、利用方法、改善等の技術的な問い合わせや調査依頼に対応すること。

③ 本システムを運用していく上で必要な情報の提供に努め、問い合わせ等には速やかに対応すること。

（4） 定期点検

① 定期の点検及び清掃、消耗品の交換補填、機器の正常動作を確保するための作業等の保守作業を実施すること。

② 定期点検等でメンテナンスがある場合、事前に本市と協議し業務への影響を最小限に抑えること。

（5） セキュリティ

① 契約期間満了日までの間、ソフトウェア（OS 含む）のセキュリティアップデートの適用、不具合対応のアップデート作業を行うこと。パッチ適用は、本市と協議の上で速やかに対応すること。

② 契約期間満了日までの間のＯＳやブラウザのバージョンアップに無償で対応すること。

③ システムに影響を及ぼす可能性のあるセキュリティ情報は速やかに提供すること。

④ ファームウェア、ソフトウェア及びミドルウェアのセキュリティパッチ等が公開された場合、その適用の要否を検証し、必要な場合は適用を行うこと。

（6） 障害対応

① 障害保守は「4.1(4)対応窓口の設置②」記載の期間、時間帯を原則とするが、障害の内容に応じて本市が必要と判断した場合は、時間外でも対応を行うこと。

② 障害が発生した場合、30 分以内に解決に向けた初動（障害の現状把握、対策及び復旧の目途の報告）を実施すること。また、ハードウェア、ソフトウェア、サービスの復旧作業を行うこと。

③ 障害復旧に必要な情報や手順については、適時に本市へ提供し、復旧後は障害原因および対策についてログ等の分析を行い、報告書を提出すること。

（7） 運用

① 定期人事異動時の環境変更、データ移行及び設定について、本市の設定作業を支援すること。但し、当該作業の具体的な作業手順についてドキュメント化されており、本市にて容易に実施できる場合はオンサイトでの対応は不要とする。

5 納入成果物及び検査

5.1 納入成果物

本構築業務の成果物は以下のとおりとする。納入図書は正副１部と図書の電子ファイル（PDF ファイル及び MS Office ファイルを保存した CD-ROM 等）を提出すること。以下の納入図書以外のドキュメント又は異なる内容で納入する場合は、本市と受託者間で協議するものとする。

（1） 納入図書

区分・ドキュメント名		内容	提出時期
１	業務計画書	業務プロジェクト全体をまとめたもの	契約締結後速やかに
２	設計・仕様書	要件定義及びシステムの設計をまとめたもの	初期打合せ完了後
３	納入計画書	納入体制、納入スケジュール、納入物品、機器仕様等をまとめたもの	納入前
４	テスト資料	テスト計画、テスト結果をまとめたもの	テスト実施前及びテスト実施後

5	保守・運用設計書	保守・運用の考え方、作業計画、作業内容等をまとめたもの	導入完了時
6	マニュアル	運用、保守、管理、操作（管理者用、利用者用）、障害時対応マニュアル	導入完了時
7	研修資料	研修計画書、研修テキスト	研修前
8	構成図	システム構成図、ネットワーク構成図、ラック構成図、機器一覧、ソフトウェア一覧、データフロー図	導入完了時
9	設定資料	各種設定資料	導入完了時
10	各種ライセンス書類	ライセンス等の書類	導入完了時
11	議事録	打合せの議事録	会議開催後７日以内
12	その他	本市が指定する書類	随時

（2） 納入物件

「3.1 基本要件」記載のとおり。

（3） 納入場所

那覇市役所本庁舎（沖縄県那覇市泉崎１丁目１番１号）及び本市が指定する場所

5.2 検査

本業務は、受託者が作成し本市が承認した検査仕様書に基づく検査の合格をもって業務完了とする。規定に適合しないときは、直ちに本市と協議し、必要な要件を満たすよう修正等を行い、再検査を受けなければならない。また、この修正、再検査に要する費用は受託者の負担とする。

5.3 契約不適合責任

検収後、納入成果物の不適合（バグも含む。）が判明した場合には、受託者の責任及び負担において、本市が相当と認める期日までに不具合を修正すること。ただし、受託者がかかる修正責任を負うのは、本市が不適合を知ったときから１年以内に本市から通知がなされた場合に限るものとする。

６ その他要件

6.1 機密保持

受託者は、業務実施において知り得た行政内部情報（周知の情報は除く）及び個人情報について、本業務の目的以外に使用し又は第三者に開示若しくは提供してはならない。業務上で使用するデータは、その情報が漏洩することのないよう厳格に取り扱うこと。

受託者は、本市の許可なく、取り扱う情報を指定された場所から持ち出し、あるいは複製しないこと。

6.2　遵守法令等

受託者は、関係法令を遵守し、稼動するシステムが適切適法な環境のもとで稼動及び利用できるよう業務を実施するものとする。

6.3　業務引継ぎ

本業務の履行期間の終了、一部の終了又はその他契約の終了事由の如何を問わず本業務が終了する場合は、受託者は本市が定めるところに従い、本業務終了日までに本業務を本市が継続して遂行できる必要な措置を講じなければならない。他システムへの移行及び業務引継ぎに関しては本市に対して誠意をもって支援協力するものとする。

受託者は、業務引継ぎに際しては、引き継ぐべき内容について、業務の流れ、進捗状況、資産資源の明細、資料保管場所、その他関連する業務情報等を記録した業務引継書を作成し、被引継者に対し本業務が停滞することのないように十分な説明を行った後に引き渡すものとする。

6.4　データ移行支援

次期システムに移行する場合、速やかにシステム更新ができるよう、受託者は、誠意を持って協力すること。また、本市がシステム設定情報等のデータ提供を求めた際は、無償で汎用性のあるデータ形式（CSV ファイルやテキスト等）で提供すること。

6.5　契約期間満了時における記憶媒体等の取扱い

（１）本システムの契約期間満了、または契約解除に伴い機器を撤去する際、受注者は、本システムに組み込まれた全てのハードディスクドライブ、ソリッドステートドライブ、その他一切の記憶媒体（以下「記憶媒体等」という）を、発注者に無償で引き渡すものとする。

（２）前項の引き渡しにあたり、受注者は発注者に対し、記憶媒体等に係る所有権を無償で移転するものとする。

6.6　業務適用範囲の確認

本業務の実施について、社会一般に通常実施される情報システムの構築、運用保守における作業項目は、本仕様書に記載のない事項であっても業務の範囲とする。受託者は、当該項目について疑義があるときは本市と協議することができる。