

東広島市入退室管理システム等 構築業務調達仕様書

令和 8 年 9 月 2 4 日

東広島市

1 調達内容

(1) 調達物件の名称

東広島市入退室管理システム等構築業務（以下「本業務」という。）

(2) 調達仕様書の位置付け

本業務の調達仕様書（以下「本仕様書」という。）は東広島市（以下「本市」という。）が取り組む本業務に係る提案説明資料として作成したものである。

なお、本業務の調達は公募型プロポーザル方式を採用することから、本仕様書において市が提示した要件を達成するための解決方法や実現方法などについて提案することができる。

本仕様書に記載された要件はすべて、本市が必要とする要件である。

この要件が実現できない場合、もしくは代替案による場合は、提案書に必ずその旨を明記すること。

(3) 用語の定義

本仕様書に用いる用語の意味は、次のとおりである。

① ネットワーク

本市のネットワーク体系を以下に定義する。

A 基幹系ネットワーク

住民記録・税系・福祉系等、本市の基幹業務系システムが稼動するネットワーク。

B 内部系ネットワーク

グループウェア・財務会計等、内部情報系システムが稼動するネットワーク。

C インターネット系ネットワーク

インターネット（Web ブラウズ・メール）専用パソコン及びサーバのみが属するネットワーク。

(4) 調達の方法

本業務で調達する入退室管理システム等は、本市用に単独構築するものである。

プロポーザル参加希望者は、本市に対して本仕様書並びにサービスレベル協定（以下「SLA」という。）に定められたシステムを提供する。

(5) 契約方法

本業務の提供に係る契約は、市が実施する今回の公募型プロポーザルの結果に基づき、市と提供事業者が契約する。

契約の締結は、初期導入に係る契約、運用保守に係る契約及び延長運用保守に係る契約の3種類となる。

ただし、延長運用保守に係る契約については、本プロポーザルにおいて提案対象とし、参加者はその内容を承知した上で提案を行うものとする。なお、契約の締結については、本市と提供事業者が協議の上決定するものとし、本市は当該契約の締結を保証するものではない。

(6) 契約

① 初期導入に係る契約

契約期間は、契約締結日から令和9年3月31日までとする。

② 運用保守に係る契約

契約期間は、令和9年4月1日から令和14年3月31日までとする。

③ 延長運用保守に係る契約

契約期間及び運用保守費は本市と提供事業者が協議の上決定する。

2 業務の概要

(1) 概要

本庁舎に導入済みのＩＤ統合管理サーバ（※１）及び入退室管理システムを更新する。入退室管理システムは、管理コンピュータ、入退室制御装置、照合装置から構成され、入退室管理を行う。不審者及び不正利用者の侵入を防ぐこと、及び利便性の向上を目的とし、利用者はＩＣカード、デジタル身分証または生体情報を照合装置で認証し、扉の解錠を行うものとする。また、人事給与システムと連携して利用者情報の自動更新を行うものとする。また、入退室管理システムと連携し稼働中の公用車管理システムは更新対象としないが、現状どおりの運用ができるよう、連携を行うこと。

（※１）各システムに連携する職員データを管理するサーバ

(2) 課題（問題点）

近年、自治体における情報資産の重要性の高まりに伴い、庁舎内の物理的セキュリティ対策は、情報セキュリティ対策の基盤として位置付けられている。

入退室管理は、こうしたリスク対策の出発点であり、庁舎内の安全確保及び情報資産の保護を実現する上で極めて重要な役割を担っている。

外部委託業者や来庁者の増加に伴う、庁舎利用形態の変化により、従来の運用を前提とした管理手法では、適切な管理と利便性の両立が難しくなっている。このため、リアルタイム性や柔軟性を備えた入退室管理の仕組みが求められている。

こうしたことから、本業務の調達にあたっては、次の事項を重点的に解決する施策と位置付け、セキュリティ向上と業務の効率化・利便性の向上を図る。

- ① 本市庁舎への不審者侵入対策を強固なものにすること。
- ② 個人情報も多く保有する電算室/印刷室/ＳＥ室/作業室には、さらなる強固な不正侵入対策や機器の不正操作、不正な情報の持ち出しを抑止させる施策を講じること。
- ③ 休日や夜間における外来者の入館対応について、職員による個別対応を不要とする仕組みを構築し、業務の効率化を図ること。
- ④ 利用者がＩＣカードを携帯していない場合であっても、スマートフォン、生体認証その他の認証手段により本人確認を行ったうえで入退室を可能とすること。
- ⑤ 将来的なＩＣカード運用の見直しや認証技術の変化を踏まえ、多様な認証方式に対応可能なシステムであること。
- ⑥ ＩＤ統合管理サーバに係る運用保守対応を行い、職員情報連携及びＩＤ管理運用の継続性を担保できる構成とすること。
- ⑦ 入退室管理システムから公用車管理システムへの利用者情報連携に使用している中継ＰＣを更新または廃止し、利用者情報連携機能の継続性及び保守性を確保すること。

3 調達の範囲

本業務の全体概要を「図 3-1 東広島市入退室管理システム等構築業務全体イメージ」に示す。

(1) 調達物件

調達の範囲は、入退室管理システム等構築に関わる、コンサルタント業務、設計、機器設置、ソフトウェア開発、環境設定、及びその他構築に必要な業務である。

① 各種打合せ及び資料作成

本業務の実施に必要な打合せ、現地調査及び進捗確認会議等に参加するとともに、機器設置及びシステム構築に必要な各種資料を作成する。

② 設計

入退室管理システム等に関わるシステム設計・設備設計・各種システムの連携設計を行う。

③ 機器の設置作業

入退室管理システム等に関わる設備の設置を行う。

既設の認証機を撤去する場合は、撤去後の壁面等について原状回復を行った上で、新たな認証機を設置すること。撤去、処分及び補修に係る費用は本業務に含むものとする。

④ ソフトウェア開発

入退室管理システム等構築に関わるソフトウェア・データベースの開発作業を行う。

⑤ 環境設定

入退室管理システム等の環境設定、入退室管理システム等を構築する際に発生する市所有のパソコン・周辺機器への設定変更作業を実施する。

⑥ 試験・移行業務

システムの試験実施方針を決定し、具体的な試験計画を決める。試験計画にもとづき、各システムが設計どおりに動作することを確認する。

⑦ システム研修

今回調達したシステム一式を本番稼動開始する前に必要となる運用方法等の研修を、本市職員に対し実施する。

⑧ 本番立会

本システムの各機能等の正常な運用が確認できるまでの間は、本市からの問い合わせや障害対応に関して、即座に対応できるよう適切な支援体制を整え、立ち上げ支援を行うこと。

⑨ 運用保守

入退室管理システム等構築業務において、構築したシステム（機器・ソフトウェアを含む）の安全で正常な運転を維持するため、運用保守業務を行う。

⑩ ドキュメントの作成

設計資料、構築時の各種設定情報、運用に必要な資料を作成し納品すること。

(2) 納品物

- ① 機器（環境設定含む）
- ② ソフトウェア
本システムを正常に稼動させるために必要なライセンス数を提供すること。
- ③ 各種設計資料
 - ・実施計画書
 - ・構築体制/運用保守体制図
 - ・要件定義書、基本設計書、詳細設計書及び各種設定資料
 - ・ラック搭載図（設置機器がある場合）
 - ・電源コネクタ資料（形状、数量、電圧、電流のわかるもの）
 - ・調達機器の消費電力及び発熱量データ表（想定電力消費がわかるもの）
- ④ 操作説明書
 - ・運用保守手順書（システム管理者用）
 - ・操作説明書(利用者用)
- ⑤ 打ち合わせ議事録

(3) スケジュール

本システムの基本スケジュール(案)を下表に示す。

本業務の構築に係る詳細スケジュールについては、提案書に記載すること。

時 期	内 容
令和8年11月	入退室管理システム等構築作業に着手
	システムの仕様確定
	ハードウェアの調達
令和9年1月	機器設置（配線工事含む）
	入退室管理システム等動作検証・操作研修
令和9年3月	入退室管理システム等稼動開始

表3-1 基本スケジュール

(4) 調達の前提条件

① 現在の運用状況

本市における現在の運用状況は次のとおりである。

ア ICカード発行状況

正規職員用：1,850 枚（年間発行枚数：約 80 枚）

会計年度任用職員用：350 枚

貸出用：200 枚

イ 公用スマートフォン

正規職員に対して 1 人 1 台配布しており、Microsoft Intune により一元管理している。

現在は iPhone を利用しているが、将来的に Android 端末へ変更する可能性がある。

ウ BYOD

私用端末（BYOD）の業務利用環境を整備しており、Microsoft Intune による端末管理及びセキュリティ対策を実施している。

BYOD 端末については、iOS 及び Android の双方を利用可能としている。

エ 認証方式

職員証として利用している FeliCa 規格の IC カードを入退室認証に利用している。

② 現行設備の取扱い

認証機や制御盤については流用を妨げないものとする。ただし、流用対象機器は本仕様書に定める機能要件及び保守要件を満たし、契約期間中の保守継続が可能であること。

配線については、既設の配線設備を原則として再利用するものとする。

認証機、制御盤その他本システムを構築する機器については、有線接続または無線接続のいずれも提案可能とする。

その他、入退室管理システム等構築に必要な配線がある場合は、提供事業者にて実施すること。その際、極力配線等が目立たないような配線施工を行うこと。

無線接続を採用する場合は、通信の暗号化、端末認証、アクセス制御その他必要なセキュリティ対策を講じること。

また、電波干渉、通信障害及び停電等を考慮した可用性及び運用継続性を確保するとともに、その内容を提案書に記載すること。

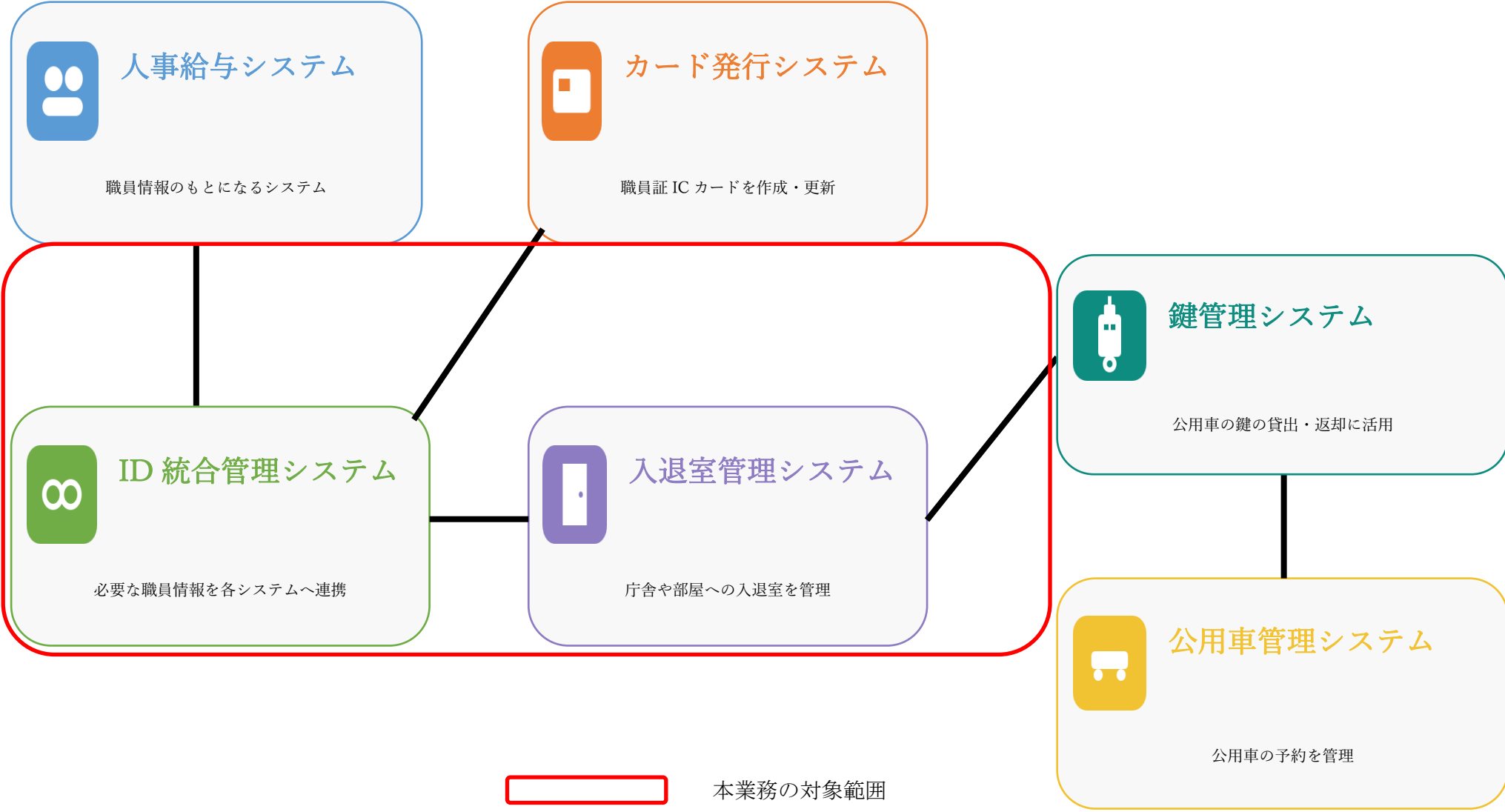
③ 電子錠について

「表 3-2 ドアタイプ及び電子錠の型番」に示す扉のドアタイプ及び型番に合った非接触カードリーダーを設置する。

ただし、サムターンカバーは設置していないため、必要に応じて設置すること。

場所	ドアタイプ・型番
本館 1F 出入口 (防災センター前)	自動ドアを制御すること。
北館 1F 出入口	美和ロック製 AL3MHD
上記以外の IC カード等 認証機を設置する扉	美和ロック製 U9AUT51-1 型(ST)

表 3-2 ドアタイプ及び電子錠の型番



「図 3 - 1 東広島市入退室管理システム等構築業務全体イメージ」

4 構築要件

「2 業務の概要」を十分理解し、セキュリティ向上と業務の効率化・利便性を向上させるよう構築すること。また、構築するに当たり、必ず次の要件を満たし構築すること。

4.1 システム基盤要件

(1) 配置形態

本システムはオンプレミス型、クラウド型のいずれの方式も提案可能とする。

提案事業者は、提案するシステム構成、通信経路、認証方式、セキュリティ対策、可用性及び保守性について明示すること。

① オンプレミス型の場合

ア 本市が採用する自治体情報システム強靱性向上モデル（α'モデル）の趣旨を踏まえ、本市ネットワークとの接続に必要なセキュリティ対策を講じること。

イ 利用者情報、認証情報及びログデータ等の重要情報については、適切な保護措置を講じること。

ウ OS、ミドルウェア及びファームウェアについて、セキュリティパッチ等を適切に適用できる構成とすること。

② クラウド型の場合

ア 本市が採用する自治体情報システム強靱性向上モデル（α'モデル）の趣旨を踏まえ、十分なセキュリティ対策を講じること。

イ 本市との通信は、LGWAN 又は閉域網等による特定通信を基本とする。

ウ ただし、インターネット経由による接続方式を提案する場合は、多要素認証、通信暗号化、アクセス制御その他十分なセキュリティ対策を講じるとともに、その安全性を提案書に記載すること。

エ 利用者情報、認証情報及びログ情報等の重要情報について、保存時及び通信時に適切な保護措置を講じること。

オ 障害発生時に備えたバックアップ及び復旧手段を備え、業務継続性を確保すること。

カ 運用保守契約終了時には、本市が保有するデータを標準的な形式で提供するとともに、事業者が保有するデータを適切に消去できること。

(2) B C P（業務継続）

サーバ、データベース及びネットワーク機器については、障害発生時の業務継続を考慮した冗長構成を採用すること。構成機器の一部に障害が発生した場合であっても、入退室管理機能を継続して利用できることとし、B C Pの観点から可用性を確保すること。

障害発生時、あらかじめ登録された認証情報を用いて入退室が可能であることとし、復旧後に認証ログを集約できる仕組みを有すること。

4.2 認証方式

(1) 基本方針

本市における認証方式は、I Cカードに限定しないものとする。

現在利用している FeliCa 規格の I Cカードを利用可能であることが望ましいが、本市は将来的な認証技術の変化及び運用負荷軽減を考慮し、スマートフォン認証、生体認証、Q Rコード認証その他同等以上の認証方式を活用した提案を推奨する。

また、認証媒体については、将来的なデジタル身分証サービスその他の認証サービスとの連携又は移行を妨げない構成であること。利用者情報及びアクセス権限情報は、認証媒体と分離して管理できることが望ましい。

提案事業者は、提案する認証方式について、安全性、運用性、利便性、保守性、将来性及び認証媒体の追加又は変更への対応性を明示すること。

(2) ICカード認証

現在職員証として利用している FeliCa 規格の IC カードが利用可能であること。

カード発行については、現在運用中のカード発行システムとの連携又は継続利用を妨げないものとする。

ただし、提案する認証方式においてカード発行システムとの連携を必要としない場合は、この限りではない。

(3) スマートフォン認証等

本市は正規職員に公用スマートフォンを配布しており、BYOD 環境についても整備している。

このため、公用スマートフォン又は BYOD 端末を活用した認証方式を提案する場合は、特定のスマートフォン OS に依存しないことが望ましく、iOS 及び Android の双方で利用可能であること。また、認証媒体の追加又は変更を行う場合においても、利用者情報及びアクセス権限情報を維持したまま運用継続できることが望ましい。なお、将来的な拡張性や互換性については本調達の必須条件とはしないが、対応方針を提案書に記載すること。

その他にも、提案事業者は、生体認証や QR コード認証その他同等以上の認証方式を提案できるものとする。

(4) 認証機器

① 書庫・議会図書室は入室側のみ認証機を設置し、退出時は手動でサムターンを回して開錠し退室できること。(別紙 1 庁舎図面参照)

② 本館 1 F 出入口、北館 1 F 出入口、電算室、印刷室、S E 室、作業室、1 F ロビー及び 10 F ラウンジは、入室側・退室側双方に認証機を設置すること。

③ 無線接続を利用する場合は、通信方式、暗号化方式、認証方式及び障害発生時の対応方法を提案書に記載すること。

(5) 生体認証

① 電算室については、生体認証機器を出入り口に設置すること。

② 生体認証方式は、指静脈認証、顔認証、指紋認証その他同等以上の認証方式を提案可能とする。

4. 3 入退室管理

(1) 基本要件

本システムは、職員、会計年度任用職員、委託事業者その他利用者ごとに入退室権限を設定し、庁舎及び各室への入退室を適切に管理できること。

認証方式の種別にかかわらず、統一的な利用者管理及び権限管理が行えること。

(2) 入退室ログ管理

認証ログ、入退室ログや管理者操作ログを取得し、検索、抽出できること。

(3) 入退室制御

認証成功時のみ解錠できること。

扉の開放状態が一定時間継続した場合は警報または通知を行えること。

(4) セキュリティ機能

アンチパスバック機能を有し、設定有無を選択できること。

異常時又は停電時の閉じ込め防止対策を備えること。

4. 4 ID 統合管理

(1) IC カード発行/入退室管理システム/公用車管理の「ID 情報」・「操作権限情報」を一元管理する。利用者 ID、認証媒体及びアクセス権限情報については、論理的に分離して管理できることが望ましい。

- (2) 人事異動やＩＣカード紛失時の失効処理を確実に行之、さらに運用管理の負担軽減が可能な機能を提案すること。

4. 5 システム連携機能

稼動中の人事給与システム、カード発行システム、鍵管理システムと連携し、下記の要件を満たすこと。ファイル連携方式は問わないが、運用性、保守性及びセキュリティを考慮した方式を提案すること。また、デジタル身分証サービスその他認証サービスとの連携を考慮し、標準的なデータ交換方式又はアプリケーション連携方式を採用していることが望ましい。これらの連携に当たっては、通信暗号化、アクセス制御、連携エラー検知及び連携履歴の確認機能を有することが望ましい。

(1) 人事給与システム連携

- ① 人事給与システムから、入退室管理サーバの指定フォルダ内に出力される利用者情報ＣＳＶファイルを随時監視し、ファイルがある場合に取得し、利用者の新規登録、及び登録済の利用者の更新ができること。

なお、利用者情報の定期連携処理は毎日午前３時４０分に自動実行するものとする。

- ② ＣＳＶファイルについては既存システムと同じ仕様とすること。連携データ項目は別紙２「連携項目一覧」のとおりとする。

(2) カード発行システム

- ① 新規カード発行及びカード再発行に必要なＣＳＶデータを出力し、カード発行システムに送信すること。

- ② カード発行システムからカード発行後に出力されるＣＳＶファイルを取得し、入退室管理システムの利用者情報を更新できること。

- ③ ＣＳＶファイルについては既存システムと同じ仕様とすること。連携データ項目は別紙２「連携項目一覧」のとおりとする。

(3) 鍵管理システム

- ① 鍵管理システムの利用者登録・更新・削除に必要なＣＳＶファイルを、鍵管理システム管理コンピュータの指定フォルダ内に出力すること。

- ② ＣＳＶファイルについては既存システムと同じ仕様とすること。連携データ項目は別紙２「連携項目一覧」のとおりとする。

(4) 連携システム更新提案

- ① 入退室管理システムの利用者は、現状ＩＤ８桁で登録されている（職員ＩＤ６桁＋更新回数２桁）。システム更新時に、職員ＩＤ６桁での管理に変更することが望ましい。この場合、更新回数はカード情報として管理し、紛失したカード等、最新のカード以外は利用できないようにすること。

4. 6 本番立会と稼動支援

本システムの本番稼動に際して、初期設定の確認及び各機能等の正常な運用が確認できるまでの間（１か月間程度を想定。）は、本市からの問い合わせや障害対応に関して、即座に対応できるよう適切な支援体制を整え、立ち上げ支援を行うこと。

4. 7 教育要件

本システムの機能を理解し、管理方法等を習得するために本番稼動開始前に本市職員に対する研修を実施すること。

研修の種類・方法等のイメージを以下に示す。具体的な研修方法を提案書に記載すること。

実施項目	内容
対象者	管理者（主に職員課・DX推進チーム・管財課の職員）
研修回数	1回程度
研修時間	3時間程度／1回
研修内容	管理者が習得すべき事項についての研修を行う。
その他	研修会場は本市で用意するが、講師及び研修参加人数分の研修テキストは、提供事業者が用意する。

表4-1 運用保守研修

5 運用要件

5. 1 セキュリティ

本システムの情報セキュリティ要件は、「情報セキュリティマネジメントシステム（ISMS）適合性評価制度」に適合していること。

情報セキュリティ要件を「表5-1 情報セキュリティ要件」に示す。

管理の方法	内容
システムセキュリティ	各種資源（データ、プログラム、ネットワーク、入出力機器、記憶領域等）へのアクセス権限者を明確に定めること。 ID、パスワードの登録、発行、更新、抹消、保管について管理方針を定め、特定のものが管理できること。

表5-1 情報セキュリティ要件

5. 2 導入機器の保守

本業務にて導入する機器一式は、令和9年3月1日から令和14年3月31日までの使用を前提としており、使用期間中は保守できるものとする。

使用期間中の保守ができない機器がある場合は、新しい機器に更新する費用とそれに伴う作業費を提案に含めること。

5. 3 運用保守管理

(1) 稼動時間

本システムの稼動時間を「表5-2 稼動時間」に示す。

計画停止及び予定外の停止時間については、SLAにおいて基準値を設定すること。

機器・システム	稼動時間
全般	24時間 365日

表5-2 稼動時間

※法定点検による停電に伴う一時停止等は認める。

※バックアップ等によるサーバの一時停止・サーバの再起動は含めない。

（認証機、鍵管理BOXは除く）

(2) 保守管理

システムの安定的運用を図るための保守管理方法を「表 5-3 保守管理内容」に示す。

OS セキュリティパッチ・ファームウェアアップデート等修正情報の適用については、SLA において基準値を設定すること。ハードの不具合割合について、SLA において基準値を設定すること。

保守管理の方法	内容	
ソフトウェア保守	必要に応じて、ソフトウェアの機能改善や変更を行うこと。 また、使用期間中に WindowsOS やサーバ OS のセキュリティ情報のアップデートサービスのサポートがなくなった場合は、サポートがあるバージョンの WindowsOS やサーバ OS、スマートフォンの OS に対応すること。	
ハードウェア保守	入退室管理 (本館 1 F 出入口、北館 1 F 出入口、 1 F ロビー、10 F ラウンジのみ)	24 時間 365 日
	上記以外の機器	平日 8:30~17:15

※一定割合以上での不具合が発生するハードウェアについては、ハードウェアの機能改善や変更を行うこと。

表 5-3 保守管理内容

(3) SLA の締結

本システムの提供に当たり、「表 5-4 サービス品質基準」及び応募者からの提案をもとに、提供事業者は、本市と協議して運用保守開始日までに SLA を締結する。

SLA の提案は、サービスレベルのモニタリング実施方法及びサービスレベル基準値を満たすことができなかった場合のサービス対価の減額等のルールも含めて提案すること。

サービスレベル項目		内容	基準値
システムの信頼性	障害復旧予定時刻の報告	障害の連絡から本市へ復旧予定時間を報告するまでの時間	24 時間以内
	障害対応時の保守員到着時刻	障害の連絡から現場に到着し、障害調査を開始するまでの時間	2 時間以内
	障害状況の一時報告	障害の連絡から本市へ障害状況を一時報告をするまでの時間	当日中
	リカバリーポイント	障害発生時の復旧が可能な基点	直近バックアップ時点

表 5-4 サービス品質基準

① SLA の見直し

SLA の項目及び基準値は、必要に応じ、本市と提供事業者が協議して見直すことができる。

② SLA 達成状況の報告

提供事業者は、障害に関する事項について随時報告すること。

(4) データ管理

入退室管理システム運用のために必要なデータや設定情報については定期的にバックアップを行うこと。

データ管理の方法及び内容を「表 5-5 データ管理内容」に示す。

データ管理項目	データの管理方法	内容
バックアップ	定期バックアップの実施	障害時の回復目標に対してバックアップ手法を定めること。バックアップツール等を導入し、定期的にバックアップが行えること。 バックアップは少なくとも1日1回自動取得することとし、取得したバックアップデータは1年以上保管すること。 また、バックアップデータの保存期間、保存世代数及び取得頻度について提案書に記載すること。 障害発生時には、バックアップデータを用いてシステム及びデータを復旧できること。
リストア		想定される障害について、あらかじめ取得したバックアップからのリカバリー方法が示されていること。

表 5-5 データ管理内容

(5) 構成管理

稼動後に、認証機等の増設等の使用環境変化に対応できること。

(6) ドキュメント管理

必要とするドキュメントの管理を「表 5-6 ドキュメント管理一覧」に示す。

ドキュメント	内容
各種技術資料	機器・サーバ運用保守に係る各種技術資料を整備すること。 必要に応じて改定し、常に最新の状態に保つこと。
各種操作説明書の整備	操作説明書等各種マニュアル類を整備すること。 必要に応じて改定し、常に最新の状態に保つこと。
議事録	打合せ等の結果は、議事録を作成し本市の承認を得ると共に保管すること。

表 5-6 ドキュメント管理一覧

(7) 実績報告

運用実績について報告すること。

運用実績報告に必要な項目を「表 5-7 実績報告書項目一覧」に示す。

報告事項	報告時期	内容
S L Aに関する報告	必要時	S L Aの達成状況に関する報告
障害報告	半期	障害対応実績（障害発生 of 報告を除く。）
その他	都度	上記以外の一時的業務遂行についての報告 更なるサービス品質向上に向けた提案

表 5-7 実績報告書項目一覧

5. 4 運用支援

(1) 研修

人事異動により、新たに本システムの運用保守業務に従事することとなった本市の職員に対し、契約期間中、少なくとも年1回操作研修を実施すること。

操作研修の内容を「表5-8 操作研修内容」に示す。

研修形態	実施時期	内容
集合研修	毎年4月～5月	パーソナルコンピュータを使って、実際に運用管理ソフトウェアを利用して運用管理の実習を行う。 研修会場、パーソナルコンピュータは、本市で用意する。

表5-8 操作研修内容

6 関連システム環境要件

入退室管理システム等に関わる関連機器・システムの環境要件を以下に示す。

6. 1 ネットワーク環境

(1) パソコン等機器のセグメント

機器(パソコン、認証機など)を設置するネットワークセグメント体系は、基幹系ネットワークセグメント・内部系ネットワークセグメント・設備系ネットワークセグメント・インターネット系ネットワークセグメントの4つあり、それぞれのセグメントにある機器間の通信は原則不可としている。

ただし、必要に応じて一部の内部系ネットワークセグメントにある機器(パソコンなど)と設備系ネットワークセグメントにある機器との通信を許可する。

今回調達するシステムに接続するパソコンは、内部系ネットワークセグメントにあるパソコンと、インターネット系ネットワークセグメントにあるパソコンを想定している。

なお、本業務に関わるパソコン環境を、「図6-1 入退室管理システムに関わるネットワークイメージ」に示す。

(2) サーバセグメント

サーバが属するセグメントは、内部系サーバセグメント・設備系サーバセグメント・インターネット系サーバセグメントの3つある。

内部系サーバセグメントにあるサーバは、内部系ネットワークセグメントにあるパソコンと通信が可能である。インターネット系サーバセグメントにあるサーバは、インターネット系ネットワークセグメントにあるパソコンと通信が可能である。

なお、設備系サーバセグメントにある機器(サーバなど)は、内部系ネットワークセグメントにある機器(パソコンなど)と通信は可能とする。

それぞれのサーバセグメントにある機器(サーバなど)は、他のサーバセグメントとの通信は不可とする。

ただし、内部系サーバセグメント内の機器と設備系サーバセグメント内の機器との間で通信が必要な場合は許可する。

インターネット系サーバセグメントは、他のサーバセグメントとの通信は許可をしない。

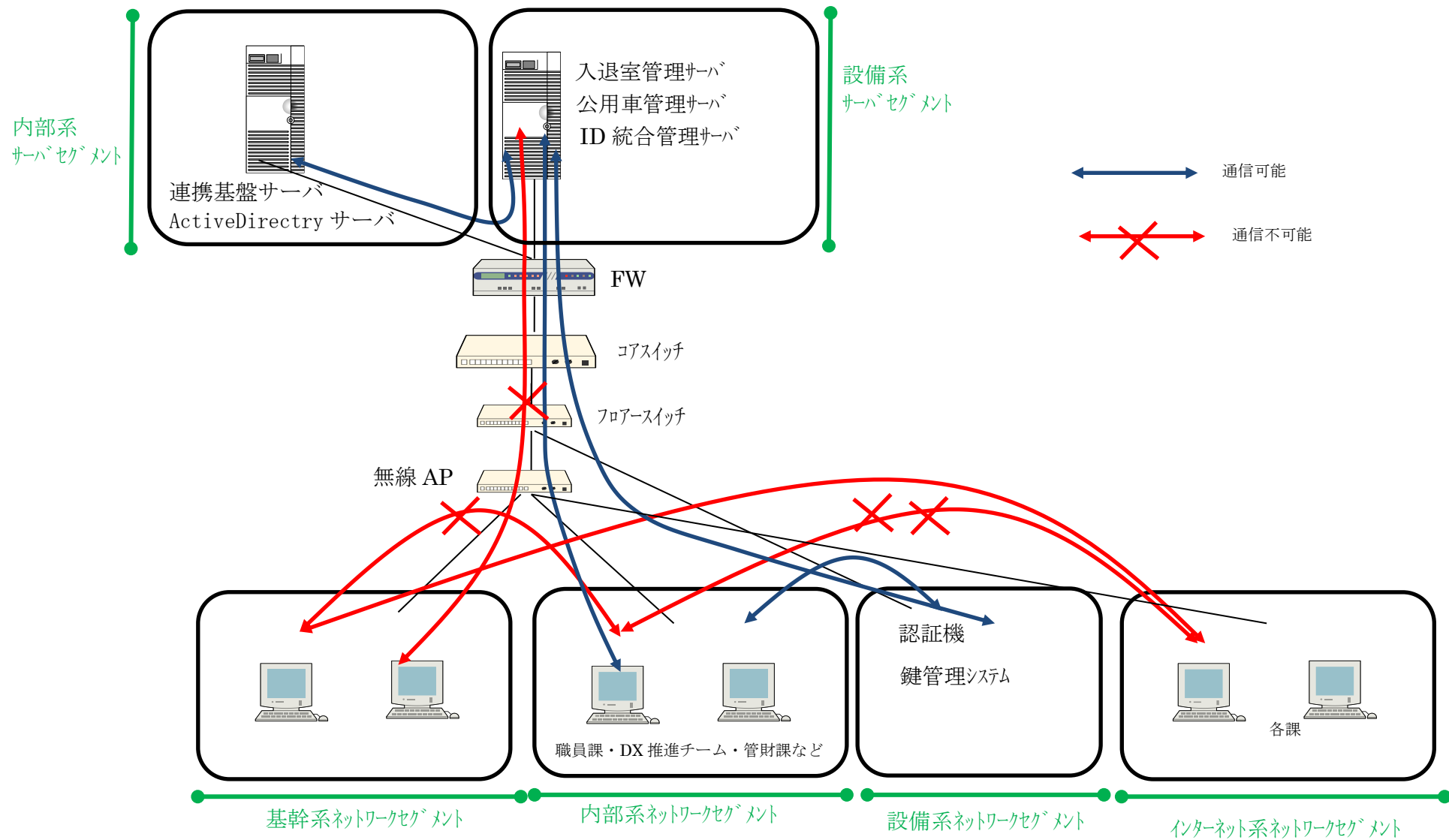


図 6 - 1 入退室管理システムに関わるネットワークイメージ

7 移行要件

7. 1 契約期間満了時の扱い

本システムの運用保守契約が満了した際、本市は、契約を終了するか延長するか、あるいは、契約の一部を終了（※１）し一部を延長するか、選択できるものとする。

契約を延長する場合（一部延長）の運用保守費用は、当初契約の期間満了月（最終月）の月額運用保守費用と同額、またはそれ以下（※２）とすることを基本に、協議の上、決定するものとする。

なお、延長契約が満了した際の扱いも、原則、同様とする。

（※１）基本機能以外（いわゆるオプション機能）の使用中止などを想定

（※２）一部を終了すること等による運用保守費用の引き下げを想定

7. 2 契約期間終了後の扱い

(1) 移行支援

本システムの提供に係る運用保守契約が終了（一部終了を含む。）し、別事業者が次期システムを構築する場合、提供事業者は、本市と協議の上、設定情報の提供等必要な支援作業を行い、円滑な移行に寄与すること。

(2) 機器等の無償譲渡

本システムの提供に係る契約が終了し、本市が希望する場合は、本業務により導入した機器、附属設備その他システム運用に必要な資産について、本市へ無償譲渡すること。

また、無償譲渡に際しては、当該機器等の設定情報、運用保守に必要な資料及びライセンスの利用権限（譲渡可能なものに限る。）を併せて引き継ぐこと。

8 情報の管理

提供事業者は、本システムの提供にあたっての情報管理については、次の点に留意すること。

- (1) 本システムの提供に携わる者は、秘匿情報等の管理を適性かつ厳格に行うこと。
- (2) 本システムの提供に携わる者は、業務の遂行を通じて知り得た情報を漏らしてはならない。その職を退いた後も同様とする。
- (3) 本市が定めるセキュリティポリシーを遵守すること。