【様式4】 生体認証仕様書兼確認表

提案する製品が各項目の仕様を満たしている場合は「〇」を、
満たしていなければ「×」を適合欄に記載すること。
なお、仕様を満たしていない場合は提案できない。

大項目	項目No	項目名	生体認証（顔認証）	適合
構成	1-1	ACLサーバー ・冗長化 ・負荷分散	・認証/設定管理サーバーは、生体情報に基づき認証を行うこと。 ・既存のActive Directory及びEntra IDに変更を加えないこと。 （ソフトウェア等をインストールしたり、認証情報を保存したりしないこと） ・認証/設定管理サーバーは、ユーザーの属性やWindows認証のための情報、アプリケーション権限、暗号鍵、 アプリケーション認証用パスワード、クライアント設定情報などを管理、格納できること。 ・認証/設定管理サーバーは、クライアント端末にインストールするクライアントモジュールの設定情報を管理し、 ネットワーク経由で自動的にクライアントモジュールの更新インストール作業を行う機能を有すること。 ・認証/設定管理サーバーは、冗長化及び負荷分散構成が可能であること。	
	1-2	マネージャー端末 ・複数分散配置対応	・認証/設定管理サーバーに対して、ユーザー情報、生体認証情報、クライアントモジュール設定情報などを、 登録/変更/削除する専用の管理コンソールを有すること。 ・管理コンソールは、複数インストールが可能であること。また管理コンソールにログインするユーザーの 権限に応じた操作制限が可能であること。 ・管理コンソールは、リモートデスクトップ接続での利用が可能であること。	
	1-3	ログサーバー	・管理コンソールの操作ログや、クライアント端末から送信されたログを受信し、CSV等に 出力できること。 ・出力されたログを閲覧・検索できる機能を標準で有すること。	
	1-4	クライアント端末 ・オンライン／オフライン対応	・クライアント端末は、生体情報を使った二要素によるログイン認証がおこなえること。	
	1-5	認証要素	・顔認証の機能を有すること。 ・QRコードを利用した認証機能と併用できること。 ・写真によるログインを防止するなど、なりすまし対策の機能を有効にできること。	
	1-6	認証デバイス	・顔認証に用いる認証デバイスは、外付けのWEBカメラ（※）、またはコンピュータ内蔵カメラが使用できること。 ※本市において使用するWEBカメラは以下のとおり。 ・ELECOM UCAM-CF20FBBK 1920X1080 ・ELECOM UCAM-C310FBBK 1280X720 ・機器仕様書No.4のWEBカメラ	
動作環境	2-1	ACLサーバー	認証/設定管理サーバーは下記の環境で動作すること。 ・対応OS： Windows Server 2019 Datacenter/Standard x64 Windows Server 2022 Datacenter/Standard x64 Windows Server 2025 Datacenter/Standard x64	
	2-2	マネージャー端末	管理コンソールは下記の環境で動作すること。 ・対応OS： Windows Server 2019 Datacenter/Standard x64 Windows Server 2022 Datacenter/Standard x64 Windows Server 2025 Datacenter/Standard x64 Windows 11 Home/Pro/Education/Enterprise x64 生体情報の登録ツールは下記の環境で動作すること。 Windows 11 Pro/Enterprise x64	
	2-3	ログサーバー	ログ収集サーバーは下記の環境で動作すること。 ・対応OS： Windows Server 2019 Datacenter/Standard x64 Windows Server 2022 Datacenter/Standard x64 Windows Server 2025 Datacenter/Standard x64	
	2-4	クライアント端末	クライアントモジュールは下記の環境で動作すること。 ・対応OS： Windows 11 Pro/Enterprise x64	
	2-5	CPU	・機器仕様書No.1及びNo.2の端末で動作すること。	
データ保全機能	3-1	システムのデータの保全 ・暗号通信機能 ・認証管理サーバーでの対策	・認証/設定管理サーバーに格納されるパスワード情報、生体認証情報は暗号化されていること。 ・認証/設定管理サーバーとクライアント端末間において、通信を暗号化するか否か選択できること。 ・認証/設定管理サーバーに格納される生体情報は、生体画像から特徴点を抽出してデータ化・暗号化した状態 で格納され、デー タからの生体画像の復元は不可能であること。	
導入支援機能	4-1	一括登録 ・ユーザー情報の一括登録	・ユーザー情報をCSVファイルで、認証/設定管理サーバーにインポートするツールを有すること。 ・画像データから顔認証情報を一括登録できる機能を有すること。 ・画像データから登録された認証情報を利用する場合、初回認証時に使用した現在の顔を認証情報として、 サーバーに自動更新されること。	
	4-2	ユーザーによるWindowsパスワード 登録	・ユーザーが利用しているWindowsパスワードを管理者が知らなくとも、ユーザーによる初回ログオン時に、 Windowsパスワードの入力を求め、Windowsパスワードをユーザー情報として認証/設定管理サーバーに 登録できること。	
	4-3	クライアント登録機能	・クライアント端末に認証ソフト導入後、初回ログオン時に生体情報の登録が行えること。 ・ユーザーが利用する端末から生体情報の登録が可能なこと。かつ、生体情報の登録はユーザーの操作で完結すること。	
	4-4	クライアントインストール	・サイレントインストールが可能なこと。	
運用管理機能	5-1	マネージャー端末認証 ・管理者認証	・管理コンソールを操作する管理者を、管理者用パスワード及び生体認証に対応した端末では 生体情報で認証する機能を有すること。	
	5-2	ユーザー情報変更機能	・人事異動時などに変更情報をCSVファイルでインポートすることで、各ユーザー権限の一括変更処理が行えること。 ・顔認証成功時に定期的に認証/設定管理サーバーに格納されている顔認証情報を自動更新する機能を有すること。	
	5-3	認証デバイス登録・失効	・生体情報の有効化・無効化が設定できること。	
	5-4	パスワードポリシーの変更	・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（複雑性、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、ユーザーによるパスワードの変更が可能で あること。	
	5-5	分散管理機能	・管理コンソールを操作できる管理者権限をロールとして分類して、管理権限を委譲、分散できる機能を有すること。 ・管理コンソールの操作をログとして記録できること。	
	5-6	OUへの対応	・認証/設定管理サーバーのOU毎にセキュリティ設定情報などを設定、変更し、運用が可能なこと。	
	5-7	クライアント端末 自動アップデート機能	・クライアントモジュールがアップデートされていることを検知し、自動的に更新する機能を有すること。 また、この自動更新はスケジュール（更新期日）設定が可能なこと。	
	5-8	ユーザー情報アップロード機能	・ユーザーに変更権限が与えられた情報（パスワードなど）をユーザーが変更した場合、クライアント端末から認証/ 設定管理サーバーにアップロードを行い、常に認証/設定管理サーバーに最新の情報を格納する機能を有すること。	
	5-9	認証トークン混在時の対応	・認証トークンと生体認証が混在した環境でも、1つのシステム内で運用可能なこと。 また、ユーザーごとに認証方法を選択することが出来ること。	
クライアント機能	6-1	ユーザー認証	・ユーザーは生体証成功後、 認証/設定管理サーバー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。 ・顔認証成功/失敗時の画像を保存する機能を有すること。また、保存する画像は暗号化されていること。 ・マスク着用時において、1:1認証の認証率（他人受入率10万分の1の時の本人受入率）で99.9%以上の認証率を実現すること。 ・マスク着用時に照度変化や顔の向き、角度変動があった場合でも本人認証エラーを低減する仕組みを用いていること。 ・写真や動画によるなりすまし対策の機能を有すること。 ISO/IEC30107-3規格準拠。LevelA(低照度環境も含む）写真・スマホ等の顔画像を判定できること。 ・複数の顔を検知した際に、警告表示を行い、顔認証に移行させない機能を有すること。	
	6-2	ログオン画面の画像変更	・ログオン画面の画像を任意の画像に変更できること。	
	6-3	ロック機能	・スクリーンセーバー起動時にPCがロックする機能を有すること。 ・スクリーンセーバー起動までの時間設定が0分から999分までの間で設定可能であること。 ・離席時にPCをロックする機能を有すること。またその機能のオンオフを選択できること。	
	6-4	ロック解除	・ユーザー毎にロック解除を許可する他のユーザーを指定できること。 ・ロック解除時も二要素で解除できること。	
	6-5	緊急時の対応	・PCメンテナンス時等、一時的にクライアントモジュールを停止させるパスワードを使用できること。 ・クライアントモジュールを停止させるパスワードは、有効期限、利用可能回数、使用目的の制限が設定可能であること ・クライアントモジュールを停止させるパスワードは、数字・英文字・記号を含む複雑性を確保していること。 ・生体情報を利用できない際のユーザーに対する緊急救済装置として、生体情報の代用になるパスワードを利用できること。 ・生体情報の代用となるパスワードは、 有効期限、利用可能回数の制限が設定可能であること。 ・生体情報の代用となるパスワードは、数字・英文字・記号を含む複雑性を確保していること。	
	6-6	シングルサインオン機能	・Windows認証、Webのベーシック認証、HTMLフォーム認証に対して概ね100個程度のIDやパスワードを登録しておき、 認証要求に応じて自動的にIDやパスワードを送出し、ログインボタン等を押す機能を有すること。	
	6-7	ログ機能	・クライアントの認証時やロック解除時のログをローカルやログサーバーに出力する機能を有すること。 ・認証スコア（類似度）がログに出力されること。	