

注 文 書

- 1 契約番号 2026001204
- 2 件 名 内部情報系基盤システム賃貸借
- 3 場 所 大崎市古川七日町1番1号 外
- 4 期 間 令和10年1月1日から令和14年12月31日まで
- 5 別添書類
 - (1) 調達仕様書
 - (2) 参考明細書
- 6 担 当 課 市民協働推進部デジタル戦略課

内部情報系基盤システム賃貸借
調達仕様書

令和8年度

大崎市

目次

1	概要	1
1.1	調達名称	1
1.2	目的	1
1.3	本調達の方針	1
1.4	賃貸借の期間及び賃借料支払方法	1
1.5	賃貸借の範囲	2
2	本調達の要件	5
2.1	内部情報系基盤システムの要件	5
2.1.1	導入場所・セキュリティモデル・クラウドサービス要件・稼働実績	5
2.1.2	サプライチェーン・リスク対策関連要件	6
2.1.3	セキュリティ対策確認書の提出	7
2.2	成果品及び納品場所	7
2.3	対象機器の要件	8
2.3.1	対象機器・システム・利用者	8
2.3.2	更新対象システムのデータ	8
2.4	システム要件	8
2.4.1	ライフサイクルコスト	8
2.4.2	システム機能	9
2.4.3	システム性能	9
2.4.4	ユーザビリティ	9
2.4.5	本市の情報システム管理者による接続環境	9
2.4.6	ハードウェア及びソフトウェア	9
2.4.7	ネットワーク構成	11
2.4.8	他の情報システムとの連携	13
2.5	情報セキュリティ要件	13
2.5.1	権限	13
2.5.2	情報セキュリティ対策（サーバ・LGWAN 接続系クライアント端末）	13
2.5.3	情報セキュリティ対策（業務システム）	14
2.6	システム構築（要件定義，開発，テスト）要件	14
2.6.1	スケジュール	14
2.6.2	要件定義	14
2.6.3	設計	15
2.6.4	試験	15
2.7	導入（工事，設置）要件	15
2.7.1	工事	15
2.7.2	ハードウェア設置	16

2.8	移行要件.....	18
2.8.1	データ移行.....	18
2.8.2	システムデータ等移行.....	19
2.8.3	システム移行.....	20
2.9	次期システムへのデータ移行協力要件	20
2.10	システム運用要件.....	20
2.10.1	運用・操作マニュアル.....	20
2.10.2	定常運用.....	20
2.10.3	オンライン稼働時間帯.....	21
2.10.4	稼働率.....	21
2.10.5	バックアップ.....	21
2.10.6	災害対応.....	21
2.10.7	サービスレベル管理.....	21
2.10.8	運用計画.....	22
2.11	システム保守要件.....	22
2.11.1	保守マニュアル.....	22
2.11.2	定期保守（ハードウェア）	22
2.11.3	構成管理.....	22
2.11.4	インシデント管理（障害事前対策）	22
2.11.5	障害保守.....	22
2.11.6	問題管理（障害事後対策）	23
2.11.7	リリース管理.....	23
2.11.8	キャパシティ管理.....	23
2.11.9	変更管理.....	23
2.11.10	ソフトウェアのバージョンアップ.....	23
2.11.11	情報セキュリティ管理.....	24
2.11.12	ウイルス対策.....	24
2.11.13	セキュリティパッチ等の適用.....	24
2.11.14	サービスレベル管理.....	25
2.11.15	機器保守.....	25
2.12	問合せ対応要件.....	25
2.13	データセンター要件.....	25
2.13.1	立地仕様.....	25
2.13.2	建物仕様.....	26
2.13.3	機器設置室仕様.....	27
2.13.4	停電対策.....	27
2.13.5	セキュリティ対策.....	28
2.13.6	その他.....	28
2.14	プロジェクト管理要件.....	28

2.14.1	プロジェクト計画.....	28
2.14.2	プロジェクト体制.....	28
2.14.3	構築環境.....	29
2.14.4	作業場所.....	29
2.14.5	進捗管理.....	29
2.14.6	課題・問題管理.....	29
2.14.7	リスク管理.....	30
2.14.8	標準化.....	30
2.14.9	品質管理.....	30
3	留意事項.....	30
3.1	検収方法.....	30
3.2	資料の貸与.....	30
3.3	秘密保護・個人情報保護.....	30
3.4	特許権等の帰属.....	31
3.5	著作権の帰属.....	31
3.6	第三者の権利侵害.....	32
3.7	再委託.....	32
3.8	契約不適合責任.....	32
3.9	作業における注意事項.....	33
3.10	契約にかかる注意事項.....	33
4	添付資料.....	35

1 概要

1.1 調達名称

内部情報系基盤システム賃貸借

1.2 目的

財務会計，文書管理，電子決裁，人事給与等の行政事務を支える内部情報系システムは，令和9年12月末に契約期間の満了を迎える。

当該内部情報系システムのうち，共通基盤，ウイルス対策，共有フォルダ，資産管理システム，二要素認証システム，LGWAN メール，LGWAN サーバ（以下「内部情報系基盤システム」という。）を調達するものである。

1.3 本調達の方針

(1) 信頼性・安定性の確保されるシステムの導入

システムの信頼性が保たれるよう，十分な実績や体制を備えているシステムとする。また，障害発生が少なく，仮に障害が発生しても運用停止が短時間で済むようなサポート体制を確立しているシステムとする。

(2) 業務継続性に優れたシステムの導入

データセンターを活用し，災害時や障害発生時等において，業務遂行を中断させない業務継続性の高いシステムとする。共通基盤を専用線又は広域イーサネットあるいは閉域 IP_VPN で接続できるクラウドサービス上に構築することも認めるが，その場合は業務継続性の高いクラウドサービスを採用すること。なお，本調達仕様書記載の「データセンター」とは，特段の記載がない限り，αモデルでも利用可能であり，かつ，専用線又は広域イーサネットあるいは閉域 IP_VPN で接続できるクラウドサービスを提供するデータセンターを含むものとする。

(3) 拡張性・経済性に優れたシステムの導入

開発に要する費用が安価に抑えられるよう経済性に優れたシステムとする。

(4) 情報セキュリティが万全なシステムの導入

情報漏洩や外部からの侵入など，現在のネットワーク社会でさまざまな問題が起きていることを踏まえ，情報セキュリティに十分配慮したシステムとする。

(5) 大崎市情報セキュリティポリシーの遵守

「大崎市情報セキュリティポリシー」（令和8年4月1日改正）を遵守したシステムとする。

1.4 賃貸借の期間及び賃借料支払方法

(1) 令和10年1月1日から令和14年12月31日までとする。賃借料は月払（60ヶ月）とし，初期費用・構築費用も含めて，60ヶ月に平準化して，本稼働後に支払うものとする。

(2) システム本稼働時期は，令和10年1月4日とするが，仮想サーバ及びサーバ OS

のうち、財務会計、契約管理、備品管理、起債管理、庶務事務、人事給与、人事評価、文書管理、電子決裁、グループウェア（インターネットメールサーバ含む）及びこれらのシステム間の連携機能（以下「内部情報系アプリケーション」とする）を導入する部分については、令和9年6月30日までに構築すること。なお、内部情報系アプリケーションは、「IPKNOWLEDGE（富士通 Japan）」と「desknet's NEO（NEOJAPAN）」である。

- (3) データセンターと本市庁舎内サーバ室（以下「本市サーバ室」とする。）を接続する回線については、令和9年7月1日から令和14年12月31日まで提供すること。ただし、令和9年6月30日以前に同回線を内部情報系基盤システムの構築に必要な場合は、同回線が必要な日から令和14年12月31日まで提供すること。
- (4) 別途調達する LGWAN 接続系クライアント端末の設定に必要な DNS 設定情報、ウイルス対策インストーラー、資産管理システムインストーラー、二要素認証システムインストーラーは、令和9年5月28日までに本市に提供すること。ただし、別途調達する LGWAN 接続系クライアント端末が各拠点に配備された後に、令和9年12月17日までに、受注者が各拠点にて同端末にて内部情報系基盤システムを利用できるように必要な設定作業を実施する場合は、この限りではない。
- (5) 資産管理システムのうち、下記の機能は令和9年12月17日までに提供すること。
 - ・別途調達する LGWAN 接続系クライアント端末にプログラムを配布実行する機能
 - ・別途調達する LGWAN 接続系クライアント端末をリモートコントロールする機能
- (6) 上記期間経過後も、状況に応じて、本市が求めるシステム運用・保守を行うこと。その場合の追加費用負担等の必要事項については、本市及び受注者の双方が協議の上、決定するものとし、同追加費用は本調達には含めない。

1.5 賃貸借の範囲

- (1) ハードウェア及びソフトウェアの調達、システム構築（仕様確認、構築）、導入（工事、設定）対象とする物品は、次の通りとする。

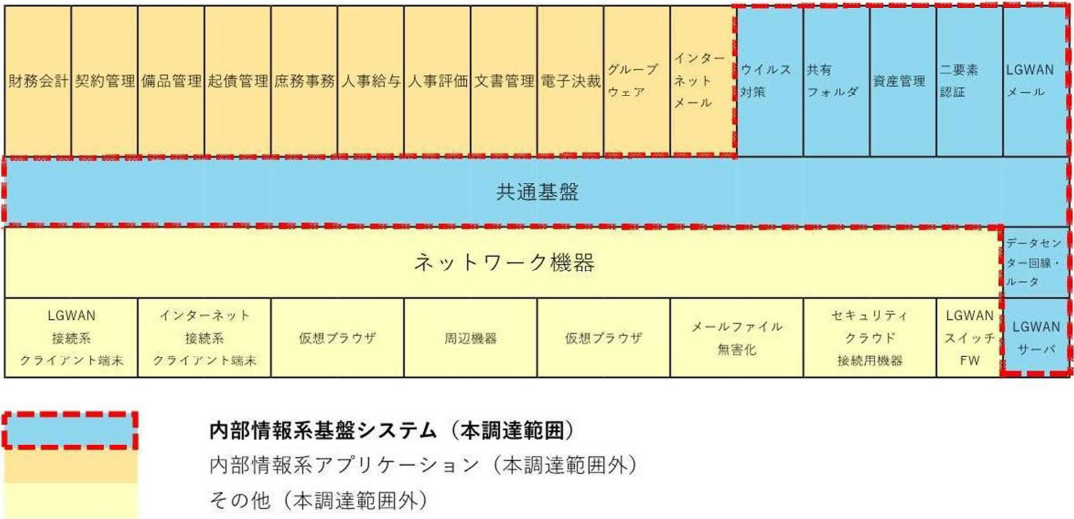
No	物品名
1	共通基盤
2	ウイルス対策（サーバ及び LGWAN 接続系クライアント端末）
3	共有フォルダ
4	資産管理システム
5	二要素認証システム（AD（DNS）サーバ含む）
6	LGWAN メール（Web メール機能等）
7	LGWAN サーバ（メールスプール及び NTP）

なお、本調達範囲イメージは下記の表のとおりである。内部情報系アプリケーションは本調達の範囲外であるが、内部情報系アプリケーションを導入するため

の仮想サーバとサーバ OS は本調達範囲内とする。データセンターに構築するサーバは、下記の要件を満たすこと。

- CPU のオーバーコミットを実施する場合は、オーバーコミット率を 200%以下とすること。ただし、稼働率 99.9%以上の SLA（サービス品質保証）を設定しているクラウドサービス上に仮想サーバを構築する場合は、CPU のオーバーコミット率 200%以上になっても構わない。
- メモリのオーバーコミットは実施しないこと。ただし、稼働率 99.9%以上の SLA（サービス品質保証）を設定しているクラウドサービス上に仮想サーバを構築する場合は、この限りではない。
- 仮想サーバ用 OS は本市の指示に基づいて、「Windows Server 2025 Datacenter Edition」を調達すること。ただし、内部情報系アプリケーションを導入するための仮想サーバ上以外の OS については、受注者で動作を保証できる場合に限り、「Windows Server 2025 Datacenter Edition」以外の OS を調達しても構わない。

本調達範囲イメージ



本調達の範囲内の仮想サーバ上に導入するソフトウェアのイメージは、下記の表のとおりである。なお、下記の表記載のソフトウェアのうち、業務パッケージソフト、業務固有ソフト、運用管理ソフト、DBMS については、ウイルス対策、共有フォルダ、資産管理システム、二要素認証システム、LGWAN メール、LGWAN サーバが本仕様書の記載の要件を全て満たすために必要なものを調達すれば十分であり、必ずしも各システムについて、業務パッケージソフト、業務固有ソフト、運用管理ソフト、DBMS を全て調達しなくても構わない。

データセンター

各システム	財務会計 契約管理 備品管理 起債管理	庶務事務	文書管理	電子決裁	人事給与 人事評価	グループ ウェア	インター ネット メール サーバ 無害化前	インター ネット メール サーバ 無害化後	ウイルス 対策	共有 フォルダ	資産管理	二要素 認証 及び AD	LGWAN メール	LGWAN サーバ
	業務 パッケージ ソフト	業務 パッケージ ソフト	業務 パッケージ ソフト	業務 パッケージ ソフト	業務 パッケージ ソフト	業務 パッケージ ソフト	業務 パッケージ ソフト	業務 パッケージ ソフト	業務 パッケージ ソフト	業務 パッケージ ソフト	業務 パッケージ ソフト	業務 パッケージ ソフト	業務 パッケージ ソフト	業務 パッケージ ソフト
	業務固有 ソフト	業務固有 ソフト	業務固有 ソフト	業務固有 ソフト	業務固有 ソフト	業務固有 ソフト	業務固有 ソフト	業務固有 ソフト	業務固有 ソフト	業務固有 ソフト	業務固有 ソフト	業務固有 ソフト	業務固有 ソフト	業務固有 ソフト
	運用管理 ソフト	運用管理 ソフト	運用管理 ソフト	運用管理 ソフト	運用管理 ソフト	運用管理 ソフト	運用管理 ソフト	運用管理 ソフト	運用管理 ソフト	運用管理 ソフト	運用管理 ソフト	運用管理 ソフト	運用管理 ソフト	運用管理 ソフト
	DBMS	DBMS	DBMS	DBMS	DBMS	DBMS	DBMS	DBMS	DBMS	DBMS	DBMS	DBMS	DBMS	DBMS
共通基盤	OS				OS	OS	OS	OS	OS	OS	OS	OS	OS	OS
	バックアップ機能													
	システム監視機能													
	仮想化機能													
バックアップ基盤（バックアップソフト、OS）														

 本調達範囲

- (2) 移行（データ移行，システムデータ等移行，システム移行）
- (3) システム運用・保守（ウイルス対策，共有フォルダ，資産管理システム，二要素認証システム，LGWAN メール，LGWAN サーバのミドルウェアソフトウェアのバージョンアップ及びセキュリティパッチ適用に伴う動作保証を含む）
- (4) 問合せ対応
- (5) データセンター，データセンター内のサーバラック（データセンターにて発生する光熱水費は受注者の負担とする。）
- (6) クラウドサービス（クラウドサービス上に共通基盤等を構築する場合に限る。クラウドサービス利用料は受注者の負担とする。また，同クラウドサービス利用料が内部情報系基盤システム構築期間及び運用期間内にて値上げになった場合は，同値上げ分も受注者にて全て負担すること。同クラウドサービス利用料の変動を理由とした本市との変更契約は実施しない。）
- (7) 構築及び保守用に受注者がデータセンターに接続するための通信回線（閉域網又はVPN）及びネットワーク機器（本市サーバ室と受注者を接続する回線でも構わない。）
- (8) 本市サーバ室とデータセンターにある本番サーバを接続する専用線又は広域イーサネットあるいは閉域 IP_VPN の通信回線及びネットワーク機器（ルータ等）
- (9) 賃貸借満了時の本調達機器の撤去作業及びデータ消去作業

2 本調達の要件

2.1 内部情報系基盤システムの要件

2.1.1 導入場所・セキュリティモデル・クラウドサービス要件・稼働実績

- (1) 内部情報系基盤システムは、本仕様書に設置場所を指定しているもの及び特別にデータセンター以外の場所に設置することを容認する旨記載しているもの以外はデータセンターへ導入すること。
- (2) 本市のセキュリティモデルは業務端末を LGWAN 接続系に設置する α モデルを採用しているため、LGWAN 接続系端末で直接アクセスできるようにシステムを構築すること。よって、LGWAN 接続系端末では、仮想デスクトップや仮想ブラウザを介さないと利用できないシステムや、 α 〳モデル、 β モデル、 β 〳モデルでないと直接業務端末からアクセスできないクラウドサービスの導入は認めない。また、内部情報系基盤システムを専用線又は広域イーサネットあるいは閉域 IP_VPN で接続できるクラウドサービスなど、「地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省）」で規程されている外部監査を実施しなくても、LGWAN 接続系端末から直接接続できるクラウドサービスに限り、同クラウドサービス上にて構築・運用することも認めるが、同クラウドサーバの構築運用費用やクラウドサービス利用料を含む全ての費用を受注者が負担すること。なお、同クラウドサービス利用料が内部情報系基盤システム構築期間及び運用期間内にて変動した場合のリスクは、受注者にて全て負担すること。
- (3) 専用線又は広域イーサネットあるいは閉域 IP_VPN で接続できるクラウドサービスを利用する場合は、同クラウドサービスは下記のア～ウの要件を全て満たしていること。
 - ア クラウドサービスデータセンター（データの保管場所）及び裁判所の管轄は、日本国内に限定すること。
 - イ ISMS（ISO/IEC27001）を取得していること。
 - ウ 以下の（ア）～（エ）のいずれかを満たしていること。
 - （ア） ISMAP を取得していること。
 - （イ） ISO/IEC27017 を取得しているプライベートクラウド（仮想プライベートクラウドを除く）であること。
 - （ウ） ISO/IEC27017 及び ISO/IEC27018 を取得しており、仮想プライベートクラウドを構築できるクラウドサービスであること。
 - （エ） ISO/IEC27017 を取得しており、仮想プライベートクラウドを構築できるクラウドサービスであり、同クラウドサービスが本仕様書記載の秘密保護及び個人情報保護に関する要件を満たしていることを受注者の責任において担保できること。
- (4) 地方公共団体（人口 10 万人以上の自治体）において、導入実績及び稼働実績を有しているハードウェア・ソフトウェアであること。また、稼働実績を有しない

場合には、受注者の責任の下、安定した稼働を保証すること。

2.1.2 サプライチェーン・リスク対策関連要件

受注者は本調達範囲の機器等（ネットワーク、情報システム、ネットワーク又は情報システムに関する施設及び設備、電磁的記録媒体等の情報資産をいう。以下同じ。）が以下の（１）及び（２）を満たしていることを担保すること。

（１）基本的なセキュリティ対策として、下記のア～エを全て満たしていること。

- ア 必要なセキュリティ機能を含んでいること。
- イ 設置時や保守時のサポート体制が確立されていること。
- ウ 利用マニュアル・ガイダンスが適切に整備されていること。
- エ 脆弱性検査等のテストの実施が確認できること。

（２）サプライチェーン・リスク対策として、下記のア又はイを満たしていること。

ア 情報資産の分類に応じて、「セキュリティ要件適合評価及びラベリング制度（JC-STAR，経済産業省）」、「政府情報システムのためのセキュリティ評価制度（ISMAP，ISMAP-LIU，国家サイバー統括室・デジタル庁・総務省・経済産業省）」又は「デジタルマーケットプレイス（DMP，デジタル庁）」（以下「政府の評価・登録制度」という。）に登録等がなされていることが確認できること。

イ 政府の評価・登録制度に登録等がなされていない機器等（政府の評価・登録制度の対象とならない製品分野に属する機器等を含む。）に関しては、次のとおり適切なサプライチェーン・リスク対策が講じられていることが確認できること。

（ア）機器等の開発等のライフサイクルにおいて、不正な変更が加えられない管理がなされていることが確認できること。具体的には以下のa～dを全て満たしていること。

- a 製造工程（開発工程を含む。以下同じ。）において、機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者（再委託先事業者等を含む。以下同じ。）による信頼できる品質保証体制が確立されていること。
 - b 製造工程における不正な変更の有無について、機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者において、定期的又は随時に確認を行うこと。
 - c 製造環境（開発環境を含む。）において、定められた要員以外がアクセスできないよう、機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者が、アクセス可能な要員を物理的（監視カメラ等の入退室管理等）かつ論理的（データシステム等へのアクセス制御）に適切に制限していること。
 - d 調達した機器等に不正な変更やそのおそれがあることを発見した場合には、機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者並びに当該機器等の設置、保守等の役務を提供する事業者及びその委託先事業者に対して、必要に応じて追跡調査や立入検査を行う等、本市と受注者が連携して原因を調査・排除できる体制を整備していること。
-

- (イ) 機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者並びに当該機器等の設置、保守等の役務を提供する事業者及びその委託先事業者について、当該事業者等の本社等（当該事業者等の総株主等の議決権の過半数を直接又は間接に保有する者の本社等を含む。）の立地する場所の法的環境や外部主体の指示等により、当該機器等に係る開発・供給又は役務の提供等の適切性が影響を受け、これにより悪意ある機能や不正な変更が機器等に組み込まれる又は当該機器等が取り扱う情報が窃取・破壊される等のリスクに係る懸念が払拭できない機器等を調達しないこと又は役務の提供を受けないこと。
- (ウ) ISO/IEC 15408 等、国際標準に基づく第三者認証の取得又は第三者による監査結果により、セキュリティ機能の適切な実装、開発環境の管理体制の検査、脆弱性テスト等について客観的に評価できること。
- (エ) ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認を必要とする場合には、SBOM（Software Bill of Materials：ソフトウェア部品表）の作成、提供等を行っていること。

2.1.3 セキュリティ対策確認書の提出

受注者は、本調達仕様書に定めるサプライチェーン・リスク対策を含めたセキュリティ対策の実施について、必要な確認を行い、確認書を提出すること。

2.2 成果品及び納品場所

受注者は、以下に示す成果品等、必要なドキュメント等の中から、本市及び受注者の双方が協議の上、納品物・納期限等を決定し、指定の数量を指定の形式で本市が指定する場所に納品すること。

項番	工程	成果品
1	要件定義	要件定義書
2		会議議事録
3	設計	設計書（基本設計書，詳細設計書）
4	試験	試験計画書
5		試験結果報告書
6	導入	論理構成図
7		ソフトウェア一覧表
8		物理構成図
9		納品物一覧表
10	データ移行	データ移行計画書
11		データ移行設計書
12		データ移行手順書
13		データ移行完了報告書
14		移行データー一覧表
15	運用	操作マニュアル

項番	工程	成果品
16		運用マニュアル
17		運用作業計画書
18		初動対応計画書
19	保守	保守作業計画書
20		変更実施報告書
21		障害報告書
22	プロジェクト管理	プロジェクト計画書
23		実施スケジュール表
24		プロジェクト進捗管理表
25		課題管理表
26		会議議事録
27	検収	引渡書
28	撤去作業	引き上げ計画書
29	データ消去	データ消去作業完了証明書

※成果品は、原則として A4 版とし、パイプ式ファイルなどで製本すること。ただし、本市と受注者との協議において、ページ数が膨大であるなどの理由で、紙媒体での納品が困難であると認められる部分については、電子データのみの提出を認める。

※電子データは、正本として PDF ファイル、副本として Microsoft Office (Word 又は Excel) ファイルとし、DVD-R に格納すること。ただし、データ容量が膨大であり、DVD-R に格納することが困難である場合は、USB メディア、外付け HDD 等で保存して、提出することを認める。

2.3 対象機器の要件

2.3.1 対象機器・システム・利用者

本事業において、更新する機器、業務システム、主管部署及び利用者数を別紙 1 「業務別利用者数一覧表」に示す。また、機器設置台数を別紙 2 「部署別機器設置台数一覧表」に示す。ただし、LGWAN 接続系クライアント端末、複合機、プリンタは本調達の範囲外である。

2.3.2 更新対象システムのデータ

本調達において更新する業務システムのデータ件数を別紙 3 「対象データ件数表」に示す。

2.4 システム要件

2.4.1 ライフサイクルコスト

ライフサイクルコストは、内部情報系基盤システムが本稼働後 5 年間稼働する想定で算出すること。

2.4.2 システム機能

- (1) システムに求める仕様を別紙4「各システムハードウェア仕様一覧表」に示す。
別紙4記載の仕様を全て満たしているシステム・ハードウェアを導入すること。
- (2) ログに記録される時刻にずれが生じないように、受注者がデータセンターに導入する物理機器や仮想マシンの時刻同期を行うこと（NTP サーバの構築含む）。また、別途調達するアプリケーション, LGWAN 接続系クライアント端末及びネットワーク機器の時刻同期について必要な設定情報等を提供すること。また、時刻同期については本市で定める別セグメントにも提供できること。

2.4.3 システム性能

SLA項目定義については、システム稼動前に受注者とサービスレベルを合意の上締結するが、別紙6「サービスレベル（SLA）定義表」に本市が想定するサービスレベルを示す。

2.4.4 ユーザビリティ

- (1) 共有フォルダについては、マウス及びキーボードでも操作が行えること。
- (2) 資産管理システムについては、本市の情報システム管理者（市民協働推進部デジタル戦略課所属職員）がマウスで操作が行えること。

2.4.5 本市の情報システム管理者による接続環境

本市の情報システム管理者（市民協働推進部デジタル戦略課所属職員）が LGWAN 接続系クライアント端末からのリモートデスクトップ接続等により、仮想サーバにアクセスできるように設定すること。

2.4.6 ハードウェア及びソフトウェア

本市の要求要件を踏まえて、業務遂行に必要なハードウェア及びソフトウェアを納入すること。サーバについては、別紙5「各システムリソース要件」に記載した数量・性能を満たしているものを納入すること。内部情報系アプリケーション、クライアント端末、プリンタ、周辺機器（スキャナ等）については、別途調達とするが、本市が使用するクライアント端末、プリンタ、周辺機器（スキャナ等）について、別紙2「部署別機器設置台数一覧表」に示す。

なお、本市に設置するハードウェア及びソフトウェアの選定に当たり、以下の事項に留意すること。

- (1) 信頼性
 - ・障害時にも影響を最小限に留める耐障害性に優れた構成であること。
 - ・高耐久性が求められる構成部品・ユニットは二重化及び冗長化構成とするなど、ハードウェア、ネットワークに起因する障害等が発生しても、業務に重大な影響を及ぼさないような構成であること。本市サーバ室に設置するサーバについては、無停電電源装置を設置すること。
 - ・導入するハードウェアについて過去5年以内に地方公共団体又は機構承認団体（地方公共団体情報システム機構総合行政ネットワーク基本規程（改正令和6

年9月4日)第7条)における稼働実績を有すること。

- ・障害発生時においても業務データの損失を防止し、かつ業務データの整合性を保持できること。
- ・災害時には、優先度を考慮した段階的な復旧ができること。

(2) 保守性

- ・サーバについては、監視、解析及び通知等の機能を有していること。
- ・サーバについては、活性交換の機能を有すること。なお、αモデルでも運用できるクラウドサービスを利用する場合はその限りでない。
- ・障害予防としての定期点検、故障時に修理が可能な保守サポート体制があること。
- ・オンサイト保守サービスによる定期点検の実施、故障時の修理等が可能である製品から構成すること。また、カタログに掲載されている機種を採用すること。(カタログを提出すること。) αモデルでも運用できるクラウドサービスを利用する場合はその限りでない。
- ・運用期間中はサポートが保証される製品であること。なお、契約満了後、9ヶ月間又は1年間の再賃貸借について、本市と受注者で協議できる製品を納品すること。

(3) 拡張性

- ・機器の拡張や変更に伴い構成変更が柔軟に行えること。
- ・将来的な機能追加、業務量増加に伴いメモリ及び補助記憶装置(磁気ディスク装置等を拡張できること。

(4) 経済性

- ・本体価格、ライセンス料及び付帯的な費用(搬入、インストール及び設定・調整)がそれぞれ明確であること。

(5) 前方互換性

- ・サービス利用開始当初のOS、ミドルウェア等のバージョンに係るサポート期間がサービス利用期間中に終了した際には、本市と新たなバージョンに移行すべきか協議すること。新たなバージョンに移行することが適切である場合は、新たなバージョンに迅速かつ円滑に対応し、移行すること。また、そのために、サービス利用期間中において、問題なくサポートを受けられる製品を選択すること。

(6) LGWAN 接続系クライアント端末

- ・LGWAN 接続系クライアント端末及び液晶モニタについては別途調達するため、本業務の範囲外とする。ただし、下記の性能のLGWAN 接続系クライアント端末で、問題なく運用できるシステムを導入すること。

OS: Windows11 Pro x64 (日本語版)

CPU: コア数6, (Intel Core i5 第12世代 相当又は AMD Ryzen 5 5000 シリーズ 相当)

RAM : 8GB

SSD : 256GB

無線 LAN : Wi-Fi5

Web カメラ : 顔認証対応

- ・資産管理システムに別途本市が提供する LGWAN 接続系クライアント端末 1320 台の情報を登録すること。なお、LGWAN 接続系クライアント端末の情報は、本市から受注者へ令和 9 年 9 月末までに提供する。LGWAN 接続系クライアント端末 1320 台のうち、132 台（全体の 10%）を令和 9 年 9 月末までに本市ネットワークに接続できる状態にし、残り 1,188 台は同年 10 月～11 月頃に順次本市ネットワークに接続できる状態にする想定である。
 - ・LGWAN 接続系クライアント端末にプログラム等のインストールが必要な場合は、インストール媒体及び手順書も提供すること。なお、端末へのインストール作業は別調達での作業範囲とする。
 - ・LGWAN 接続系クライアント端末に二要素認証システムにて本市職員（Windows ユーザー）がログインした場合、初期のデスクトップ画面に内部情報系アプリケーションログイン、共有フォルダのショートカットが表示されるように Active Directory Domain Services のグループポリシー等を利用して設定すること。
 - ・本調達範囲である二要素認証システムの Active Directory Domain Services のグループポリシーにて、LGWAN 接続系クライアント端末に本市が受注者へ提供する証明書を配布すること。
 - ・LGWAN 接続系クライアント端末の Windows Server Device CAL ライセンスは別途調達するため、本調達の範囲外である。
- (7) プリンタ（複合機を含む）
- ・プリンタについては別途調達するため、本業務の範囲外とする。ただし、当該機器の調達に必要な仕様及び設定情報等を提示すること。
- (8) 周辺機器
- ・周辺機器（スキャナ等）については別途調達するため、本業務の範囲外とする。ただし、当該機器の調達に必要な仕様及び設定情報等を提示すること。

2.4.7 ネットワーク構成

- (1) ネットワーク概要・機器の設置場所については、別紙 7「ネットワーク概要図」、別紙 8「設置場所別ハードウェア一覧」に示す。受注者が本市サーバ室に設置するルータから本番サーバまでに必要にあるネットワーク機器は本調達の範囲内であるが、同ルータから大崎市庁舎側のネットワーク機器は本調達の範囲外である。また、無線 LAN コントローラ、ネットワーク監視サーバ、DHCP サーバ、RADIUS サーバ、Proxy サーバは本調達の範囲外である。ただし、本仕様書記載の要件を充足するために追加の機器・ライセンスが必要な場合は、同機器・ライセンスも調達すること。

-
- (2) 本市サーバ室とデータセンターを接続する回線については新規で用意することとし、その費用は受注者が負担すること。また、以下要件を満たすこととする。
- ・主回線（1Gbps）と従回線（100Mbps 以上）とで二重化すること。主回線は、業務システムの利用に支障をきたさない帯域保証回線（SLA あり）を採用し、且つデータセンター側は冗長化接続すること。
 - ・主回線が不通になった場合は、主回線不通時から 10 分間以内に従回線でデータセンターと地域コアスイッチの通信ができるようにすること。
 - ・主回線従回線ともに、専用線又は広域イーサネットあるいは閉域 IP_VPN を活用し、第三者によるアクセスを確実に遮断するセキュアなネットワーク接続環境を提供すること。また、接続拠点の追加に対応できること。
 - ・無害化処理前メールサーバ（インターネット接続系ネットワーク）と無害化処理後メールサーバ（LGWAN 接続系ネットワーク）を運用するため、1 回線で 2 つ以上のネットワークを運用できる回線を調達すること。
 - ・主回線従回線ともに、ONU とルータは受注者の負担で調達すること。
 - ・主回線用の ONU 及びルータ、従回線用の ONU 及びルータをそれぞれ本市サーバ室に設置すること。なお、ONU とルータを接続する通信ケーブルが、カテゴリ 5e 又は 6 の LAN ケーブルで構わない場合は、同 LAN ケーブルの調達及び配線は本市で実施する。
 - ・同ルータと別途調達する地域コアスイッチ（本市サーバ室）を RJ-45 対応 LAN ケーブルで接続すること。なお、ルータと地域コアスイッチを接続する LAN ケーブルが、カテゴリ 5e 又は 6 で構わない場合は、同 LAN ケーブルの調達及び配線は本市で実施する。
 - ・同ルータについては、センドバック保守を実施すること。
 - ・同ルータはポートベース VLAN、IEEE 802.1Q タグベース VLAN に対応していること。
 - ・通信経路については海外を経由しないこと。
- (3) 受注者が仮想サーバを運用・保守するために、受注者がデータセンターに接続する通信回線は、専用線又は広域イーサネットあるいは閉域 IP_VPN を使用し、同回線の費用は受注者が負担すること。なお、受注者と本市サーバ室を接続する回線を調達し、本市サーバ室の地域コアスイッチ（別調達）を経由して、受注者とデータセンターを接続する方法でも構わない。
- (4) 各拠点間の通信は、別途調達している広域イーサネットサービス又は大崎市管理の自営光ケーブルで実施している。
- (5) 内部情報系アプリケーション受注者が構築・保守用として仮想サーバにアクセスするための回線は、本調達の範囲外であるが、同回線を利用して内部情報系アプリケーション受注者が仮想サーバにアクセスできるように設定すること。内部情報系アプリケーション受注者が、同受注者執務室と本市サーバ室に接続する回線を調達し、本市サーバ室の地域コアスイッチ（別調達）及び本市サーバ室設置予
-

定のルータ等（内部情報系基盤システム受注者が調達予定）を経由して、内部情報系アプリケーション受注者執務室とデータセンター間を通信することを想定している。ただし、受注者、内部情報系アプリケーション受注者、本市の3者の協議において、内部情報系アプリケーション受注者が同受注者執務室とデータセンターを直接接続する回線を調達する方を適切と判断した場合は、この限りではない。なお、同回線を利用してリモート保守をする場合は、大崎市情報セキュリティポリシー（令和8年4月1日改正）を遵守し、かつ、αモデルを維持することができる方法で実施すること。

- (6) LGWAN 接続系クライアント端末から、下記の接続方式を経由して共通基盤へアクセスできるように、設定すること。

- ・イーサネット (Ethernet)
- ・無線 LAN (Wi-Fi 5 / Wi-Fi 6)

- (7) 通信およびネットワーク設計において、IPv4 を使用すること。

2.4.8 他の情報システムとの連携

内部情報系アプリケーションにおいては、データ連携が可能であること。内部情報系アプリケーションの主なデータ連携について、別紙9「情報システム間連携」に示す。データ連携自体は本調達の範囲外であるが、データ連携のために必要な仮想サーバの構築、仮想サーバ間にて通信ができるように設定する作業は本調達の範囲内である。なお、本仕様書記載のサーバに追加してデータ連携サーバが必要な際の必要スペックについては別途本市より情報提供を行う。その場合の追加費用については、本市と協議し別途費用にて対応することも検討する。

2.5 情報セキュリティ要件

2.5.1 権限

- (1) 正職員及び再任用職員（約 1,150 人）が LGWAN 接続系クライアント端末を利用するにあたり、Windows (LGWAN 接続系クライアント端末) ログイン時に ID と顔認証を必須とすること。会計年度任用職員（約 800 人）のうち、約 200 人は Windows (LGWAN 接続系クライアント端末) ログイン時に ID と顔認証を必須とし、残り約 600 人は Windows (LGWAN 接続系クライアント端末) ログイン時に ID とパスワード認証を必須とする。
- (2) 正職員及び再任用職員の内部情報系アプリケーションのユーザ認証は、シングルサインオンとする。会計年度任用職員の同ユーザ認証はシングルサインオン又は ID とパスワード認証とする。

2.5.2 情報セキュリティ対策（サーバ・LGWAN 接続系クライアント端末）

- (1) サーバ・LGWAN 接続系クライアント端末毎のセキュリティパッチ適用状況の監視、一元管理を行い、セキュリティパッチ未適用の同クライアント端末に対し適用指示ができること。

- (2) USB メモリ等外部媒体の使用制限・管理が行えること。
- (3) 利用者操作のログを収集・保管でき、不正利用を抑止する効果と、万一の事故発生時の原因特定ができること。
- (4) 収集するログは次のとおりとし、それぞれ成功と失敗及びその理由を記録できること。
 - ・ログオン及びログオフ
 - ・ファイルの参照
 - ・ファイルの保存
 - ・ファイルの移動及びコピー
 - ・ファイルの削除
 - ・ファイルの印刷

2.5.3 情報セキュリティ対策（業務システム）

- (1) 共有フォルダ、資産管理システム、二要素認証システム、LGWAN メールの利用者操作のログを収集・保管でき、不正利用を抑止する効果と、万一の事故発生時の原因特定ができること。
- (2) 収集するログは次のとおりとし、それぞれ成功と失敗及びその理由を記録できること。
 - ・ログイン及びログアウト

2.6 システム構築（要件定義、開発、テスト）要件

2.6.1 スケジュール

新システムの構築スケジュールについて、下の表にて示す。

なお、下の表にて示す各工程のスケジュールは本市の想定であり、契約締結後に受注者と協議のうえ決定するものとする。

システム構築スケジュール

	R8年度						R9年度						R10年度									
	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月		
共通基盤	機器等の調達設置、仮想サーバの構築、回線調達									内部情報系アプリケーション構築支援						本番稼働						
ウイルス対策	ソフトウェアの調達									システム構築						検証・本番移行		本番稼働				
共有フォルダ	ソフトウェアの調達									システム構築						検証・本番移行		本番稼働				
資産管理システム	ソフトウェアの調達									システム構築						検証・本番移行		本番稼働				
二要素認証システム	ソフトウェアの調達									システム構築						検証・本番移行		本番稼働				
LGWANメール	ソフトウェアの調達									システム構築						検証・本番移行		本番稼働				
LGWANサーバ	ソフトウェアの調達									システム構築						検証・本番移行		本番稼働				

2.6.2 要件定義

(1) 要件定義の打合せ

要件定義に関する本市との打合せについては、本市と協議し日程調整すること。

打合せ後5日以内（開庁日）に「議事録」を作成し、本市の承認を得ること。やむ

を得ない事情により打合せ後 5 日以内（開庁日）までに議事録等の作成ができない場合は、打合せ後 5 日以内（開庁日）までに本市担当職員にその旨連絡し、担当職員が指定した日までに作成すること。

(2) 打合せ場所

打合せ等の場所は原則として本庁舎内とし、会議室はその都度本市が用意する。ただし、打合せの内容の性質上、Web 会議にて開催しても支障がない場合は、Web 会議による開催も可とする。その場合の Web 会議システムの主催アカウントは本市が用意する。

(3) 要件定義結果

調整した要件定義結果をまとめた「要件定義書」を作成し、本市の承認を得ること。

2.6.3 設計

「基本設計書」「詳細設計書」を作成し、本市の承認を得ること。

2.6.4 試験

- (1) 共有フォルダ・二要素認証システム・LGWAN メールについては、試験実施前に、「試験計画書」を作成・提出し、本市の了承を得たうえで実施すること。
- (2) 共有フォルダ・二要素認証システム・LGWAN メールについては、同試験実施後に「試験結果報告書」を本市に提出すること。
- (3) 関連する他システム等との調整の上、実施すること。
- (4) 同試験の実施にあたり以下の事項に留意すること。
 - ・試験計画には、負荷試験、障害回復試験、性能試験が含まれていること。
 - ・サービスの利用開始前に品質を確認するための十分な試験期間を確保すること。
- (5) 共通基盤、ウイルス対策、資産管理については、本稼働前に動作確認・疎通確認を実施すること。また、同動作確認・疎通確認を実施した後に「試験結果報告書」を提出すること。

2.7 導入（工事、設置）要件

2.7.1 工事

(1) 電源工事

ハードウェア新設に伴い、電源工事が必要となる場合は受注者が実施すること。なお、本市サーバ室のサーバラックの電源は、単相交流 100V である。

(2) LAN 工事

本市庁舎内の LAN ケーブルは既存の LAN ケーブルを使用すること。

ハードウェア新設に伴い、データセンターに LAN 工事を実施する必要がある場合は、受注者の負担にて実施すること。

(3) 回線工事

本調達範囲の専用線又は広域イーサネットあるいは閉域 IP_VPN の光回線工事は受注者の負担にて実施すること。（ONU の設置、光コードの敷設も含む。）

2.7.2 ハードウェア設置

(1) ハードウェア導入（ハードウェア選定，調達，設置，初期設定）

- ・導入機器は，全て新品とすること。
- ・導入機器は，製品の動作保証が確認されたものであること。
- ・安定した稼働が可能な機器を採用すること。
- ・ソフトウェアは，期間中，保守可能な安定したバージョンとすること。
- ・特定のベンダーによる独自性の高い技術に基づかない機器を採用すること。
- ・本市サーバ室に設置する機器については，電源供給停止時には正常にサーバーをシャットダウンできるよう無停電電源装置を導入すること。
- ・データセンターに物理サーバを設置する場合は，ハードウェアを含む全てを冗長化し，自己修復機能又はフェールオーバー機能を有した管理機能により，障害発生時も自動で即時ミラー（複製）を再構築し，安定した運用環境を提供すること。また，専用線又は広域イーサネットあるいは閉域 IP_VPN で接続できるクラウドサービス上に仮想サーバを構築する場合は，自己修復機能又はフェールオーバー機能を有した管理機能により，障害発生時も自動で即時ミラー（複製）を再構築し，安定した運用環境を提供すること。ただし，同クラウドサービス上に仮想サーバを構築する場合は，別論理テナントに仮想サーバを構築し，システムの分散化を図ることにより，可用性及び耐障害性を確保する方法でも構わない。
- ・システムバックアップサーバに限っては，ストレージが冗長化されていれば，CPU を冗長化する必要はない。
- ・高速記憶装置である SSD を一時領域のみではなく，実データ領域としても有効活用し，高いパフォーマンスを実現すること。
- ・本仕様書に設置場所を指定しているもの及び特別にデータセンター以外の場所に設置することを容認する旨記載しているもの以外は，受注者にて準備するデータセンターに導入すること。
- ・LGWAN サーバは，別紙4「各システムハードウェア仕様一覧表」LGWAN サーバの「LGWAN サーバを本市サーバ室に設置する場合の追加要件」を全て満たしている場合に限り，本市サーバ室に設置することを容認する。
- ・多要素認証システムの Active Directory Domain Services セカンダリサーバ（DNS セカンダリサーバ）は，別紙4「各システムハードウェア仕様一覧表」多要素認証システムの「Active Directory Domain Services セカンダリサーバを本市サーバ室に設置する場合の追加要件」を全て満たしている場合に限り，本市サーバ室に設置することを容認する。
- ・具体的な設置場所及びレイアウトは，本市と協議すること。
- ・契約期間満了時のデータ消去及び受注者が本市に設置した機器撤去費用については，本調達に含むものとする。

-
- ・共有フォルダサーバ及びストレージについては、別紙4「各システムハードウェア仕様一覧表」共有フォルダの「共有フォルダサーバ及びストレージを本市サーバ室に設置する場合の追加要件」を全て満たしている場合に限り、本市サーバ室に設置することを容認する。

(2) 賃貸借期間終了時のハードウェア撤去・データの消去

ア 本調達機器の賃貸借期間終了時、本市の敷地内又はデータセンター敷地内から搬出する際には、引き上げる機器に内蔵又は付属する電磁的記録媒体に保存されているデータについて、搬出前にデータ復元ソフトウェア等を用いても再度データを入手できないよう完全にデータを消去すること。消去の方法は、引き上げ計画書の作成時において、本市と協議し承認を得ること。

イ USB メモリに関しては、専用の破壊装置やシュレッダーを使用し、破壊すること。

ウ 光学媒体については、メディアシュレッダーやメディアクラッシャー等の機器にて記録層を破壊すること。

エ HDD に関しては、下記のいずれかの方法でデータ消去を実施すること。

- ・専用の破壊装置やシュレッダーを使用し、破壊する。
- ・暗号化消去により、除去する。
- ・ATA コマンドの「SECURITY ERASE UNIT」コマンドを「Enhanced Erase mode」で使用し、除去する。
- ・SCSI コマンドの「SCSI SANITIZE」コマンドや「SCSI Format」コマンドを使用し、除去する。
- ・消磁を行い、除去する。

オ SSD に関しては、下記のいずれかの方法でデータ消去を実施すること。

- ・専用の破壊装置やシュレッダーを使用し、破壊する。
- ・暗号化消去により、除去する。
- ・ATA コマンドの「BLOCK ERASE」コマンドを使用し、除去する。
- ・SCSI コマンドの「SCSI SANITIZE」コマンドや「SCSI Format」コマンドを使用し、除去する。
- ・NVMe (PCIe) コマンドの「NVM Express Format」コマンドや「NVM Express SANITIZE」コマンドを使用し、除去する。

カ データ消去作業完了時に、データ消去作業完了証明書を提出すること。除去する場合は、データの抹消方法、作業履歴を記載し、作業が正常に終了したことの証跡を添付すること。破壊する場合は、破壊処理の前後が確認できる証拠写真及び記録媒体のシリアルナンバーを添付すること。

キ クラウドサービスを利用する場合は、内部情報系基盤システム運用期間満了後に、上記ア～カと同等程度にデータが確実かつ復元不可能な状態に消去できる方法で、データ消去作業を実施すること。

(3) ネットワーク導入・運用（ハードウェア選定、調達、設置、初期設定）

-
- ・ネットワーク概要について、別紙7「ネットワーク概要図」に示す。
 - ・基本的には庁舎内及び庁舎間では、現行ネットワーク（ハブ、配線等）を使用する。なお、並行稼働時と単独稼働時において、設定変更及び追加機器が必要になる場合は必要な情報を提示し、本市及び本市現行ネットワーク保守事業者と協議すること。
 - ・本賃貸借の期間中に、無線 LAN コントローラ、ネットワーク監視サーバ、DHCP サーバ、RADIUS サーバ、Proxy サーバ、各拠点ネットワーク機器の更新を予定しているため、同更新時に必要になる作業を実施すること。また、同更新時に必要になる LGWAN 接続系クライアント端末の設定変更作業は本市で実施するが、同設定変更作業時に本調達範囲の Active Directory Domain Services のグループポリシー機能を本市（又は LGWAN 接続系クライアント端末保守事業者あるいは LGWAN 接続系ネットワーク機器調達事業者）が使用することを容認するか、受注者にて本市の指示に従いグループポリシーの設定を実施すること。
 - ・本市のセキュリティモデルは α モデルを採用しているため、LGWAN 接続系クライアント端末から内部情報系アプリケーション、共有フォルダに接続できるように設定すること。
 - ・メールファイル無害化サービスは、本調達の範囲外であるが、内部情報系アプリケーション受注者が構築する無害化処理後のメールを管理するメールサーバがメールファイル無害化サービスに接続できるように設定すること。

2.8 移行要件

2.8.1 データ移行

共有フォルダについては、現行共有フォルダから新共有フォルダへ下記のとおりデータ移行すること。

- (1) データ移行の前に「データ移行計画書」を作成・提出し、本市の了承を得たうえで実施すること。
- (2) 「データ移行設計書」「データ移行手順書」を作成し本市の承認を得ること。データ移行作業スケジュールの検討に当たっては、移行作業の実施が通常業務に影響を与えないよう配慮すること。
- (3) 移行作業完了後、「データ移行完了報告書」「移行データ一覧表」を本市に提出すること。
- (4) 現行共有フォルダにおける移行データについては、本市が主体となり、現行共有フォルダ運用事業者と協議の上、提供方法を提示する。
- (5) 提供する移行データに対する問合せに関しては本市が受け付け、現行共有フォルダ運用事業者に照会した結果を本市が回答する。問合せ期間は本調達で提供されるシステム稼働日までとし、回数は20回を上限とする。
- (6) 移行データの提供については、調査用1回、検証用1回、本番移行用1回の計3回を原則とする。調査用1回、検証用1回のデータの範囲は本市と受注者にて協

-
- 議の上、決定する。（また、本市が提供する移行データの作成費用は、本市の負担とする。）
- (7) 提供するデータの媒体については、本市と協議すること。
 - (8) 移行作業は、できる限り手作業での入力を避けること。また、新共有フォルダにおいて必須となる項目が現行共有フォルダに存在しない場合は、受注者がデータエントリ等によりデータの作成を行うこととする。
 - (9) データ移行においてデータの不整合が生じた場合は、受注者の責任において速やかに対応すること。ただし、その原因が現行共有フォルダにあることが確認された場合は、本市及び受注者の双方が協議の上、対応方法を決定するものとする。
 - (10) 現行共有フォルダと新共有フォルダの並行稼働における二重入力等、担当職員の作業負担をできる限り軽減する対応とすること。
 - (11) 受注者が別紙3「対象データ件数表」を基に、移行データの取込みを行うこと。
 - (12) 移行対象とするデータは本市より提供する現行共有フォルダより切り出された全てのデータとする。
 - (13) 共有フォルダへのデータ移行については、本市が提供した移行データを元に、受注者が主体となり調査分析するとともに、必要に応じて移行プログラムを用意するなどして、移行作業とデータ検証を行うこと。
 - (14) 移行データに不足があった場合は本市と十分協議した上で対応方針を決定すること。
 - (15) データ移行後の最終結果確認は本市職員が責任をもって実施するが、受注者は、正確かつ迅速な移行・確認作業が行なえるよう協力すること。
 - (16) 作業場所は、本市庁舎内又は庁舎外においても入退室管理やデータへのアクセス制御、データ等の搬入出制限ができる施設も可とする。この場合、事前に作業場所について本市に届出るものとし、本市の情報セキュリティ監査を受けなければならないものとする。
 - (17) データの授受運搬については施錠できる専用ケースを用意すること。
 - (18) データについては、不正アクセス対策を講ずるとともに、記憶媒体や紙媒体が発生する場合は、施錠できる保管庫又は施錠若しくは入退室管理の可能な保管室に保管するなど適正に管理すること。
 - (19) データ移行時に使用する回線は、現行データセンターと本市サーバ室を接続する回線（本調達範囲外）と本市サーバ室と新データセンターを接続する回線（本調達範囲内）を使用することを想定している。受注者にて他の回線を使用したい場合は、当該回線の工事費用、初期費用、月額使用料等の発生する費用は全て受注者にて負担すること。

2.8.2 システムデータ等移行

- (1) 受注者が初期データ設定、パラメータ設定等、内部情報系アプリケーションのデータ移行をするために必要な初期設定を行うこと。なお、内部情報系アプリケーションのデータ移行作業自体は本調達の範囲外であるが、同データ移行のために
-

必要になるネットワーク設定等は本調達の範囲内である。

- (2) 二要素認証システムについては、本市から受注者に正職員及び再任用職員の顔写真データ（JPG ファイル）を提供する。同データに基づいて、正職員及び再任用職員が顔認証で Windows（LGWAN 接続系クライアント端末）にログオンできるように設定すること。
- (3) LGWAN メールについては、下記のいずれの方法で対応すること。
 - ・本市が提供する旧 LGWAN メールデータを受注者が新 LGWAN メールに取り込む。
 - ・受注者にて、旧 LGWAN メールデータの取り込み方法を記載したマニュアルを作成し、本市に提出する。

2.8.3 システム移行

- (1) 内部情報系アプリケーションのリハーサルは、内部情報系アプリケーション受注者にて実施するため、本調達の範囲外である。ただし、リハーサル実施中に仮想サーバの設定、ネットワーク機器の設定について、本市及び内部情報系アプリケーション受注者から問合せがあった場合は、回答すること。
- (2) 本稼働後、1 日間は本庁舎及び各総合支所内に常駐して立ち会うこと。

2.9 次期システムへのデータ移行協力要件

共有フォルダについては、本賃貸借期間の満了に伴い、次期保守業者の対応とするが、次の業務は本調達の範囲内とする。

- ・内部情報系基盤システムの共有フォルダから次期共有フォルダへデータを送信できるように、双方の通信を許可する設定作業
- ・内部情報系基盤システムの共有フォルダのデータ容量、クォータ設定、フォルダ階層の状況を次期共有フォルダ保守業者に提供する業務

2.10 システム運用要件

2.10.1 運用・操作マニュアル

- (1) 「運用マニュアル」、「操作マニュアル」を作成し本市の承認を得ること。
- (2) 必要に応じて改良しオペレーションミス防止を図ること。

2.10.2 定常運用

- (1) 主な運用委託内容を以下に示す。ただし、市民協働推進部デジタル戦略課職員が随時リソースの状態を確認することができる場合は、リソースを常時監視する必要はない。
 - ・サーバ処理。
 - ・定常処理、オンラインサービスの起動・停止、サーバの起動・停止等のスケジュール登録。
 - ・バックアップ処理。
 - ・リソース監視（本市設置機器を含む）。
- (2) 共有フォルダ・二要素認証システムの 4 月人事異動・組織名変更時の運用

毎年度４月に実施する本市の人事異動・組織名変更により発生する Windows ユーザーの追加・設定変更・削除の作業を受注者にて実施すること。人事異動・組織名変更に伴い共有フォルダのアクセス権限や二要素認証システムの設定変更が必要な場合は、受注者にて実施すること。

なお、人事異動・組織名変更後のデータは毎年度３月２７日までに受注者に提供する。

(3) 共有フォルダ・二要素認証システムの４月以外の人事異動時の運用

４月以外の人事異動に伴う Windows ユーザーの追加・設定変更・削除の作業及び共有フォルダのアクセス権限や二要素認証システムの設定変更については、人事異動時に必要になる設定の操作手順を記載したマニュアルを受注者にて作成し、本市職員に提供する場合、本市職員にて実施する。やむを得ない事情により、同マニュアルを作成・提供できない場合は、同作業・設定変更は、受注者にて実施すること。

2.10.3 オンライン稼働時間帯

オンライン稼働は原則２４時間３６５日とする。

2.10.4 稼働率

稼働率の目標値は９９％以上とすること。同目標値に到達しなかったことをもって、直ちに不可とはしないが、同目標値に到達しなかった場合は、本市の業務を遂行する上で支障とならないように運用方法等を本市と協議すること。

2.10.5 バックアップ

システムバックアップ及び共有フォルダのデータバックアップは本調達の範囲内とする。また、内部情報系アプリケーションのデータバックアップ作業は本調達の範囲外であるが、内部情報系アプリケーションのデータバックアップを実施するためのバックアップ領域の提供は本調達の範囲内とする。

- (1) システムバックアップの詳細仕様は、別紙４「各システムハードウェア仕様一覧表」の「共通基盤」に記載する。
- (2) 共有フォルダのデータバックアップの詳細仕様は、別紙４「各システムハードウェア仕様一覧表」の「共有フォルダ」に記載する。
- (3) 内部情報系アプリケーションのデータバックアップを実施するためのバックアップ領域の詳細は、別紙５「各システムリソース要件」に記載する。

2.10.6 災害対応

災害時に本調達対象システムの運用を継続するための緊急連絡体制、要員の参集・安否確認等の「初動対応計画書」を策定して、本市の承認を得ること。

2.10.7 サービスレベル管理

2.4.3 の通り、受注者とはＳＬＡを締結する予定のため、ＳＬＡの内容調整に協力すること。また、あらかじめ合意したサービスレベルの達成に向けて、維持・改善を図ること。

2.10.8 運用計画

内部情報系基盤システム稼働前に本市人事異動時の対応フロー，障害時の連絡先，対応フロー等を記載した「運用作業計画書」を作成・提出し，本市の了承を得たうえで実施すること。

2.11 システム保守要件

2.11.1 保守マニュアル

「保守マニュアル」を作成し本市の承認を得ること。「操作マニュアル」や「運用マニュアル」と一体化していても構わない。

2.11.2 定期保守（ハードウェア）

受注者が本市に設置した機器の定期保守等によるシステムの計画停止は，「保守作業計画書」を作成し，本市と調整を行い，承認を得ること。

2.11.3 構成管理

I T環境の構成要素を正しく把握し，常に最新状態に保つために，資産管理システム等により受注者が本市に設置した機器，別途調達する LGWAN 接続系クライアント端末・プリンタ，OS，アプリケーション等についての構成を把握し，記録すること。

2.11.4 インシデント管理（障害事前対策）

- (1) システム監視の結果検出された事象を記録し，回避策を実施し，通常サービスへの回復を図ること。
- (2) 障害の発生に備え，システムバックアップ，ウイルス対策，共有フォルダ，資産管理システム，二要素認証システム，LGWAN メールの入力トランザクションの保持，DBログの採取等を行うこと。
- (3) 障害発生時に速やかに復旧できるよう，連絡網を確立すること。
- (4) 本市からの作業依頼など，日々発生するQA対応などのインシデントを管理ツールで保存管理し，傾向分析することで，運用改善を提案すること。

2.11.5 障害保守

- (1) 常時システムの稼働監視及び障害監視を行い，障害が発生又は検知された時は，速やかに状況を把握・分析し，障害箇所の特定を行うこと。
 - (2) 職員等から障害連絡を受けた時は，状況の把握等を行い，障害箇所の特定を行うこと。また，必要部署への連絡を行うとともに，現地対応を実施すること。
 - (3) 受注者がサービスを提供するシステムの障害については，影響範囲の調査，初期対応，根本対応を行うこと。
 - (4) サーバ等のハードウェア及びOS等の障害については，復旧対応作業について，各メーカーへの指示及び全体の進捗管理を行うこと。
 - (5) 内部情報系アプリケーション又はネットワーク機器あるいはクライアント端末の障害については，本市からの依頼により，障害事象の確認，障害箇所の特定，障害原因の調査，復旧に向けた作業の切り分け等の調査に協力すること。
-

-
- (6) 障害復旧後に各種ソフトウェアやデータの復旧作業を行うこと。
 - (7) 内部情報系アプリケーション受注者が実施する障害原因の切り分けにおいて、本調達範囲に起因することが疑われる調査依頼がなされた場合は、以下の対応を行うこと。
 - ・内部情報系アプリケーション受注者からの調査依頼に対し、速やかに技術的見地から調査回答を行うこと。
 - ・障害原因が本調達範囲にあるか特定できない場合であっても、内部情報系アプリケーション受注者が実施する調査作業に対し、ログの提供や解析協力、検証環境での試験など、早期解決に向けた積極的な協力を行うこと。また、技術的知見から解決策を提案すること。

2.11.6 問題管理（障害事後対策）

- (1) 収集した障害情報を基に根本的な原因を特定し、同様の障害が発生しないよう是正処置・予防措置を講じること。
- (2) 業務への影響を最小限にすべく対策を講じること。また、原因、影響範囲、対処方法、再発防止策を取りまとめ、「障害報告書」として本市に報告すること。

2.11.7 リリース管理

システム変更時は、本市の承認を得た後、システム変更内容を確実に実装し、変更記録を管理すること。

2.11.8 キャパシティ管理

受注者が本市及びデータセンターに設置した機器のシステム資源（CPU、メモリ容量、ディスク容量等）の利用状況監視を行い、必要な対策案（システムチューニング、リソースの追加等）の検討及び対策の実施に伴う作業を行うこと。ただし、市民協働推進部デジタル戦略課職員が随時システム資源の利用状況を確認できるのであれば、受注者が常時監視する必要はない。

2.11.9 変更管理

- (1) 適切なシステム管理を実施するため、必要に応じてプロジェクトマネージャ、開発担当者、本市の情報システム管理者等による主要関係者での協議の場を設置すること。
- (2) 受注者が本市及びデータセンターに設置した機器のハードウェア、ソフトウェア等の資源に対する本格運用開始後の変更は、「保守作業計画書」を本市に提出し、承認後、作業等を実施すること。
- (3) 本市は、変更依頼に対してメリット、デメリット、リスク、影響範囲を総合的に評価し、承認、却下、保留の判断を行う。また、受注者は必要に応じて対案、修正案を提示する等、適切なアドバイスを行うこと。
- (4) 受注者は、変更作業完了後、「変更実施報告書」を本市に提出し確認を得ること。

2.11.10 ソフトウェアのバージョンアップ

- (1) OS、ウイルス対策、共有フォルダ、資産管理システム、二要素認証システム、

-
- LGWAN メール、LGWAN サーバのミドルウェア、アプリケーション等、ソフトウェアのバージョンアップに関しては、その適用の判断に必要な調査・評価を行うこと。
- (2) 本市の指示により受注者が本市に設置した機器のバージョンアップ版の提供及びインストール作業を行うこと。また、クライアント端末のバージョンアップが必要な場合は、設定情報等を提示すること。
 - (3) クライアント端末のアプリケーションの変更が必要な場合は、設定情報等を提示すること。また、クライアント端末にプログラム等のインストールが必要な場合は、インストール媒体及び手順書も提供すること。

2.11.11 情報セキュリティ管理

内部情報系基盤システムに対する不正アクセスについて、定期的又は随時、アクセスログ等をチェックするとともに、必要な対策を提案すること。

また、受注者は下記の資格を取得していること。

- ・品質マネジメントシステム（ISO 9001, QMS）（品質マネジメントを担当する再受託者が取得していれば、受注者が取得していなくても構わない。）
- ・情報セキュリティマネジメントシステム（ISO/IEC27001, ISMS）（セキュリティを担当する再受託者が取得していれば、受注者が取得していなくても構わない。）
- ・ISMSクラウドセキュリティ認証（ISO/IEC 27017）（クラウドサービス提供を担当する再受託者が取得していれば、受注者が取得していなくても構わない。）

2.11.12 ウイルス対策

- (1) 各サーバ及びLGWAN 接続系クライアント端末にコンピュータウイルス対策ソフトウェアを導入し、直ちにコンピュータウイルスを発見し、迅速な駆除対策の支援を行うこと。各サーバ及び別途調達するLGWAN 接続系クライアント端末用のコンピュータウイルス対策ソフトウェアのライセンスを調達し、各サーバへの導入・設定及びパターンファイル更新等のためのウイルス対策用サーバを構築すること。また、LGWAN 接続系クライアント端末については、導入・設定等は本調達の対象外であるが、コンピュータウイルス対策ソフトウェアの設定に必要な情報等を提示すること。
- (2) 必要に応じて、来庁して対応すること。
- (3) ウイルス対策用サーバを参照することにより、自動又は手動にてパターンファイルの更新を行うこと。
- (4) ウイルス対策用サーバのパターンファイルの更新方法を提案すること。同更新方法は、セキュリティ確保の観点から、「大崎市情報セキュリティポリシー」（令和8年4月1日改正）を遵守する必要がある。

2.11.13 セキュリティパッチ等の適用

受注者が本市に設置した機器のソフトウェアのセキュリティパッチ等の適用の要否を確認し、報告すること。（報告書の作成は不要である。ただし、本市からセキュリティパッチの適用状況の問合せがあった場合は、2.12 問合せ対応要件に基づいて、

回答すること。) セキュリティパッチ適用後の動作確認を実施すること。また、クライアント端末のセキュリティパッチ等の適用が必要な場合は、設定情報等を提示すること。

2.11.14 サービスレベル管理

2.4.3 の通り、受注者とは S L A を締結する予定のため、S L A の内容調整に協力すること。また、あらかじめ合意したサービスレベルの達成に向けて、維持・改善を図ること。

2.11.15 機器保守

- (1) 受注者が本市及びデータセンターに設置した機器を保守すること。
- (2) 本市サーバ室において使用する DHCP サーバ、RADIUS サーバ、地域コアスイッチの保守は、別途契約とする。ただし、本市からの依頼により内部情報系基盤システムの導入時及び機器修復後に必要な設定情報等を提示すること。
- (3) 本市各拠点において使用する L3 スイッチ、出先ルータ、PoE スイッチ、PoE インジェクター、無線アクセスポイント、メディアコンバータ、クライアント端末、プリンタ等の保守は、別途契約とする。ただし、本市からの依頼により内部情報系基盤システムの導入時及び機器修復後に必要な設定情報等を提示すること。

2.12 問合せ対応要件

- (1) 市民協働推進部デジタル戦略課職員からの内部情報系基盤システムに関する運用方法に関する問合せに回答すること。問合せ内容、回答内容、結果を事例として整理し、同様の問い合わせに対して迅速に対応できる仕組みとすること。
- (2) 問い合わせ内容の傾向を分析し、情報システムの改善等を図ること。本調達範囲外の機能やライセンス等がないと改善ができない事項は、本調達の範囲外である。
- (3) 内部情報系アプリケーション受注者からの問合せについても受付すること。この場合の対応方法は 2.12(1)～(2)を準用する。

2.13 データセンター要件

データセンターは、本項 (2.13) の要件を全て満たすものを提供すること。ただし、本仕様書 2.1.1 に規定する要件を満たすクラウドサービスを利用する場合については、同クラウドサービスが提供する標準のファシリティ基準・セキュリティ基準をもって、本項 (2.13) の要件を全て満たしているものとみなす。また、本仕様書 2.1.1 の要件を満たすクラウドサービスの提供しているデータセンターと同一のデータセンター内に物理サーバを設置し、運用する場合も同様とする。

2.13.1 立地仕様

- (1) 活断層による建物設備の危険が少ない場所
国土地理院の都市圏活断層図でデータセンターの敷地全域が活断層上にないこと。
- (2) 水災害による建物設備の被害の危険が少ない場所

都道府県の津波浸水予測図（津波浸水想定図）、国土交通省及び都道府県の洪水浸水想定区域図で、下記の基準を満たしていること。

- ・原則としてデータセンターの敷地全域が津波・高潮・洪水による水災害発生時における浸水深予測が0メートルであること。
- ・データセンターの敷地全域が津波・高潮・洪水による水災害発生時における浸水深予測が1メートル未満の場所に設置する場合は、本調達範囲の機器を同データセンターの2階以上のフロアに設置すること。また、実際に1メートル未満の浸水が発生した場合でも、本調達範囲の機器への電力供給、通信に影響が出ないこと。

(3) 液状化現象による影響が少ない場所

都道府県及び市町村の液状化想定図（液状化予測図、液状化危険度予測図）で、下記のいずれかの条件を満たしていること。

- ・データセンターの敷地全体が「液状化の可能性なし」若しくは「極めて低い（P L値が示されている場合は、 $PL=0.0$ ）」とされていること。
- ・データセンターの敷地全体が「液状化の可能性が低い（P L値が示されている場合は、 $PL \leq 5.0$ ）」とされており、必要な地盤改良・ライフライン対策が実施されていること。
- ・データセンターの敷地全体が「液状化の可能性がやや高い（P L値が示されている場合は、 $PL \leq 10.0$ ）」とされており、抗が液状化の恐れがない固い地層まで到達している杭基礎を採用し、地盤改良の実施した上で（深層混合処理工法又は浅層混合処理工法若しくは注入工法）、ライフラインの液状化対策が十分に行われていること。

(4) 災害時に立入り制限がかかる危険が少ない場所

- ・土砂災害警戒区域等における土砂災害防止対策の推進に関する法律（平成12年5月8日法律第57号）の土砂災害警戒区域（同法第6条）及び土砂災害特別警戒区域（同法第8条）に指定されていないこと。
- ・活動火山対策特別措置法（昭和48年法律第61号）第3条第1項に規程される火山災害警戒地域に指定されていないこと。
- ・データセンターの敷地が石油コンビナート等災害防止法（昭和50年法律第84号）第2条第2項に規定される石油コンビナート等特別防災区域に指定されていないこと。
- ・データセンターの敷地から半径100メートル以内に消防法（昭和23年法律第186号）による指定数量以上の危険物製造設備、火薬製造設備、高圧ガス設備がないこと。

2.13.2 建物仕様

(1) 地震への対策

-
- ・免震建築物の構造方法に関する安全上必要な技術的基準を定める等の件（平成12年10月17日建設省告示第2009号）に規定する免震建築物の基準を満たすこと。
 - ・基礎免震構造であること。（中間階免震構造は不可）
 - ・官庁施設の総合耐震計画基準及び同解説に規定する耐震安全性の分類の構造体がⅠ類相当であること。ただし、免震構造によって、Ⅰ類相当と同等以上の機能継続性と安全性が確保されると認められる場合は、この限りではない。

(2) 火災への対策

- ・建築基準法（昭和25年法律第201号）に規定する耐火建築物であること。
- ・サーバールームには防火システムを完備し、超高感度煙検知システムを採用、窒素ガスによるガス消火方式を採用すること。

(3) 落雷への対策

- ・外部雷保護対策として、避雷設備は、日本工業規格（JISA4201）に準拠していること。
- ・内部雷保護対策として、IEC（国際電気標準会議）が規定する内部雷保護システムに対応していること。
- ・建物の出入口は、監視カメラにより24時間常時監視されていること。ただし、建物内のデータセンターエリアとそれ以外のエリアが分離されており、双方のエリアを往来できる全ての場所を監視カメラにより24時間常時監視されている場合は、この限りではない。

2.13.3 機器設置室仕様

- (1) 建築基準法（昭和25年法律第201号）に基づく独立した防火区画であること。
- (2) 常時、温度18～27℃、湿度40～55%を保つことができる空調設備を整えていること。ただし、受注者が導入する機器のメーカー推奨条件を満たせる範囲であり、データセンター設置機器を内部情報系基盤システムの運用に支障がないよう管理できることを受注者に責任で担保できる場合は、湿度40～55%範囲外の条件で運用することを許容する。
- (3) 全ての入退室情報が記録され、1年以上の入退館ログが管理されていること。
- (4) 火災、水害、落雷等の影響を受けにくくする設備を備えていること。
- (5) サーバ室は2階以上で、建物外に接する窓がない部屋であること。
- (6) 室内は、監視カメラにより24時間常時監視されており、データを3か月間保持されていること。
- (7) 機器や記録媒体に影響を与えない消火薬剤や消防用設備等を備えていること。
- (8) 出入口扉は、十分な強度を持つ防火扉等となっていること。
- (9) 保守に必要な空間が確保されていること。
- (10) 複数の通信事業者の通信回線（マルチキャリア）が敷設できること。

2.13.4 停電対策

- (1) 停電時にシステムを運用するために十分な電源容量を持つ非常用自家発電装置を
-

備えていること。

- (2) 停電時に非常用発電装置が安定的に起動するまでの間、瞬断することなくシステムに十分な電力供給が可能な無停電電源装置を設置していること。
- (3) 非常用発電装置の燃料容量は48時間継続運転が可能であり、また稼働中の給油が可能であること。ただし、受注者が保有する燃料備蓄と稼働中給油体制により、非常用発電装置を48時間継続運転が可能である場合は、この限りではない。
- (4) 落雷等による過電流に対してサーバ等の機器を保護するための措置を実施していること。

2.13.5 セキュリティ対策

生体認証、ICカード等を用いた認証により不正な者の侵入を防止できること。

2.13.6 その他

- (1) 本調達機器の設置するサーバールームがあるフロアはデータセンター専用のフロアで、データセンター事業のみで使用されていること。ただし、建物内のデータセンターエリアとそれ以外のエリアが分離されている上、双方のエリアを往来できる全ての場所を監視カメラにより24時間常時監視されており、データセンターエリアがデータセンター事業のみで使用されている場合はこの限りではない。
- (2) 電気については、変電所からの受電系統（特別高圧、本線・予備線方式）を複数引くこと。また、データセンター内においても、複数の受電系統から給電が可能であること。
- (3) 建築基準法（昭和25年法律第201号）や消防法（昭和23年法律第186号）等の関連法規を満たしていること。
- (4) データセンターの設置場所やアクセス区域、裁判所の管轄は、日本国の法律が及ぶ国内に限定していること。
- (5) 定期的に情報セキュリティ監査（内部監査を含む）を実施していること。
- (6) 本市（監査の委託事業者を含む。）による立入監査の実施に協力する（監査に必要な情報の開示を含む。）こと。ただし、2.1.1(3)イ及びウを満たす事業者が運営するデータセンターである場合は、立入不可や一部情報の非開示を認めるものとする。
- (7) 24時間365日入退室可能であること。

2.14 プロジェクト管理要件

2.14.1 プロジェクト計画

契約締結後、速やかに「プロジェクト計画書」を提出し、本市の承認を得ること。

2.14.2 プロジェクト体制

- (1) 受注者におけるプロジェクト管理者は、行政法人 情報処理推進機構が実施する情報処理技術者試験のうちプロジェクトマネージャ試験の合格者又は米国 PMI 若しくは一般社団法人 PMI 日本支部が認定する PMP の資格を有すること。ただし、（本市を含めて）本市と同等以上の規模の自治体において、本調達と同規模のプロ

ジェクト管理経験を有することが経歴等において明らかな者については、これを認める場合がある(その根拠を明確に示し、本市が承認した場合に限る。)。また、プロジェクトマネージャは原則として本調達の開始から本格運用開始まで同一人物とすること。

- (2) プロジェクトマネージャの選任は、事前に業務経歴書を本市に提出し、承認を得ること。

2.14.3 構築環境

構築・システム評価等の作業のために必要なハードウェア、ソフトウェア、回線等は受注者が準備すること。ただし、内部情報系アプリケーションの構築に必要なソフトウェア、回線は内部情報系アプリケーション受注者が調達するため、本調達の範囲外とする。

内部情報系アプリケーションが必要とする機能及び各リソースを情報収集し、一覧にまとめること。また、内部情報系アプリケーションから内部情報系基盤システムへの要求リソースが過大である等、内部情報系アプリケーションと内部情報系基盤システムとの間に認識の齟齬がある場合は、本市の職員が窓口となって実施するシステム間の調整の支援を行うこと。

2.14.4 作業場所

構築・システム評価等は、本市が指定又は承認した場所で作業すること。庁舎外で実施する場合は、入退室管理やデータへのアクセス制御、データ等の搬入出制限ができる施設とすること。この場合、本市の情報セキュリティ監査を受けなければならないものとする。作業場所を確保するための費用等は、受注者が負担するものとする。

2.14.5 進捗管理

- (1) WBS (Work Breakdown Structure) 等により、作業項目を明確にし、ガント図等により工程を明確にした「実施スケジュール表」を作成し進捗管理を行うこと。
- (2) 構築期間中は1か月に1回以上、「プロジェクト進捗管理表」を作成し、進捗報告のための会議を行い、会議後、5日以内(開庁日)に「議事録」を作成し、本市の承認を得ること。やむを得ない事情により打合せ後5日以内(開庁日)までに議事録等の作成ができない場合は、打合せ後5日以内(開庁日)までに本市担当職員にその旨連絡し、担当職員が指定した日までに作成すること。
- (3) 作業遅延等の問題が発生した場合は、問題点及び対策を明確にし、その対策が妥当なのか判断できる材料を合わせて本市に提示すること。

2.14.6 課題・問題管理

課題対応状況を的確に把握するために、「課題管理表」を作成し、進捗報告等の会議で報告すること。なお、解決が中長期的にかかる見込みの課題は、問題管理として管理すること。

2.14.7 リスク管理

各工程のリスク分析を実施し、リスク状況を進捗報告等の会議で報告すること。

2.14.8 標準化

品質向上、保守の容易性を図るために、設計及び開発の標準化を行うこと。

2.14.9 品質管理

- (1) 品質を評価するための品質管理基準を設けること。
- (2) 各工程の品質を確保するため成果品に対するレビューを実施すること。
- (3) レビュー結果を進捗報告等の会議で報告し、本市の承認を得ること。

3 留意事項

3.1 検収方法

- (1) 試験環境における事前検証と、本番環境における最終検証を行うこと。
- (2) 事前検証、最終検証とも事前に「試験計画書」を本市に提出し承認を得た上で実施すること。
- (3) 「試験計画書」は、本仕様書及び別紙に規定されている全ての機能が正常に動作することが確認できるように作成すること。
- (4) 事前検証、最終検証の結果は「試験結果報告書」にまとめて本市に提出すること。
- (5) 新システムへの移行完了時、「システム移行完了報告書」にまとめて本市に提出すること。
- (6) 本市が「システム移行完了報告書」を承認したことで検収とする。
- (7) 本市は「システム移行完了報告書」を受領後、完了検査を実施し、検査実施10日以内に検査結果を通知する。

3.2 資料の貸与

- (1) 本調達履行に伴い、必要となる本市情報システムに関する資料やデータ等については、必要に応じて本市より貸与する。
- (2) 本市への返却が必要となるもの及び本市庁舎外への持出しが禁じられているものに該当するものについては、本調達契約書で定める秘密保持契約条項に基づき、所定の手続きにより貸与するものとする。
- (3) 貸与品について、返還の指示があった場合、本調達遂行上不要となった場合又は契約が終了したときは、速やかに返還すること。

3.3 秘密保護・個人情報保護

- (1) 業務の遂行上知り得た秘密を他に漏らしてはならない。また、契約期間の終了又は解除後も同様とする。
- (2) 成果品（業務の過程で得られた記録等を含む。）を本市の許可なく第三者に閲覧、複写させたり、貸与又は譲渡してはならない。
- (3) 業務の遂行のために本市が提供した資料、データ等は本調達以外の目的で使用し

てはならない。

- (4) 業務の実施における個人情報等の取扱いについては、大崎市個人情報保護条例に基づき、個人情報の保護の重要性を十分認識し個人の権利利益を侵害することのないよう必要な措置を講じること。
- (5) 業務に従事する者に対して秘密保護及び個人情報保護の教育訓練を行うこと。
- (6) 受注者は、内部情報系アプリケーション、共有フォルダ等に格納される本市の個人情報について、本市の指示による保守・運用目的以外でのアクセス、処理、独自の利用を一切行ってはならない。また、保守作業時における管理者アクセスのログを取得し、同ログの改ざんを防止するとともに、必要最小限の人員でのみ作業にあたること。
- (7) 受注者は、個人情報の漏洩発生時に本市に速やかに通知すること。
- (8) 受注者は、法執行機関から個人情報開示要求があった場合、法的に許される範囲で本市に通知すること。

3.4 特許権等の帰属

- (1) 業務遂行の過程で生じた発明その他の知的財産又はノウハウ等（以下、あわせて「発明等」という。）に係る特許権その他の知的財産権（特許その他の知的財産権を受ける権利を含む。ただし、著作権は除く。）、ノウハウ等に関する権利（以下、特許権その他の知的財産権、ノウハウ等に関する権利を総称して「特許権等」という。）は、当該発明等を行った者が属する当事者に帰属するものとする。
- (2) 受注者は、(1)に基づき特許権等を保有することとなる場合、本市に対し、本市が契約に基づき新システムを使用するのに必要な範囲について、当該特許権等の通常実施権を許諾するものとする。なお、新システムに、重要事項説明書において一定の第三者に使用せしめる旨を重要事項説明書に特掲されたソフトウェア（以下「特定ソフトウェア」という。）が含まれている場合は、重要事項説明書の掲載に従った第三者による当該ソフトウェアの使用についても同様とする。なお、特定ソフトウェアの使用許諾の対価は、受託金額に含まれるものとする。

3.5 著作権の帰属

- (1) 業務遂行の過程で生じた著作権（著作権法（昭和45年法律第48号）第27条及び第28条の権利を含む。）は、本市又は第三者が従前から保有していた著作物の著作権を除き、受注者に帰属するものとする。
- (2) 受注者は、新システムに係る著作物のうち自己が著作権を持つもの及び前項に従って自己に帰属するものについて、本市に対し、本市が新システムを本契約の条件に従って利用できるように利用許諾し、これについて著作者人格権を行使しないものとする。なお、新システムに、特定ソフトウェアが含まれている場合は、重要事項説明書の掲載に従った第三者による当該ソフトウェアの利用についても同様とする。なお、特定ソフトウェアの使用許諾の対価は、受託金額に含まれるものとする。

-
- (3) 新システムに係る著作物のうち第三者が著作権を持つものの権利関係については、当該権利者と本市との間の契約条件に従う。
 - (4) システム運用によって蓄積されるデータの著作権、利用権、所有権は、本市に帰属する。

3.6 第三者の権利侵害

成果品に第三者が権利を有する著作物が含まれている場合、受注者は当該著作権の使用に関する負担を含む一切の手続きを行い、第三者の著作権その他の権利を侵害していないこと。

3.7 再委託

- (1) 本調達を再委託する場合、書面にて、事前に再委託先及び再委託内容、再委託理由、情報管理方法等並びに再委託先との契約を示す書類を本市に提示し承認を得ること。
- (2) 再委託範囲は受注者が責任を果たせる範囲とし、再委託先に問題が生じた場合は受注者の責任において解決すること。
- (3) 再々委託は原則禁止する。ただし、本市と協議のうえ、情報セキュリティ対策、及び構築体制と責任区分に不備が無く適正と認められる場合はその限りではない。

3.8 契約不適合責任

- (1) 本市は、履行された業務又は引き渡された成果物が種類又は品質に関して契約の内容に適合しないもの（バグも含む。以下「契約不適合」という。）であるときは、受注者に対し、本市の意図する業務の履行又は成果物の修補若しくは代替物の引渡しによる履行の追完を請求することができる。
 - (2) (1)の場合において、受注者は、本市に不相当な負担を課するものでないときは、本市が請求した方法と異なる方法による履行の追完をすることができる。
 - (3) (1)の場合において、本市が相当の期間を定めて履行の追完の催告をし、その期間内に履行の追完がないときは、本市は、その不適合の程度に応じて代金の減額を請求することができる。ただし、次の①～④のいずれかに該当する場合は、催告をすることなく、直ちに代金の減額を請求することができる。
 - ① 履行の追完が不能であるとき。
 - ② 受注者が履行の追完を拒絶する意思を明確に表示したとき。
 - ③ 業務又は成果物の性質又は当事者の意思表示により、特定の日時又は一定の期間内に履行しなければ契約をした目的を達することができない場合において、受注者が履行の追完をしないでその時期を経過したとき。
 - ④ ①～③の場合のほか、本市が(3)による催告をしても履行の追完を受ける見込みがないことが明らかであるとき。
 - (4) 本市は、引き渡された成果物に関し、引渡しを受けた日から3年以内でなければ、契約不適合を理由とした履行の追完の請求、損害賠償の請求、代金の減額の請求又は契約の解除(以下「請求等」という。)をすることができない。
-

-
- (5) (4)の請求等は、具体的な契約不適合の内容、請求する損害額の算定の根拠等当該請求等の根拠を示して、受注者の契約不適合責任を問う意思を明確に告げることで行う。
 - (6) 本市が(4)の契約不適合に係る請求等が可能な期間(以下「契約不適合責任期間」という。)の内に契約不適合を知り、その旨を受注者に通知した場合において、本市が通知から1年が経過する日までに(5)の方法による請求等をしたときは、契約不適合責任期間の内に請求等をしたものとみなす。
 - (7) 本市は、(4)の請求等を行ったときは、当該請求等の根拠となる契約不適合に関し、民法の消滅時効の範囲で、当該請求等以外に必要と認められる請求等を行うことができる。
 - (8) (4)～(7)の規定は、契約不適合が受注者の故意又は重過失により生じたものであるときには適用せず、契約不適合に関する受注者の責任については、民法の定めるところによる。
 - (9) 民法第637条第1項の規定は、契約不適合責任期間については適用しない。
 - (10) 本市は、業務完了の通知又は成果物の引渡しの際に契約不適合があることを知ったときは、(4)にかかわらず、その旨を直ちに受注者に通知しなければ、当該契約不適合に関する請求等を行うことはできない。ただし、受注者がその契約不適合があることを知っていたときは、この限りでない。
 - (11) 業務又は引き渡された成果物の契約不適合が設計図書の記載内容、本市の指示又は貸与品等の性状により生じたものであるときは、本市は当該契約不適合を理由として、請求等を行うことができない。ただし、受注者がその記載内容、指示又は貸与品等が不适当であることを知りながらこれを通知しなかったときは、この限りでない。

3.9 作業における注意事項

- (1) 受注者が本調達に関して本市施設内に出入りする際は、事前に本市に対し連絡を行い指示に従うこと。また、施設内では名札を着用すること。
- (2) 本調達を通じて知り得た情報については、本調達の用に供する目的以外には利用しないこと。また、情報等は秘密とし、第三者に開示しないこと。ただし、書面等により本市の承認を受けている場合はこの限りではない。
- (3) 本調達に関連して、他の業者との打合せ等を行う場合には、事前に本市の承認を得ること。また、打合せ等の終了後は、速やかにその内容を書面にて本市に報告すること。

3.10 契約にかかる注意事項

- (1) 諸般の事情の変遷により、契約締結内容は本市と受注者合意の上、本仕様書及び別紙に記載された内容を一部変更することができるものとする。
- (2) 本仕様書に記述がない事項又は疑義が発生した場合は、本市及び受注者の双方が協議の上、決定するものとする。

(3) 契約期間満了時には、データセンター及び本市に設置した記憶装置や記憶媒体で保有する全データを消去又は廃棄すること。また、消去・廃棄したデータの一覧表を作成して、本市に提出すること。なお、データ消去に伴う費用は本調達の委託範囲に含むものとする。

(4) 三者契約について

三者契約も可とする。

なお、三者契約を行う場合は次のとおりとする。

①入札は、公告の入札に参加する者に必要な資格に関する事項に記載のとおり
の業種、部門に登録のある業者が行う。

②第三者は大崎市の入札参加登録業者とする。

③公告の入札後審査郵送方式一般競争入札公告共通事項3（1）ウに記載のある
書類の他に、第三者の入札参加登録通知書の写しを同封する事とする。

4 添付資料

別紙 1 業務別利用者数一覧表

別紙 2 部署別機器設置台数一覧表

別紙 3 対象データ件数表

別紙 4 各システムハードウェア仕様一覧表

別紙 5 各システムリソース要件

別紙 6 サービスレベル（S L A）定義表

別紙 7 ネットワーク概要図

別紙 8 設置場所別ハードウェア一覧

別紙 9 情報システム間連携

業務別利用者数一覧表

No	業務システム	主管部署	正職員 再任用職員 利用者数	会計年度 任用職員 利用者数	合計 利用者数	最大同時 接続端末数	備考
1	財務会計システム	財政課、会計課	約1,150人	約200人	約1350人	約1,200台	仮想サーバ及びサーバOSを調達すること。
2	契約管理システム	財政課	約1,150人	約200人	約1350人	約1,200台	仮想サーバ及びサーバOSを調達すること。
3	備品管理システム	財政課	約1,150人	約200人	約1350人	約1,200台	仮想サーバ及びサーバOSを調達すること。
4	起債管理システム	財政課	約20人	0人	約20人	約20台	仮想サーバ及びサーバOSを調達すること。
5	庶務事務システム	人財育成課	約1,000人	約800人	約1,800人	約1,200台	仮想サーバ及びサーバOSを調達すること。
6	人事給与システム	人財育成課	約20人	0人	約20人	約20台	仮想サーバ及びサーバOSを調達すること。
7	人事評価システム	人財育成課	約1,000人	0人	約1,000人	約1,000台	仮想サーバ及びサーバOSを調達すること。
8	文書管理システム	総務課	約1,150人	約200人	約1350人	約1,200台	仮想サーバ及びサーバOSを調達すること。
9	電子決裁システム	デジタル戦略課	約1,150人	約200人	約1350人	約1,200台	仮想サーバ及びサーバOSを調達すること。
10	グループウェア（インターネットメール含む）	デジタル戦略課	約1,150人	約180人	約1,330人	約1,300台	仮想サーバ及びサーバOSを調達すること。
11	ウイルス対策システム	デジタル戦略課	約1,150人	約800人	約1,950人	約1,300台	
12	共有フォルダ	デジタル戦略課	約1,150人	約350人	約1,500人	約1,300台	
13	資産管理システム	デジタル戦略課	約1,150人	約800人	約1,950人	約1,300台	操作ログの監視対象Windowsユーザーは約1,950人であるが、管理者画面にログインするのは8名程度。LGWAN接続系クライアント端末1,350台登録すること。
14	二要素認証システム	デジタル戦略課	約1,150人	約800人	約1,950人	約1,300台	顔認証をするWindowsユーザーが約1,350人程度であり、ID・パスワード認証をするWindowsユーザーは約600人程度

※個々のアカウントのライセンスの適用を柔軟にON/OFFできないシステムなど、人事異動処理を円滑に実施するために追加のライセンスが必要なシステムを導入する場合は、人事異動時に新規採用職員のライセンスをONにしてから、退職者のライセンスをOFFにするまでの期間に生じる重複分のライセンスも調達すること。

【別紙2】

部署別機器設置台数一覧表

No	部 署	運用場所	LGWAN接続系 クライアント端末	備 考
1	総務課	大崎市役所本庁舎	11	
2	人財育成課	大崎市役所本庁舎	11	
3	秘書広報課	大崎市役所本庁舎	14	
4	財政課	大崎市役所本庁舎	22	
5	税務課	大崎市役所本庁舎	40	
6	納税課	大崎市役所本庁舎	14	
7	防災安全課	大崎市役所本庁舎	13	
8	政策課	大崎市役所本庁舎	11	
9	行政管理課	大崎市役所本庁舎	8	
10	まちづくり推進課	大崎市役所本庁舎	13	
11	おおさき日本語学校	おおさき日本語学校	11	
12	環境保全課	大崎市役所本庁舎	11	
13	デジタル戦略課	大崎市役所本庁舎	8	
14	社会福祉課	大崎市役所本庁舎	42	
15	子育て支援課	大崎市役所本庁舎	29	
16	子育てわくわくランド	子育てわくわくランド	7	
17	古川北町保育所	古川北町保育所	10	
18	古川西保育所	古川西保育所	9	
19	松山あおぞら園	松山あおぞら園	14	
20	三本木ひまわり園	三本木ひまわり園	21	
21	鹿島台なかよし園	鹿島台なかよし園	16	
22	岩出山保育所	岩出山保育所	10	
23	田尻すまいる園	田尻すまいる園	18	
24	高齢障がい福祉課	大崎市役所本庁舎	32	
25	健康推進課	大崎市役所本庁舎	47	
26	夜間急患センター	夜間急患センター	4	
27	保険年金課	大崎市役所本庁舎	13	
28	市民課	大崎市役所本庁舎	24	
29	農政企画課	大崎市役所本庁舎	22	
30	農村環境整備課	大崎市役所本庁舎	15	
31	産業商工課	大崎市役所本庁舎	11	
32	観光交流課	大崎市役所本庁舎	10	
33	都市計画課	大崎市役所東庁舎	15	
34	建設課	大崎市役所東庁舎	34	
35	流域治水課	大崎市役所東庁舎	8	
36	建築住宅課	大崎市役所東庁舎	17	
37	建築指導課	大崎市役所東庁舎	11	
38	会計課	大崎市役所本庁舎	10	
39	検査課	大崎市役所東庁舎	4	
40	松山総合支所地域振興課	松山総合支所	14	
41	松山総合支所市民福祉課	松山総合支所	15	
42	三本木総合支所地域振興課	三本木総合支所	15	
43	三本木総合支所市民福祉課	三本木総合支所	12	
44	鹿島台総合支所地域振興課	鹿島台総合支所	19	
45	鹿島台総合支所市民福祉課	鹿島台総合支所	14	
46	岩出山総合支所地域振興課	岩出山総合支所	23	

No	部 署	運用場所	LGWAN接続系 クライアント端末	備 考
47	岩出山総合支所市民福祉課	岩出山総合支所	17	
48	鳴子総合支所地域振興課	鳴子総合支所	20	
49	鳴子総合支所市民福祉課	鳴子総合支所	13	
50	鬼首出張所	鬼首公民館	1	
51	田尻総合支所地域振興課	田尻総合支所	19	
52	田尻総合支所市民福祉課	田尻総合支所	19	
53	経営管理課	上下水道部庁舎	22	
54	上水道施設課	上下水道部庁舎	18	
55	下水道施設課	上下水道部庁舎	18	
56	教育総務課	大崎市役所本庁舎	19	
57	大崎南学校給食センター	大崎南学校給食センター	4	
58	大崎東学校給食センター	大崎東学校給食センター	4	
59	岩出山学校給食センター	岩出山学校給食センター	3	
60	田尻学校給食センター	田尻学校給食センター	4	
61	学校教育課	大崎市役所本庁舎	20	
62	古川第一小学校	古川第一小学校	5	
63	古川第二小学校	古川第二小学校	7	
64	古川第三小学校	古川第三小学校	7	
65	古川第四小学校	古川第四小学校	7	
66	古川第五小学校	古川第五小学校	7	
67	古川北小学校	古川北小学校	3	
68	敷玉小学校	敷玉小学校	3	
69	松山小学校	松山小学校	5	
70	三本木小学校	三本木小学校	5	
71	鹿島台小学校	鹿島台小学校	4	
72	岩出山小学校	岩出山小学校	4	
73	田尻小学校	田尻小学校	3	
74	沼部小学校	沼部小学校	3	
75	大貫小学校	大貫小学校	3	
76	古川中学校	古川中学校	6	
77	古川西小中学校	古川西小中学校	6	
78	古川北中学校	古川北中学校	4	
79	古川東中学校	古川東中学校	7	
80	古川南中学校	古川南中学校	5	
81	松山中学校	松山中学校	3	
82	三本木中学校	三本木中学校	3	
83	鹿島台中学校	鹿島台中学校	4	
84	岩出山中学校	岩出山中学校	4	
85	鳴子小中学校	鳴子小中学校	8	
86	田尻中学校	田尻中学校	4	
87	心のケアハウス	心のケアハウス	8	
88	生涯学習課	大崎市役所本庁舎	15	
89	青少年センター	大崎市役所本庁舎	3	
90	地域交流センター	地域交流センター	7	
91	松山公民館	松山公民館	8	
92	三本木公民館	三本木総合支所	5	

【別紙2】

部署別機器設置台数一覧表

No	部 署	運用場所	LGWAN接続系 クライアント端末	備 考
93	鹿島台公民館	鹿島台公民館	6	
94	岩出山公民館	岩出山公民館	8	
95	鳴子公民館	鳴子総合支所	6	
96	沼部公民館	沼部公民館	7	
97	文化財課	大崎市役所本庁舎	10	
98	図書館	図書館	15	
99	大崎市民会館	市民会館	5	
100	大崎市民ギャラリー緒絶の館	緒絶の館	5	
101	大崎市祥雲閣	祥雲閣	2	
102	瑞・華・翠交流館	鎌田記念ホール	4	
103	田尻総合体育館	田尻総合体育館	5	
104	選挙管理委員会事務局	大崎市役所本庁舎	2	
105	議会事務局	大崎市役所本庁舎	9	
106	監査委員事務局	大崎市役所東庁舎	7	
107	農業委員会事務局	大崎市役所東庁舎	19	
108	大崎広域	大崎地域広域行政事務組合	2	
109	大崎市民病院	大崎市民病院	11	
110	大崎市民病院鹿島台分院	大崎市民病院鹿島台分院	1	
111	大崎市民病院岩出山分院	大崎市民病院岩出山分院	1	
112	大崎市民病院鳴子分院	大崎市民病院鳴子分院	1	
113	予備機	大崎市役所東庁舎	62	
114	貸出用	大崎市役所本庁舎	3	
115	テレワーク	大崎市役所本庁舎	10	
小計1_1	運用場所別小計	大崎市役所本庁舎	522	
小計1_2	運用場所別小計	おおさき日本語学校	11	
小計1_3	運用場所別小計	子育てわくわくランド	7	
小計1_4	運用場所別小計	古川北町保育所	10	
小計1_5	運用場所別小計	古川西保育所	9	
小計1_6	運用場所別小計	松山あおぞら園	14	
小計1_7	運用場所別小計	三本木ひまわり園	21	
小計1_8	運用場所別小計	鹿島台なかよし園	16	
小計1_9	運用場所別小計	岩出山保育所	10	
小計1_10	運用場所別小計	田尻すまいる園	18	
小計1_11	運用場所別小計	夜間急患センター	4	
小計1_12	運用場所別小計	大崎市役所東庁舎	177	
小計1_13	運用場所別小計	松山総合支所	29	
小計1_14	運用場所別小計	三本木総合支所	32	
小計1_15	運用場所別小計	鹿島台総合支所	33	
小計1_16	運用場所別小計	岩出山総合支所	40	
小計1_17	運用場所別小計	鳴子総合支所	39	
小計1_18	運用場所別小計	鬼首公民館	1	
小計1_19	運用場所別小計	田尻総合支所	38	
小計1_20	運用場所別小計	上下水道部庁舎	58	
小計1_21	運用場所別小計	大崎南学校給食センター	4	
小計1_22	運用場所別小計	大崎東学校給食センター	4	
小計1_23	運用場所別小計	岩出山学校給食センター	3	

【別紙2】

部署別機器設置台数一覧表

No	部 署	運用場所	LGWAN接続系 クライアント端末	備 考
小計1_24	運用場所別小計	田尻学校給食センター	4	
小計1_25	運用場所別小計	古川第一小学校	5	
小計1_26	運用場所別小計	古川第二小学校	7	
小計1_27	運用場所別小計	古川第三小学校	7	
小計1_28	運用場所別小計	古川第四小学校	7	
小計1_29	運用場所別小計	古川第五小学校	7	
小計1_30	運用場所別小計	古川北小学校	3	
小計1_31	運用場所別小計	敷玉小学校	3	
小計1_32	運用場所別小計	松山小学校	5	
小計1_33	運用場所別小計	三本木小学校	5	
小計1_34	運用場所別小計	鹿島台小学校	4	
小計1_35	運用場所別小計	岩出山小学校	4	
小計1_36	運用場所別小計	田尻小学校	3	
小計1_37	運用場所別小計	沼部小学校	3	
小計1_38	運用場所別小計	大貫小学校	3	
小計1_39	運用場所別小計	古川中学校	6	
小計1_40	運用場所別小計	古川西小中学校	6	
小計1_41	運用場所別小計	古川北中学校	4	
小計1_42	運用場所別小計	古川東中学校	7	
小計1_43	運用場所別小計	古川南中学校	5	
小計1_44	運用場所別小計	松山中学校	3	
小計1_45	運用場所別小計	三本木中学校	3	
小計1_46	運用場所別小計	鹿島台中学校	4	
小計1_47	運用場所別小計	岩出山中学校	4	
小計1_48	運用場所別小計	鳴子小中学校	8	
小計1_49	運用場所別小計	田尻中学校	4	
小計1_50	運用場所別小計	心のケアハウス	8	
小計1_51	運用場所別小計	地域交流センター	7	
小計1_52	運用場所別小計	松山公民館	8	
小計1_53	運用場所別小計	鹿島台公民館	6	
小計1_54	運用場所別小計	岩出山公民館	8	
小計1_55	運用場所別小計	沼部公民館	7	
小計1_56	運用場所別小計	図書館	15	
小計1_57	運用場所別小計	市民会館	5	
小計1_58	運用場所別小計	緒絶の館	5	
小計1_59	運用場所別小計	祥雲閣	2	
小計1_60	運用場所別小計	鎌田記念ホール	4	
小計1_61	運用場所別小計	田尻総合体育館	5	
小計1_62	運用場所別小計	大崎地域広域行政事務組合	2	
小計1_63	運用場所別小計	大崎市民病院	11	
小計1_64	運用場所別小計	大崎市民病院鹿島台分院	1	
小計1_65	運用場所別小計	大崎市民病院岩出山分院	1	
小計1_66	運用場所別小計	大崎市民病院鳴子分院	1	
	合計		1320	

【別紙3】

対象データ件数表

業 務 名	情 報 名	件数	単位	備考
共有フォルダ	共有フォルダ及びファイル	36	Tbyte	旧共有フォルダからの移行対象データが36Tbyteであり、新共有フォルダは40Tbyte以上のデータを運用可能である必要がある。
運用管理・資産管理	Active Directory ユーザ	2,359	件	過去在籍ユーザー含む
	Active Directory コンピュータ	1,320	件	
	資産管理端末	1,320	件	

共通基盤

No	業 務 分 類	機 能 要 件
1	仮想化機能	財務会計、契約管理、備品管理、起債管理、庶務事務、人事給与、人事評価、文書管理、電子決裁、グループウェア及びこれらのシステム間の連携機能（以下「内部情報系アプリケーション」とする）、ウイルス対策、共有フォルダ、資産管理、二要素認証、LGWANメールに仮想環境を提供すること。また、グループウェアの本番サーバ、インターネットメールサーバ（無害化処理前）、インターネットメールサーバ（無害化処理後）は、同一の仮想化基盤上に構築すること。
2		内部情報系アプリケーション、ウイルス対策、共有フォルダ、資産管理、二要素認証、LGWANメールを運用するための、サーバOSを調達・構築すること。
3		内部情報系アプリケーション、ウイルス対策、共有フォルダ、資産管理、二要素認証、LGWANメールが物理サーバ上の仮想サーバで動作するよう基盤を構築すること。
4		仮想サーバ及びサーバOSのうち、内部情報系アプリケーションを導入する部分については、令和9年6月30日までに構築すること
5		内部情報系アプリケーション受注者がグループウェアの機能の一つとして、メールサーバ構築するので、同サーバを構築する領域も準備すること。
6		内部情報系アプリケーション受注者が構築するメールサーバには、原本メールサーバと無害化処理後のメールを保存するサーバがある。前者は宮城県セキュリティクラウドを経由した原本メールを受信し、後者にはメール無害化サービスを経由したメールを受信できるように構築すること。
7		財務会計、契約管理、備品管理、起債管理、庶務事務、人事給与、人事評価、文書管理、電子決裁、グループウェア及びこれらのシステム間の連携機能のデータバックアップを内部情報系アプリケーション受注者で実施できるように、同バックアップ領域を提供すること。
8	バックアップ機能・バックアップ基盤	システムバックアップ・リストア機能を構築すること。
9		業務を止めることなくシステムバックアップを実施できること。
10		システムバックアップはトラブル発生時には最低でも前回のバックアップ時点の状態に復元できる仕組みとすること。
11		システムバックアップを下記のとおり実施すること。 ・全仮想サーバのイメージを毎日取得し、直近3世代以上のデータを保存すること。 ・全仮想サーバのイメージを月に1回取得し、直近2世代以上のデータを保存すること。
12		システムバックアップの方式は、完全バックアップ又は差分バックアップとし、差分バックアップを選択する場合は、年に1回以上完全バックアップを実施すること。ただし、下記の(1)又は(2)を実施する場合は、完全バックアップは運用開始時に1回実施するのみでも構わない。 (1)「完全バックアップと差分バックアップを組み合わせたデータで、かつ、同データのみでリストアし、システムを稼働することができるもの」(以下「完全＋差分バックアップデータ」とする。)の最新のデータを1年に1回以上の頻度で共通基盤を構築しているデータセンターとは異なる建物に保管する場合 (2) クラウドサービスを利用する場合は、完全バックアップの1年に1回以上の取得に代えて、同サービスの機能により完全バックアップデータと同等以上の復元性及び整合性を確保できるデータを取得でき、最新の同データを1年に1回以上の頻度で共通基盤を構築しているデータセンターとは異なるデータセンターに保管する場合
13		システムバックアップの対象は、本番環境及び検証環境の全てのデータとする。仮想サーバ毎にシステムバックアップを取得すること。ただし、共有フォルダはデータバックアップをすることとしているため、共有フォルダ40Tbyteのストレージ部分はシステムバックアップの対象外としても構わない。
14		システム変更時には、日次システムバックアップ以外に変更前後のバックアップも実施すること。
15		広域災害時におけるデータ保全のため、下記の(1)～(3)のいずれかを実施すること。 (1)システムバックアップにて取得したデータのうち、年に1回以上の頻度で、最新の完全＋差分バックアップデータ1世代分を共通基盤を構築しているデータセンターとは異なる建物に保管すること。 (2)完全バックアップを年に1度以上実施し、最新の完全バックアップデータ1世代分を共通基盤を構築しているデータセンターとは異なる建物に保管すること。 (3)完全バックアップデータと同等以上の復元性及び整合性を確保できるデータを取得し、最新の同データを1年に1回以上の頻度で共通基盤を構築しているデータセンターとは異なるデータセンターに保管すること。 以下、保管方法の例を挙げる。(完全バックアップを年に1度以上実施する場合に限っては、「最新の完全＋差分バックアップデータ」を「最新の完全バックアップデータ」と読み替えて構わない。) ・本市サーバ室にバックアップデータ1世代分のデータを保存できるハードウェアを設置し、同ハードウェアに最新の完全＋差分バックアップデータ1世代分を送信及び保存する。なお、受注者が他に同サーバ室に設置する機器と同ハードウェア用のサーバラック(日東工業株式会社FSG100-720EKN)1台を本市から提供する。 ・共通基盤を構築しているデータセンターとは異なるデータセンターにて提供しているクラウドサービス上に最新の完全＋差分バックアップデータ1世代分を保存する。ただし、同クラウドサービスはαモデルでも利用可能なものであること。また、同クラウドサービスに利用するためのクラウドサービス利用料、回線費用は全て受注者の負担とする。 ・受注者にて、最新の完全＋差分バックアップデータ1世代分を外部媒体に保存し、当該外部媒体を共通基盤を構築しているデータセンターとは異なる建物の室内(所在地及び裁判所の管轄が国内であり、本調達仕様書2.13.3及び2.13.5の要件を満たしている保管場所)に保管する。 ・クラウドサービスの機能により完全バックアップデータと同等以上の復元性及び整合性を確保できるデータを取得し、最新の同データを1年に1回以上の頻度で共通基盤を構築しているデータセンターとは異なるデータセンターに保管すること。ただし、同クラウドサービスはαモデルでも利用可能なものであること。また、同クラウドサービスに利用するためのクラウドサービス利用料、回線費用は全て受注者の負担とする。
16		取得したシステムバックアップデータは、外部媒体への保存が可能なこと。ただし、クラウドサービス上でシステムバックアップを実施し、下記の(1)～(2)の要件を全て満たしている場合は、外部媒体への保存ができなくても構わない。 (1)共通基盤を構築しているデータセンターが災害等により使用不可になったときに、異なるデータセンターのクラウドサービス上で、システムバックアップをリストアし、システムを稼働できること。 (2)外部媒体への保存と同等以上のデータ安全性を有する方法により、バックアップ基盤以外の障害の影響を受けない状態でのデータ保全を実現できること。

別紙4 各システムハードウェア仕様一覧表

17		データ喪失時は、システムバックアップのリストア後2日以内にシステムを稼働すること。
18	システム監視機能	内部情報系基盤システムを構成するハードウェア及びソフトウェアの運用状況を監視すること。ただし、本市市民協働推進部デジタル戦略課職員が随時運用状況を確認できる場合は、受注者が常時監視する必要はない。
19		仮想サーバの稼働環境を監視、監理すること。ただし、本市市民協働推進部デジタル戦略課職員が随時稼働状況を確認できる場合は、受注者が常時監視、監理する必要はない。
20	本番サーバとデータセンター側ONU間の通信機器等について	データセンター側のONUから仮想サーバ(本番サーバ)までの通信をするために必要な機器(L3通信制御装置等)及び通信ケーブルを調達及び設置すること。
21		データセンター側のONUから仮想サーバ(本番サーバ)までの通信をするために調達設置した機器について、オンサイト保守を実施すること。
22		データセンター側のONUから仮想サーバまでの通信機器及び通信経路は、下記のいずれかを満たしていること。 ・通信経路二重化し、一つの系統の通信経路で障害が発生した場合に、もう一つの系統の通信経路でネットワークの運用を継続できるようにすること。 ・通信機器を二重化するか、CPU カード 電源 ラインカードが二重化してある機器を調達、設置すること。

ウイルス対策

No	業 務 分 類	機 能 要 件
1	基本的な考え方	LGWAN接続系クライアントパソコン(WindowsOS)1,320台をリアルタイムでウイルス、スパイウェアから保護できること。
2		サーバをリアルタイムでウイルス、スパイウェアから保護できること。
3		ウイルス対策担当職員が庁内のウイルス対策状況を一元管理できること。
4		ウイルス対策ソフトウェアのサポート窓口があること。

共有フォルダ

No	業 務 分 類	機 能 要 件
1	基本的な考え方	Active Directory Domain Servicesと連携し、共有フォルダに所属でアクセス権が設定できること。また、当該設定は管理者のみ行えること。
2		人事異動時は人事データから一括してアクセス権を設定できること。
3		職員個人用フォルダには、職員個人フォルダごとにクォータを設定できること。
4		部署用フォルダには、部署用フォルダごとにクォータを設定できること。
5		WindowsOSが搭載されているクライアント端末であれば、動作保証がある。
6		エクスプローラーで管理・閲覧できること。
7	データバックアップ	業務を止めることなく共有フォルダのデータバックアップを実施できること。
8		共有フォルダのデータバックアップは、1日1回以上実施すること。
9		共有フォルダのデータバックアップにより取得したデータは30世代以上(日次)保存できるように設定すること。
10		共有フォルダのデータバックアップにより取得した毎月1日のデータは7世代以上(月次)保存できるように設定すること。
11		共有フォルダのデータバックアップは、WindowsServerOSの標準機能を使用しても構わない。
12		障害により損失した共有フォルダの特定データについて、バックアップで取得していたデータからリカバリを行えること。また、その場合は他業務について運用を停止することなく行えること。
13	移行	現行システムからデータ移行ができる。
14		下記のいずれかを満たすこと。 ・令和9年12月28日まで現行サーバで運用し、12月29日～1月3日の間でデータを移行し、令和10年1月4日からは新サーバで稼働することができる。 ・令和10年1月4日までに新サーバにデータを移行し、新サーバを稼働することができる上、令和9年12月28日までの旧共有フォルダを使用した本市の業務遂行に、支障ならないデータ移行計画書を作成し、本市の承認を得た上でデータ移行作業ができること。
15	共有フォルダサーバ及びストレージを本市サーバ室に設置する場合の追加要件	共有フォルダのサーバ及びストレージを本市サーバ室に設置する場合は、高機能無停電電源装置(UPS)を設置すること。(受注者が同サーバ室に設置する他の機器とUPSを共用しても構わない。)
16		共有フォルダのサーバ及びストレージを本市サーバ室に設置する場合は、同サーバ室停電時に安全に自動でシャットダウンできること。
17		共有フォルダのサーバ及びストレージを本市サーバ室に設置する場合は、1年に1度、共有フォルダデータの完全バックアップを実施し、当該バックアップデータを下記のア、イのいずれかの方法で保管すること。 ア 当該バックアップデータを受注者が提供するデータセンターにあるストレージ等に保存する。同ストレージ等は受注者の負担で調達すること。 イ 所在地及び裁判所の管轄が国内であり、本仕様書2.13.3及び2.13.5の要件を満たしている保管場所を受注者の負担で提供し、当該バックアップデータを保存したハードウェアを保管すること。同ハードウェアは受注者の負担で調達すること。
18		共有フォルダのサーバ及びストレージを本市サーバ室に設置する場合は、同サーバ室計画停電時の対応マニュアルを作成し、本市に提出すること。ただし、同サーバ計画停電時に受注者にてシャットダウン等の必要な作業を実施する場合は、この限りではない。
19		共有フォルダのサーバ及びストレージを本市サーバ室に設置する場合は、ルータ(本調達範囲)又は地域コアスイッチ(別調達)から共有フォルダのサーバ間に追加のネットワーク機器が必要な場合は、受注者の負担で調達すること。
20		共有フォルダのサーバ及びストレージを本市サーバ室に設置する場合は、受注者が同サーバ室に設置する他の機器と共用した上で、サーバラック(日東工業株式会社FSG100-720EKN)1台で運用できること。なお、本市サーバ室のサーバラックの電源は、単相交流100Vである。
21		共有フォルダのサーバ及びストレージを本市サーバ室に設置する場合は、サーバラック(日東工業株式会社FSG100-720EKN)に同サーバを設置するために必要な物品を受注者の負担で調達すること。
22		共有フォルダのサーバ及びストレージを本市サーバ室に設置する場合も、データセンターに設置する場合と同様に、ハードウェアを含む全てを冗長化し、自己修復機能又はフェールオーバー機能を有した管理機能により、障害発生時も自動で即時ミラー(複製)を再構築し、安定した運用環境を提供すること。

資産管理システム

No	業 務 分 類	機 能 要 件
1	基本要件	L2WAN接続系クライアント端末1,320台を運用できること。
2		下記の機能があること。 ・クライアント端末をリモートコントロールできること。 ・クライアント端末にメッセージを配信できること。 ・クライアント端末にファイルを配布できること。 ・クライアント端末にプログラムを実行できること。 ・クライアント端末の操作ログを収集できること。
3		サーバプログラム、管理者プログラムはクライアント端末のライセンス数内で制限なく使用できること。
4		ネットワーク負荷対策としてNICの速度性能を基準とした帯域調整が可能であること。
5		クライアントモジュール自身のプロセスを落とした場合でも自動復旧を行えること。
6		管理コンソールからネットワーク上のクライアントPCに対してクライアントモジュールのインストールをリモートで行えること。
7		CSVファイルのインポートにより一括でクライアントを指定して、リモートインストールできること。IPアドレス範囲を指定して端末一覧を検索し、検索結果からインストール対象の端末を選択する方法で対応しても構わない。
8		クライアント端末から、OSとネットワークに関連する基本的な情報を取得できること。 ・マシン名 ・IPアドレス ・MACアドレス ・サブネットマスク ・ドメイン/ワークグループ名 ・Active Directory ドメイン名 ・ログオンユーザー名 ・OS名 ・OSサービスパック ・OS 種別 ・OSバージョン ・OSビルド番号 ・OSプロダクトID ・クライアントバージョン
9		管理対象端末以外のハードウェアを手動登録にて、一括して所属グループの変更が可能であること。
10		管理対象端末以外のハードウェアをCSVファイルからインポートして、一括登録、一括編集、所属グループの変更が可能であること。
11		システム管理者は管理コンソールの全ての操作を行えること。
12		管理対象となるクライアント端末のグループ分けが手動により可能であること。
13		フィルター機能を有し、フィルター条件を入力することで、該当情報がリアルタイムで一覧表示に反映されること。
14		アラートログを出力したクライアント端末の情報を、管理者にポップアップで通知可能であること。
15		設定したスケジュールに従って、データベースを自動的にバックアップ可能であること。
16		下記のいずれかに対応していること。 ・『閲覧用データベース』にバックアップデータをリストアすることで、現在の運用データに影響を与えることなくバックアップデータを閲覧可能であること。 ・バックアップデータのログをリストアすることなく閲覧可能であること。
17		データベースに登録されている、運用ポリシーとシステム設定の情報をエクスポートできること。
18		運用データベースに問題が発生した場合、このデータをインポートすることで復旧可能であること。
19		管理コンソールで、誰が、いつ、どのような操作を行ったかを検索できること。
20		クライアントが起動時に管理サーバとの通信が行えなかった場合に、通信が確立したタイミングで基本インベントリ情報を自動で送信すること。
21		管理コンソールに表示されているログデータを、CSVファイルにエクスポートできること。
22		管理コンソールからクライアントPCに対してメッセージ配信が可能であること。
23	PC資産管理	ネットワークに接続されたクライアントPC全てにて自動収集が可能であること。
24		スケジューリングによるインベントリ収集が可能であること。
25		任意のタイミングでのインベントリ収集が可能であること。
26		ハードウェアに関連する以下のインベントリ情報の取得が可能であること。なお、レジストリ収集にてバージョン情報を収集する方法でも構わない。 ・ベンダー名 ・モデル名 ・BIOS/バージョン ・メモリ容量 ・システムドライブ容量 ・システムドライブ空き領域 ・コンピューターの説明 ・ディスプレイデバイス名 ・Internet Explorer/バージョン ・MDAC/バージョン ・Outlook Express/バージョン ・.NET Framework/バージョン ・画面の解像度
27		クライアントPCに登録されているプリンタードライバーから以下の情報を取得可能であること。 ・プリンターの名前 ・プリンターのポート番号
28		クライアントPCのNICごとに設定されている以下の情報を取得可能であること。 ・デバイス名 ・MACアドレス ・DHCP設定 ・IPアドレス ・サブネットマスク ・デフォルトゲートウェイ ・優先DNSサーバ ・代替DNSサーバ
31		各アプリケーションから以下の情報を取得できること。 ・アプリケーション名 ・インストール日付 ・製品バージョン

別紙4 各システムハードウェア仕様一覧表

32		ウイルス対策ソフトの以下の情報を収集できること。 ・トレンドマイクロ社: ウイルスバスター/ウイルスバスターコーポレートエディション ・シマンテック社: Norton AntiVirus/Symantec Endpoint Protection ・マカフィー社: McAfee VirusScan/McAfee VirusScan Enterprise/McAfee Total Protection ・キャノンITソリューションズ社: ESET NOD32アンチウイルス ・カスペルスキー社: Kaspersky Endpoint Security for Windows
33		エディションやバージョンにより、『ソフトウェア名』が異なるソフトウェアをまとめて管理できること。
34		以下の条件に該当するハードウェア情報を取得したら、管理者にアラートメールを送信できること。なお、IPアドレス重複とMACアドレス重複については、資産情報の変更発生時にアラートメールを送信する方式でも構わない。 ・システムドライブの空き容量不足 ・IPアドレス重複 ・MACアドレス重複
35	アプリケーション配布	以下の種別のタスクが作成可能であること。 ・ファイル配布 ・プログラム実行 ・ファイル配布プログラム実行 ・INIファイル編集 ・レジストリ編集 ・OSシャットダウン ・OS再起動 なお、INIファイル編集については、差替え後のINIファイルを配布することができるのであれば、直接的な編集機能がなくても構わない。 また、レジストリ編集については、レジストリを更新するスクリプトを準備し、そのスクリプトを配布実行できるのであれば、直接的な編集機能がなくても構わない。
36		実行タイミングについて、以下の設定が選択可能であること。 ・OS起動時 ・OSログオン時 ・指定時間にランダムに開始 ・タスクランチャーから選択
37		配布時にファイルを圧縮、配布終了時には自己解凍が可能であること。
38		配布の適用時間・期間を設定可能であること。
39		指定したスケジュールに従って適用期間内に該当プランを繰り返し実行することが可能であること。
40		配布実行結果の成功、失敗、中止、未実施と状況を把握できること。
41		PC単位、グループ単位でファイルの配布が可能であること。
42		クライアントPCのデスクトップ、ProgramFilesフォルダなど、任意の配布先を指定できること。
43		クライアントPC側の作業無しにバックグラウンドで配布を実行可能であること。
44		配布及び実行条件はスクリプトを使用せずにGUI画面にて設定できること。
45		サイレントインストールに未対応アプリケーションであってもクライアントにWindows管理者権限のIDパスワード入力をさせることなく、管理者権限でインストールが可能であること。
46		ログオンしているユーザーの権限に依存せずアプリケーション・パッチのインストールが実行可能であること。
47		ネットワークへの負荷を考慮したマルチキャストによる配布ができること。
48		ファイルダウンロード中に通信が遮断した場合、次回通信時にダウンロードの途中から再開できる自動再開(レジューム)機能があること。
49		マルチキャスト配布によるファイル配布時は管理コンソール上でファイル配布の状況が把握できること
50	ログ収集機能	クライアントPCで起動している、以下のプロセスの情報が取得できること。 ・プロセス名 ・アカウント名 ・起動日時 ・起動していた時間
51		クライアントPCでアクティブになっているウィンドウの情報が取得できること。 ・プロセス名 ・ウィンドウタイトル ・URL(Google Chrome及びMicrosoft Edgeの場合)
52		指定のアプリケーションの起動を検知して、クライアント端末に警告メッセージを表示可能であること。
53		ファイル操作のログ(作成/コピー/移動/リネーム/削除)を取得できること。 ・操作対象のファイル名 ・操作対象のファイルパス ・操作元のドライブ種別 ・変更後のファイル名 ・プロセス名 ・コピー/移動先のファイルパス ・コピー/移動先のドライブ種別
54		クライアントPCで印刷された、ドキュメントの情報を取得できること。 ・ドキュメント名 ・ファイル名 ・プリンター名 ・印刷枚数 ・ファイルパス
55		外部デバイスへのファイル持ち出しログの抽出が容易に可能であること。
56		クライアントPCでドライブの追加と削除を検知して、以下の情報を取得可能であること。 ・ドライブ種別: ローカルディスク、リムーバブルディスク、ネットワークドライブ、FD、CD/DVD、ポータブルデバイス ・ドライブ名 ・UNCパス(ネットワークドライブの場合) ・デバイス名(USBデバイス/ポータブルデバイスの場合) ・ベンダー名(USBデバイス/ポータブルデバイスの場合) ・プロダクトID(USBデバイス/ポータブルデバイスの場合) ・シリアルナンバー(USBデバイス/ポータブルデバイスの場合)
57		以下のイベントを検知して、情報を取得できること。 ・クライアント起動 ・OSログオン ・OSログオフ ・スリープ ・スリープ解除 ・スクリーンセーバー ・スクリーンセーバー解除 ・OSシャットダウン要求 ・OSシャットダウン なお、スリープ・スリープ解除はそれぞれ操作終了・操作開始として記録される方法、スクリーンセーバーはアプリケーションログの「.scr」の開始時間と期間で確認する方法、OSシャットダウン要求はOSシャットダウンのログと同様に電源OFFのログとして記録する方法でも構わない。

別紙4 各システムハードウェア仕様一覧表

58		ハードウェア、アプリケーション、それぞれの視点で、クライアント端末の24時間の稼働状況をグラフ表示し、アラートを検知した時間を赤で表示できること。アラート検知した時間を表示する機能はない場合でも、代替としてアラート検知の件数をダッシュボードで確認でき、そこから具体的なログに遷移することで具体的な時間を確認することできる場合は、可とする。
59		以下の条件を指定して、クライアントPCの操作履歴ログを検索できること。 ・マシン名、クライアント端末、ログオンユーザー名 ・ウィンドウタイトル/URL:ウィンドウタイトル警告のみ、ウィンドウタイトル/URL、プロセス名、アプリケーション名 ・クリップボード操作ログ:コピー文字列、ファイルパス、画像/プリントスクリーン ・ファイル操作:ファイル操作警告/禁止のみ、ファイルパス、ファイル名、プロセス名、アプリケーション名 ・検索対象:全てのドライブ種別、ローカルドライブのみ、リムーバブルディスクのみ、共有フォルダのみ、アップロードのみ ・メール添付ログ:ファイル操作警告のみ、ファイル名 ・印刷ログ:ファイル名/ドキュメント名、プリンター名 ・メール送信ログ、Webフォーム送信ログ、Webアプリ操作ログ、簡易Webフィルタリング結果 ・アラートプロセスの起動警告/禁止、停止監視プロセスの停止 ・使用禁止USBデバイスの接続:USBデバイス名、シリアルナンバー ・ドライブの追加と削除:ドライブの追加と削除、ドライブの追加のみ、ドライブの削除のみ、USBデバイス名、シリアルナンバー ・ログオン、ログオフ、スリープ、シャットダウン
60		特定ファイルの操作履歴を基点として該当ファイルに対して行われた一連の操作ログを追跡できること。
61		指定した期間に、各クライアントPCに接続されたUSBデバイスの情報をCSVファイルに出力できること。
62	デバイス制御機能	クライアントPCに接続した以下のUSBデバイスの情報を取得可能であること。 ・USBシリアルナンバー ・USBデバイス ・USBベンダー ・USBプロダクトID
63		グループ、ユーザーごとに、指定したUSBデバイスの制御を行えること。 ・書き込み許可 ・読み込み専用 ・使用禁止
64		新規に検知したUSBデバイスの初期設定を変更できること。 ・書き込み許可 ・読み込み専用 ・使用禁止
65		使用を禁止しているUSBデバイスの接続、読み込み専用に設定したUSBデバイスへの書き込みを検知して、クライアント端末に警告メッセージを表示できること。
66		グループごとに、クライアント端末のFD/SDカードドライブの使用を制御できること。 ・書き込み許可 ・読み込み専用 ・使用禁止
67		グループ、ユーザーごとにクライアント端末のCD/DVD/Blu-rayドライブの使用を制御できること。 ・書き込み許可 ・読み込み専用 ・使用禁止
68		スマートフォン、オーディオプレイヤー、デジタルカメラ等、Windowsポータブルデバイスとして認識されるデバイスが接続された際に、その情報を取得できること。 ・デバイス名 ・ベンダー ・プロダクトID ・シリアルナンバー
69		USBデバイスに格納されているファイルの一覧を取得することができること。
70	ネットワーク接続管理	ネットワーク上から、クライアント以外のハードウェアを自動的に検知できること。
71		ネットワークからハードウェアを検知、遮断したら、管理者にアラートメールを送信可能であること。
72	リモートコントロール	管理者からクライアントPC画面を遠隔操作が可能なこと。 (PCの固有情報の変更、ファイルのコピー/削除/作成、再起動/ログオン/ログオフ、Ctrl+Alt+Delete等のキーストローク)
73		管理者から対象クライアントPCのデスクトップ監視が可能なこと。
74	その他	WindowsOSが搭載されているクライアント端末であれば、動作保証がある。
75		コンピューターウイルスに感染した場合に、クライアントコンピューターをネットワークから遮断しつつ資産情報やログを収集するため、特定イベントの検出時に、ネットワークからの遮断を除外する通信を設定できること。また、本ソフトウェアによる通信は維持できること。
76		標的型攻撃およびランサムウェア対策のため、指定した重要なフォルダに対して、許可したアプリケーション以外によるアクセスを禁止できること。なお、ローカルフォルダも重要なフォルダとして指定できること。

二要素認証システム

No	業 務 分 類	機 能 要 件
1	基本的な考え方	ユーザー数1,950名を運用できること。
2		下記の機能があること。 ・Windowsユーザーを管理できること。(受注者が構築したActive Directory Domain Servicesサーバへ、リモートデスクトップ接続でアクセスして、Windowsユーザーアカウントを作成・削除・変更できるのであれば、顔認証システムにパッケージとして、Windowsユーザーアカウントそのものを直接作成・削除・変更する機能がなくても構わない。) ・二要素認証でWindowsにログオンできること。 ・内部情報系アプリケーション(IPKNOWLEDGE(富士通Japan)、desknet's NEO(NEOJAPAN))にシングルサインオン又は顔認証によるログオンができること。
3	認証方式	顔認証方式で、二要素認証を行えること。
4		ユーザIDと二要素目情報(生体情報等)の1:1認証方式に対応していること。
5		認証情報登録画面および認証画面において、センサーが撮影している二要素目の情報(顔認証情報等)を利用者がリアルタイムに確認できるようになっていること。ただし、利用者が顔認証をするときに、センサー(カメラ)が顔を認識するために、顔の位置、向き、距離などを調整する画面上のガイド等が、認証画面上にて存在する場合は、センサーが撮影している二要素目の情報(顔認証情報等)を利用者がリアルタイムに確認できるのは、認証情報登録画面のみでも構わない。
6	認証回避機能	クライアントPCがネットワーク障害等で認証サーバーと通信できない場合は、以下の回避策を用意していること。 → 同一端末において直近でログオンしていたユーザーのログオン情報をキャッシュしておき、キャッシュ情報を使った認証によりセキュアにログオンできること。
7		怪我等で登録あるいは認証が容易に出来ない場合には、管理者が発行する一時的なパスワードにより認証させることができるなどの代替措置をとることが可能であること。
8	データ登録	二要素目の認証データ(顔認証データ等)登録が簡単におこなえること。
9		氏名、ユーザーID、パスワード等のユーザー情報を、CSV形式にて一括登録／更新／削除が可能なこと。また、登録済みユーザー情報はCSV形式にて抽出可能なこと。ただし、Active Directoryのユーザー情報(氏名、ユーザーID、パスワード等)を、手動で同情報を生体認証システムに入力しなくても、同システムにて使用できる場合は、CSV形式の一括登録／更新／削除機能及びCSV形式の抽出機能に対応していなくても構わない。
12	アプリケーションログオン設定	以下のいずれかに対応していること。 ・業務システムのURL・ID・パスワード等を登録することにより、ブラウザで運用できる業務システムにシングルサインオンすることができること。 ・業務システムAPIを組み込むことで、業務システムログイン時に二要素認証を呼び出すことができること
13		アプリケーションログオン機能の利用にあたっては、対象となる業務アプリケーションに対して、修正が入らないこと。
14	Windowsログオン時及びロック解除	Windowsログオン及びPCロック、スクリーンセーバーロックの解除時の認証に利用可能なこと。
15		直前の認証成功者のユーザーIDが二要素認証画面にプリセットされるなどの方法により、利用者のユーザーID入力の手間を省く仕組みを持つこと。
16	クライアント動作環境	PC内蔵の通常のカメラ(VGA(640×480)以上の解像度)を認証装置として利用するなど、PC内臓の装置で二要素認証をすることができ、追加の機器を必要としない。
17	管理者機能	全ての認証端末(LGWAN接続系クライアント端末)において、管理者機能が使えること。 ※管理者機能とは、認証情報・テキスト系情報(氏名)の登録・更新処理や、認証サーバへのテキスト系情報の一括更新などを指す。
18	サーバ動作環境	認証サーバーのユーザー情報の管理は Active Directory Domain Servicesを利用すること。
19		Active Directory Domain Servicesサーバ(DNSサーバ)を調達・構築・運用すること。また、同サーバは冗長化すること。
20		認証情報(生体情報、IC カード、パスワード 情報等)は認証サーバーに保存できること。
21		認証システム内で保持するパスワードは、管理者が設定、変更が可能なこと。また、ユーザーが設定したパスワード(Windowsパスワードとアプリケーションパスワード)は、アスタリスク等で見えない状態となっていること。
22		認証サーバーに登録される顔情報は、認証に必要な特徴情報のみ保持し、画像データとして保持しない設定が可能なこと。
23	Active Directory Domain Servicesセカンダリサーバを本市サーバ室に設置する場合の追加要件	本市サーバ室にActive Directory Domain Servicesセカンダリサーバを設置する場合は、高機能無停電電源装置(UPS)を設置すること。(受注者が同サーバ室に設置する他の機器とUPSを共用しても構わない。)
24		本市サーバ室にActive Directory Domain Servicesセカンダリサーバ(DNSセカンダリサーバ)を設置する場合は、計画停電時の対応マニュアルを作成すること。
25		本市サーバ室にActive Directory Domain Servicesセカンダリサーバ(DNSセカンダリサーバ)を設置する場合は、同サーバ室停電時に安全に自動でシャットダウンできるように設定すること。
26		本市サーバ室にActive Directory Domain Servicesセカンダリサーバ(DNSセカンダリサーバ)を設置する場合は、ルータ(本調達範囲)又は地域コアスイッチ(別調達)あるいはLGWAN下位スイッチ(別調達)から同サーバ間に追加のネットワーク機器が必要な場合は、受注者の負担で調達すること。
27		本市サーバ室にActive Directory Domain Servicesセカンダリサーバ(DNSセカンダリサーバ)を設置する場合は、受注者が同サーバ室に設置する他の機器と共用した上で、サーバラック(日東工業株式会社FSG100-720EKN)1台で運用できること。なお、本市サーバ室のサーバラックの電源は、単相交流100Vである。
28		本市サーバ室にActive Directory Domain Servicesセカンダリサーバ(DNSセカンダリサーバ)を設置する場合は、サーバラック(日東工業株式会社FSG100-720EKN)に同サーバを設置するために必要な物品を受注者の負担で調達すること。

LGWANメール

No	業 務 分 類	機 能 要 件
1	基本的な考え方	最大35のメールアドレスを運用できること。(1つのメールアドレスを複数の職員で利用することを想定している。)
2		LGWANメールの送受信ができること。SMTPサーバ及びIMAPサーバ機能を構築・運用すること。
3	ユーザー	ユーザー(メールアドレス)ごとに、メールBOX容量制限ができる。
4		ユーザー(メールアドレス)ごとに、メールアドレス容量制限の通知ができる。
5		ID・パスワードでログインして、利用できる。
6		自動返信機能がある。
7		自動転送機能がある。
8		ユーザー(メールアドレス)ごとに、特定メールのブロック設定ができる。
9		MTA上でのフィルタリングブロック機能がある。
10		ブラウザで利用できる。
11		受信メール及び送信済みメールをフォルダで管理できる。なお、下記のいずれの方法でも構わない。 ・受信フォルダ・送信済みフォルダを上位フォルダとして、下位に別フォルダを作成する方法 ・受信フォルダ・送信済みフォルダと同階層にフォルダを作成する方法
12		メールをインポートできる。
13		メールをエクスポートできる。
14		ユーザー(送受信可能なメールアドレス)を任意で作成・修正・削除できること。なお、修正を、既存のメールアドレスの削除及び再作成で実施しても構わない。
15	管理者画面	管理者画面にブラウザでアクセスできる。
16	その他	現行のメールアドレスをそのまま使用できる。
17		WindowsOSが搭載されているクライアント端末であれば、動作保証がある。
18		令和9年12月31日まで現行システム(PostOffice)で運用し、令和10年1月1日からは新システムで稼働することができる。

LGWANサーバ

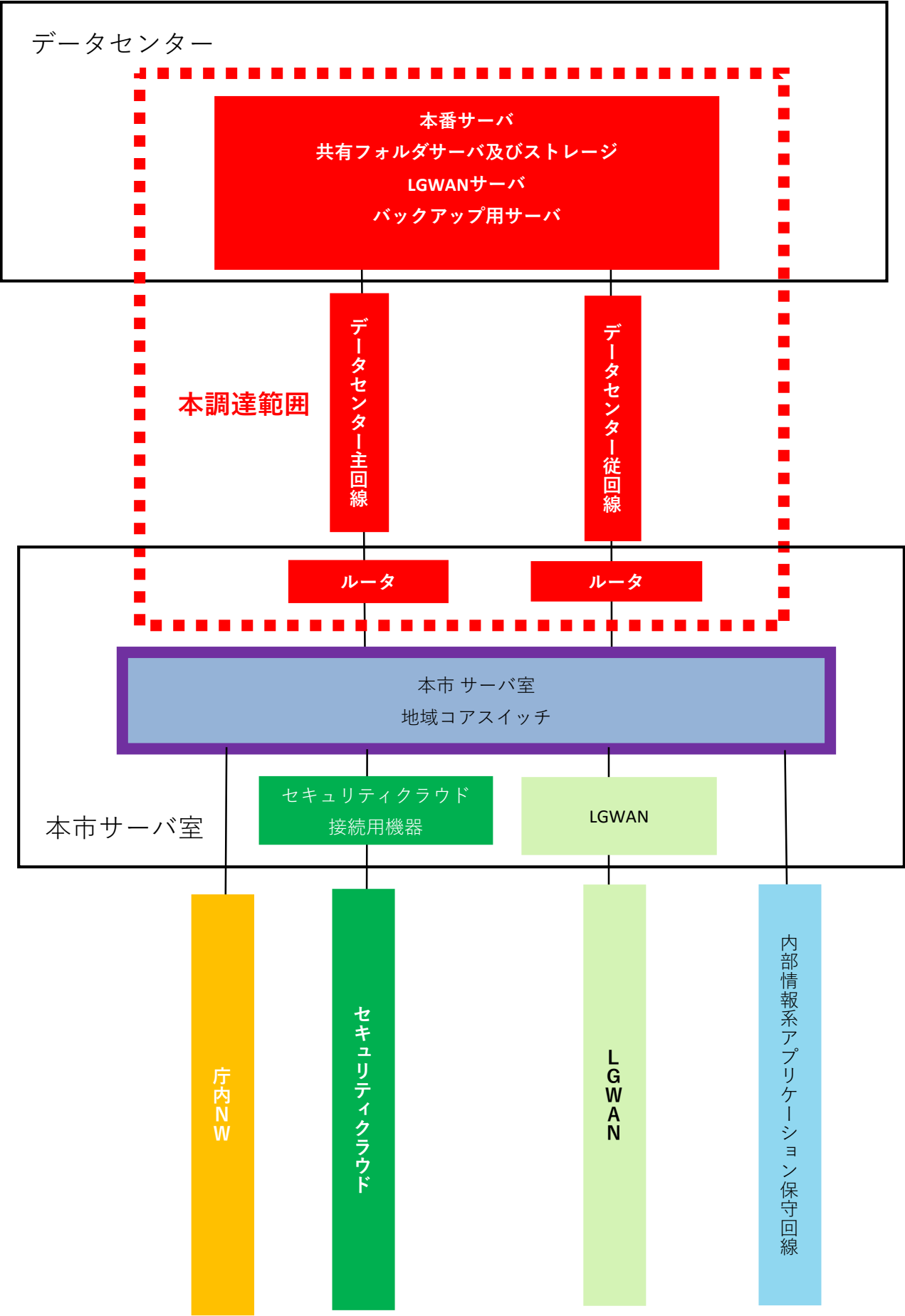
No	業 務 分 類	機 能 要 件
1	基本的な考え方	LGWAN/NTP サーバ及びLGWANメールスプールサーバ機器を調達すること。
2		オンサイト保守に対応していること。
3	J-LIS提供サービスとの連携	LGWAN/NTP サーバは、J-LIS提供NTP(時刻同期)サービスと連携すること。ただし、下記の条件を満たす場合に限り、J-LIS提供NTP(時刻同期)サービスと連携しない方法で、NTPサーバを構築することを認める。 ・高精度時刻同期サービスを基準としてNTPサーバ自体の時刻誤差を10ミリ秒以内にすること。 ・ α モデルでも利用できるように構築すること。(α 'モデルでないと利用できないものは不可である。) ・大崎市情報セキュリティポリシー(令和8年4月1日改正)を遵守すること。 ・本調達範囲の仮想サーバが、同NTPサーバと通信して時刻同期できること。
4		LGWANメールスプールサーバは、J-LIS提供DNS(名前解決)サービスと連携すること。
5		LGWANメールスプールサーバは、J-LIS提供SMTP(メール)サービスと連携すること。
6	設置・初期設定	サーバの初期設定を行うこと。
7		マイナンバー系ドメインサーバが時刻同期できるように、LGWAN/NTP サーバへの通信許可設定をすること。
8		初期設定時は、現行サーバの設定情報を全て引き継ぐこと。
9		LGWANへのメール送信を「DNS参照によるMX配送」で行うこと。
10	保守	終日オンサイト保守を実施すること。
11	LGWANサーバを本市サーバ室に設置する場合の追加要件	本市サーバ室にLGWAN/NTP サーバ及びLGWANメールスプールサーバ機器を設置する場合は、高機能無停電電源装置(UPS)を設置すること。(受注者が同サーバ室に設置する他の機器とUPSを共用しても構わない。)
12		本市サーバ室にLGWAN/NTP サーバ及びLGWANメールスプールサーバ機器を設置する場合は、計画停電時の対応マニュアルを作成すること。
13		本市サーバ室にLGWAN/NTP サーバ及びLGWANメールスプールサーバ機器を設置する場合は、同サーバ室停電時に安全に自動でシャットダウンできるように設定すること。
14		本市サーバ室にLGWAN/NTP サーバ及びLGWANメールスプールサーバ機器を設置する場合は、ルータ(本調達範囲)又は地域コアスイッチ(別調達)あるいはLGWAN下位スイッチ(別調達)から同サーバ間に追加のネットワーク機器が必要な場合は、受注者の負担で調達すること。
15		本市サーバ室にLGWAN/NTP サーバ及びLGWANメールスプールサーバ機器を設置する場合は、受注者が同サーバ室に設置する他の機器と共用した上で、サーバラック(日東工業株式会社FSG100-720EKN)1台で運用できること。なお、本市サーバ室のサーバラックの電源は、単相交流100Vである。
16		本市サーバ室にLGWAN/NTP サーバ及びLGWANメールスプールサーバ機器を設置する場合は、サーバラック(日東工業株式会社FSG100-720EKN)に同サーバを設置するために必要な物品を受注者の負担で調達すること。

別紙5_各システムリソース要件

No	摘要	項目	構成	数量	対象	必要リソース	備考
1	財務会計 契約管理 備品管理 起債管理 庶務事務 文書管理 電子決裁	本番，検証 用，データ バックアップ サーバ	仮想	1	CPU性能	Xeon4コア×2 個相当以上	CPUは下記の（１）又は （２）の要件を満たして いること。 （１）Xeon Silver第3世 代以上であること。 （２）Xeon Gold第2世 代以上であること。 また，No.3～No.5は， 同一の仮想化基盤上に構 築すること。
					メモリ容量	96GB以上	
					ディスク容量	8TB以上	
2	人事給与 人事評価	本番，検証 用，データ バックアップ サーバ	仮想	1	CPU性能	Xeon 4コア×1 個相当以上	
					メモリ容量	32GB以上	
					ディスク容量	4TB以上	
3	グループウェア	本番サーバ	仮想	1	CPU性能	Xeon 12コア×1 個相当以上	
					メモリ容量	32GB以上	
					ディスク容量	5TB以上	
4		インターネット メールサーバ	仮想	1	CPU性能	Xeon 4コア×1 個相当以上	
		無害化処理前 原本メール			メモリ容量	8 GB以上	
					ディスク容量	2TB以上	
5		インターネット メールサーバ	仮想	1	CPU性能	Xeon 4コア×1 個相当以上	
		無害化処理後 メール			メモリ容量	8 GB以上	
					ディスク容量	2TB以上	
6	予備	予備	仮想	1	CPU性能	Xeon 4コア×1 個相当以上	
					メモリ容量	8 GB以上	
					ディスク容量	300GB以上	
7	ウイルス対策	サーバ及びク ライアント端 末の監視等	仮想	ウイルス対策を運用するために必要な数量・性能の仮想サーバを調 達すること。			
8	共有フォルダ	共有フォルダ	仮想	40Tbyte以上のデータを保存できる共有フォルダを運用するために必 要な数量・性能の仮想サーバを調達すること。			

9	資産管理	LGWANクライアント端末の管理等	仮想	1320台のLGWANクライアント端末の管理等をする資産管理システムを運用するために必要な数量・性能の仮想サーバを調達すること。
10	二要素認証 (ADサーバ含む)	顔認証システム、Windowsユーザーの管理等	仮想 (ADセカンダリサーバに限り物理でも可)	二要素認証システム（冗長化されたADサーバ（DNSサーバ）含む）に必要な数量・性能の仮想サーバを調達すること。Windowsユーザを管理する Active Directory Domain Servicesサーバは冗長化すること。
11	LGWANメール	Webメール機能等	仮想	LGWANメールを運用するために必要な数量・性能の仮想サーバを調達すること。LGWANメールの1アカウントに割り当てる容量は、1GBを想定しており、最大35アカウントの運用する見通しである。
12	LGWANサーバ	メールプールサーバ、NTPサーバ等	仮想又は物理	メールプールサーバ、NTPサーバを運用するために必要な数量・性能のサーバを調達すること。
13	システムバックアップ	システムバックアップ	仮想又は物理	仕様書記載のシステムバックアップの運用をするために必要な数量・性能のサーバを調達すること。

大項目	中項目	小項目	実 施 基 準	
オンライン運用	オンライン運用管理	サービス運用	サービス運用時間	①運用時間 24時間365日 ②障害受付時間 9:00～17:00(土日及び祝日(もしくは振替休日)、年末年始(12月29日から1月3日)は除く) ※緊急時は随時対応とする
		サービス稼働率	(サービス提供時間-停止時間)÷サービス提供時間[%]	99%以上
バッチ運用	ジョブ実行管理	ジョブ管理	登録情報に反映するまでの時間 実行状況を確認するまでの時間	適用の3日前まで 実行終了後から30分以内
		バッチ処理完了時間遵守	完了時間遵守率	95.0%以上
稼働管理	計画停止予定通知	機器保守及びファンリ ティ設備保守点検	サービス停止に関する事前連絡の提出時期	1ヶ月前
		システム保守	運用停止に関する事前連絡の提出時期	14日前
	システム運転時間 保守作業	運転時間の管理	システム運転時間の管理	スケジューラ等のツールによる運転時間の管
		保守スケジュール	保守時間・定期点検時間のスケジュール管理	スケジューラ等のツールによる保守時間・定期 点検時間のスケジュール、履歴の管理
		保守完了率	保守時間・定期点検時間のスケジュールの 提出時期 (時間内にハードウェア保守を完了した件数) ÷(ハードウェア保守実施件数)[%]	月次:該当月の前月の20日まで 年次:該当年度の前年度3月の20日まで 100% オンサイト保守:4時間以内 修理・交換:2日以内
	状態監視	死活監視 (サーバ・ネットワーク)	応答確認の頻度	1回/15分以上
		メッセージ監視	通知メッセージの監視回数	1回/時間以上
		ハードウェア監視	異常を検知してから報告までの時間	検知後30分以内
		サービスの稼働	サービス稼働状況の確認頻度	1回/時間以上
		時刻同期	サーバを提供するサーバ間の時刻同期の 頻度	1回/日 遵守率99%以上
障害管理	障害対応	障害通知	障害検出から通知までの時間	検知後30分以内
		1次切り分け	1次切り分けを行ってから報告までの時間	1次切り分け後60分以内
		復旧対応	連絡を受けてから復旧作業を開始するまで 最低限の機能を復旧するまでの時間	連絡を受けてから90分以内 検知後8時間以内
		目標復旧地点	復旧完了までの時間 データの復旧地点	翌朝8時まで 又は 検知後24時間以内 システム障害:原則、障害による停止直前 大規模災害 :災害発生前日
		障害報告	障害の復旧後に報告書を提出するまでの時 間	障害復旧後3日以内
		重大障害件数	重大障害の発生件数	2回/年以内
セキュリティ管理	不正アクセス管理	不正アクセスの監視	不正アクセス検知から報告までの時間	検知後30分以内
	ウィルス対策	定期ログ集計報告	対応措置を開始するまでの時間	検知後60分以内
		パターンファイルの更新	ログ集計内容の報告回数	1回/月
		発見、検知時の対応	パターンファイルの更新頻度	ベンダーリリースから24時間以内
			ウィルスの発見、検知までの時間	リアルタイム
			ウィルス発見、検知から報告までの時間	ウィルスの発見、検知後30分以内
			ウィルス発見、検知から対応開始までの時間	発見、検知後60分以内
構成管理	変更管理	ハードウェア・ソフトウェ ア・ネットワーク	変更内容を構成情報に反映するまでの時間	構成変更から3日以内
	ドキュメント管理	運用ドキュメント管理	ドキュメント管理体系の整備	変更が必要な事案発生後、1週間以内
	マニュアル、媒体管理	ハードウェア情報管理	変更内容を管理台帳に反映するまでの時間	資産変更から3日以内
	ライセンス管理	ソフトウェア情報管理	変更内容をライセンス情報に反映するまでの バージョンアップ実施回数	資産変更から3日以内 1回/年以上
	ソフトウェア管理	バージョンアップ対応	不具合が確定してから報告までの時間	確定から3日以内
リリース管理	ソフトウェア管理	不具合対応	不具合が確定してから作業完了までの時間	確定から翌日まで
		パッチ適用	パッチ適用が確定してから作業完了までの時 間	確定から3日以内
			システムのバックアップの頻度	1回/日(ただし、システム変更時、即時)
バックアップ管理	バックアップ計画	バックアップ作業	共有フォルダのデータのバックアップの頻度	1回/日
			正常バックアップ率	100%
		ストレージ管理	ハードディスク残容量の管理	閾値超え検知後60分以内の報告
		媒体管理	保管台帳への反映	変更の発生から24時間以内
		世代管理	管理台帳に反映するまでの時間	2日以内に管理台帳に反映
性能管理	性能情報収集	リストア管理	リストア後システム稼働までの時間	2日以内
		サーバ性能管理	サーバのCPU使用率を測定	閾値超え検知後60分以内の報告
			ディスクの使用率を測定	閾値超え検知後60分以内の報告
			サーバのメモリ使用率を測定	閾値超え検知後60分以内の報告
サポートデスク	問合せ対応	トラフィック監視	定期記録時間	30分/回
		サポート時間	サポート時間	・9:00～17:00(土曜、日曜、祝日(もしくは振替休日)、年末年始(12月29日から1月3日)は除く) ※サービス提供時間帯外はメール受付を
		業務問合せ対応	1次回答までの時間	1時間以内
			未対応状況	全体の5.0%未満



本調達範囲のデータセンター設置ハードウェア一覧

摘要	数量	単位	備考
L3通信制御装置	1	式	必要な場合に限る。必要な場合は、通信機器を二重化するか、CPUカード電源ラインカードが二重化してある機器を調達、設置すること。
本番サーバ(仮想サーバ用)	1	式	
LGWANサーバ	1	式	本市サーバ室に設置しても構わない。本市サーバ室に設置する場合は別紙4「各システムハードウェア仕様一覧表」LGWANサーバの「LGWANサーバを本市サーバ室に設置する場合の追加要件」を全て満たしている必要がある。
共有フォルダサーバ及びストレージ	1	式	本市サーバ室に設置しても構わない。本市サーバ室に設置する場合は、別紙4「各システムハードウェア仕様一覧表」共有フォルダの「共有フォルダサーバ及びストレージを本市サーバ室に設置する場合の追加要件」を全て満たしている必要がある。
システムバックアップ用サーバ	1	式	

上記記載のハードウェアは最低限調達が必要であるものを記載しただけであり、調達仕様書及び別紙記載の要件を充足するために、追加の機器・ライセンスが必要である場合は、当該機器・ライセンスも調達すること。

上記記載のハードウェアの全部又は一部を仮想化しても構わない。

本調達範囲の本市サーバ室設置機器一覧

摘要	数量	単位	備考
ルータ(主回線用)	1	台	
ルータ(従回線用)	1	台	
高性能無停電電源装置(UPS)	1	式	LGWANサーバ及び共有フォルダサーバ及びストレージを本市サーバ室に設置しない場合は、ルータ及びONU用の無停電電源装置のみで構わない。

No	業務システム	方向	連携(元・先)システム	連携(元・先)情報
1	財務会計システム	←	人事給与システム	職員データ、人件費データ、源泉徴収票データ、金融機関 口座振替データ、共済負担金データ
2		←	電子決裁システム	決裁データ
3		←	金融機関	金融機関 口座振替データ
4		←	インフラ資産管理	固定資産データ
5		←	収納消込(総合収納システム)	税等収納データ
6		←	固定資産税	固定資産税評価額データ・残高データ
7		←	後期高齢者医療	保険料収納データ
8		←	介護保険	保険料収納データ
9		←	総務省 電子調査表	実態調査データ
10		←	財産管理システム	固定資産データ
11		←	備品管理システム	固定資産データ
12		←	契約管理システム	実績(契約・執行)データ
13		→	総務省 電子調査表	実態調査データ
14		←	公振くん	公共料金事業者受信データ
15		←	金融機関	金融機関 総合振込データ
16		→	源泉徴収システム	源泉徴収データ
17	契約管理システム	←	財務会計システム	予算データ
18		←	人事給与システム	職員データ
19		→	財務会計システム	実績(契約・執行)データ
20		→	文書管理システム	原義文書データ
21	備品管理システム	←	人事給与	組織データ、職員データ
22		←	財務会計	予算データ
23	起債管理システム	→	特別会計、公営企業会計	地方債現在高データ
24		→	特別会計、公営企業会計	地方債償還額データ
25		→	特別会計、公営企業会計	決算統計に係る各種帳票作成データ
26	庶務事務システム	←	人事給与システム	組織データ、職員データ、給与支給明細データ、還付調書データ
27		←	電子決裁システム	決裁データ
28		→	人事給与システム	勤務実績データ
29	人事評価システム	←	電子決裁システム	職員データ
30		→	人事給与システム	評価(能力・業績)データ
31	人事給与システム	←	庶務事務システム	勤務実績データ
32		←	人事評価システム	評価(能力・業績)データ
33		←	住民税	住民税データ
34		→	財務会計システム	職員データ、人件費データ、源泉徴収票データ、金融機関 口座振替データ、共済負担金データ
35		→	文書管理システム	職員データ
36		→	グループウェア	職員データ
37		→	庶務事務システム	組織データ、職員データ、給与支給明細データ、還付調書データ
38		→	契約管理システム	職員データ
39		→	人事評価システム	職員データ
40		→	電子決裁システム	職員データ
41		→	共済組合	共済報告明細データ、給料表データ、組合員申告書データ
42		→	金融機関	金融機関 給与振込データ
43		→	総務省 電子調査表	実態調査データ
44		→	e-TAX	源泉徴収票データ
45	文書管理システム	←	契約管理システム	原義文書データ
46		←	電子決裁システム	職員データ
47		←	電子決裁システム	文書(決裁対象・回覧対象)データ
48	電子決裁システム	←	人事給与	職員データ
49		→	文書管理システム	文書(決裁対象・回覧対象)データ
50		→	財務会計システム	決裁データ
51	グループウェア	←	人事給与システム	職員データ

【内部情報系基盤システム賃貸借】

参考明細書

項番	摘要	単価	数量	単位	金額(円)	備考
1	共通基盤		60	ヶ月		
2	ウイルス対策		60	ヶ月		
3	共有フォルダ		60	ヶ月		
4	資産管理システム		60	ヶ月		
5	二要素認証システム		60	ヶ月		
6	LGWANメール		60	ヶ月		
7	LGWANサーバ		60	ヶ月		
8	データセンター(クラウドサービス利用料含む)		60	ヶ月		
9	回線費用		60	ヶ月		
10	その他費用		60	ヶ月		
合計						
消費税(10%)						
合計(税込)						