地方独立行政法人大阪市民病院機構
情報基盤の構築・移行業務委託及び
クラウドサービス提供業務仕様書

令和８年８月

地方独立行政法人大阪市民病院機構

第 1 章　総則

1.1 調達件名

情報基盤の構築・移行業務委託及びクラウドサービス提供業務

1.2 調達の概要

地方独立行政法人大阪市民病院機構（以下、「発注者」という。）は平成 21 年９月に、主に事務系職員が利用する情報基盤として『病院事業ネットワーク』の構築を行い、また平成 22 年 10 月には医師向け情報基盤として『医学情報収集ネットワーク』の構築を行った。

令和９年１月 31 日にこれら情報基盤システムの契約が満了となり、リプレースが必要となるため、『病院事業・医学情報収集ネットワークシステム』（以下、「本システム」という。）の調達を実施する。あわせて AWS への通信回線の調達を実施する。

本システムでは、必要となる各機能をクラウドサービスとして利用する。

1.3 基本方針

本調達における基本方針を以下に示す。

1. 構築期限

受注者は必要なサービスを提供する基盤の構築及びデータ移行などを実施し、令和９年１月 31 日までに本システムを稼働させる。

2. システム構築

受注者はサーバ機器等のハードウェアを自社資産としてデータセンター等に導入しサービス提供する（以下、「プライベートクラウド」という）、もしくはパブリッククラウドを利用したサービス提供を行うこと。

3. 既存パソコン等の継続利用

病院事業ネットワークおよび医学情報収集ネットワークを利用するパソコン等は下表のとおり。

（内訳表）令和８年５月末時点

	設置場所	パソコン	プリンタ
病院事業（貸与）	センター	646 台	75 台
	十三	146 台	17 台
	住之江	7 台	4 台
病院事業（人事給与・財務会計システム専用端末）	センター	29 台	12 台
	十三	7 台	4 台
	住之江	2 台	2 台
医学情報（貸与）	センター	357 台	12 台
医学情報（十三）	十三	3 台	3 台

パソコンの OS はすべて Microsoft Windows 11 Professional

表 1.3.1 既存パソコンの利用状況一覧

1.4 システムの全体像

構築時のシステム全体構成図を下記に示す。

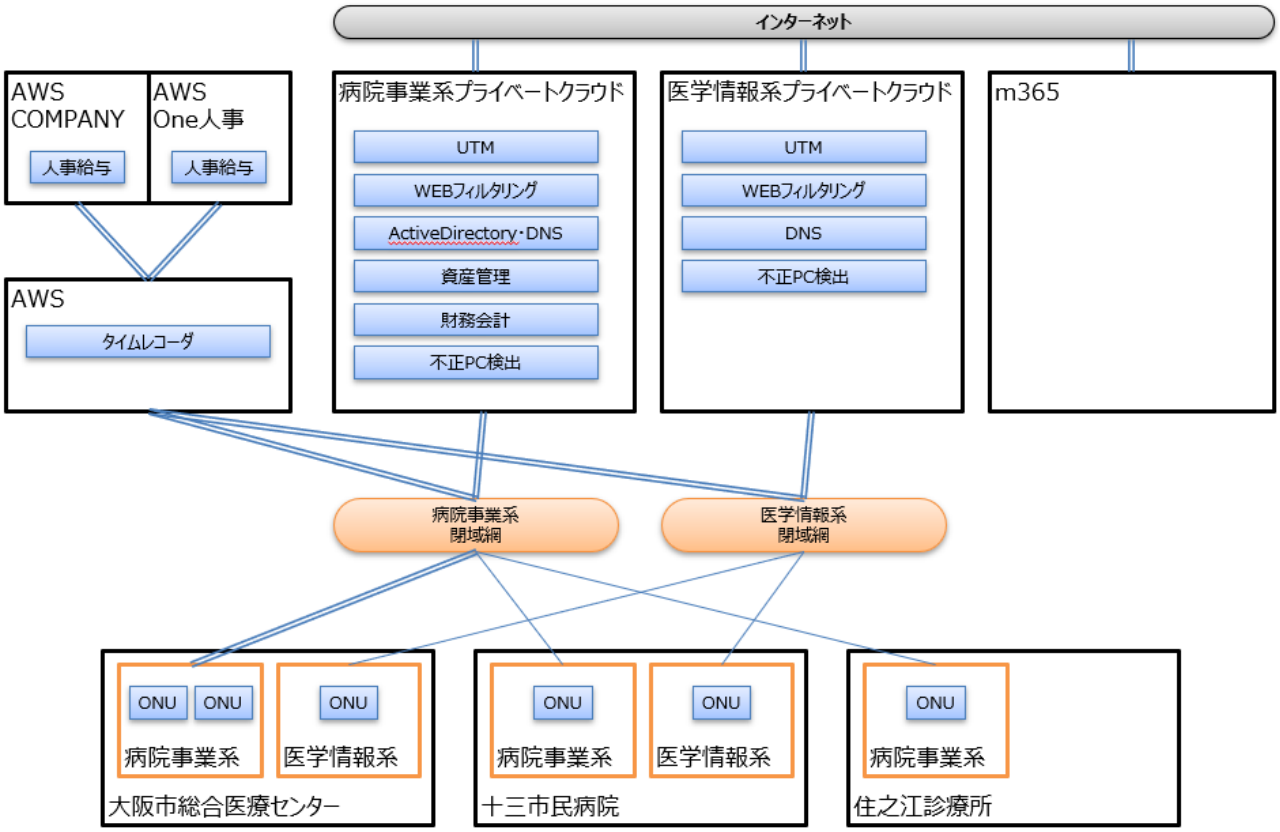

図 1.4.1　システム構成図

1.5 協議など

発注者及び受注者は、本仕様書の各条項の解釈に疑義のある場合及び本仕様書に定めなき事項については互いに誠意をもって協議し、その解決を図ること。

第 2 章　調達の概要

2.1 全体の調達概要

本システムの構築、移行及びサービス利用について、本仕様書による調達を行うこと。

2.2 場所一覧

本システムを利用する場所を以下に示す。

名称	住所
総合医療センター	大阪市都島区都島本通 2-13-22
都島センタービル	大阪市都島区中野町 5-15-21
十三市民病院	大阪市淀川区野中北 2-12-27
住之江診療所	大阪市住之江区東加賀屋 1-2-22

表 2.2.1 場所一覧

2.3 調達範囲

本調達における作業範囲を以下に示す。なお、受注者は構築するシステムの稼働責任を負うこと。発注者及びアプリケーションベンダーからの問い合わせ窓口を一元化し、回答については発注者と協議のうえ受注者の責任において主体的に行うこと。

(1) 本システムの構築及び運用にかかる運用保守環境等構築

(2) AWS、本システム、インターネットへ接続するための通信回線ならびに回線終端装置の調達、接続や連携方法の提案及び発注者が承認した提案に沿った作業

(3) 本システム調達に伴い発生する既存ネットワーク機器の設定変更、端末の設定変更作業、新規ネットワーク機器への置き換えが必要な場合はその調達と構築作業

(4) 本システムの構築及び運用するためのソフトウェア及びハードウェア機器等の選定ならびに構築、必要な契約手続

(5) AWS 上の２システム（人事給与：COMPANY、人事給与：One 人事）に対する接続に必要なコンポーネント(TGW など)一式の構築、及びタイムレコーダサーバ向けの IaaS 提供、及び v2v 移行。AWS の運用、請求代行。

(6) その他(1)から(5)を行うために必要な業務

2.4 調達及び契約

2.4.1 調達スケジュール

本システムの調達に関する期間を以下に記載する。

(1) 構築、移行にかかる業務

契約締結日から令和９年１月 31 日まで

(2) サービス利用期間

令和９年２月１日から令和 14 年１月 31 日まで。ただし、住之江診療所に関しては閉院に伴い、令和９年２月１日から令和９年４月 30 日までとする。

2.5 納入物

2.5.1 提出物

本業務に伴う提出物は紙と電子媒体により提出すること。なお、提出物の著作権は当センターに帰属するものとし、提出期日や部数等については別途協議のうえ決定する。

No	提出物	提出期限	概要
1	情報セキュリティ誓約書	契約締結後１週間以内	セキュリティ要件を遵守する誓約書
2	プロジェクト体制図	契約締結後１週間以内	受注者の指揮監督系統を示す体制表 業務に従事する従事者の名簿
3	プロジェクト計画書	契約締結後１週間以内	プロジェクトの範囲や工程、組織・要員計画、移行方針等を記載したドキュメント
4	システムテスト仕様書兼結果報告書 運用テスト計画書 運用テスト実施手順書	作業時随時提出	試験観点、試験の開始／終了条件、試験管理方法等、試験の実施要領及び試験結果の報告を行うドキュメント
5	作業完了報告書	作業時随時提出	事前準備作業結果及び作業実施結果等を報告するドキュメント
6	システム基本設計書	令和９年１月 31 日	環境設計及び見直し等を行った結果を記載したドキュメント
7	システム詳細設計書	令和９年１月 31 日	システムの詳細設計及び見直し等を行った結果を記載したドキュメント
8	サービス仕様書	令和９年１月 31 日	SaaS の仕様を記載したドキュメント
9	ヒアリングシート	令和９年１月 31 日	SaaS の利用に際し､ヒアリング結果を記載したドキュメント
10	管理者マニュアル ユーザマニュアル	令和９年１月 31 日	システム管理者に必要なマニュアル及びユーザマニュアル等の関連ドキュメント
11	障害時対応マニュアル	令和９年１月 31 日	システムの障害対応に必要なマニュアル及び関連ドキュメント
12	WindowsOS 更新プログラム配布マニュアル	令和９年１月 31 日	IT 資産管理機能での WindowsOS の更新プログラムの配布方法を示したドキュメント

表 2.5.1.1 提出物一覧

2.5.2 納入場所

地方独立行政法人大阪市民病院機構

大阪市都島区都島本通 2-13-22　大阪市立総合医療センター　4F　医事課（システム）

2.5.3 検収

受注者は納入場所において発注者による検収を受けること。

(1) 検収の結果、納入物の全部または一部に不合格品が生じた場合には、受注者は発注者が指定した日時までに修正したものを再納品し、再検査を受けること。

第3章　病院事業及び医学情報収集ネットワークの要件

3.1 基本方針

本システムをクラウド上に構築し、クラウドへ接続するための通信回線敷設もあわせて実施する。病院事業ネットワークと医学情報収集ネットワークそれぞれに必要とする機能は本章の各項に記載のとおり。

3.2 病院事業・医学情報収集ネットワークの設計及び構築作業

本仕様書で示す要件に基づき、本システムの設計及び構築作業を実施すること。作業にあたっては、発注者に作業内容等を事前に提示し承認を得ること。業務影響が発生する作業は基本的に夜間および休日・祝日で行うこと。発注者の立ち会いについて、最小限の負担になるよう考慮すること。

3.3 機能要件

3.3.1　共通要件

3.3.1.1 システム管理機能

ユーザ情報の登録、削除等の管理機能やその他システム運用に必要な設定を行う管理機能については、Web ブラウザまたは GUI とすること。

3.3.1.2 プロトコル

ネットワークプロトコルは、原則として TCP/IP とすること。

やむを得ずその他の通信プロトコルを使用する場合は、発注者に説明を行い、承認を得ること。

3.3.1.3 ドメイン

ドメイン名については、既存のドメイン名（osakacity-hp.or.jp, med.osakacity-hp.or.jp）を使用するものとする。

ドメインの移行及び維持管理は本業務に含むものとすること。

3.3.1.4 インターネット接続

院内ネットワークと外部インターネットとの境界には、UTM 機能付きファイアウォールの設置等セキュリティ対策を講じること。受注者において選定および必要な手続きを行うこと。

3.3.2　通信回線

3.3.2.1 WAN 回線

総合医療センター、十三市民病院、住之江診療所の各拠点から本システム、及び AWS へ接続する専用回線を整備すること。 Microsoft 365 サービスへは本システムを経由する通信経路でアクセスすること。通信回線の構成については「データセンター集約型構成」にて整備すること。なお、以下の項目で指定がない場合、病院事業ネットワークおよび医学情報収集ネットワーク共通要件として取り扱うこと。

(1) クラウド基盤、AWS への通信回線は閉域網回線サービス(広域イーサネットまたは IP-VPN)により接続すること。

(2) 病院事業ネットワークと医学情報収集ネットワークでそれぞれ別の回線を整備すること。また、回線速度は以下の通りとすること。

病院事業ネットワーク	
拠点名	WAN 回線
総合医療センター	メイン 500Mbps 以上帯域確保、バックアップ 100Mbps 以上帯域確保の２回線提供すること。メイン回線とバックアップ回線は異局異ルートの冗長構成とすること。 バックアップ回線については、ベストエフォートでも可能とするが 60Mbps 以上の安定した帯域が提供できること。 また、閉域回線に接続するための既存ルータをリプレースすること。リプレースの際、既存ルータの設定を踏襲すること。
十三市民病院	100Mbps 以上帯域確保
住之江診療所	10Mbps 以上帯域確保
クラウド接続回線	メイン 600Mbps 以上帯域確保、バックアップ１Gbps 以上ベストエフォートの２回線提供すること。メイン回線とバックアップ回線は異局異ルートの冗長構成とすること。ベストエフォート回線は、帯域は他ユーザーとの共用を可能とするが光ファイバの分岐は認めない。なお、 Microsoft 365 通信が発生しない回線はこの限りではないが、必要十分な回線を準備すること。
AWS 回線	100Mbps 以上ベストエフォート　※大阪市内　※冗長構成をとること

医学情報収集ネットワーク	
拠点名	WAN 回線
総合医療センター	400Mbps 以上帯域確保
十三市民病院	100Mbps 以上帯域確保
クラウド接続回線	メイン 500Mbps 以上帯域確保、バックアップ 100Mbps 以上帯域確保の２回線提供すること。メイン回線とバックアップ回線は異局異ルートの冗長構成とすること。 Microsoft 365 通信が発生しない回線はこの限りではないが、必要十分な回線を準備すること。
AWS 回線	100Mbps 以上ベストエフォート　※大阪市内　※冗長構成をとること

(3) 閉域網及びアクセス回線区間は 24 時間 365 日監視を行うこと。障害を検知した場合は、速やかに故障通知、復旧対応を行うこと。また障害受付窓口として 24 時間 365 日受付可能な体制を有すること。

(4) 計画的な工事、または定期的な保守等に伴いネットワークを停止する場合は、その２週間前までに発注者に連絡し了承を得ること。重大な脆弱性の発見等により、至急ネットワーク停止を伴うメンテナンスが必要となった場合は、ただちにその旨を発注者へ連絡し対応方針を協議、決定すること。

3.3.2.2 インターネット

インターネット接続については本システムのクラウド経由でアクセスするデータセンター集約型構成とする。

(1) インターネット回線は信頼性が高い法人専用の回線であること。

(2) インターネット接続に伴う接続料及びプロバイダ契約は本契約に含む。
またトラフィックに流量制限がなく、制限超過による費用変動が起きないようにすること。

(3) インターネットプロバイダとの接続は２系統用意すること。片方に障害が発生した場合は業務において重要な通信への影響が最小限となるよう、２回線の冗長構成とすること。メイン回線は１Gbps 以上の帯域確保、バックアップ回線は１Gbps ベストエフォート以上を準備すること。

(4) インターネットとの接続点にはファイアウォールを設置し、冗長構成とすること。

(5) ファイアウォールのポリシーは、既存 UTM の設定情報から踏襲すること。また、病院事業ネットワーク・医学情報収集ネットワークそれぞれに対応したポリシーを適用するため、ファイアウォールを分けること。

(6) ファイアウォールを通過するトラフィックに対して、UTM 機能を提供すること。また、検査はパケット単位ではなくファイル単位で検査できること。

(7) インターネットとの接続点となるファイアウォールは、上記機能および使用を実現するために導入する次世代ファイアウォールとし、UTM 機能・ルーティング機能などを有効にした場合でも、業務影響のない帯域利用が可能な性能を有すること。

(8) ファイアウォールは、ポリシーで許可した宛先アドレスが変更となってもアクセスが遮断されないよう、外部 WEB サーバから提供されるリスト（IP アドレスや URL 等の一覧）を自動的に取り込み、ポリシーに適用する機能を有すること。

(9) 脆弱性攻撃へのリスク低減のため、ファイアウォールは病院事業ネットワーク・医学情報収集ネットワークで統一し、管理コンソールへのアクセスについてはローカルネットワークに限定する。

(10) ファイアウォールの設定およびログ情報について、拠点ごとの管理ではなく、一元管理する仕組みを導入すること。

(11) インターネット回線の保守体制として 24 時間 365 日のネットワーク監視及び障害受付が対応可能な保守体制を有すること。また、障害発生時の故障修理・復旧体制を有すること。

(12) インターネット回線の計画的な工事または定期的な保守等に伴うネットワーク停止を実施する場合は、遅くともその２週間前までに発注者へ連絡し了承を得ること。なお、運用を続けると明らかに障害に至る恐れがある場合は、その旨をただちに発注者に連絡したうえで、発注者と協議して対応を決めることとする。

(13) インターネット向けのドメインは現在のドメイン（osakacity-hp.or.jp, med.osakacity-hp.or.jp）を使用することとし、既存プロバイダからのドメイン権限委譲、維持管理を実施すること。

(14) 総合医療センター、十三市民病院、住之江診療所の各拠点において、障害などによるネットワーク切断が発生した場合においても他の拠点に影響を及ぼさない構成とすること。

(15) グローバル IP アドレスを追加する際に、回線を増やすことなく追加できるインターネット回線サービスを導入すること

(16) 接続元グローバル IP アドレスによる認証を行う Web サイトへの通信は単一グローバル IP アドレスで接続可能な設計とすること。

(17) Microsoft 365 関連通信を識別し、当該通信については、運用要件に応じて SSL 復号、アン

チウイルス検査その他必要なセキュリティ検査の除外設定が可能であること。

3.3.3 クラウド基盤

3.3.3.1 全般（プライベートクラウド）

病院事業ネットワーク及び医学情報収集ネットワークの基盤として、サーバを仮想化し、仮想化されたサーバを物理的に複数のサーバで冗長化すること。

(1) サーバ基盤については、下記の要件を満たす構成とすること。
- 仮想化 OS は汎用 OS 以外で実装されていること。
- ハイパバイザー型の完全仮想化ソフトウェアであること。

(2) データを保管するストレージは冗長化された基盤とし、ディスクは RAID 構成により複数のハードディスクが故障してもデータに影響を及ぼさない構成とすること。

(3) 仮想マシンのリソースについては、特に指定のない限り3,000ユーザ程度、2,500台程度の端末で問題なく動作するスペックを実装すること。

(4) 発注者と協議のうえ、使用する通信プロトコル及び通信ポート以外での接続、データ通信を拒否するなどのコントロールを実施するとともに、ログ取得する仕組みを用意すること。

(5) 本システムのサーバOSやファイアウォールに関しては、適切な権限設定、不要なサービスの停止、セキュリティパッチの適用等脆弱性を排除したセキュリティの維持管理が行えること。なお、適用するセキュリティパッチは発注者と協議のうえ受注者が行うこと。

(6) 管理者等のユーザID、パスワードについては発注者のセキュリティポリシーを遵守した管理ができること。各サーバには１セッション以上のリモート接続ができること。

(7) 仮想化サーバ上のサーバOSには受注者が用意するウイルス対策ソフトをインストールすること。ただし、IaaS提供のサーバを除く。

(8) 必要となるクライアントアクセスライセンス(CAL)については受注者にて用意すること。

3.3.3.2 全般（パブリッククラウド）

(1) サーバ基盤については、下記の要件を満たす構成とすること。
- 仮想サーバは、クラウド事業者が提供する仮想化基盤上で稼働すること。
- 仮想化方式は、ハイパバイザー型の完全仮想化又はこれと同等以上の分離性及び安全性を有する方式であること。
- 仮想サーバを稼働させる物理基盤は、クラウド事業者により電源、ネットワーク、ホスト機器等の冗長化が図られていること。
- 採用するクラウドサービスについて、構成概要、可用性及びセキュリティに関する資料を提示できること。

(2) データを保管するストレージは、クラウド事業者が提供する冗長化されたストレージ基盤を利用すること。なお、基盤側で冗長性が確保され、単一ディスク又は単一機器の故障により直ちにデータ消失が発生しない構成とすること。物理ディスクの RAID 構成を利用者側で直接管理できない場合においても、これと同等以上の耐障害性及び可用性を有することを示せること。

(3) 仮想マシン、ストレージ、ネットワークその他のリソースについては、特に指定のない限り、3,000 ユーザ程度、2,500 台程度の端末（スマホ等含む）利用を考慮したうえで、業務に支障なく安定稼働できるスペックを実装すること。なお、必要に応じてリソースの増強又は変更が可能な構成とすること。

(4) 発注者と協議のうえ、使用する通信プロトコル及び通信ポート以外での接続又はデータ通信

を拒否するなどのアクセス制御を実施すること。また、通信制御及びアクセス状況を記録するログ取得の仕組みを用意し、必要に応じて追跡及び確認ができること。

(5) 本システムで利用するサーバOS、ミドルウェア、仮想サーバ、ネットワーク制御機能及びファイアウォール等に関しては、適切な権限設定、不要なサービスの停止、セキュリティパッチの適用その他脆弱性対策を実施し、セキュリティを維持管理できること。なお、適用するセキュリティパッチは発注者と協議のうえ受注者が実施すること。ただし、クラウド事業者が管理する基盤部分については、当該事業者の責任範囲において適切に維持管理されていること。

(6) 管理者等のユーザID、パスワードについては発注者のセキュリティポリシーを遵守した管理ができること。各サーバには１セッション以上のリモート接続ができること。

(7) 仮想化サーバ上のサーバ OS には受注者が用意するウイルス対策ソフトをインストールすること。ただし、IaaS 提供のサーバを除く。

3.3.3.3 認証基盤(Active Directory)

外部からの不正侵入を防止するために、病院事業ネットワークへのログインはMicrosoft® Windowsドメインコントローラーにて管理をするとともに、端末起動時にドメインユーザとしての認証を行い、不正侵入の防止を図ること。

以下の要件を満たしたうえで、本システムへのネットワーク認証基盤として、Windowsドメインコントローラーによる認証制御を行うこと。

本機能は病院事業ネットワークのみ導入する。

(1) メーカサポートが受けられるOSバージョン上で動作するActive Directoryであること。

(2) Active Directoryは２台以上の冗長構成であること。

(3) ユーザ及びコンピュータ（端末）を管理し、Active Directoryのグループポリシーを利用して制御できること。

(4) コンピュータ情報、ユーザ情報は組織に応じた適切なOU(Organization Unit)構成で管理できること。

(5) セキュリティグループ情報を登録し、Active Directoryの機能によってアクセス制御を実現できること。

(6) DNS(Domain Name System)機能を実装し、イントラネットの名前解決及び外部のDNSと連携しインターネットの名前解決ができること。DNS 機能においては、現在発注者が利用している外部ドメイン「osakacity-hp.or.jp」「med.osakacity-hp.or.jp」を維持管理すること。既存のゾーン情報、レコードを引き継ぎ、本ネットワークシステムサービスを構築する上で必要になったレコードは追加すること。

(7) 利用期間は2027年２月１日から2028年１月31日までとする。

3.3.3.4 IT資産管理機能

本機能は病院事業ネットワークに導入し、提供するライセンス数は端末830台とする。製品については現在「SKYSEA Client View」を使用しているため、同製品の最新バージョンで構築すること。

WindowsOSの更新プログラムの配布方法に関するマニュアルを提供すること。

3.3.3.5 アクセス制御

すべての端末はProxyを経由してインターネットへ接続すること。Proxyには、URLフィルタ機能を病院事業ネットワーク及び医学情報収集ネットワーク共に実装し、URLフィルタにおいては、以下

の機能を有すること。

(1) URL フィルタはカテゴリ毎でのフィルタリング設定可能な専用製品を用意し、すべての HTTP/HTTPS 通信に適用可能な設計とすること。
(2) カテゴリ毎に閲覧、規制などのアクセス制御の設定ができること。
(3) グループ単位で設定した規制ルールを適用できること。
(4) Youtube などの動画閲覧サイトにおいて、特定の動画のみの閲覧許可または閲覧制限の設定ができること。また、本機能を実装するにあたり SSL デコードを利用する場合、SSL 証明書エラーが表示されないよう、すべての端末へ証明書をインストールすること。なお本項目の適用範囲は病院事業ネットワークに限る。
(5) 閲覧禁止メッセージのカスタマイズが可能であること。
(6) Web アクセスログ、フィルタリングログ等を取得できること。
(7) 病院事業ネットワーク、医学情報収集ネットワークそれぞれ別にフィルタ設定を行えること。使用する端末数は病院事業ネットワーク 2,000 台程度、医学情報収集ネットワーク 500 台程度とする。

3.3.3.6 不正接続検知

不正接続検知は、以下の要件を満たすこと。本機能は病院事業ネットワーク及び医学情報収集ネットワークに導入すること。端末及びプリンタの 3,000 台程度(約 6,000MAC アドレス)を対象とし、監視するセグメントは病院事業（有線・無線)、人事給与・財務会計（有線)、医学情報収集ネットワーク（有線・無線）とし、総合医療センター、十三市民病院はそれぞれ 5 セグメントを想定すること。

※総合医療センター：すべて、十三市民病院：すべて、住之江診療所：病院事業（有線)、人事給与・財務会計（有線)

(1) 登録されていない MAC アドレスを不正接続として速やかに検知し、自動的に接続を遮断できる機能を有すること。またその情報を管理者へ通知できること。
(2) MAC アドレスを自動で収集できること。
(3) 端末へのソフトウェアのインストールが不要であること。
(4) 総合医療センター、十三市民病院、住之江診療所へのセンサー等の機器導入に伴う設置が必要な場合は設置作業を行うこと。

3.3.3.7 監視

本システムの仮想サーバに対して死活監視、リソース監視、プロセス監視を行うこと。プライベートクラウドの場合、仮想化基盤に対しても死活監視、リソース監視、プロセス監視を行うこと。SaaS を利用したサービス提供の場合、SaaS 業者がサーバに対して死活監視を実施すること。

3.3.3.8 財務会計システム

財務会計システムは現状本システムクラウド基盤上で稼働している。これらのシステムにおいては、IaaSの提供を調達範囲とし、ミドルウェアアプリケーションは発注者で実装する。また、財務会計システムに必要なミドルウェアを含むライセンスは発注者にて準備する。以下の要件に対応する仮想化サーバを１台提供すること。以下、共通要件を示す。

(1) メモリは32GB以上を割り当てること。
(2) ハードディスクは800GB以上を割り当てること。
(3) CPUは８コア以上を用意すること。

(4) サーバOSはWindows Server 2025を用意すること。
(5) 導入時に発注者から指定したWindowsOSに対して、最新のセキュリティパッチを適用すること。
(6) 病院事業ネットワークからリモートデスクトップにて接続できること。同時接続数は各システム毎に１セッションとする。
(7) 本システムをAWS上に構築すること。
(8) 人事給与・財務会計ネットワークから接続できること。

3.3.3.9 保守用サーバー（Window）ならびに Syslog（RHEL）

受注者が運用保守をするにあたって保守用サーバが必要な場合、他のサーバと併用せず、専用のサーバを準備すること。

3.4 マニュアル等

3.4.1 マニュアル等の作成

本システムの運用にあたって業務フローに則したマニュアルを作成すること。
本システムで必要となるマニュアルは次のとおりである。

3.4.1.1 管理者マニュアル

アカウント管理、権限管理、パラメータ変更その他管理業務について操作方法を記述したもの。

3.4.1.2 ユーザマニュアル

導入後、ユーザ（利用者）単位で必要な設定等の操作方法を記述したもの。

3.4.1.3 障害時対応マニュアル

緊急時の対応方法、確認方法、復旧方法について、専門的な知識がなくても理解できるよう具体的な手順等を記述したもの。

第４章　移行要件

4.1 基本方針

現行の病院事業及び医学情報収集ネットワークから本システムへの移行にあたり、業務継続に影響を与えることなく、速やかかつ確実に実施するため、移行業務に関する要件を以下のとおり示す。受注者は、本業務における移行手順及び接続テストの内容の詳細を発注者に提案し、承認を得たうえで実施すること。

4.2 移行要件

4.2.1 認証基盤(ActiveDirectory)

現在、病院事業ネットワークで利用中の ActiveDirectory サーバを移行させること。移行が必要な作業やデータ等の内容は以下が見込まれるが、既存設定を確認し現在利用している設定項目を引き継ぐこと。

(1) FSMO
(2) 各種ディレクトリデータベース
(3) DNS レコード

(4) ログオンスクリプト
(5) 各種グループポリシー
(6) OU

また認証基盤サーバの IP アドレス変更が見込まれるが、発注者が利用している端末の設定変更(優先、代替 DNS サーバアドレス設定等)が必要な場合、受注者にて設定変更を行うこと。

4.2.2 IT 資産管理機能(SKYSEA)

現在、病院事業ネットワークで利用中の IT 資産管理サーバに設定されている情報を引き継ぐこと。

(1) マスタ設定
(2) デバイス情報
(3) 管理機、端末機権限情報
(4) USB デバイス制御（グループ、端末、特定 USB デバイス許可等）
(5) ソフトウェア配布設定
(6) 各種アラート設定
(7) 各種レポート機能

など

ただし、既存の IT 資産管理機能サービス仕様上マスタサーバへの OS 及びファイルアクセスが不可能であるため、SKYSEA の管理コンソール上の情報を確認し、引継ぎ作業を実施すること。

また、上述のマスタサーバにおけるファイルアクセス制限により、新規でマスタサーバを構築することになる場合、すでに端末へインストールされた SKYSEA エージェントへの関連付けを受注者により実施すること。

4.2.3 Web アクセス制御

現在、病院事業ネットワーク、医学情報収集ネットワークで利用中の Web アクセス制御サーバに設定されている情報を引き継ぐこと。

(1) 各種認証設定
(2) 認証除外 IP アドレス
(3) カテゴリ設定
(4) グループ設定
(5) ブラックリスト、ホワイトリスト、認証除外リスト

など

4.2.4 DNS(Domain Name System)

内部・外部ドメインに紐づくレコード情報を引き継ぐこと。

4.2.5 不正接続検知

現在、病院事業ネットワーク、医学情報収集ネットワークで利用中の不正接続検知サーバに設定されている情報を引き継ぐこと。

(1) LAN 接続された機器情報(通信許可、不許可の MAC アドレスおよび機器情報、接続を検知し記録された MAC アドレス及び機器情報)など

4.2.6 ファイアウォール

現在、病院事業ネットワーク、医学情報収集ネットワークで利用中のファイアウォールに設定されている情報を踏襲すること。

(1) ルーティング設定

(2) ポリシー設定

(3) NAT 設定

(4) セキュリティプロファイル

(5) アドレスオブジェクト及びグループ

(6) サービスオブジェクト及びグループ

4.2.7 その他

データ移行用回線が必要な場合、本調達に含むこと。帯域は現行のデータセンターとの接続回線が 100M 確保であるため、100M 確保を上限に受注者にて用意すること。

既設ネットワーク機器について、現行保守業者が問題なく保守できるように事前協議の上、受注者負担により実施すること。(現行保守業者への委託も可とする)

財務会計システムのアプリケーションについては、発注者でマイグレーションを行う。

第 5 章　信頼性等要件

5.1 基本方針

高い信頼性とデータの保全、整合性の確保を必要とするため、システム及びデータのバックアップが行える環境を構築すること。

(1) 可用性

障害による停止が長時間にわたらないように可及的速やかに復旧できるシステムであること。

(2) 冗長性

ハードウェア及び仮想化基盤の冗長性を確保し、物理ホスト障害時においても、自動復旧、自動切替、自動再配置又はこれらと同等の仕組みにより、仮想サーバを継続又は速やかに再稼働できること。

データを保管するストレージは、RAID構成又はこれと同等以上の耐障害性を有する冗長化された基盤とし、本番環境とロケーションが異なる領域にバックアップデータを保管のうえ、１日１回以上バックアップを実施し、本番環境障害によるデータ損失を防止するとともに、バックアップデータから可及的速やかに復旧できること。

第 6 章　導入要件

6.1 基本方針

本システムは、令和９年２月１日よりサービスの利用を開始するため、令和９年１月 31 日までに構築を完了すること。ただし、令和８年 10 月１日より m365 の利用を開始するため、既存 UTM への設定変更、PAC ファイルの作成、及び配布に必要な環境を整えること。

6.2 導入の範囲

「第 2 章 調達の概要」「第 3 章　病院事業及び医学情報収集ネットワークの要件」「第 4 章 移行要件」「第 5 章　信頼性等要件」等に示した各条件、要件を満たすシステム(ソフトウェア、ハードウェア等)及びサービスを提供すること。

また、本システムが稼働するためのクラウド基盤については、「6.8 ファシリティ要件」を満たす施設に構築し運用を行うこと。

6.3 運用要件

(1) 基本的な考え方

① システム稼動時間は、24 時間 365 日とする。

② 本システムのバックアップは、原則としてオンラインバックアップとする。サービスの停止を伴う場合は、1 時間以内でサービスを再開できること。バックアップは夜間帯に実施することとし、詳細については発注者との協議に応じること。

③ あらかじめ計画されている定期メンテナンスに伴うサービス停止については、事前に発注者へ通知し、作業日時など詳細について協議のうえ実施すること。

(2) 通常運用業務の概要

想定する主な通常運用業務の内容は以下のとおりである。

① バックアップ

バックアップスケジュールとしては、日次毎に差分バックアップを取得する。バックアップデータとして最低 21 世代以上の世代管理ができること。バックアップ取得方法については発注者との協議に応じること。サーバ OS、ファイアウォールへのパッチ適用は発注者と協議の上、保守内で実施すること。ただし、財務会計システム、タイムレコード（以下、関連システム）においてはアプリケーション導入業者にて、サーバ OS のパッチ適用、アプリケーションのバージョンアップを実施する。

② 稼動監視

各種サーバの稼働監視により、サービスに問題が発覚した場合は早急に発注者へ通知し、復旧対応を行うこと。

6.4 運用テストについて

(1) 運用テストの方針策定、準備及び運用テストに関する調整については、発注者と協議のうえ行うこと。

(2) 運用テスト完了後、発注者による受入テストを実施すること。レビューの結果、機能要件を満たさない場合は再度、運用テストと受入テストを実施すること。

(3) 運用テスト計画書(案)、運用テスト実施手順書(案)を作成すること。

6.5 運用・保守要件

受注者は、以下の運用が可能となるような本システムの構築を行うこと。

6.5.1 保守対応時間と作業内容

(1) システム運用・保守に係る対応時間

・ 監視・障害受付 ： 24 時間、365 日

・ 問合せ対応 ： 発注者の外来診療日 8 時 45 分から 17 時 15 分

・ 業務支援等 ： 発注者の外来診療日 8 時 45 分から 17 時 15 分

(2) システム運用・保守に係る作業

① システム機能改善や追加・変更等に伴ってサービス仕様書、管理者マニュアル、ユーザマニュアル及び障害時対応マニュアル、WindowsOS 更新プログラム配布マニュアルに変更が生じた際は各マニュアルの修正を行うこと。

② 発注者のシステム運用に依存するサーバーサイドの設定変更等について発注者が実施すること。

③ 端末の新規導入や移設・故障時において、各種アプリケーションのインストールや基本設定など発注者のシステム運用によって発生する設定変更等は発注者にて実施すること。
④ 受注者は障害時の切分け作業等、障害の分析及び障害箇所を特定すること。
⑤ 受注者は障害対応（修正、点検等）を行う。また、障害復旧時には障害の事象、影響、原因及び対策方法等をまとめた報告書を作成し、発注者へ遅滞なく提出すること。
⑥ 受注者は少なくとも、毎年サーバのパッチ適用、エラーログの確認等を実施すること。セキュリティリスクの高い脆弱性が見つかった場合、発注者と協議の上、速やかにセキュリティパッチを適用すること。
⑦ ハードウェア・ソフトウェア・サービスともに製品及び技術情報の提供を行うこと。

6.6 関連システムとの連携

6.6.1 関連システム担当者への技術的サポート

受注者は本システムの開発作業時に、発注者や関連システム担当者からの問合せやレビュー等への参加要請等に対し、ハードウェア及びソフトウェアに関するエラー対応や技術的サポート等、主体的に必要な支援を行うこと。

6.7 機器及びネットワーク設定・検証について

(1) 本契約における受注者の実施する設定・検証作業とは、本システムを構築するための導入作業をいう。既存端末に対して設定変更及びアプリケーションのインストール、本ネットワークサービスで提供する新規アプリケーション関連作業が見込まれるが、本作業にその費用も含まれる。
(2) 受注者が設定する際に必要な情報については、発注者より文書で提示すること。
(3) 契約締結後は発注者、受注者、関連システム担当者等、すべての関係者で導入調整会議等を行い、打合せ内容に従った円滑な導入を行うこと。
(4) 本システムの導入及び移行作業時に必要な調整を行うこと。既存ネットワーク機器の設定変更不備、ネットワーク接続不可などの障害が発生した場合、受注者及び関連システム担当者間で切り分けを行い、原因調査や動作検証等を行うこと。その後、発注者へ再発防止策含め報告を行うこと。なお、原因調査や動作検証等に要する費用については、発注者立会いの元、受注者及び関連システム担当者間で協議すること。
(5) 既存ネットワークへの設定変更が必要と見込まれる場合、既存ネットワーク構築業者により継続保守を行う必要があるため、別途見積もりの上作業を委託すること。

6.8 ファシリティ要件

6.8.1 設備要件（プライベートクラウドの場合）

(1) 立地
① 日本国内にデータセンターを利用すること。
(2) 建物の災害対策
① クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムが設置されている建物（情報処理施設）である為、地震・水害・火災・落雷等自然災害に対する対策が行われていること。
(3) 電源・空調の維持と災害対策
① クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所には、停電や電力障害を想定し非常時電源を確保すること。また、設置機器による発熱を抑えるのに、十分な容量の空調を提供すること。

(4) 建物の情報セキュリティ対策

① 重要な物理的セキュリティ境界（建物内出入口、有人の受付等）に対し、個人IDカードや生体認証による個人認証システムを用いること。アンチパスバックによる共連れ防止を行うこと。従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。

② 重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像をあらかじめ定められた期間保存すること。

③ 重要な物理的セキュリティ境界の出入口に破壊対策ドアを設置すること。

④ 重要な物理的セキュリティ境界に警備員を常駐させること。

⑤ サーバルームやラックの鍵管理を行うこと。

6.8.2 設備要件（パブリッククラウドの場合）

(1) 立地

① 本システムで利用するデータ保管先及びサービス提供拠点は、日本国内の複数リージョンを利用できること。

② データセンターの所在地は、物理的セキュリティ確保の観点から詳細非公開であること。

③ データセンターは、電力、災害リスク等を考慮して選定された施設であること。

(2) 建物の災害対策

① 本システムで利用するデータ保管先及びサービス提供拠点は、日本国内の複数リージョンを利用できること。

(3) 電源・空調の維持と災害対策

① データセンターは、停電時においても継続して電力供給可能なよう、無停電電源装置（UPS）及び非常用発電設備等の冗長化された電源設備を有すること。

② データセンターは、設置機器の安定稼働に必要な温度及び湿度を維持するための空調設備を有すること。

③ 電源設備及び空調設備は、単一障害点を排除することを考慮した構成であること。

(4) 建物の情報セキュリティ対策

① データセンターへの物理的な入退館は、許可された者のみに制限されていること。

② データセンターの重要な物理的セキュリティ境界に対しては、個人認証、多要素認証その他これに準ずる本人確認手段を用いた入退館管理が行われていること。

③ 入退館の履歴が記録され、監査可能であること。

④ 建物内外及び重要区画に対して監視カメラ等による24時間365日の監視が行われていること。

⑤ サーバ設置区画、保守区画その他重要区画については、一般区画と分離されたアクセス制御が行われていること。

⑥ 記憶媒体及び故障機器の廃棄時には、情報漏えい防止のため、適切な消去又は物理破壊等の措置が講じられていること。

6.9 発注者の利用パソコンへの対応

受注者は発注者の利用パソコンに対する設定を含めて、本システムへの切替作業を行う。

切替作業については、原則として外来診療日以外で行うこと。

なお、作業にあたっての発注者の立ち会い等については、最小限の負担となるよう考慮すること。

受注者は、発注者の利用パソコンに対して Intune などを用いた設定変更が必要となる場合、変更内容、対象端末及び希望時期を整理の上、発注者へ作業依頼を行うこと。実施方法及び作業日程は、発注者と

受注者で協議の上決定する。

第 7 章　特記事項

7.1 SLO（サービスレベル目標）

7.1.1 品質基準

クラウド稼働率（毎月 1 日から当該月末日まで）　99.5%以上

（当初予定した稼働時間―停止時間）／当初予定した稼働時間×100

当初予定した稼働時間とは、「当該月の日数×24 時間」を意味する。

(*) メンテナンスによる計画停止や「7.1.4 免責事項」に該当する場合は停止時間から除外する

7.1.2 測定方法例

プロセスの稼働ログ等により、サーバ機能の停止時間を確認する。

通信回線の停止については、クラウド基盤の全サーバの機能停止として停止時間を算出する。

また、一部機能の停止については、機能停止サーバ数／全サーバ数で按分して停止時間を算出する。

上記は測定方法例とし、測定方法は障害の性質により適切な方法を採用すること。

7.1.3 サービスレベル目標を満たさない場合

契約者の責めによらない理由により、サービスレベル目標を満たさない事象が生じた場合に、対策等について発注者に書面で提案を行い、発注者の承認を得たうえで改善措置を講じること。

7.1.4 免責事項

「7.1.2 対象サービスの測定方法」の規定にかかわらず、次の要件に該当する場合には、停止時間から除外する。

(1) 地震、雷等自然災害に起因する障害

(2) 発注者の都合によって障害復旧が行えなかった場合

(3) 連携他システムの停止・障害等に起因する場合

（別紙）

暴力団等の排除に関する特記仕様書

大阪市民病院機構（以下「発注者」という。）が締結する契約等から暴力団を排除する措置については、「大阪市暴力団排除条例」（以下「条例」という。）、「大阪市暴力団排除条例施行規則」及び「大阪市契約関係暴力団排除措置要綱」（以下「要綱」という。）に準拠し、大阪市と同様の措置を講じる。

1　暴力団等の排除について

（1）受注者（受注者が共同企業体であるときは、その構成員のいずれかの者。以下同じ。）は、大阪市暴力団排除条例（平成 23 年大阪市条例第 10 号。以下「条例」という。）第 2 条第 2 号に規定する暴力団員（以下「暴力団員」という。）又は同条第 3 号に規定する暴力団密接関係者（以下「暴力団密接関係者」という。）に該当すると認められる者と下請契約、資材・原材料の購入契約又はその他の契約をしてはならない。

（2）受注者は、条例第 7 条各号に規定する下請負人等（以下「下請負人等」という。）に、暴力団員又は暴力団密接関係者に該当すると認められる者と下請契約、資材・原材料の購入契約又はその他の契約をさせてはならない。

また、受注者は、下請負人等が暴力団員又は暴力団密接関係者に該当すると認められる者と下請契約、資材・原材料の購入契約又はその他の契約をした場合は当該契約を解除させなければならない。

（3）受注者は、この契約の履行にあたり暴力団員又は暴力団密接関係者に該当すると認められる者から条例第 9 条に規定する不当介入（以下「不当介入」という。）を受けたときは、速やかに、この契約に係る発注者監督職員若しくは検査職員又は当該事務事業を所管する担当課長（以下「監督職員等」という。）へ報告するとともに、警察への届出を行わなければならない。

また受注者は、下請負人等が暴力団員又は暴力団密接関係者に該当すると認められる者から不当介入を受けたときは、当該下請負人等に対し、速やかに監督職員等へ報告するとともに警察への届出を行うよう、指導しなければならない。

（4）受注者及び下請負人等が、正当な理由なく委託者に対し前号に規定する報告をしなかったと認めるときは、条例第 12 条に基づく公表及び大阪市民病院機構競争入札参加停止措置要綱及び大阪市競争入札参加停止措置要綱による停止措置を行うことがある。

（5）受注者は第 3 号に定める報告及び届出により、発注者及び大阪市が行う調査並びに警察が行う捜査に協力しなければならない。

（6）発注者及び受注者は、暴力団員又は暴力団密接関係者に該当すると認められる者からの不当介入により契約の適正な履行が阻害されるおそれがあるときは、双方協議の上、履行日程の調整、履行期間の延長、履行内容の変更その他必要と認められる措置を講じることとする。

2　誓約書の提出について

受注者及び下請負人等は、暴力団員又は暴力団密接関係者でないことをそれぞれが表明した誓約書を提出しなければならない。ただし、発注者が必要でないと判断した場合はこの限りでない。

職員等の公正な職務の執行の確保に関する条例に基づく特記仕様書

大阪市民病院機構（以下「発注者」という。）は、職員等の公正な職務の執行の確保に関する条例に準拠し、大阪市と同様の取扱いをするものとする。

（条例の遵守）

第１条　受注者及び受注者の役職員は、受注業務の履行に際しては、「職員等の公正な職務の執行の確保に関する条例」（平成１８年大阪市条例第１６号）（以下「条例」という。）第５条に規定する責務を果たさなければならない。

（公益通報等の報告）

第２条　受注者は、受注業務について、次の各号に定める場合、速やかに、その内容を発注者（地方独立行政法人大阪市民病院機構 法人運営本部内部監察室）へ報告しなければならない。

（１）　条例第２条第１項に規定する公益通報を受けたとき

（２）　発注者の職員から、違法または不適正な要求を受けたとき

２　受注者は、公益通報をした者又は公益通報に係る通報対象事実に係る調査に協力した者から、条例第１２条第１項に規定する申出を受けたときは、直ちに、当該申出の内容を発注者（地方独立行政法人大阪市民病院機構 法人運営本部内部監察室）へ報告しなければならない。

（調査の協力）

第３条　受注者及び受注者の役職員は、発注者又は大阪市公正職務審査委員会が条例に基づき行う調査に協力しなければならない。

（公益通報に係る情報の取扱い）

第４条　受注者の役職員又は受注者の役職員であった者は、正当な理由なく公益通報に係る事務の処理に関して知り得た秘密を漏らしてはならない。

（発注者の解除権）

第５条　発注者は、受注者が、条例の規定に基づく調査に正当な理由なく協力しないとき又は条例の規定に基づく勧告に正当な理由なく従わないときは、本契約を解除することができる。

○ 地方独立行政法人大阪市民病院機構 法人運営本部内部監察室の連絡先：06-6929-3275

個人情報等の保護に関する特記仕様書

この契約の履行にあたって個人情報は、市民の個人情報保護の重要性に鑑み、個人情報の保護に関する法律及び大阪市個人情報の保護に関する法律の施行に関する条例の趣旨を踏まえ、適切に取り扱わなければならない。