（長期継続契約）かがわ電子自治体システム利用用端末機器等調達に関する仕様書

1. 業務名称

（長期継続契約）かがわ電子自治体システム利用用端末機器等賃貸借

2. 履行期間

・機器調達、設置工事、動作確認並びに設定・接続確認：契約締結日から令和13年9月30日午後5時15分まで
・賃貸借並びにサービス利用、保守期間：令和8年10月1日から令和13年9月30日まで（60ヶ月）
・契約は、高松市、賃貸借会社及び導入業者間において、第三者賃貸借方式（民法第537条）による賃貸借契約を結び、賃貸借料は賃貸借会社に支払うものとする。
・自社で取り扱うことが可能な、仕様を満たす奨励製品を提案し、高松市の物品・委託・役務の提供等入札参加資格者名簿の業種名「事務用機器類」の営業種目「コンピュータ機器類」、業種名「情報・通信」の営業種目「システムの設計・開発」及び「システムの保守・管理」に登載されて、連続して2年を経過していること。
加えて、信頼性、実績ともに優良と認められる賃貸借会社を選定し、入札時に賃貸借会社を明記した**「賃貸借会社指名届」**を本市に提出すること。契約期間内において、賃貸借会社が仕様どおりに業務を履行しない場合は、導入業者の責任において履行しなければならない。
・自社で賃貸借も行う場合は、高松市と導入業者間で賃貸借契約を締結する。この場合は、導入業者及び賃貸借会社の業務を一括するものとし、**「賃貸借会社指名届」**の提出は不要とする。

3. 業務概要

・高松市内13施設（詳細は 1. 2 拠点設置設備一覧 参照）にネットワーク機器及び、業務用端末等設置、接続確認。
・インターネット環境の整備を行う。
・有害サイトへのアクセスを抑制するWebフィルタリング、セキュリティを確保するためのウィルスチェックを管理するための機器導入及び据付調整工事の実施。
・電話･メールでの問い合わせ対応、故障機器については、オンサイト保守を行う。

4. 成果物

以下の成果物を別途指定する期限までに納品すること。

（1） 機器一覧表
（2） 機器配置図
（3） 機器設置写真台帳 （設置前・設置後）
（4） 業務用端末設定台帳
（5） プリンタ設定台帳
（6） ルータ設定台帳
（7） ファイアウォール設定台帳（UTM 設定を含む）
（8） ファイルサーバ設定台帳
（9） 商用リモートコントロールソフト操作手順書
（10） 事前動作確認成績書
（11） 動作確認成績書

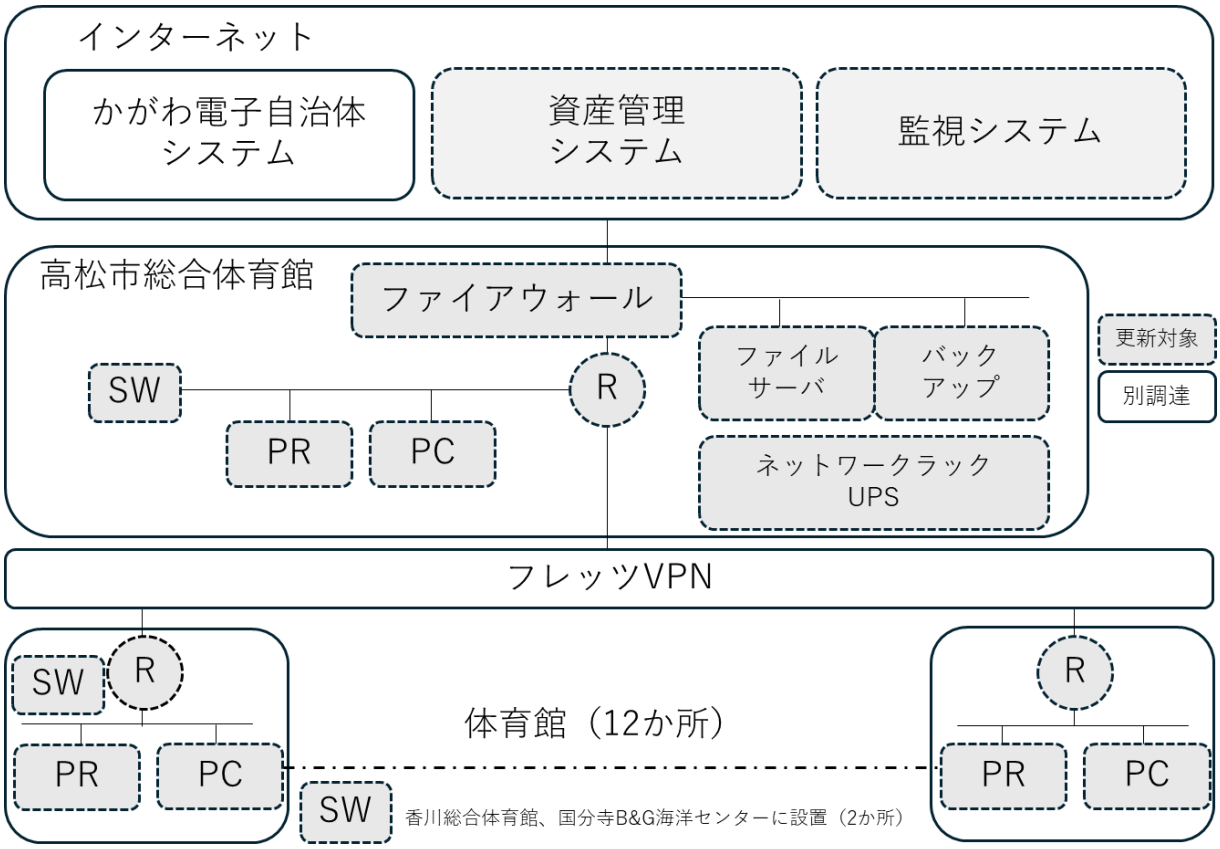
（12）保守マニュアル（保守体制・保守対象一覧）

ICカード又は生体認証登録等設定・保守マニュアル

1. システム構成

1. 1システム構成

本システムの構成は以下の通り。



※全拠点の利用者端末・業務用端末でかがわ電子自治体システムが利用できるよう設定をすること。

1. 2 拠点設置設備一覧

No	施設名	業務用端末（ノート型）	業務用端末認証用ICカードリーダ	業務用端末認証用ICカード	プリンタ	ルータ	UPS	スイッチ
1	高松市総合体育館	11	11	18	5	1	2	1
2	西部運動センター	1	1	6	1	1		
3	高松市亀水運動センター	2	2	6	2	1		
4	かわなベスポーツセンター	2	2	9	2	1		
5	仏生山公園体育館	2	2	9	2	1		
6	牟礼総合体育館	2	2	7	1	1		
7	牟礼中央公園運動センター	1	1	6	1	1		
8	香川総合体育館	4	4	9	2	1		1
9	国分寺B＆G海洋センター	3	3	10	2	1		1
10	香南体育館	1	1	3	1	1		
11	東部運動公園	2	2	8	1	1		
12	高松市屋島競技場	1	1	11	1	1		
13	高松市ヨット競技場	1	1	4	1	1		
小計		33	33	106	22	13	2	3

14	予備機	1	1	4	－	－	－	－

合計		34	34	110	22	13	2	3

※ ネットワーク接続で工事が必要な場合は、工事費は賃貸借料に含めること。
機器の接続に必要なケーブル等についても本調達に含めること。
なお、配線が困難な場合は、高松市と協議の上、変更することもある。
生体認証を導入する場合、業務用端末認証用 IC カードリーダと業務用端末認証用 IC カードは不要とする。

1. 3 高松市総合体育館収容機器一覧

高松市総合体育館に以下の機器を導入すること。

(1) ファイルサーバ　1台
(2) バックアップストレージ　1台
(3) センター用ルータ　1台
(4) センター用ファイアウォール　1台
(5) センター用ネットワークラック　1台
(6) センター用UPS　2台
(7) センター用スイッチ　1台

2. 拠点設備仕様

(1) 機器の搬入・設置・設定については次のとおりとする。

・搬入場所は、仕様書内「1-2 施設設置設備一覧」に記載されている13拠点とする。
・作業時間は、原則、各拠点の営業日の営業時間内の午前9時～午後5時とする。
※これ以外の時間帯で作業を実施する場合は、事前に高松市と協議すること。
・具体的な作業日程は、別途、高松市と協議の上決定すること。
・作業に係る諸経費、作業は全て導入業者又は賃貸借業者の負担とする。
・梱包類は導入業者又は賃貸借業者により廃棄すること。
・導入するソフトウェアには5年間のメーカ保守を付与すること。

2. 1 業務用端末(ノート型)

(1) ハードウェア仕様

- CPU は Core i5-1335U 以上であること。
- 画面は 15.6 型 1,366×768 ドット以上であること。
- メモリは 16GB 以上であること。
- SSDは 256GB 以上で暗号化機能付きあること。
- DVD-ROM は USB 接続で14 台付属させること。
- 1000BASE-T/100BASE-TX/10BASE-T LAN に対応できること。
- 無線 LAN 内蔵型の場合は、BIOS で無効化できること。
- JIS 標準配列準拠又は OADG 準拠の日本語キーボードで、テンキーは一体型であること。
- USB 光センサーマウスとマウスパッドを付属させること。
- Windows 11 Professional (64bit)であること。(※マスタ展開時にライセンス違反しないこと)
- バッテリ駆動時間(JEITA3.0)で約3時間以上駆動できること
- USB ポートは PC の左・右・背面の3方向に搭載し 5 個以上を有すること。
- 一定時間操作をしなかった場合に、スクリーンアウトする機能があること。
- ログイン時のパスワードを定期的に変更する設定機能があること。
- エコマークに対応していること
- ECO キーを搭載していること
- .NetFramework3.5 がインストール＆有効化されていること。

(2) 5年間の当日オンサイト保守(平日9時－17時)とし、情報漏洩対策として交換したディスクは市に返却

すること。

(3) 商用リモートコントロールソフト（LAPLINK 又はLANSCOPE リモートデスクトップ powered by ISL Online 相当）導入し、各拠点間で遠隔操作が行えること。

(4) ウィルス対策ソフトは WindowsDefender を導入すること。

(5) Microsoft Office Professional Plus 2024(J/E) （ガバメントライセンス）を導入すること。

(6) マスタ PC イメージの作成、展開、システムリカバリが行えるよう構築すること

(7) PC の一元管理、コンプライアンス、セキュリティ対策、ヘルプデスクの効率化、コスト削減を目的とした情報収集を実施するため、クラウド型資産管理ソフト（LANSCOPE 相当）を導入すること。なお、資産管理ソフトの要求仕様は下記のとおりとする。

【基本要件】

- 国又は地方公共団体での実績を有すること。
- クラウド製品であること。
- 100 台のデバイスを1つの環境で管理できること。
- WindowsOS に対応していること。

【資産管理要件】

- 適正な IT 資産管理のために、以下の情報を自動取得できること。

デバイス情報	OS バージョン、コンピューター名、NetBIOS 名、デバイス名、製品名、製造元、シリアル番号、CPU 名、CPU 周波数、メモリ、OS アーキテクチャ、システムドライブ、ファイルシステム、ボリューム名、 ストレージ使用容量、ドメイン・ワークグループ名、ログオンユーザー名、ログオンユーザーSID、国番号、モデル名、モデムファームウェア、IMEI、プロセッサ数、CPU コア数、ドライブ数、フルネーム（表示名）、モデム、Windows プロダクト ID、SCSI 機器、BIOS バージョン、Windows サービスパック、Internet Explorer バージョン、IE サービスパック、ドライブ情報
ネットワーク	Wi-Fi 状態、Bluetooth 状態、NIC 情報（NIC 名・NIC の種別・MAC アドレス・IP アドレス・サブネットマスク・デフォルトゲートウェイ・DNS サーバ）、電話番号、現在のキャリア、SIM の状態、ICCID
セキュリティ	ファイアウォール状態、Windows アップデート、アンチウィルス状態、 アンチウイルス更新ステータス、リモートワイプ実行可否、BitLocker 回復キー、Defender パターンバージョン、Defender エンジンバージョン、 Defender バージョン、AuroraPROTECTt バージョン、AuroiraPROTECT モード、Deep Instinct バージョン、DeepI nstinct 連携設定

- デバイスの情報を一覧表示でき、表示項目の変更や並び替えが容易に行えること。
- ルータやプリンター等のエージェントがインストールできない IT 周辺機器を 100 台登録できること。
- メッセージ配信ができ、メッセージにはファイルが添付できること。
- アンケート配信ができ、アンケート結果を資産台帳に反映できること。
- デバイス情報を軸にしたアラート設定が可能で、アラート発生時は管理者にメールで通知できること。
- デバイスの稼働状況を把握できるレポート機能を有していること。

【アプリ管理要件】

- インストールアプリ情報を自動取得できること。
- インストールアプリごとにどのデバイスにインストールされているかを確認できる機能を有すること。
- アプリのバージョン情報を自動取得できること。
- 「デスクトップアプリ」か「ストアアプリ」かどうかの「アプリ種別」の情報を取得できること。
- Bits を利用したアプリ(ファイル)配信ができること。

【操作ログ管理要件】

- 情報漏洩リスクを軽減する為に、Windows で以下のログを取得できること。

ログオン・ログオフログ	ウィンドウタイトルログ
ファイル操作ログ（ファイル・フォルダのコピー/移動/作成/上書き/削除/名前の変更)	Web アクセスログ（閲覧・アップロード・ダウンロード・書き込み)
プリントログ	周辺機器接続ログ
~~アプリ稼働ログ~~	~~アプリ通信ログ~~
アプリ禁止ログ	脅威検知ログ(LANSCOPE サイバープロテクション powered by Aurora Protect／Deep Instinct で検知した脅威のログ)ただし、利用する場合は、別途連携機能の利用申し込みが必要

PC の操作ログについては、最大 5 年間保存できること。

【セキュリティ管理要件】

- 操作ログのうち、違反操作のアラート設定ができ、アラート操作のみを確認できること。
- 違反操作のアラートが発生した場合、Power Automate の有償ライセンスを利用し、システム管理者にメール・ビジネスチャットで通知できること。
- SIM カードの抜き差しを検知し、アラート通知できること。
- BitLocker の設定状態および回復キーを自動取得できること。
- Windows Defender パターンバージョン、エンジンバージョンを自動取得できること。
- Aurora Protect のバージョンを自動取得できること。
- Deep Instinct のバージョン情報を自動取得できること。
- 記録メディア(USB 機器、SD カード、WPD 機器等)の制御機能を有すること。
- 制御設定の状態でも、シリアルナンバー、VID/PID、フレンドリーネームで特定の記録メディアを除外する機能を有すること。
- 日時を指定して、指定した端末で一定期間記録メディアの利用を許可する機能を有すること。
- 機能更新プログラム(FU)および品質更新プログラム(QU)、更新プログラムの適用状況把握と未適用デバイスへのパッチ配信機能を有すること。
- 最新の Windows アップデートが未適用のデバイスのネットワーク接続を自動で遮断できる機能を有すること。ただし、別途オプション(デバイス検査)契約が必要

【管理コンソール要件】

- 管理コンソールにログイン可能な IP アドレスを制限できること。
- 管理コンソールにログインするアカウントのパスワードについてパスワードポリシーを設定できること。

・ 管理コンソールログイン時に 2 要素認証を設定できること。
・ 管理コンソールの操作履歴を取得できること。
・ 管理コンソールにログインするアカウントは、アカウント毎に閲覧可能な部署やメニューを設定できること。

【品質・性能要件】

・ クラウドサービスに関するガイドライン ISO27017 を取得していること。
・ 利用者のデバイスと、システムとの間のインターネット通信は、SSL/TLS 通信（TLSv1.0 以上）によって
・ 暗号化されていること。
・ システムで利用している OS、ミドルウェア等に関する脆弱性情報を定期的に収集していること。
・ システムで利用しているコンポーネントに対する脆弱性パッチが公開された場合、検証を経た後、速やかにパッチ適用すること。

【運用・保守要件】

・ ソフトウェア保守
・ 保守期間の間であれば常に最新バージョンが利用できること。
・ Windows10 および Windows11 の各バージョン(FU)リリース後、1 ヶ月を目処に動作確認完了、
・ または対応バージョンのリリースを以って対応を表明していること。
・ 本クライアント管理ソフトは、日本国内のメーカが開発・サポートしていること。
・ ソフトウェアの保守については、本クライアント管理システムを提供するソフトウェア開発メーカに直接の電話、E-mail、有人チャットでの問い合わせが可能であること。

(8) 市提供の「施設予約システム用プログラム」を導入し、かがわ電子自治体システムのログイン画面（ID／パスワードの投入画面)までの接続確認を行い、職員の業務確認実施完了まで、現地立ち会いを実施すること

(9) 既設業務用端末より必要な設定とデータを移行するために必要な手順書を作成すること。また移行作業に必要な支援をすること。なお、移行するデータは、以下の通りとする

・ マイドキュメント
・ デスクトップ上のファイルとショートカット
・ ネットワークドライブ設定
・ お気に入り（ブックマーク）
・ メール環境（Outlook）
・ 上記のメールアドレス帳

(10) 二要素認証

ID、パスワードに加え、ICカード又は生体認証（顔認証）を用いてログインするようローカルで設定する。生体認証を選択する場合は、下記の条件内の「ICカード」を全て、生体認証と読み替える。

・ ID、パスワード及びICカード認証を用いて、Windows ドメイン環境下及びワークグループ環境下の端末へログオン可能な機能を有すること。
・ ネットワークダウン時も IC カード認証が行えること。
・ ログは各 Windows 端末のイベントログへ出力され管理されること。なお、ログ管理用に Microsoft SQL Server もしくは Oracle Database などのデータベース製品のインストールが不要なこと。

- 端末のロック解除に関しては ID の入力が不要であること。また、パスワードとICカード認証でロック解除するか、ICカード認証のみでロック解除するかを選択可能であること。
- ログオン後のセキュリティを担保するため、ログオン中も一定間隔にて認証を実施し、認証が不可となった場合は自動的に画面がロックされる機能を有すること。
- 各端末の登録情報や設定を閲覧・操作する管理者権限を設定する機能を有すること。
- ID、パスワード及びICカード認証を用いて、Windows ドメイン環境下及びワークグループ環境下の端末へログオン可能な機能を有すること。
- 生体認証を用いる場合は、実運用環境を鑑み、マスクを着用した状態でも顔認証が可能であること。
- 生体認証を用いる場合は、登録した生体データを完全に抹消できること。

2.2 モノクロレーザプリンタ

- ハードウェア仕様A3対応モノクロレーザプリンタであること
- ファーストプリント 7.5 秒以下であること
- 両面印刷機能を有すること。
- 印刷スピード： 33 枚／分 （A4横送り）以上であること
- 印刷スピード（両面印刷）： 22 枚／分 （A4横送り）以上であること
- 給紙トレイ（標準）： 300枚可能であること
- 給紙トレイ（増設）： 600枚可能であること
- インタフェース：1000Base-T/100Base-TX/10Base-T を標準搭載していること

(1) 業務用端末から標準カセットへの印刷、拡張カセットへの印刷、手差しトレイへの印刷と3パターン印刷が行えるよう、プリンタドライバのセットアップ、印刷設定を実施すること
(2) 導入設置時、各施設担当職員に対して操作説明を実施すること
(3) 5年間の当日~~メーカー~~オンサイト修理保守（定期交換部品を含まない）を付属すること

2.3 施設用ルータ

(1) ハードウェア仕様
- WAN 用のインタフェースは RJ-45 を持ち用途に応じて使い分けられること
- 1000BASE-T に対応した LAN4 ポート以上内蔵していること
- 基本転送性能は最大 2Gbps、IPsec 暗号化性能 1.2Gbps 以上であること
- ルーティング機能として RIP (v1, v2)、OSPFv2, BGP4 をサポートすること
- セキュリティ機能として、IPSec をサポートすること
- フレッツ光のブロードバンドサービスに対応していること
- コンソールポートを有すること。
- WANプロトコルとして、PPP、PPPoE、に対応していること

(2) 機器交換後は拠点間通信と業務の正常性確認を実施すること
(3) クラウド型統合管理サービスに対応していること
(4) 5年間のオンサイト保守（平日日中）をおこなうこと

2.4 施設用スイッチ

(1) ハードウェア仕様

- 1000BASE-T に対応した LAN ポートを8ポート以上内蔵していること
- スイッチング容量は 16.0Gbps 以上であること
- 転送レートは 11.9Mpps 以上であること

(2) 5年間のオンサイト保守(平日日中)をおこなうこと

3. 高松市総合体育館収容機器仕様

3.1 19 インチサーバボックス(参考:CP-SVNC4 12U・奥行き 600mm、鍵付き)

(1)以下の機器を収納しシステム環境を構築すること(UPS は 4 時間以上稼働すること)

インターネット回線(ONU) ※別調達

フレッツ VPN 回線(ONU) ※別調達

センター用ファイルサーバ+バックアップストレージ

センター用ルータ

センター用スイッチ

センター用ファイアウォール

センター用UPS

3.2 センター用ファイルサーバ+バックアップストレージ

(1) ファイルサーバ仕様

- Windows に対応した製品であること
- Microsoft Edge 126 以降をサポートすること
- CPU は ARM Cortex-A55 Quad core 1.8GHz 以上であること
- メモリは 2GB 以上であること
- HDD は2台以上搭載し、容量は 4TB 以上(RAID1 で 2TB 以上)であること
- 冗長化は RAIDeX/RAID1/RAID0 に対応していること
- 同時接続台数(目安)は 50 台以上であること
- バックアップ機能を有すること
- 故障予兆通知機能を有すること
- ウィルス対策機能を有すること
- 5 年間のデリバリ保守が付属し、オンサイトで保守を行うこと

(2) バックアップストレージ仕様

ファイルサーバに対応したカートリッジ式 HDD であること

HDD の容量は4TB 以上であること

5 年間のデリバリ保守が付属し、オンサイト保守を行うこと

3.3 センター用ルータ

(1) ハードウェア仕様

- WAN 用のインタフェースは RJ-45 を持ち用途に応じて使い分けられること
- 1000BASE-T に対応した LAN を 10 ポート以上(うち 8 ポートは SW-HUB)内蔵していること

- 基本転送性能は最大 2Gbps、IPsec 暗号化性能 1.2Gbps 以上であること
- ルーティング機能として RIP (v1, v2)、OSPFv2, BGP4 をサポートすること
- セキュリティ機能として、IPSec をサポートすること
- フレッツ光のブロードバンドサービスに対応していること
- コンソールポートを有すること。
- WANプロトコルとして、PPP、PPPoE、に対応していること

(2) 機器交換後は拠点間通信と業務の正常性確認を実施すること

(3) クラウド型統合管理サービスに対応していること

(4) 5年間のオンサイト保守（平日日中）をおこなうこと

3.4 センター用スイッチ

(1) ハードウェア仕様

- 1000BASE-T に対応した LAN ポートを 24 ポート以上内蔵していること
- スイッチング容量は 48.0Gbps 以上であること
- 転送レートは 35.7Mpps 以上であること
- 1U ラックマウント型であること

(2) 5年間のオンサイト保守（平日日中）をおこなうこと

3.5 センター用ファイアウォール

(1) ハードウェア仕様

- 最大 28Gbps のファイアウォールスループットを有すること
- ファイアウォール同時セッション数は、1.5M 以上の性能を有すること
- ファイアウォールポリシー数は、5,000 以上の性能を有すること
- 仮想 UTM（VDOM10）の機能を有すること
- UTMライセンスをフルバンドルすること

(2) UTMは5年間継続利用できるライセンスで納入すること

(3) 5年間のオンサイト保守（24時間365日）が付属すること

3.6 センター用UPS

(1) ハードウェア仕様

- 3.1（1）のすべての機器が停電時に 4 時間以上バックアップできること
- 負荷容量 200W で 4 時間以上バックアップできること
- 19 インチサーバボックスにラックマウントできること

(2) 5年間の無償保証期間延長サービス（無償修理＋交換バッテリ無償提供）が付属すること

4. 機器セットアップ要件

4.1 共通事項

既存データの移行が必要な機器等については、既存システム業者と調整の上、実施すること。
尚、当該作業において費用が発生する場合は、受注者の負担とすること。

4.2　業務用端末

（1） ネットワーク設定を行い、かがわ電子自治体システムのログイン画面（ID／PWの投入画面）までの接続確認を行うこと。

（2） プリンタドライバのインストール及び、プリンタ設定を行い、動作確認を行うこと。

（3） リモートコントロールソフトをインストールし、リモート接続可能なように設定すること。

（4） ファイルサーバに格納するファイルは指定管理者ごと（最大5社程度）にフォルダを分け、適切なアクセス権限を設定すること。

（5） 各拠点に割当てられているICカードの認証登録を行うこと。（顔認証を用いる場合はICカード枚数分の顔認証登録を行うこと。）※業務用端末1台につき、拠点に割当てられているICカード枚数分の登録が必要

4.3　ネットワーク

（1） フレッツ VPN を利用したネットワーク設計を行い、ネットワーク機器への設定・接続確認を行うこと。

- フレッツは既存の回線を利用するため、回線利用料金は調達に含まない。
- 高松市総合体育館に接続するためのフレッツ回線工事費用は高松市で負担する。

（2） 今回対象施設以外からの施設からも接続されているので、影響を与えない様にネットワーク機器の切り替えを行うこと。

（3） 機器の導入については既存システム業者と調整の上実施し、運用に支障を与えないこと。

4.4　高松市総合体育館収容機器

（1） インターネットとのセキュリティ対策のためファイアウォールを導入すること。

（2） セキュリティ対策として、URL フィルタ、HTTP/FTP ウィルス対策、メールウィルス対策を行うこと。

（3） ハードウェア障害に備え、ファイルサーバ内のデータバックアップを実施すること。バックアップは最低 1 週間分保持すること。

（4） データセンターに設置されてるファイルサーバのデータ移行を行うこと。データ移行は現行のネットワーク経由で行うこと。もし、現在使用中のデータセンター内に立入って作業が必要な場合や、別途ネットワークを接続して作業を行う場合は、既存業者に移行方式を説明の上見積を取得し、作業費用に含めること。

（5） フレッツ VPN 接続用としてルータを用意すること。

5. インターネット回線仕様

高松市総合体育館にインターネット回線を 1 本導入すること。仕様は以下の通り。

（1） インターネット外部への通信が可能な回線であること

（2） 回線容量は最大 1Gbps 以上（ベストエフォート型）とすること。

（3） グローバル IP アドレス※を1個以上付与すること。

（※必要があれば、固定のグローバルIPアドレスを付与すること。）

（4） 回線契約については、落札業者決定後、別途協議の上、契約書を締結することとする。

6.　運用・保守要件

6.1　運用・保守サービスの内容

運用・保守サービスは大きく分けて、定常保守と故障対応の2種類とするが、導入者は納入する全ての機器・ソフトウェア等の不具合・故障について、高松市からの問い合わせに一次対応する。一次対応後、各メーカへのエスカレーション等を実施し、責任をもって不具合・故障の状況及び原因について高松市に報告し復旧対応することとする。また、障害発生時に端末状況等を確認する方法は、「現地オンサイト対応（受付から翌日以内の駆付け）を実施する」か「リモート保守拠点を設置して実施する」かのどちらかを選択可能とする。

【定常保守】

- スポーツ振興課からの問い合わせ対応
- 業務用端末に対する「リモート保守拠点からの確認」又は「現地オンサイト（受付から翌日以内の駆付け）」による端末状況確認
- 業務用端末に対してクローンイメージ作成ソフト等によるリカバリメディアの作成
- 毎年、人事異動（年 1 回を想定）の際に各拠点での認証登録設定作業（※生体認証を用いる場合のみ）
- 指定管理者ごと（最大 5 社程度）にアクセスできるフォルダのアクセス権限を設定
- 指定管理者に変更が入った場合の、アクセス権限の変更作業
- ファイアウォールの脆弱性通知サービスを導入しバージョンアップを実施（1 回/年）
- 高松市総合体育館の点検作業による停電時の立ち会い（1 回/年　4 時間 UPS にて稼働）

【故障対応】

- 故障状況確認及び、修理スケジュール調整
- 故障原因の切り分け（端末機器、端末機器 OS、資産管理ソフト、ネットワーク、かがわ電子自治体システム）
- 二要素認証の不具合、障害、故障対応
- 資産管理の不具合、障害、故障の復旧対応
- 故障原因、障害状況の報告及び故障・障害原因に応じた具体的かつ有効な解決方法の提示
- 業務用端末の場合は、故障機のクローンイメージを利用した代替機のセットアップ
- 業務用端末／プリンタに対する当日出張修理保守
- 高松市総合体育館収容機器に対する当日オンサイト保守

7.2　運用・保守サービスに関する対応時間

機器種別	時　間	内　容
スポーツ施設設置機器	平日　9:00～17:00（※）	統制窓口による電話受付、一次対応、故障修復 その他運用・保守全般
高松市総合体育館収容機器	24時間365日	統制窓口による電話受付、一次対応、故障修復 その他運用・保守全般

※障害発生時等の緊急時には、緊急連絡先を設け、電話での一次対応等を行うこと

7.3　保守拠点（リモート保守作業拠点）

※現地オンサイト対応（受付から翌日以内に駆付け）実施を選択する場合は、設置する必要はない。

・受注者は、各スポーツ施設での障害・故障対応のため、保守拠点を設け、調査用端末を設置し、遠隔保守を行える環境を整えること。（保守用回線等は、受注者で準備すること。また、回線費が発生する場合はそれを負担すること。）

※遠隔端末用回線：現在はフレッツ光回線を使用しています。

・リモート保守拠点からの接続について責任者を定め、責任者は、不正アクセス及びウィルス感染等が発生しないよう必要な対策を講じなければならない。（保守体制一覧に責任者を記載すること。）

・リモート保守拠点からの接続は、保守に必要最低限度にとどめ、情報漏洩及びウィルス感染等が発生しないようセキュリティ環境を確保すること。

・保守拠点からのリモート接続が原因で、情報漏洩及びウィルス感染等のインシデントが発生した場合は、その調査・対応及び復旧にかかる全ての責任と費用を導入者が負担すること。

8. 情報セキュリティ

8.1 かがわ電子自治体システムは、個人情報に関する情報を扱うことから、受注者は情報セキュリティについては、十分に配慮すること。

8.2 契約期間満了後の機器の取扱について

契約期間満了後の機器については、下記のいずれかの方法で処理した上で搬出するかを、本市と協議の上、決定するものとする。

①契約期間満了に伴う返却機器の搬出に当たっては、本市と協議の上、搬出するものとする。

②契約期間後の機器の取扱いについては、部品リサイクル処理、産業廃棄物処理、寄贈、リユース等の指定はしない(注1)が、必ずハードディスク等記録媒体のデータ消去を行い、データの復元及び読み取りを不可能にし(注2)、適切な処理を行った旨の報告書(注3)を本市に提出すること。これら、処置にかかる諸経費、作業は全て導入業者又は賃貸借業者の負担とする。

（注1)機器をリサイクル処理、廃棄処理等を行う場合、必ず廃棄物処理法の認可事業者にて実施すること。

（注2)データ消去方法については、

- 米国国防総省規格やNATO規格に準拠した方式等にてデータを消去
- 特殊の装置で電気的、磁気的に強磁界をかけて消す
- 物理的に破壊する

のいずれかの方法で処理を行うこと。

（注3)物理的破壊もしくはデータ消去証明書及び産業廃棄物処理証明書等