# 別紙_機能要件一覧

| 項番 | 分類 | 機能要件 | 必須 | オプション |
|---|---|---|---|---|
| 1 | 認証機器 | クライアント端末内蔵のWEBカメラが利用できること | ○ | |
| 2 | | 内蔵WEBカメラがない場合は、外付けの認証機器が利用できること | ○ | |
| 3 | | 外付けの認証機器は、USBのAタイプで動作すること | ○ | |
| 4 | | 外付けの認証機器は、バスパワーとすること | ○ | |
| 5 | 認証要素等 | 多要素認証が可能であること | ○ | |
| 6 | | 少なくとも生体情報として顔または静脈が利用できること | ○ | |
| 7 | | 二要素認証として、少なくとも生体認証システム独自のユーザーパスワードと生体情報が利用できること | ○ | |
| 8 | | 生体情報による認証が拒否された場合の代替機能があること | ○ | |
| 9 | | 利用者の変化に合わせた生体認証が可能であること | ○ | |
| 10 | | 本市と同等以上の人口規模もしくは職員数かつ2つ以上の地方公共団体に導入実績があること | ○ | |
| 11 | 生体情報の管理 | 生体情報を登録できる人数は1100人程度であること | ○ | |
| 12 | | 生体情報の保管は生体認証サーバに保存されること | ○ | |
| 13 | | 生体情報は万が一漏洩しても元の生体情報を復元することができない状態で保存されていること | ○ | |
| 14 | | 生体情報が万が一漏洩しても本生体認証システムで使用する生体情報として再利用できない状態で保存されていることが望ましい | | ○ |
| 15 | | 生体認証サーバに保存されるドメインパスワードは万が一漏洩してもパスワード解析されない状態で保存されること | ○ | |
| 16 | | 生体認証システムの管理者を認証するための機能として、IDとパスワード以外の要素を併用できることが望ましい | | ○ |
| 17 | | 生体認証システムをインストールするOSの管理者権限でも生体認証システムの管理者権限を取得することができないこと | ○ | |
| 18 | Active Directory関連 | Active Directoryと連携すること | ○ | |
| 19 | | 1つの生体認証サーバに2つのActive Directoryを連携できることが望ましい | | ○ |
| 20 | | 二要素認証のうち、連携するActive Directoryごとに利用する生体情報を設定できることが望ましい | | ○ |
| 21 | | Active Directoryに登録されているドメインユーザー情報を生体認証システムが自動で利用できることが望ましい | | ○ |
| 22 | 運用 | 本市が運用する現行の生体認証システム（C-539R-01）と少なくとも6か月間は並行運用が可能であること（クライアント端末内の併存を除く） | ○ | |
| 23 | | 被認証者の認証ログが取得できること | ○ | |
| 24 | | 生体認証システムの管理者権限での作業ログ取得ができること | ○ | |
| 25 | | 作業ログは管理者権限で改ざんされないことが望ましい | | ○ |
| 26 | | 作業ログを確認するための機能があること | ○ | |
| 27 | | 生体認証用IDの一時的な制限を行うことが可能であること | ○ | |
| 28 | | 生体認証サーバが一時的に停止してもクライアント端末及び生体認証機器のみでドメインログオンを継続できるオフライン生体認証機能を持つこ | ○ | |
| 29 | | オフライン生体認証機能の有効期間は設定可能であること | ○ | |
| 30 | | 生体認証の複数ID・生体情報に対して1つのドメインID及びパスワード（共有ID）に変換する機能があることが望ましい | | ○ |
| 31 | | 生体認証用IDの作成・変更・削除が用意であること | ○ | |
| 32 | | 生体認証情報の登録・再登録は被認証者自身で行えること | ○ | |
| 33 | | 生体認証情報の登録・再登録を被認証者自身が行えないよう制限する機能があることが望ましい | | ○ |
| 34 | | 被認証者自身で生体認証情報の変更が可能である場合、その機能が制限できることが望ましい | | ○ |
| 35 | | 生体認証システムがWindowsのケルベロス認証やドメイン認証を利用したシングルサインオンに影響を与えないこと | ○ | |
| 36 | ハードウェア等 | 保守業務期間中においてシステムの性能低下が発生せず、また機器の増設や増強が必要のないハードウェア構成・仕様にすること | ○ | |
| 37 | | 生体認証サーバは冗長構成とすること | ○ | |
| 38 | | UPSを設置すること | ○ | |
| 39 | | 構築する生体認証サーバは5U以内であること | ○ | |
| 40 | | 設置するUPSはラックマウントで3U以内であること | ○ | |
| 41 | | サーバ機器等のサポートは、少なくとも令和11年度末まであること | ○ | |
| 42 | セキュリティ | 通信の暗号化など、認証情報及びログインパスワード情報等がが通信途上で漏洩することを防止できること | ○ | |
| 43 | | 暗号化されていたとしても、上記通信パケット等が再利用されることを防止できることが望ましい | | ○ |
| 44 | | 生体認証サーバとADサーバの間にファイアウォールが設置されていても問題なく動作すること | ○ | |
| 45 | | 生体認証サーバとクライアント端末の間にファイアウォールが設置されていても問題なく動作すること | ○ | |
| 46 | | 生体認証サーバは資産管理ソフトウェア「SKYSEA」による監視対象となること | ○ | |
| 47 | | 生体認証サーバで動作するOS、ミドルウェア、ソフトウェアのセキュリティパッチは可能な限り速やかに適用すること | ○ | |

# 別紙_テスト要件一覧

| 項番 | 分類 | 機能要件 | 必須 |
|---|---|---|---|
| 1 | 作業プロジェクト | 検証については、事前に計画を本市に説明し、承諾を得てから実施すること | ○ |
| 2 | | 検証の状況や検証項目及び検証結果について、打合せ等において報告すること | ○ |
| 3 | | 検証において不具合が発生し他場合は、早急に対応を行うこと | ○ |
| 4 | | 本市の指摘に応じて必要な検証を追加すること | ○ |
| 5 | 総合テスト | 各機能が設定仕様どおりに実現されていることを確認する機能検証を行うこと | ○ |
| 6 | | クライアント端末から見た操作性を中心に、所定の性能を満たしていることを確認する性能検証を行うこと | ○ |
| 7 | | 生体認証情報、ドメイン情報の登録・変更・削除機能について、所定の性能を満たしていることを確認する性能検証を行うこと | ○ |
| 8 | | ハードウェア障害、ソフトウェア障害（論理的不整合データの発生等）からの復旧を確認する障害復旧検証を行うこと | ○ |
| 9 | | 大量のアクセス等に対して、システムが正常に機能することを確認する負荷テストを行うこと | ○ |
| 10 | | 制限外のデータが入力された場合においても、システムが正常に動作もしくは想定通りにエラー出力されるか確認する例外テストを行うこと | ○ |
| 11 | | 受託者のみのテストだけでなく、本市環境でも十分なテストを行うこと | ○ |
| 12 | | その他必要なテストを行うこと | ○ |
| 13 | 運用テスト | 本市が主体となって行う受け入れテストのテスト項目等参考となる情報を提供し、本市の支援を行うこと | ○ |
| 14 | | 本市が主体となって行う運用リハーサルテストのテスト項目等参考となる情報を提供し、本市の支援を行うこと | ○ |
| 15 | | 項番13及び14のテストについて、管理者、ユーザーそれぞれの立場でテストを実施する。テストを行う本市職員の負担が軽減する工夫を講じるこ | ○ |
| 16 | | 本市側のテスト期間を十分に確保すること | ○ |
| 17 | | 運用テスト時に提供したテスト環境は、保守業務期間中も提供され、システム改修や新機能追加及びその他動作確認等に随時利用できること | ○ |
| 18 | 連携テスト | Active Direstoryとの連携機能について、設計仕様通に実現されていることを確認する連携テストを行うこと | ○ |
| 19 | | その他本市が利用しているシングルサインオン機能に影響がないことを確認すること | ○ |
| 20 | | CSVファイル等によるドメインユーザ情報のインポート機能についてテストを実施すること | ○ |
| 21 | | その他必要な連携テストを行うこと | ○ |