

仕 様 書 (リース、レンタル用)

総合企画局デジタル化戦略推進室
(担当 富田、三田 電話 222・3257)

件 名	ファイル共有システム一式賃貸借
契 約 期 間	令和9年10月1日～令和14年9月30日
契 約 条 件	<p>1 支払方法 年度払い。ただし、端数が生じた場合は初回支払に含めるとともに、初年度支払は6か月分、最終支払は6か月分とすることから、支払金額については以下のとおり。</p> <p>(1) 令和9年度 契約金額の60分の6及び端数。</p> <p>(2) 令和10年度～令和13年度 契約金額の60分の12（小数点切り捨て）。</p> <p>(2) 令和14年度 契約金額の60分の6（小数点切り捨て）。</p> <p>2 期間満了後の物件の取扱い 業者引取り ・ 本市無償譲受け</p> <p>3 保守管理 含む ・ 含まない 詳細については、詳細仕様書参照</p> <p>4 予算が減額された場合等の措置 この契約は、「長期継続契約」とする。</p> <p>(1) 京都市（以下「本市」という。）は、翌年度以降において当該賃貸借料に係る歳出予算の金額について減額又は削除があった場合は、この契約を解除することができる。</p> <p>(2) 前項の規定により、本市がこの契約を解除した場合において、この契約の賃貸借の対象となった物件に係る受注者（複数の事業者で構成する連合体が委託業務を履行する場合にあっては、当該連合体の全ての構成員をいう。）の取得費用及び付随費用の合計額が、既に本市が受注者に対して支払った賃貸借料を上回っていても、受注者は、その差額を本市に請求することはできない。</p> <p>(3) 受注者は、前項に定めるもののほか、第1項の規定により本市がこの契約を解除したために生じた損害の賠償について、本市に請求することはできない。</p> <p>5 その他 別紙の「データセンターラック詳細」及び「京都市情報セキュリティ対策基準」は契約課で交付する。</p>

注 本仕様について不明な点がある場合は、契約課の指示に従ってください。

ファイル共有システム一式賃貸借 詳細仕様書

京都市総合企画局デジタル化戦略推進室

目次

1	概要	- 1 -
(1)	件名	- 1 -
(2)	契約期間	- 1 -
(3)	目的	- 1 -
(4)	機器調達範囲と作業範囲	- 1 -
(5)	調達内容と納入納品物	- 1 -
2	システムの要件	- 3 -
(1)	機能要件	- 3 -
(2)	外部インターフェース要件	- 7 -
3	規模及び性能の要件	- 8 -
(1)	規模要件	- 8 -
(2)	性能要件	- 9 -
4	信頼性等の要件	- 9 -
(1)	信頼性	- 9 -
(2)	情報セキュリティ	- 10 -
(3)	拡張性	- 11 -
(4)	互換性	- 12 -
(5)	システム中立性	- 12 -
5	システムの稼働環境	- 12 -
(1)	全体構成	- 12 -
(2)	ハードウェア要件及びソフトウェア要件	- 12 -
(3)	ネットワーク接続要件	- 18 -
6	テスト要件	- 18 -
7	移行等の要件	- 18 -
(1)	データ移行	- 18 -
(2)	既存ファイル共有システムの回収	- 19 -
(3)	研修	- 19 -
8	保守の要件	- 19 -
(1)	データ移行	- 19 -
(2)	ハードウェア保守	- 20 -
(3)	ソフトウェア保守	- 20 -
9	実施体制等の要件	- 20 -
(1)	実施体制	- 20 -
(2)	管理方法	- 21 -
(3)	導入	- 21 -
10	制約条件	- 21 -
11	特記事項（著作権について）	- 21 -
(1)	著作権その他の権利の帰属	- 21 -

(2) 第三者が権利を有する権利の利用	- 21 -
(3) 本市に帰属しない著作物	- 21 -
12 留意事項	- 21 -
(1) 業務遂行方法	- 21 -
(2) 内容及び成果	- 22 -
(3) 成果物	- 22 -
13 用語の説明	- 22 -

1 概要

(1) 件名

ファイル共有システム一式賃貸借

(2) 契約期間

令和 9 年 10 月 1 日から令和 14 年 9 月 30 日まで

(3) 目的

本市では、平成 18 年度からファイル共有システムを利用しているが、令和 4 年度に更新したシステムの耐用年数を迎える。また、働き方改革や DX 推進対応等によるファイル共有システムの利用拡大から、保存容量やファイル数の増加、セキュリティリスクに対応する必要がある。

本調達においては、老朽化したシステムの更新に併せて、以下ア～ウの対応を図ることを目的とする。

ア データ損失が発生せず短期間でデータ移行を行うこと。

イ 導入したファイル共有システムが一体的に運用管理できること。

ウ ランサムウェア対策を講じること。

(4) 機器調達範囲と作業範囲

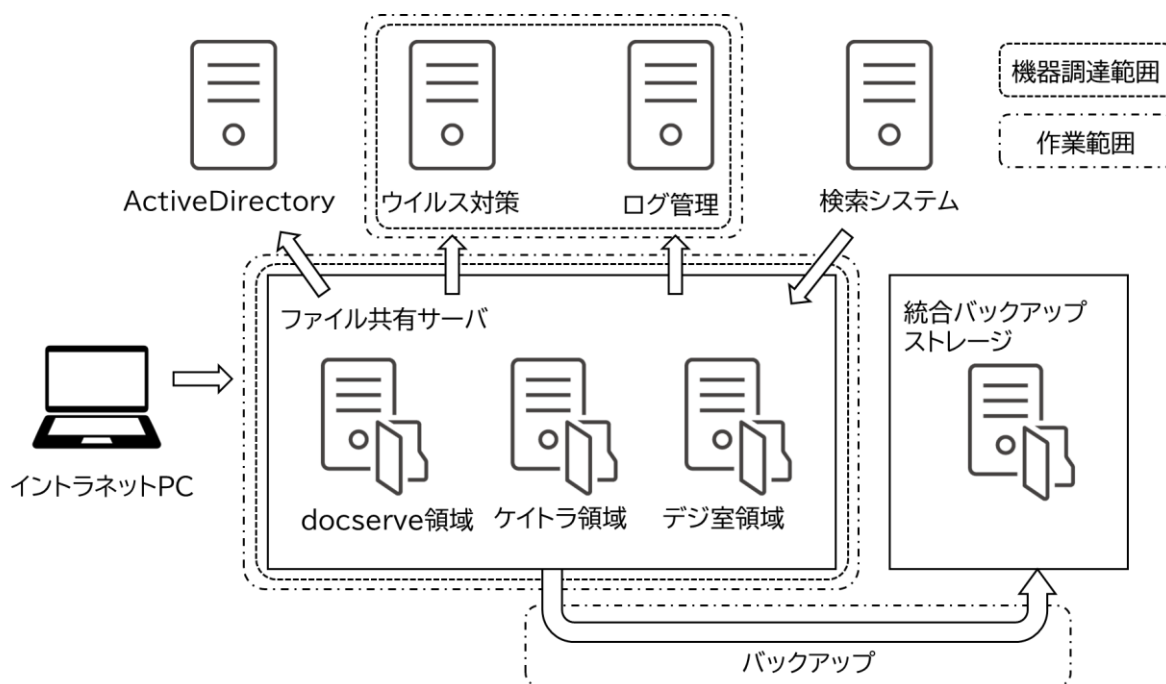


図 1：機器調達範囲と作業範囲

(5) 調達内容と納入納品物

ア 調達内容

- (ア) ハードウェア一式（保守込）
- (イ) ソフトウェア一式（保守込）
- (ウ) ライセンス一式

- (エ) ファイル共有システムの構築
- (オ) 機器の設置及び設定（ネットワーク機器設定を含む。）
- (カ) 既存システムからのデータ移行
- (キ) ファイル共有システム全体の動作確認
- (ク) 旧機器のデータ消去、ラックからの取外し及び回収、本市の指定する場所に保管
- (ケ) 納品物の作成及び納入
- (コ) 操作方法の引継ぎ（研修会の実施）

イ 納品物

- (ア) 納品物の納入とその時期

納品物は以下のとおりである。納入時期については、京都市の指定する時期とする。

No	納品物	内容
1	ハードウェア一式	ファイル共有システムを構成する機器
2	ソフトウェア一式	ファイル共有システムを構成するソフトウェア一式
3	ライセンス一式	保証書、ライセンス証書（又はそれに代わる資料）
4	業務実施計画書	業務の目的、実施体制、実施内容、スケジュール、管理方法等を実施計画としてまとめたもの。
5	WBS	必要作業を細分化したもの。WBS は作業項目の明確化とともに、スケジュール管理、工数の割り出しを行うため、作業項目にスケジュール及び工数を併せて記載したもの。
6	システム構成図	システム全体の構成を記載した図面
7	基本設計書 （外部設計書）	実装すべき機能、画面操作や入出力に関する事項、生成及び保管されるデータの概要等、基礎的な事項をまとめたもの。
8	詳細設計書 （内部設計書）	基本設計書で定められた内容を実現するために、プログラムやシステムとして、それをどう実現するかを具体的に定める。機能別の設計書や内部プログラムの使用など、技術的な事項をまとめたもの。
9	設定書	各機器への設定情報をまとめたもの
10	導入機器一覧	本調達で導入した機器の一覧。本市所定の様式で作成し、一覧には、障害発生時の連絡に必要な保守コード等の情報を含めること。
11	テスト計画書	構築したシステムの品質を検査するために実施する試験の内容について定義したもの。
12	テスト仕様書兼結果報告書	テスト環境に関する仕様書及びテストの結果報告
13	移行計画書	既存システムから新システムへ移行する手順、方法等をまとめたもの。
14	移行結果報告書	移行計画書に基づき実施した移行作業の結果をまとめたもの。

15	研修計画書	システムの操作方法等について、ネットワーク運用業者に対して操作手順書を元に実施する研修の内容、方法をまとめたもの。
16	ラック搭載図	機器をラック搭載した場合の図面。図面様式については、本市が準備している様式を利用すること。
17	電源接続図	機器の構築に必要な電源等の配線図をまとめたもの。
18	操作手順書及び運用手順書（システム管理者用）	システム管理者用の操作手順書及び運用マニュアルをまとめたもの。
19	操作手順書及び運用手順書（一般利用者用）	一般利用者用の操作手順書をまとめたもの。
20	障害対応マニュアル	障害時における復旧手順等についてまとめたもの。

納品物については、内容等について本市と事前に協議し、協議内容が反映されていることの確認を受けること。

(イ) 納入方法

ドキュメント等の納品物については、当該納品物を記録した DVD-R 等の媒体で 2 部を納品すること。データについては Microsoft 365 以降で編集できること。なお、付属マニュアルや取扱説明書、ライセンス等は PDF 化すること。

(ウ) 納品場所

本市総合企画局デジタル化戦略推進室が指定する場所とする。

(エ) 納品期限

契約開始日までに、機器設置、構築、テスト等を完了し、利用可能な状態にすること。

(オ) 納入完了後の納品物の修正

受注者は契約期間中において、納品したドキュメントに修正の必要が発生した場合、原則として修正後の全編を提出すること。

(カ) リース満了後の対応

リース満了後、受注者にて機器設定等のデータ消去を行い、引取りを行うこと。また、消去を行った日時、担当者名及び処理内容を記録した、データ消去作業完了証明書を本市に提出すること

2 システムの要件

(1) 機能要件

ア ファイル共有機能

(ア) クライアントパソコンに対してネットワーク経由でファイル共有機能を提供すること。

(イ) クライアントパソコンのデスクトップ上のアイコンからファイル共有システムへアクセスできること。

※ クライアントパソコンへのファイル共有システムのアイコン配布については、調達の

範囲外である。

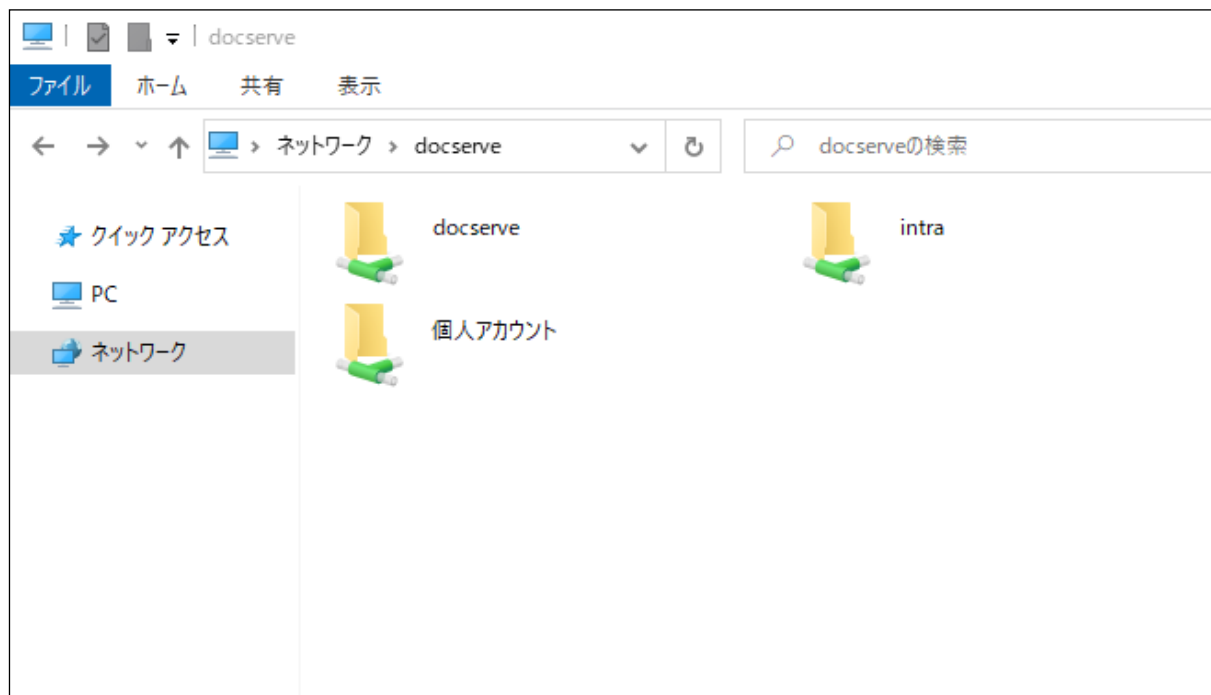


図 2：クライアントパソコン上のアイコンイメージ

- (ウ) 現在、ファイル共有システム (docserve) では、「free_space (所属等の共有フォルダ)、account (個人フォルダ)、intra、~SnapShot (バックアップ)」の各フォルダを利用している。

なお、クライアントパソコンのデスクトップ上のアイコン(¥¥docserve へのリンク)から「docserve フォルダ、個人フォルダ、intra フォルダ」にアクセスできるようにすること。

【参考】フォルダ名称と機能

フォルダ名称	機能
free_space	全庁、局及び課の共有フォルダ。共有の範囲によって、対象者の誰もが閲覧、編集、保存、削除が可能。docserve フォルダの配下にすべての free_space フォルダが配置される。free_space フォルダへのアクセスは利用者にて行う。
account	個人フォルダ用。対象の個人のみがアクセス可能
intra	利用者用ヘルプデスクのツールフォルダ。閲覧可。編集、保存、削除は不可
~SnapShot	スナップショット用のバックアップフォルダ。保存、編集、削除は不可 (隠しフォルダ)

- (エ) 必要時応じて、異なる AD に参加可能なファイル共有 (仮想のファイルサーバ) を 512 以上構成できること。

イ ミラーリング機能

ミラーリング機能は、ストレージの設定及びユーザーデータを別領域へ保存することでシステムの可用性及び信頼性を高めることを目的とする。

- (ア) ミラーリングはユーザが利用する領域とは異なるコントローラ・ディスク装置に行うこと。
- (イ) ミラーリングを実行するスケジュールの設定機能を有すること。
- (ウ) 2回目以降のミラーリングについては、データ差分ブロックのみを反映し、ネットワーク負荷を最小限に抑えること。
- (エ) ミラーリング時に重複排除、圧縮の効果が失われずにデータの転送ができること。
- (オ) ミラーリング時に暗号化通信を利用してデータを転送できること。また、セッション単位あるいはノード単位で帯域制御ができること。
- (カ) 本番領域と異なるディスクタイプ間でも問題なくミラーリング設定できること。
- (キ) ユーザが利用する領域に障害が発生した場合、ミラーリング領域を利用する機能を有していること。
- (ク) ユーザが利用する領域からミラーリング領域への切替えについては、運用管理者が切り替え操作で行えること。
- (ケ) ミラーリングは1ボリュームを複数ボリュームにミラーする Fan-Out 構成やカスケード構成など柔軟に構成できること。また、関連する一連のボリュームのデータとともに、そのボリュームに関連する設定情報や構成情報もバックアップ機へミラーリングできること。
- (コ) バックアップ機にて運用が発生した場合、本番機が復旧すれば、初期同期ではなくバックアップ機での更新差分のみを本番機にミラーリングし、短時間でデータの同期が図れること。
- (サ) バックアップ機は AWS や Azure、Google Cloud などのパブリッククラウド上に構築することが可能であること。

ウ スナップショット機能

スナップショット機能は、バックアップイメージの取得及びユーザレベルでのファイルリカバリの実現により利便性を高めること及び管理者業務負担の軽減を目的とする。

- (ア) ドラックアンドドロップ等の簡易な操作で、ユーザ自らデータの復元を行える機能を有すること。(直観的に操作することが可能である GUI (Graphic User Interface) であること。)
- (イ) スナップショットを取得するスケジュールの設定機能を有すること。スケジュールの設定については、時刻指定、日次、週次の単位での設定を行えるものとする。また、14世代以上の世代取得が行えること。
- (ウ) スナップショットを用いたデータの復元については、ボリューム単位での復元およびファイル単位での復元をそれぞれ行えること。なお、ボリューム単位での復元を行った場合はスナップショット取得時点の状態への一括ロールバックとなる。また、フォルダ単位での復元については、標準機能の範囲では原則として提供しないものとする。

エ クォータ管理機能

- (ア) 「free_space」、「account」、「intra」フォルダにおいて、個人及び課単位に容量制限を設定することができる。また設定された容量制限を超えるデータの書込みを行う場合、書込みを拒否することができる。

- (イ) 「free_space」フォルダにおいて、クォータ管理ができること。

オ ボリューム設定機能

- (ア) ボリューム容量の拡張だけでなく、縮小もシステムの利用を継続した状態で可能であること。
- (イ) 未使用領域を散在させずに、効率的な容量の割当てが行えること。

カ リモート通報機能

ハードウェア及びソフトウェアの異常及び障害予兆が発生した場合に、登録した宛先へ自動的に e-mail を発信する機能を有すること。

キ 管理機能

- (ア) Web ブラウザによってアクセスする管理インターフェースを有すること。アクセスには管理者用の ID・パスワードによってログインできること。
- (イ) 管理インターフェースは日本語表記に対応していること。
- (ウ) 管理インターフェース上からは、状態の監視（CPU の使用状況、ファイル共有システムの容量利用状況、トラフィック等）、ファイルシステムの作成及び拡張、クォータの設定等が行えること。
- (エ) 管理インターフェース上からスナップショットの作成が行えること。
- (オ) GUI については、管理者が容易に理解しやすいものであること。
- (カ) SMTP ベースの監視ツールを装備していること。定期的にシステムの状態を送信したり、重大なシステム・イベントが発生したりしたときに警告を送信できること。
- (キ) 一定期間（例：1 か月）アクセスがないデータの総容量を検出できる機能を有すること。
- (ク) 導入したストレージシステムのシステム情報を、AI/機械学習/集合知を元に分析（性能、ベストプラクティスに沿った構成情報の比較、リスク分析）し、可視化した SaaS 型サービスが無償で利用できること。またこのサービスは日本語に対応していること。

ク 重複排除機能

- (ア) ファイル共有システムの容量の効率的な活用のため 4K 以下ブロック単位のインライン及びバックグラウンドの重複排除機能を有していること。
- (イ) スケジュールの設定機能を有すること。スケジュールの設定については、時刻指定、日次、週次の単位での設定を行えるものとする。

ケ 圧縮機能

- (ア) ファイル共有システムの容量の効率的な活用のためインライン及びバックグラウンド圧縮機能を有していること。
- (イ) 重複排除機能と圧縮機能の適用については、任意の組合せにて利用できること。

コ コンフィグバックアップ機能

クラスタおよびノード構成の設定情報を取り出せる仕組みを有すること。また、ファイル共有システム一部の設定情報に変更があった場合も、システム全体の設定情報を取り出せる仕組みを有すること。

サ コンフィグリストア機能

コンフィグバックアップ機能により取得した設定情報を利用して構成を復元する仕組み

を有すること。

シ ローカルバックアップ機能

(ア) バックアップの範囲

ファイル共有システムに保存されている全てのデータを、統合バックアップストレージを対象にバックアップすること。

(イ) バックアップの取得方法

ネットワーク帯域の有効活用の観点から、バックアップストレージへの転送は、初期転送完了後には差分ブロックのみの転送が可能で、最小 1 分単位で転送時間の設定が可能であること。

(ウ) バックアップの運用方法

転送時間のスケジュール設定が可能なこと。

ス リストア機能

ローカルバックアップ機能で取得したデータを利用してファイル共有システムのデータの復元が可能なこと。

セ ウイルス検索機能

(ア) ストレージと連携し、ユーザが閲覧、編集、保存、削除した際にウイルス検索ができること。

(イ) ウイルス検知時に、対象ファイルを自動的に隔離、削除できる機能を有すること。

ソ ログ監査管理機能

(ア) ストレージの監査イベントログを収集し、アクセスログに分析・変換できること。

(イ) ログの自動圧縮機能を有し、ログを 1 年間分以上保管が可能となること。

(ウ) アクセスログの分析結果をレポート出力できること。

(2) 外部インターフェース要件

ファイル共有システムで提供されるフォルダへのアクセスについては、本市で管理する Active Directory のユーザ情報を用いて制御するものとする。

なお、「free_space」フォルダにおいても、アクセス制限の制御を行えるようにすること。

No	処理	連携システム	方法	頻度
1	ファイル共有システムアクセス	Active Directory	Active Directory に登録されているユーザ情報を元にファイル共有システムへのアクセス制御を行えること。	随時
2	人事異動	Active Directory	Active Directory に新たに登録されたユーザに対してファイル共有システムへのアクセス制御を行えること。 新たに登録されたユーザについては、Active	週次（随時） 人事異動（年 3 回程度）

			Directory の情報を元に個人フォルダの作成を行えること。また、新たな所属の課フォルダの作成が行えること。	
--	--	--	--	--

※ 人事異動処理（随時）については、イントラネットユーザ登録を行っている。また、人事異動については、通常 4 月に 2 回（市長部局、交通局）、10 月に 1 回（消防局）行っている。

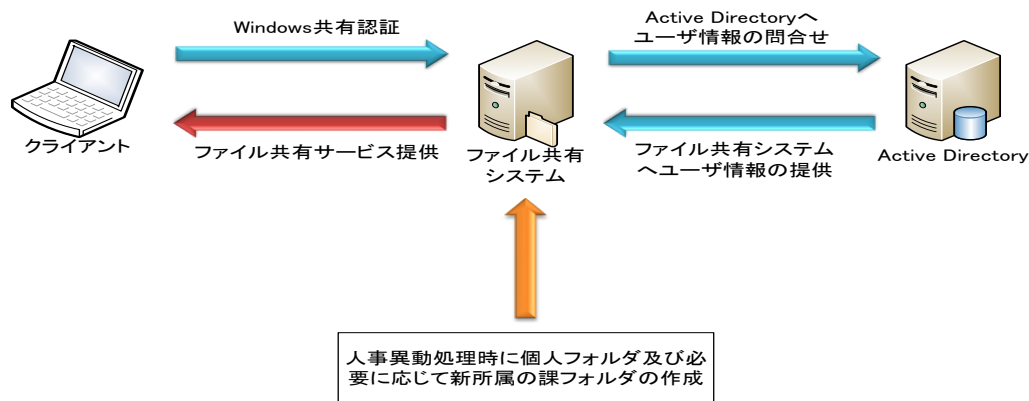


図 3：外部インターフェースイメージ

※ 人事異動時のフォルダ作成については、本調達の範囲外とする。ただし既存のファイル共有システムにある課フォルダ及び個人フォルダの作成については、本調達に含むものとする。

3 規模及び性能の要件

(1) 規模要件

ア 設置場所

京都市データセンターとする。京都市データセンターの住所は、受注者のみに連絡する。

イ 利用状況（令和 8 年 8 月時点）

(ア) 利用者数

利用者数 約 12,000 名

(イ) 利用場所

本庁舎エリア（分庁舎、西庁舎、北庁舎、消防庁舎含む）、区役所支所等（約 50 箇所）、出先機関（約 150 箇所）

(ウ) 使用容量

既存ファイル共有システム 約 36TB

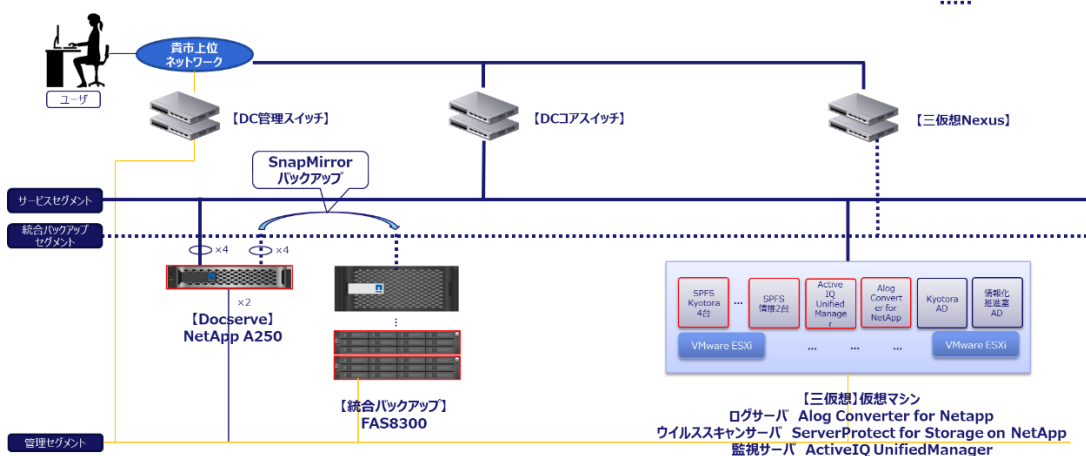
ケイトラサーバ 約 4TB

デジタル化戦略推進室管理ファイル共有システム 約 2TB

ウ 既存システム構成

既存ファイル共有システム、ケイトラサーバ及びデジタル化戦略推進室管理ファイル共有システムについて、システム確認、打合せが必要な場合、本市を通じて対応及び協議を行うこと。

- ・ミラーリング機能（Snap Mirror）を使用して Disk-to-Disk のバックアップを実施
- ・ログ監査管理サーバはクライアントからのアクセスログを収集する。
- ・ネットワークスイッチは冗長構成でデータセンター内の京都市ネットワークに接続



(2) 性能要件

All Flash ストレージ構成とすること。また、ストレージ OS の標準機能により、仮想ストレージ、ボリューム、LUN、ファイル単位で処理性能の上限（IOPS またはスループット）を指定でき、ボリューム、LUN、ファイル単位で処理性能の下限 IOPS を指定できること。また、それぞれオンラインで変更できること。

(1) 信頼性

- (ア) 最大 99.9999%の可用性を実現できるハードウェアであり、システムを構成する主要コンポーネント（コントローラ、ディスクドライブ、電源、ファン等）を冗長化構成とすること。また、主要コンポーネントに障害が発生した場合には、システムの利用を継続した状態で保守が可能であること。オンラインでストレージコントローラを変更できること。
- (イ) ファイル共有ストレージのディスクドライブについては、RAID 技術を使用してデータ保護を図ること。RAID 構成についてはディスクの二重障害に耐える方式を採用すること。ただし、RAID 技術を未採用の場合は、筐体間でのデータの冗長化を図る等ディスクの二重障害に耐える方式と同等以上のデータ保護レベルを確保すること。
- (ウ) 速やかにシステムを正常な状態に移行するため、RAID グループに対するホットスワップ機能を有すること。DISK 障害復旧（障害の発生したディスクの交換）時にスペアディスクの切り戻し作業・処理が発生しないこと。

(エ) ディスク障害時のリビルドの影響は自ノードのみに限定されること。

イ 機密性

(ア) アクセス制限

本市で管理する **Active Directory** に登録されたユーザ情報をもとにアクセス制限を実現すること。

(イ) アクセスログの取得

アクセスログを収集し、ログ分析、レポート出力する機能を有すること。

(2) 情報セキュリティ

システムの構築に当たっては、情報セキュリティ対策として市場に認知されている必要最低限の対策については、全て網羅し、『【別紙】京都市情報セキュリティ対策基準』を順守し、本市が要求する情報セキュリティ水準を満たすとともに、以下の対策を講じること。

ア 構築時点の技術で実現可能な対策を現実的な方法で行うこと。

イ ネットワーク稼働時点での必要な機能に加えて、稼働期間全体に渡っての継続的なレベルアップ（セキュリティパッチ等を遅滞なく適応することができる等）が可能であるネットワーク構成にすること。

ウ ネットワークの構築及び機器並びにソフトウェア保守においても、受注者は十分な情報セキュリティ対策を行うこと。また、運用面での対策が必要な場合、ネットワーク運用管理者への引継ぎを行うこと。なお、引継ぎに掛かる費用については、受注者負担で行うものとする。

エ 導入機器に搭載されているソフトウェア（オペレーティングシステム含む。）について、ネットワークの稼働までに発見されている脆弱性等に関して、適切な処置を行うこと。

オ 機器を運用するために必要となるアカウントを作成し、パスワードによる認証を行うこと。

カ 管理者権限を持つ ID、パスワードは、本市と協議の上、デフォルト以外のものを設定すること。また、管理者権限が存在する場合には、管理者権限と同じパスワードを利用者権限のパスワードとして設定してはならない。

キ 機器へのログイン、障害記録等の状況を把握するために必要なログを取得すること。

ク システム及びデータのバックアップが取得でき、システム及びデータの復旧を可能とすること。

ケ ファイルサーバアクセスユーザ認証方法

ユーザ認証については、本市で管理する **Active Directory** のユーザ情報を用いて認証するものとし、**Active Directory** のドメインログオンを行った端末からファイル共有システムへシングルサインオンを行うこと。

なお、**Active Directory** の OS については、**Windows Server 2019** である。

※ ユーザ認証については、**Active Directory** の管理事業者と十分な打合せを行うこと。

コ ウイルススキャン

ストレージ用ウイルス対策ソフトを導入して、リアルタイム並びに保存データのウイルス対策を実施すること。

サ 暗号化キー管理

外部サーバー等を必要とせず、ストレージ自身がデータの暗号化キー管理機能を有していること。

シ 暗号化

暗号化専用ディスク及び外部装置を使用せず、ボリューム単位もしくは RAID を束ねたストレージプール単位でデータの暗号化をストレージ OS の標準機能のみで実施できること。また、該当筐体以外ではデータの読み取りができない機能を有すること。

ス データ完全消去機能（DoD 方式）

ストレージ OS の標準機能として、正常に読み取りが可能なディスク内のデータを完全消去できること。データ消去の方式は米国国防総省方式（DoD5220.22-M）等に準じて、書き込むデータパターンと書き込み回数を指定して実施できること。

セ データ消去協議会加盟

データ消去の技術については、データの適正な消去のあり方を調査・研究し、その技術的な基準を策定している協議会に加盟しているストレージであること。

ソ ファイルスクリーニング

ストレージ OS の標準機能により、拡張子で書き込みをブロック可能とするファイルスクリーニング機能を有すること。

タ ランサムウェア自律検知・自動スナップショット

インターネットに接続せずストレージ本体の機能でユーザのファイルアクセスパターンを機械学習により分析し、ランサムウェア攻撃を示す可能性のある異常な動作をリアルタイムで検知できること。また、管理者へのアラート送信および自動的なスナップショット取得によりその時点の最新データを保護できる機能を有すること。

チ ストレージ管理ユーザ認証方法

マルチファクタ認証（2 段階認証）によるセキュリティ強化とシングルサインオンに対応でき、SAML（Security Assertion Markup Language）によるマルチファクタ認証を構成できる機能を有すること。

ツ ファイルアクセス制御

ファイルの作成、削除、リネーム、アクセスを監視し、特定拡張子の保存禁止やランサムウェア対策を実現できること。また、ネイティブ FPolicy では外部サーバ不要で拡張子ベースのブロックが可能であること。

(3) 拡張性

ア ストレージのディスク装置にハードディスクドライブの追加を行う際に、システムを停止させず、システムの利用を継続した状態でハードディスクドライブの増設が可能であること。ハードディスクドライブの増設については 1 本単位で行うことができ、ハードディスクドライブ追加の際、パリティの再配置によるパフォーマンス劣化が起らないこと。また、ディスク装置の追加についても容易に増設を行うことができること。

イ 何らかの要因で、ボリュームの使用状況にバラつきが出てきた場合、業務を中断することなくボリュームの拡張・縮小ができ、解放された領域を別ボリュームにて使用できること。

ウ ノードを追加することで、サービスを継続した状態で必要容量と処理能力の拡張が可能であること。

エ 異なる世代・モデルのストレージコントローラが混在した状態で、一つのストレージクラスターとして運用管理が可能なこと。

オ モデル・世代の異なる複数のストレージコントローラにまたがって 1 つのボリュームを作成できること。

カ ストレージ OS の標準機能にて、老朽更新対応時などにサービス停止を伴わず物理的なデータの格納場所を移動できること。

(4) 互換性

以下のイントラパソコンで動作すること。また、新たなバージョンに対しても互換性を求めるものとする。

項目	名称
OS	Microsoft Windows 11
ブラウザ	Microsoft Edge (Chromium 版)
	Google Chrome

(5) システム中立性

ア 構築事業者依存することがないように、可能な限り一般的な技術を用いること。

イ 本システムの構築に当たっては、特定の事業者が所有する特許技術に依存せず、他の事業者がシステムの保守及び改修を引き継ぐことが可能な構成とすること。

ウ 上記ア及びイについて、本市が認めた場合は、この限りではない。

5 システムの稼働環境

(1) 全体構成

システム一覧（設置場所、保守対応等）は、下記表のとおりである。

表 1：システム一覧

No.	項目	単位	設置・納入場所	保守対応
1	ファイル共有システム	1 式	データセンター	24 時間 365 日
2	ウイルス対策システム	1 式		平日 9 時～17 時
3	ログ監査管理システム	1 式		

※ 1 ハード保守対応についてはオンサイト保守とする。

※ 2 令和 9 年 10 月 1 日の契約開始から 5 年間のハード保守が可能な製品を納入すること。

※ 3 構築から契約開始までの間のハード保守についても、受注者で負担すること。

(2) ハードウェア要件及びソフトウェア要件

ア 基本項目

項目	要件
全体構成	EIA 規格（TIA/EIA-310-D 規格）の 19 インチラック(42U)に搭載可能であり、全体の構成として 4 U 以内に収めること。 データセンターで利用できるラックの仕様及び電源容量については、別紙_データセンターラック詳細を参照。

	※EIA 規格 (TIA/EIA-310-D 規格) の 19 インチラック (42U) については、調達の対象外とする。
--	---

イ ファイル共有システム

項目	要件
ファイルサーバ	<ol style="list-style-type: none"> 1 NAS (Network Attached Storage) 専用機器であること。 2 Active-Active の HA 構成で運用が可能であること。 (Active-Standby は不可)
CPU、メモリ、IO モジュールスロット	<ol style="list-style-type: none"> 1 ECC128GB 以上のメモリを搭載できること。(既存 128GB) 2 不揮発性メモリ (NVRAM) を 16GB 以上有し、電源、その他障害時に書き込みデータを保護する機能を有すること。(既存 16GB) 3 停電が発生した場合、不揮発メモリの内容を永続的なストレージに退避し、データの喪失を防ぐことができること。 4 2.10 GHz、8 コア以上の CPU を 2 個以上搭載できること。(既存 12 コア CPU を 2 つ) 5 将来的な拡張に備えて IO モジュール拡張スロットをコントローラあたり 4 スロット以上有すること。
ディスクドライブ	<ol style="list-style-type: none"> 1 ユーザが利用できる領域を構成すること。 2 ユーザが利用できる領域は、記憶媒体の二重障害に耐える方式で構成時の実効容量として 112TB 以上確保すること。 なお、この実効容量にはスナップショットの保存領域は含まないものとする。また、賃貸借期間中メーカーが容量保証する場合はストレージの効率化で得られる実効容量として算出できる。 3 ユーザが利用できる領域のスナップショットについては、ディスクの二重障害に耐える方式で構成時の実効容量として 37TB 以上確保すること。この実効容量には賃貸借期間中メーカーが容量保証する場合はストレージの効率化で得られる実効容量として算出できる。 ※ 必要に応じて、ディスクの三重障害に耐えうる機能・方式を有すること。 4 パリティディスク節約のために、1 RAID グループあたりの最大構成ディスク本数は、パリティディスクを含め 29 本以上で構成可能であること。 5 ディスクについては、NVMe の SSD を使用すること。 6 ストレージコントローラが搭載された筐体は 2U 以下の設置スペースであること、またストレージコントローラが搭

	<p>載された筐体内に 2.5 インチ SSD を 24 本以上搭載可能であること。</p> <p>7 オンラインでディスクシェルフを増設可能でインターフェースとして、コントローラあたり 12Gb SAS を 4 ポート以上増設可能であること。</p>
ネットワークインターフェース	<p>1 サービス用として 25Gbps 以上のポートを 8 ポート以上有すること。</p> <p>2 管理用として 1Gbps 以上のポートをコントローラあたり 1 ポート以上有すること。</p> <p>3 インターフェースは仮想化されており、物理ポート障害時には他の物理ポートに自動的に切り替わること。</p>
電源	<p>1 入力電圧 40-48V、100-120V、200-240V に対応可能であること。</p>
ファイルサーバ基本ソフトウェア (OS)	<p>1 セキュリティ上の観点から、独自専用 OS によるシステムとすること。Windows、Linux OS などの汎用 OS を使用した製品は不可とする。また、1 ストレージシステムで複数種の OS が搭載されている製品は不可とする。</p> <p>2 NAS 専用 OS は、ユーザ数に応じた必要ライセンスの購入の必要がないこと。(クライアントのライセンスが不要であること。)</p> <p>3 CIFS (Common Internet File System) 及び NFS(Network File System)version3 以上、S3 Object をサポートしていること。</p> <p>4 1 ストレージシステム内で複数の仮想ストレージを構成し、用途や利用者ごとに分割した運用管理が可能であること。</p> <p>5 ボリュームはストレージ全体の空き容量に依存することなく、実際の空き容量を超えたサイズであっても作成できること。</p> <p>6 将来の拡張性を考慮して、SMB1/2.x/3.x、NFS V3/V4、FC、iSCSI、NVMe、S3 Object を実装可能なユニファイドストレージであること。</p> <p>7 別の専用装置などを必要とせず、インライン及びスケジュールでのデータの圧縮・重複排除機能を有していること。</p> <p>8 容量効率化のためにストレージが管理するデータブロックサイズより小さなサイズのデータを、まとめて一つのブロックにインラインで格納する機能を有すること。</p> <p>9 ODX (Offload Data Transfer の略・"オフロードデータ転送") をサポートすること。ファイルコピーやゼロ埋めされ</p>

	<p>たファイルの作成をストレージ側でオフロード処理し、サーバおよびネットワークへ負荷をかけずに高速に処理可能なこと。</p> <p>10 一定期間アクセスがないデータを自動的に容量単価が低いオブジェクトストレージにオフロードできる機能を有すること。</p>
バックアップソフトウェア	<p>1 データの差分管理によるデータバックアップ(スナップショット機能)、装置間のデータ差分ブロックによるデータ複製機能を有していること。</p> <p>2 任意のボリュームの redirect on write 方式のスナップショットコピーを作成する機能を有すること。また、スナップショットを取得する際に稼働系に性能劣化を与えないこと。(copy on write によるスナップショットコピーは性能劣化が想定されるため提案は不可能とする。)</p> <p>3 仮想ボリューム単位で 1000 世代以上のスナップショットが作成できること。(ボリュームの特定の瞬間を保存する機能を有すること。) スナップショットを作成している間もサービスの提供を継続して行えること。スナップショットはスケジュール機能等により自動的に作成できること。</p> <p>4 スナップショット領域が不足した場合、業務を中断することなく、スナップショット領域の拡張・縮小が可能であること。</p> <p>5 スナップショット領域を容量単価が低いオブジェクトストレージ等にオフロードできること。</p>

ウ ウイルス対策システム

別途提供する仮想化基盤上（OS まで提供）に構築すること。

項目	要件
ウイルススキャン	<p>1 ファイルの入出力を監視し、リアルタイムにウイルスの検出・処置が可能なこと。</p> <p>2 ウイルス定義ファイル・検索エンジンを自動的に最新のバージョンに保つ機能を有すること。</p> <p>3 ファイルタイプを正しく識別し、感染の危険があるとされるファイルだけを検索する機能を有すること。</p> <p>4 ウイルス検出時、ウイルスの種類別に設定された推奨される各種検索処理を利用できること。</p> <p>5 通常のウイルス発見通知のほか、一定時間内に大量のウイルスが発生した場合において通知するアウトブレイクアラート機能を有すること。</p> <p>6 新種ウイルスに対処する予防ポリシーファイルによって</p>

	<p>新種ウイルスの侵入を予防できること。</p> <p>7 スパイウェアの検出・処理が可能なこと。</p> <p>8 ウイルス・スパイウェア感染時の自動復旧ができること。</p> <p>9 ルートキット検出機能を有すること。</p> <p>10 過去1週間もしくは1ヶ月間など、指定した期間内の検知イベントをPDFレポート化して管理者に通知が可能なこと。</p>
--	--

エ ログ監査管理システム

別途提供する仮想化基盤上（OSまで提供）に構築すること。また、日本語によるサポートが提供可能なこと。

項目	要件
ログ収集、変換	<p>1 いつ、誰が、どの対象に、どのような操作を行ったかといった実際の操作に沿った形式のログを変換できること。</p> <p>2 ログ収集対象にエージェントをインストールする必要があること。</p> <p>3 複数のログ取得対象サーバのログを一元管理できること。</p> <p>4 ファイルアクセスログとして、「発生日時」、「サーバ名」、「ファイル/ディレクトリ名」、「READ」、「WRITE」、「DELETE」、「RENAME」以上のログが明示的に取得できること。</p> <p>5 ユーザからのアクセス履歴は成功履歴だけでなく失敗の操作履歴も取得できること。</p> <p>6 1日に収集可能なログ総量は20GB以上であること。</p>

ログ分析、レポート	<ol style="list-style-type: none"> 1 Web ブラウザによるログの閲覧が可能であること。 2 管理サーバ以外の PC からでも、Web ブラウザ上でログの閲覧が行えること。 3 保管したログを、ユーザ、期間、ファイル、操作等で検索ができること。またその検索結果を CSV や PDF 形式でレポート出力できること。 4 予め定義した不正な操作が行われたとき、または特定の操作ログに関してあらかじめ設定した閾値を超えた際に、管理者にアラート通知できること。 5 閲覧できるログの範囲を管理者ごとに指定できること。 6 日次、週次、月次など定期的にレポートを自動作成できること。 7 複数対象のログを横断検索できること。 8 ログのブラウジング機能があり、フィルタ設定、表示項目の設定が行えること。 9 作成したレポートを管理者にメール送信できること。 10 監視設定を容易に行える GUI およびテンプレートを製品内に備えていること。 11 閾値による検出のほか、過去のアクセス状況からの変化点や単語の相関等を解析し、リスクのあるアクセスを管理者に通知できること。
ログ保管	<ol style="list-style-type: none"> 1 ログデータは1年間分以上を保管できること。 2 変換したログについて、圧縮と削除設定が行えること。 3 ログをデータベースで管理する場合、外部ディレクトリに CSV 形式で保存が可能であり、併せてデータベースのログを自動でクリアする機能を装備していること。 4 暗号化してログを保管できること。 5 GUI からログの保管期間の設定変更ができること。 6 バックアップ用にログを複数個所に保管できること。 7 一定期間を経過したログは、データベースより自動削除ができること。また、自動削除のタイミングは月単位、年単位で可能なこと。 8 ログ管理用データベースはログ監査管理ソフトウェアに標準搭載されており、別途有償のデータベースソフトウェアを利用することがないこと。 9 保存するログのうち、直近一定期間分はデータベース形式で保存し、ログの検索を高速に行えること。なお、保存期間については本市と協議のうえ設定すること。

(3) ネットワーク接続要件

- ア ファイル共有システムを稼働させるためのネットワーク設計を行うこと。
- イ いずれの機器も、十分に設計を行ったうえで、設計方針等について、本市及び本市ネットワーク運用管理業者に説明を行い、承諾を得たうえで、機器の接続を行うこと。
- ウ 既存のネットワーク機器の設定変更が必要な場合は、当該設定変更作業を行うこと。受注者の責任において本業務を完遂できない場合は、本市ネットワーク運用管理業者との十分な調整を行い、対応を協議すること。これに要する全ての費用については、受注者の負担とする。
- エ データセンターから京都市役所(ファイル共有システム利用者)までの回線については、本市が準備するものとし、本調達には含まない。

6 テスト要件

ファイル共有システムの構築及び運用開始にあたり、必要と考えられるテストとその手法をテスト計画書として取りまとめ、本市の承認を受けた後にテストを実施すること。また、テスト結果は、テスト結果報告書として取りまとめ、本市の承認をうけること。

7 移行等の要件

(1) データ移行

- ア 既存のファイル共有システムに保存されているデータ全てを移行対象とすること。
- イ 移行対象データのウイルスチェックを行ったうえ、安全に移行すること。
- ウ 移行対象データのファイルのアクセス権限を継承すること。
- エ データの移行方法については、移行データ範囲、移行方法、移行手順等を取りまとめた移行計画書を事前に作成し本市の承認を受けること。データの移行イメージについては、下記のとおりとする。ただし、移行イメージよりも効率的でより安全・確実な方法がある場合は、事前に本市の承認を得たうえで、その方法で実施すること。
 - (ア) データ移行期間中は、既存ファイル共有システムを利用できること。
 - (イ) データ移行については、安全かつ確実にデータ移行を行うこと。
 - (ウ) データ移行期間終了後は、新ファイル共有システムを利用できること。
 - (エ) 統合バックアップストレージに保存してある既存バックアップデータを継続して利用できること。
 - (オ) 既存のストレージ内に保存されているデータについては、ボリューム単位で安全かつ確実に移行できること。移行作業中もクライアントからのアクセスを継続でき、移行完了時には短時間のカットオーバー処理により移行を完了できること。また、当該移行作業についてメーカーサポートを受けられること。
 - (カ) 既存ファイルサーバに保存されているデータのうち、ファイルパスの長さ等、ファイルシステムの仕様上の制限に起因して Windows エクスプローラから操作できないファイルの移行についても、受注業者にて移行作業を行うこと。

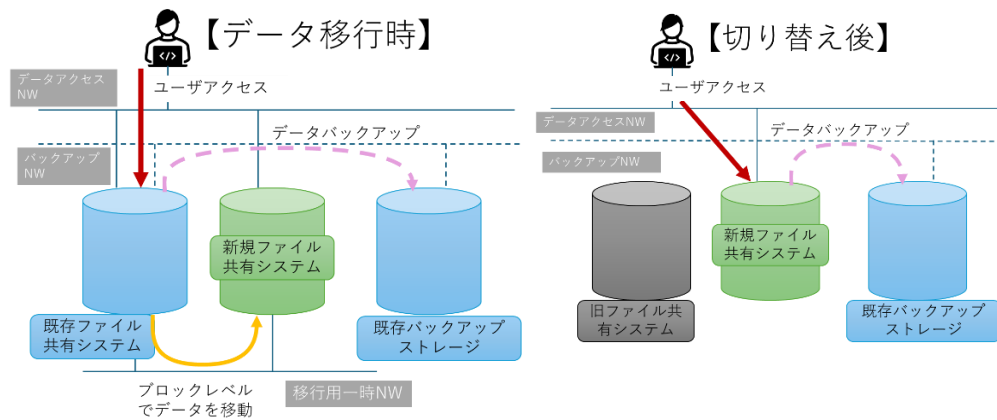


図5：移行方法イメージ

オ データ移行を実施するにあたり、既存のファイル共有システム導入業者又は現システム運用管理業者との打合せが必要な場合、本市を通じて対応及び協議を行うこと。また、既存ファイル共有システムに何らかの設定変更作業等が必要な場合、変更内容を提示すること。また、これに要する全ての費用については、受注者負担とすること。

カ データ移行を実施するにあたり、既存のファイル共有システムの停止をする場合は、日程等の協議を行い、事前に本市の承認を受けること。（原則、平日夜間及び休日のみ停止可能である。）

キ データの移行が終了した段階で、移行結果報告書を作成し、本市の承認を受けること。

ファイルレベルで移行する場合は、移行前後の容量、ファイル数、フォルダ数を含めた移行結果報告書を作成すること。

ク 次期ファイル共有システムへのデータ移行の際に、本市担当者及びファイル共有システム運用管理業者等と打合せを実施し、安全かつ確実にデータ移行が行えるよう必要な支援を実施すること。

(2) 既存ファイル共有システムの回収

データ移行完了し、安定稼働を確認後、既存ファイル共有システムのデータを消去の上、消去証明書を発行し、ラックから取外した機器を本市の指定する場所に保管すること。

(3) 研修

ア ファイル共有システムの操作説明のため、ネットワーク運用業者を対象とした研修を1回以上、必要に応じて実施すること。

イ 研修の実施時期、会場、研修用環境の構築については、本市担当者と事前に協議を行うこと。

ウ 研修テキストは操作手順書をともに行うこと。

エ 研修後も不明点等ある場合は、電話やメール（必要に応じて打合せ等）を通じて、不明点等の解決のために支援等を行うこと。

8 保守の要件

(1) データ移行

ア 保守範囲については、本調達の全てのハードウェア及びソフトウェア（オペレーティングシステムへのプログラムプロダクト保守を含む。）とする。なお、構築期間中のハードウェア及びソフトウェア保守についても本調達に含むものとする。

イ 複数業者による保守業務の煩雑さを考慮し、ネットワーク運用業者からの問合せ窓口は一覧化すること。

(2) ハードウェア保守

ア 機器に障害が発生した場合、本市担当者又はネットワーク運用業者からの連絡をもとに、速やかに技術員を派遣し、機器の修理又は取替えを行うこと。

イ 保守業務に必要となる交換部品等については、保守拠点等に常備している体制をとること。

ウ 障害発生連絡を受けてから技術員の派遣を行い、保守対象機器のもとへ 2 時間以内に到着できること。

エ ハードウェアに対して、年 1 回定期点検を行うこと。定期点検の実施時期及び内容については、事前に本市担当者の承認を受けること。

オ 統合バックアップストレージについては既存ストレージへの追加となるため、受注業者は統合バックアップストレージにおける保守移管を行うこと。移管に関しての取り決めは既存保守業者との調整とし、本費用に関する諸経費は本調達に含むこと。

(3) ソフトウェア保守

ア 本市担当者又はネットワーク運用業者からの連絡をもとに、稼働するソフトウェアの障害特定、分析及び解決の支援を行うこと。

イ ソフトウェア（オペレーティングシステムを含む。）の最新バージョンやパッチの提供、優先度・緊急性・影響を総合的に考慮した適用の可否、検証環境から本番環境への適応手順を含めて技術支援を行うこと。なお、適応作業については、ネットワーク運用業者が実施するものとする。

ウ 年 1 回、ストレージのオペレーティングシステムについては受注業者にてバージョンアップ作業を実施すること。

(4) 受付（対応）時間

ア ハードウェア保守

24 時間 365 日の受付窓口を設置し、オンサイト保守を実施すること。

イ ソフトウェア保守

平日 9 時～17 時までの受付窓口を設置し、保守対応を行うこと。ただし、前述の時間帯以外で、緊急の対応が必要となる障害が発生し、本市の業務に重大な影響を及ぼす場合は、事態收拾のため別途協議のうえ、速やかな対応を行うこと。

※ 平日とは、土曜日、日曜日、国民の祝日に関する法律に規定する休日、12 月 29 日～1 月 3 日以外の日とする。

9 実施体制等の要件

(1) 実施体制

ア 本市と同程度の規模（職員数もしくはユーザ数 10,000 名以上）の官公庁（国、都道府県又は地方自治法第 252 条の 22 第 1 項に定める政令による指定を受けた中核市以上の規模の地方公共団体）又はこれに準ずる一般企業等において、プロジェクトに参加した経験を有する者を 1 名以上含めること。

イ 本業務の実施に当たっては、プロジェクトの進行管理を適切に行うこと。

(2) 管理方法

ア プロジェクト管理

運用開始までに定期的に月 1 回以上定例会を行うこと。

イ 議事録

本市と定例会（簡易な打合せを含む。）を行った場合は、議事録を作成し 5 営業日以内に本市担当者へ提出を行うこと。（3 営業日以内に次回の定例会及び打合せがある場合は、次回定例会及び打合せまでに本市担当者へ提出を行うこと。）

ウ 構成管理報告

受注者はシステムを構成する全ての要素について最新の状態を把握すること。また、システムを構成する全ての要素について変更があった場合は、構成管理報告書の提出を本市担当へ行い、承認を受けること。

(3) 導入

ア 本市庁舎内（本市データセンターを含む。）において作業を実施する場合は、作業期間及び作業時間について事前に本市と協議すること。

イ 本市が承認した作業場所以外で業務を行わないこと。

10 制約条件

- (1) 作業の実施場所は、本市が指定し、又は許可した場所で実施しなければならない。
- (2) 本市のネットワークに外部から接続することはできない。
- (3) 本市のネットワークに、許可されていない端末を接続することはできない。
- (4) 既存のイントラネットとの連携については、正常な動作を確認し、本市担当者から承認を受けること。

11 特記事項（著作権について）

(1) 著作権その他の権利の帰属

本調達に係る業務を遂行するに当たって、新たに発生した納品物（市販の汎用アプリケーション等パッケージソフトに帰属する部分を除く。）の著作権その他権利については、本市に帰属させること。

(2) 第三者が権利を有する権利の利用

本調達の範囲内で、第三者が権利を有する著作物又は知的所有権等を利用する場合は、受注者の責任において、その権利の使用に必要な費用を負担し、使用許諾契約に係わる一切の手続を行うこと。

(3) 本市に帰属しない著作物

本契約の範囲内で、本市に帰属しない著作物がある場合にあつては、受注者は、本市に当該著作物の関連文書を納品物として納入するものとし、この関連文書についても上記(1)及び(2)に準じて取扱うこと。

12 留意事項

(1) 業務遂行方法

本業務は、本仕様書によるほか、本仕様書に定めのない事項については、本市と密な協議

を行い、その指示により実施する。

(2) 内容及び成果

本業務の内容及び成果については、受注者において充分審査のうえ実施し、又は報告する。

(3) 成果物

受注者は、本業務の内容、成果物について、本市の許可なく、他に公表、使用、譲渡、販売又は貸与してはならない。

13 用語の説明

用語	説明
ファイル共有システム	本市イントラネットに接続された端末からのみ利用可能なファイル共有システムのこと。Active Directory にて管理された Windows 系端末からアクセスするように設計されており、約 12,000 人のユーザの同時利用が可能である。
ケイトラサーバ	都市計画局専用に独立してボリュームを作成し、運用しているファイル共有システムのこと。KA_001 から KA_019 の 19 のボリュームに分けられている。

電子計算機の保守を含む賃貸借契約に係る共通仕様書

(総則)

- 第1条** この電子計算機の保守を含む賃貸借契約に係る共通仕様書(以下「共通仕様書」という。)は、電子計算機の保守を含む賃貸借において、情報セキュリティの確保など賃貸借契約の適正な履行を確保するために共通して必要となる事項を定めるものである。
- 2** 共通仕様書に定める内容と個別仕様書に定める内容との間に相違がある場合は、個別仕様書に定める内容が優先する。

(履行計画)

- 第2条** 賃貸人(複数の事業者で構成する連合体がこの契約を履行する場合にあっては、当該連合体の全ての構成員をいう。以下「乙」という。)は、この契約の履行に着手する前に、履行日程及び履行方法について京都市(以下「甲」という。)に届け出て、その承諾を得なければならない。
- 2** 乙は、甲がこの契約の内容を変更した場合に、履行日程又は履行方法を変更するときは、あらかじめ甲の承諾を得なければならない。乙の事情により、履行日程又は履行方法を変更するときも、同様とする。

(秘密の保持)

- 第3条** 乙は、この契約の履行により直接又は間接に知り得た個人情報及び秘密を第三者に漏らしてはならない。契約期間終了後又は契約解除後も、同様とする。

(目的外使用の禁止)

- 第4条** 乙は、次に掲げるものをこの契約の履行以外の目的に使用してはならない。
- (1) 賃貸物件
 - (2) 甲が乙に支給する物品(以下「支給品」という。)及び貸与する物品(以下「貸与品」という。)
 - (3) 契約の履行に関し作成された入出力帳票、フロッピーディスク、磁気テープ、磁気ディスク、光磁気ディスク、光ディスク、半導体メモリその他の記録媒体に記録された情報(賃貸物件に記録された情報及び甲が提供した情報を含む。以下「データ」という。)

(複写、複製及び第三者提供の禁止)

- 第5条** 乙は、賃貸物件、支給品、貸与品及びデータについて、複写し、複製し、又は第三者に提供してはならない。ただし、甲の書面による承諾を得た場合は、この限りでない。

(作業責任者等の届出)

第6条 乙は、この契約の履行に係る作業責任者及び作業従事者を定め、書面によりあらかじめ甲に報告しなければならない。これを変更するときも、同様とする。

2 作業責任者は、共通仕様書に定める事項を適切に実施するよう作業従事者を監督しなければならない。

3 作業従事者は、作業責任者の指示に従い、共通仕様書に定める事項を遵守しなければならない。

4 乙は、全ての作業責任者及び全ての作業従事者から共通仕様書に定める事項を遵守する旨の誓約書を徴し、甲から求めがあった場合は、これを甲に提出しなければならない。

(教育の実施)

第7条 乙は、全ての作業責任者及び全ての作業従事者に対して、情報セキュリティに対する意識の向上、共通仕様書において遵守すべき事項その他契約の適切な履行に必要な事項について、教育及び研修を実施しなければならない。

2 乙は、個人情報を取り扱うに当たっては、個人情報を取り扱う全ての作業責任者及び全ての作業従事者に対し、個人情報の保護に関する法律及び京都市個人情報保護条例の罰則規定を周知するとともに、個人情報保護のための教育及び研修を実施しなければならない。

3 乙は、前2項の教育及び研修を実施するに当たり、実施計画を策定し、及び実施体制を整備しなければならない。

(派遣労働者等の利用時の措置)

第8条 乙は、この契約を派遣労働者、契約社員その他の正社員以外の労働者に履行させる場合は、正社員以外の労働者に契約に基づく一切の義務を遵守させなければならない。

2 乙は、甲に対して、正社員以外の労働者の全ての行為及びその結果について責任を負うものとする。

(再委託の禁止)

第9条 乙は、この契約に係る義務の履行の全部又は一部を第三者へ委託（以下「再委託」という。）してはならない。ただし、甲の書面による承諾を得た場合は、この限りでない。

2 乙は、再委託する場合は、再委託の内容、再委託の相手方、再委託の理由等を付して書面によりあらかじめ甲に申請し、その承諾を得なければならない。

3 乙は、再委託する場合は、再委託の相手方にこの契約に基づく一切の義務を遵守させるとともに、甲に対して、再委託の相手方の全ての行為及びその結果について責任を負うものとする。

4 乙は、再委託する場合は、再委託の相手方との契約において、再委託の相手方を監督するための手続及び方法について具体的に規定しなければならない。

5 乙は、再委託する場合は、再委託先における履行状況を管理するとともに、甲の求めに応じて、その状況を甲に報告しなければならない。

(データ等の適正な管理)

第10条 乙は、賃貸物件及びデータの授受、処理、保管その他の管理に当たっては、内部におけ

- る責任体制を整備し、賃貸物件のき損、紛失、盗難等の事故及びデータの漏えい、滅失、き損、紛失、改ざん、盗難等の事故を防止するなどその適正な運営に努めなければならない。
- 2 乙は、この契約の履行に当たって使用する電子計算機室その他の作業場所（以下「電子計算機室等」という。）を定め、書面によりあらかじめ甲に報告しなければならない。これを変更するときも、同様とする。
- 3 乙は、甲の電子計算機室等を使用する場合は、甲に対しこの契約の履行に着手する前に、甲の電子計算機を使用する作業責任者及び作業従事者の氏名、作業内容及び従事期間を届け出なければならない。また、甲の電子計算機を使用しなくなった作業責任者及び作業従事者の氏名、理由を届け出なければならない。
- 4 乙の作業責任者及び作業従事者は、甲の電子計算機室等に入退室するときは、事前に甲の許可を受けなければならない。
- 5 乙は、第2項で定める乙の電子計算機室等について、外部からの侵入が容易でない場所に配置するとともに、地震、水害、落雷、火災、漏水等の災害及び盗難等の人的災害に備えて、必要な保安措置を講じなければならない。
- 6 乙は、第2項で定める乙の電子計算機室等について、次に掲げる入退室管理を行わなければならない。
- (1) 電子計算機室等に入室できる者を、乙が許可した者のみとすること。
 - (2) 入室を許可されていない者が電子計算機室等に入室することを防止するための必要な措置を講じること。
 - (3) 入室を許可された者が電子計算機室等に入室し、又は退室するときは、日時、氏名等を入退室管理簿に記録すること。
- 7 乙は、甲から賃貸物件及び契約の履行において利用するデータの引渡しを受けたときは、甲に受領書を提出しなければならない。
- 8 乙は、個人情報を取り扱うに当たっては、個人情報を適正に管理させるために、個人情報管理責任者を置かななければならない。
- 9 乙は、契約の履行のために入力機器、電子計算機及び記録媒体を使用するに当たっては、次に掲げる事項を遵守しなければならない。
- (1) 乙が許可した者以外の者が入力機器、電子計算機及び記録媒体を使用すること及びこれに記録されているデータを閲覧することがないように必要な措置を講じること。
 - (2) 入力機器、電子計算機及び記録媒体に、情報漏えいにつながると考えられる契約の履行に関係のないアプリケーションをインストールしないこと。
 - (3) 個人の所有する入力機器、電子計算機及び記録媒体を使用しないこと。
- 10 乙は、甲及び乙の電子計算機室等からデータを持ち出してはならない。ただし、甲の承諾を得た場合は、この限りでない。
- 11 乙は、甲及び乙の電子計算機室等からプログラム、データ等を電子データで持ち出す場合は、電子データの暗号化処理又はこれと同等以上の保護措置を施さなければならない。
- 12 乙は、賃貸物件及びデータの輸送、搬入出を自ら行わなければならない。ただし、甲の書面による同意を得た場合は、この限りでない。
- 13 甲は、データの全部又は一部の漏えい、滅失、き損、紛失、改ざん、盗難等による被害が生じ

た場合は、契約書第10条第1項第1号に該当するとして契約を解除することができる。賃貸物件のき損、紛失、盗難等による被害が生じた場合も、同様とする。

14 乙は、データの全部又は一部の漏えい、滅失、き損、紛失、改ざん、盗難等があったときは、甲の指定するところにより、代品を納め、原状に復し、損害（第三者に及ぼした損害を含む。以下同じ。）を賠償し、又は代品を納め、若しくは原状に復するとともに損害を賠償しなければならない。賃貸物件のき損、紛失、盗難等があったときも、同様とする。

15 乙はこの契約を履行するために賃貸物件の記録媒体の交換が必要となる場合は、交換により不要となった記録媒体は、記録されているデータを消去するなど復元不可能な状態にしなければならない。

（データ等の廃棄）

第11条 乙は、契約の履行が完了したとき、契約の内容が変更されたとき又は契約が解除されたときは、甲の指示に従い、データを廃棄し、消去し、又は甲に返還し、若しくは引き渡さなければならない。

2 乙は、前項の規定により、データの廃棄又は消去を行うに当たっては、次に掲げる事項を遵守しなければならない。

(1) 復元又は判読が不可能な方法により廃棄又は消去を行うこと。ただし、個人番号利用事務系（個人番号利用事務又は戸籍事務に関わる情報システムをいう。）の情報を取り扱っていた場合は、本市の承諾を受けない限り、物理的に破壊する方法により行うこと。

(2) 廃棄又は消去の際に、甲から立会いを求められたときはこれに応じること。

(3) 廃棄又は消去を行った後速やかに、廃棄又は消去を行った日時、担当者名及び処理内容を記録した証明書等により甲に報告すること。なお、甲から当該証明書等の提出期限の指定及び処理の証拠写真の提出を求められた場合には、これらに応じること。

（監督）

第12条 乙は、賃貸物件及びデータの管理状況並びにこの契約の履行状況について、甲の指示に従い、定期的に甲に報告しなければならない。

2 甲は、必要があると認める場合は、契約内容の遵守状況及びこの契約の履行状況について、いつでも乙に対して報告を求め、乙の電子計算機室等に立ち入って検査し、又は必要な指示等を行うことができるものとする。

（事故の発生のお知らせ）

第13条 乙は、賃貸物件のき損、紛失、盗難等の事故又はデータの漏えい、滅失、き損、紛失、改ざん、盗難等の事故が生じたときは、直ちに甲に通知し、その指示に従い、遅滞なく書面で報告しなければならない。契約期間終了後又は契約解除後も、同様とする。

2 乙は、賃貸物件のき損、紛失、盗難等の事故又はデータの漏えい、滅失、き損、紛失、改ざん、盗難等の事故が生じた場合に備え、甲その他の関係者との連絡、証拠保全、被害拡大の防止、復旧、再発防止の措置等を迅速かつ適切に実施するために、緊急時対応計画を定めなければならない。

- 3 甲は、賃貸物件のき損、紛失、盗難等の事故又はデータの漏えい、滅失、き損、紛失、改ざん、盗難等の事故が生じた場合は、必要に応じて当該事故に関する情報を公表することができる。

(支給品及び貸与品)

第14条 支給品及び貸与品の品名、数量、引渡時期及び引渡場所は、個別仕様書に定めるところによる。

- 2 乙は、前項に定めるところにより、支給品又は貸与品の引渡しを受けたときは、遅滞なく甲に受領書又は借用書を提出しなければならない。
- 3 乙は、支給品及び貸与品を善良な管理者の注意をもって保管しなければならない。
- 4 乙は、この契約の履行が完了したとき、契約の内容が変更されたとき又は契約が解除されたときは、個別仕様書に定めるところにより、不用となった支給品及び貸与品を、使用明細書を添えて甲に返還しなければならない。
- 5 乙は、故意又は過失により、支給品又は貸与品の全部又は一部を滅失し、又はき損したときは、甲の指定するところにより、代品を納め、原状に復し、損害を賠償し、又は代品を納め、若しくは原状に復するとともに損害を賠償しなければならない。

(検査の立会い及び引渡し)

第15条 甲は、契約書第5条第1項の検査に当たり、必要があると認めるときは、乙を検査に立ち合わせることができる。この場合において、乙が検査に立ち会わなかったときは、乙は、検査の結果について異議を申し立てることができない。

- 2 甲は、契約書第5条第1項の検査に当たり、必要があると認めるときは、賃貸物件を稼働させ検査することができる。この場合において、当該検査に直接要する費用は、乙の負担とする。
- 3 甲は、賃貸物件に障害が発生し、その障害の内容及び程度が当該情報システムの運用に重大な影響を及ぼすものであると判断する場合は、乙に対し、当該障害について報告を求めることができる。乙はこれに対し、甲が定める期間内に誠実に対応しなければならない。

(契約の解除)

第16条 甲は、乙が個別仕様書又は共通仕様書の内容に違反していると認めたときは、契約書第10条第1項第1号に該当するとして契約を解除することができる。

- 2 甲は、前項の規定により契約を解除したときは、乙に損害賠償の請求を行うことがある。
- 3 乙は、第1項の規定により契約の解除があったときは、甲にその損失の補償を求めることはできない。

(損害賠償)

第17条 乙の故意又は過失を問わず、乙が個別仕様書又は共通仕様書の内容に違反し、又は怠ったことにより、甲に損害を与えた場合は、乙は、甲にその損害を賠償しなければならない。

(契約不適合責任)

第18条 甲は、引渡しを受けた契約目的物が種類、品質又は数量に関して契約の目的に適合しないものであるとき（その引渡しを要しない場合にあっては、この契約に付随する業務が終了した時に当該業務の目的物が種類又は品質に関して契約の内容に適合しないとき）は、乙に対してその不適合（以下本条において「契約不適合」という。）の修正等の履行の追完（以下本条において「追完」という。）を請求することができ、乙は、当該追完を行うものとする。ただし、甲に不相当な負担を課するものではないときは、乙は甲が請求した方法と異なる方法による追完を行うことができる。

- 2 甲は、契約不適合により損害を被った場合、乙に対して損害賠償を請求することができる。
- 3 甲は、契約不適合について、追完の請求にもかかわらず相当期間内に追完がなされない場合又は追完の見込みがない場合で、契約不適合により契約の目的を達することができないときは、契約書第10条第1項第1号に該当するとして契約の全部又は一部を解除することができる。
- 4 乙が本条に定める責任その他の契約不適合責任を負うのは、契約書第5条第1項の検査に合格した日（契約に付随する業務にあっては、当該業務の一工程の履行が完了した日）から2年以内に甲から契約不適合を通知された場合に限るものとする。ただし、契約書第5条第1項の検査に合格した時点（契約に付随する業務にあっては、当該業務の一工程の履行が完了した時点）において乙が契約不適合を知り若しくは重過失により知らなかった場合、又は契約不適合が乙の故意若しくは重過失に起因する場合にはこの限りでない。
- 5 第1項から第3項までの規定は、契約不適合が甲の提供した資料等又は甲の与えた指示によって生じたときは適用しない。ただし、乙がその資料等又は指示が不適當であることを知りながら告げなかったときは、この限りでない。

（作業実施場所における機器）

第19条 この契約の履行に必要となる機器、ソフトウェア及びネットワーク（以下「機器等」という。）については、乙が準備するものとする。ただし、甲が機器等を貸与する場合は、この限りでない。

- 2 乙は、この契約の履行に必要となる機器等を甲のネットワークに接続する場合は、事前に甲の許可を受けなければならない。
- 3 乙は、この契約の履行のために甲の保有する機器にソフトウェアをインストールする必要がある場合、事前に甲の許可を得なければならない。また、当該ソフトウェアが不要となった場合は速やかに消去しなければならない。