吹田市二要素認証システム構築業務
仕様書

吹田市情報政策室

目次

1　背景及び目的

1.1.　調達件名

吹田市二要素認証システム構築業務（以下「本業務」という。）

1.2　背景及び目的

自治体ＤＸ　（デジタル・トランスフォーメーション）の進展に伴い、様々な個人情報や機密情報を電子的に取扱う機会が大幅に増加してきている中、さらなるセキュリティ強化が必要となってきている。そこで、LGWAN 接続系端末へのログオン時に、現行の利用者ＩＤ及びパスワードによる認証に加えて、生体情報による認証を導入することで、二要素認証によるセキュリティ強化を図ることを目的とする。

2　業務概要

2.1.　業務概要

① ＩＤ及びパスワードと生体情報（顔）を利用した二要素認証システムを本市の LGWAN 接続系端末に導入する。なお、導入について、クラウドサービス及びホスティング（ハウジング）サービスを前提とする。また、DC 等から庁内 LAN への回線構築についても作業範囲に含むものとする。

② 二要素認証システムのログオンにより Windows へのログオンができるようにする。

③ 二要素認証システム導入に必要な要件定義、設計、環境構築、テストを実施する。

④ 二要素認証システム導入に必要な、ソフトウェア、ライセンス等を調達する。

2.2.　業務期間

契約締結日から令和６年３月 31 日まで

①　構築期間、運用テスト

契約締結日から令和６年３月 31 日まで

②　本番稼働

令和６年４月１日以降（段階的なスケジュールとなるため、詳細は 2.4（2）クライアント端末環境を参照のこと。）

③　その他

令和６年４月１日以降、別途、単年度ごとの運用保守契約締結を予定しており、毎月、ライセンス費用を支払うものとする。

2.3. 業務履行場所

吹田市役所本庁舎（大阪府吹田市泉町 1 丁目 3 番 40 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 LGWAN 接続系に属する。

なお、本市ではαモデルを採用している。

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 ・原則異なる系統への通信はできないように制御されている。
2	LGWAN 接続系	・メールやグループウェア等の内部事務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	インターネット接続系	・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 （ServerBasedComputing（SBC）方式にて LGWAN 接続系からインターネット接続を行う。）

（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約 3,200 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。

① FAT 端末(一般ユーザー用)（約 2,320 台）

No.	構成	内容
1	CPU	Intel(R) Core(TM) i3
2	メモリ	8GB
3	SSD	256GB
4	I/F	USB Type-A が 3 口
5	OS	Windows 10 Pro(64bit)及び Windows 11 Pro(64bit)
6	ブラウザ	Microsoft Edge
7	ウイルス対策	Symantec Endpoint Protection

② FAT 端末(管理職ユーザー用)（約 80 台）

No.	構成	内容
1	CPU	Intel(R) Core(TM) i3

2	メモリ	8GB
3	SSD	256GB
4	I/F	USB Type-A　が 2 口
5	OS	Windows 10 Pro(64bit)及び Windows 11 Pro(64bit)
6	ブラウザ	Microsoft Edge
7	ウイルス対策	Symantec Endpoint Protection

③　シンクライアント端末（約 800 台）

No.	構成	内容
1	CPU	Intel(R) Core(TM) i3
2	メモリ	8GB
3	SSD	256GB
4	I/F	USB Type-A　が 3 口
5	OS	Windows 10 Pro(64bit)及び Windows 11 Pro(64bit)
6	ブラウザ	Microsoft Edge
7	ウイルス対策	Symantec Endpoint Protection

④　内蔵カメラ内訳

No.	構成	台数
1	あり	約 1,150 台：令和 6 年 4 月 1 日以降に本番稼働を開始する。
2	なし	約 700 台：R6.3 までに内蔵カメラ搭載 PC へ更新予定。更新後に本番稼働を開始する。 約 1,300 台：R6.8 までに内蔵カメラ搭載 PC へ更新予定。更新後に本番稼働を開始する。 約 50 台：R6.12 までに内蔵カメラ搭載 PC へ更新予定。更新後に本番稼働を開始する。

（3）その他環境

①　Active Directory（以下「AD」という。）サーバ

ア　LGWAN 接続系専用の AD サーバを設置している。

イ　AD サーバは吹田市役所本庁舎内のサーバ室に設置している。

ウ　AD サーバは仮想基盤上に構築している。

②　端末認証形態

LGWAN 接続系端末の起動後、AD サーバにて認証を行っている。

③　端末利用

１台の端末を複数人で利用する場合がある。このとき、ID を分けて運用しているケースと、共通 ID による認証を実施するケースに分けられる。また、人事異動の際に端末は移動させないため、これまで使用していた端末を別のユーザが使用する場合がある。

④　資産管理

LGWAN 接続系端末には資産管理ソフト（SKYSEA Client View）をインストールし、資産管理を行っている。

3　システム構築要件

3.1.　基本要件

本構築業務に係る調達項目及び数量は次のとおりとする。

No.	対象項目	数量	備考
1	二要素認証システム ライセンス	3,200	二要素認証導入端末 3,200 台及びユーザ 4,000 人に対応できる数量とする。
2	二要素認証システム構築	一式	本システムを提供するサーバは国内法が適用される日本国内に設置されていること。

3.2.　構成要件

（1）共通要件

① 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、ライセンス等）とすること。

② 「2.4. 前提となる環境」記載の環境で動作すること。

③ 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、仕様に含むこと。

（2）認証サーバ

⑤　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 始業等に端末 3,200 台からの認証要求が集中しても動作に影響がないよう、二要素認証システムが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、暗号鍵、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、業務が停止しない冗長化を行うこと。

⑥　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　端末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　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。

カ　障害などで OS が起動しなくなったとき、システムを再構築することなくバックアップ等から復元可能であること。

3.3.　機能要件

（1）認証機能

①　ＩＤ及びパスワードによる認証は、現行通り AD サーバにて実施できること。

②　顔による本人認証が可能であること。

③　マスクを着用した状態でも顔による本人認証が可能であること。

④　写真によるなりすまし対策ができること。

⑤　マスクを着用した状態でも写真によるなりすまし対策ができること。

⑥　1 人のユーザが複数アカウントを利用できること。

⑦　複数人のユーザが１つのアカウントの利用ができること。さらに、一度認証したユーザからログオフすることなく他のユーザに代わった場合でも、そのユーザ個人を特定できること。

⑧　認証サーバに通信でき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。

⑨　クライアント端末のメンテナンス時等、一時的に二要素認証を回避するパスワードを使用できること。このとき、有効期限又は利用可能回数等の制限が設定可能であること。

⑩　ユーザの使用する端末が変わっても本人認証が可能であること。

⑪　テレワーク勤務時（リモート接続時）においても二要素認証（場合によっては二段階認証も可）が可能であること。なお、その方法については管理者に運用負荷

を強いることがないように、協議のうえ、決定すること（カメラの使用はできないものとし、顔による認証以外も可とする）。

⑫ 代替機能における認証においても、同等程度の認証精度を実現できること。

⑬ ログオン先が WORKGROUP 環境であっても利用できること。

（2）ロック機能

① 任意の回数を超えて認証に失敗した際には認証方式のロックが可能であること。

② 端末利用ユーザが離席した際、一定時間経過後、画面ロックが可能であること。

③ 一定間隔で端末利用ユーザが本人であるということ確認し、認識できない場合、画面をロックする機能を有すること。

（3）生体情報登録機能

① ユーザ単位で生体情報を複数登録できること。

② ユーザ情報を CSV 形式などのファイルを取込むことで一括登録・変更処理を行えること。

③ 利用者の生体情報登録はクライアント端末（各ユーザー）から行うことができること。

（4）管理機能

① 認証サーバで、ユーザデータの一元管理ができること。

② マスターデータは認証成功時の最新のデータで更新できること。

③ AD に対してスキーマ拡張、新規モジュール、新規テンプレートなどを適用しなくても導入可能なこと。

④ AD にユーザ追加／削除することで自動的に認証サーバにユーザ追加／削除できること。

⑤ AD のオブジェクト単位でユーザ管理ができること。

⑥ 生体情報の生データを管理するのではなく、生体情報の特徴データを管理可能であること。

⑦ 管理者以外は生体情報の特徴データを参照・設定変更ができないこと。

⑧ 生体情報の特徴データの改ざんを防止する機能を有すること。

⑨ 管理者が生体情報の特徴データを消去できること。

⑩ 生体情報の特徴データ保存時に暗号化できること。

⑪ 実環境における運用・検証により、システム管理者が認証精度の閾値の調整が可能であること。

⑫ システム導入時期を組織又はユーザ単位で制御可能であること。

⑬ 生体情報の特徴データが未登録であるユーザを検索し表示できること。

（5）ログ機能

① 管理者の操作ログが保管されること。

② 共有アカウントを利用したログオン操作に関して、ユーザを特定できる内容が認証ログに出力されること。
③ ログを複数人の管理者が同時に閲覧できる機能を有すること。
④ 認証サーバに通信できない環境下における認証ログに関して、オンラインに切り替わった際に各端末が認証サーバに送信できること。
⑤ ログを一覧化するビューアー機能を有すること。
⑥ ログを CSV 等の形式で出力できること。
⑦ ログの保存期限は最低 5 年以上あること。
⑧ ログ出力の項目として「日時」「コンピュータ名」「IP アドレス」「ログオンユーザ名」「成否」を取得できること。

（6）運用管理機能

① 共有端末等での運用に際して、一つの Windows アカウントを複数の利用者で利用する場合、ログオフを行うことなく、利用者の入れ替わりが可能なこと。
② 認証サーバでの管理者操作画面には、認証サーバ独自の ID とパスワードでログインが可能であり、AD 上の特別な権限は不要であること。
③ クライアント端末メンテナンス操作について、運用管理者による実機操作で、生体認証なしで Windows のユーザ名、パスワードで Windows ログオン可能なこと。
④ 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（SKYSEA Client View）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。
⑤ 別途管理用の端末を用意しなくともシステムの管理ができること。
⑥ クライアント端末の設定を、サーバから変更して、クライアント側に反映させることができること。
⑦ 自動認証対象のシステムが増えた場合に、ユーザ側の設定操作なしに、管理者による認証サーバへの操作で追加設定できること。
⑧ 専用ツールなどにより容易に自動認証対象システムの追加設定が可能であること。このとき別途スクリプトを作成するなどの高度な知識がなくても追加設定が可能であること。

4　納入成果物及び検査

4.1 納入成果物

本構築業務の成果物は以下のとおりとする。原則電子ファイル（PDF ファイル及び MS　Office ファイルを保存した CD-ROM 等）を提出するものとするが、異なる方法で納入する場合は、本市と受託者間で協議するものとする。

（1）納入ドキュメント

#	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・設定書	要件定義及びシステムの設計及び各種設定をまとめたもの	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	テスト計画書	テスト計画をまとめたもの	テスト実施前
5	テスト資料	テスト結果をまとめたもの	テスト実施後
6	保守・運用設計書	保守・運用の考え方をまとめたもの	構築完了時
7	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	構築完了時
8	構成図	システム構成図、ネットワーク構成図、ソフトウェア一覧、データフロー等	構築完了時
9	各種ライセンス資料	ライセンス等の書類	構築完了時
10	議事録	打ち合わせの議事録	打合せ後７日以内
11	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。

4.2. 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。

4.3. 契約不適合責任

納入成果物に不適合があることが判明した時から１年間において、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是正を完了させること。

5　特記事項

5.1. 著作権

納入物に関する著作権（著作権法第２７条及び第２８条の権利を含む。）は、受託者又は第三者がパッケージソフトなどとして従前から著作権を有している場合を除き、

本市による代金の支払いと引換えに、本市に移転するものとする。ただし、受託者は、納入物の再利用を希望する場合は、納入物に関する著作権を取得することについて、相当な対価の額を含めて、協議を求めることができる。なお、受託者は、開発された成果物に関する著作者人格権を有する場合においても、本市及び本市の指示する者に対してこれを行使しないものとする。

5.2. 個人情報の取扱い

新システムの開発業務の中で個人情報を取り扱う場合は、本市セキュリティポリシーに則り、作業すること。なお、運用・保守業務においても同様の取扱いとなることを想定している。

「吹田市情報セキュリティポリシー」の URL を以下に示す。

https://www.city.suita.osaka.jp/shisei/1018811/1019052/1019070/1007890.html