■次期文書管理システムの非機能要件

項番	大項目	中項目	メトリクス (指標)	項目
1	性能・拡張性	業務処理量	ユーザ数	システムの利用者数は、約30,000人である。
2	性能・拡張性	業務処理量	データ量（項目・件数）	データ容量は、以下を見込んでいる。 ・移行対象データ（令和8年12月時点）：7TB ・令和9年度の文書データ：3TB システム構築後、データ容量の増加に対応できるよう、クラウドの特性を生かし容量を柔軟に拡張・縮小できるようにすること。
3	性能・拡張性	性能目標値	通常時オンラインレスポンスタイム	文書管理システムと直接接続するPC上で、通常時オンラインレスポンスタイムは1秒以内を目指すこと。
4	性能・拡張性	性能目標値	アクセス集中時のオンラインレスポンスタイム	文書管理システムと直接接続するPC上で、アクセス集中時（＝現行システムのピーク時特性である08:45前後、11:30前後、13:15前後には約45件／秒のアクセス）のオンラインレスポンスタイムは3秒以内を目指すこと。
5	性能・拡張性	性能	情報処理の正確性	システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように設計すること。
6	性能・拡張性	性能	データの正確性	システムにおいて、入力データの正確性を担保すること。
7	可用性	継続性	稼働率	7:00-22:00のサービス稼働率は99.5%とすること。
8	可用性	継続性	RPO（目標復旧地点）（業務停止時）	業務停止を伴う障害（主にソフトウェア故障）が発生した際、障害発生時の直前の状態へ復旧を行うこと。
9	可用性	継続性	RTO（目標復旧時間）（業務停止時）	業務停止を伴う障害（主にソフトウェア故障）が発生した際、障害を検知してから2時間でシステム全体の復旧を行うこと。
10	可用性	継続性	RLO（目標復旧レベル）（業務停止時）	業務停止を伴う障害（主にソフトウェア故障）が発生した際、システム全体の復旧を行うこと。
11	可用性	継続性	システム再開目標（大規模災害時）	大規模災害が発生した際、一週間以内にシステム再開ができること。また、復旧までの間、バックアップデータから業務を実施するために必要なデータを提供すること。
12	可用性	災害対策	復旧方針	大規模災害が発生した際も業務継続性を満たすために、限定された構成（最低限必要な機能＝文書作成・収受・起案・決裁・施行にかかる機能）を短期間緊急に提供するDR（Disaster Recovery）サイトで構築すること。
13	可用性	災害対策	保管場所分散度（外部保管データ）	大規模災害発生に備え、ガバメントクラウド利用方針（3.4システム環境）に則り、Multi-AZ、マルチリージョン構成を構える等の対策を行うこと（メインサイトは東京リージョン、バックアップ/DRサイトは大阪リージョンとする）
14	可用性	災害対策	保管方法（外部保管データ）	大規模災害発生により被災した場合に備え、ガバメントクラウド利用方針（3.4システム環境）に則り、大阪リージョンにバックアップを実施すること
15	可用性	変更管理	システムの変更管理	システムの脆弱性に対応するために、ウイルス対策ソフトは市の指定する製品を導入すること
16	セキュリティ	前提条件・制約条件	順守すべき規程、ルール、法令、ガイドライン等の有無	認証情報ファイルを不正利用から保護するため、情報システムで認証情報設定の情報セキュリティ強化機能がある場合は、これを有効に活用すること
17	セキュリティ	セキュリティリスク管理	リスク分析範囲	職員に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更すること（ただし、認証基盤の取組により、文書管理システムでのID/PASS保持が不要であることが確定した場合、本要件は取り下げとする）
18	セキュリティ	セキュリティリスク管理	ウィルス定義ファイル適用タイミング	システムの脆弱性に対応するために、ウイルス対策ソフトは市の指定する製品を導入すること
19	セキュリティ	セキュリティリスク管理	サーバー攻撃等への措置	サーバー等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、情報システムの停止を含む必要な措置を講じること。
20	セキュリティ	セキュリティリスク管理	セキュリティリスクの情報収集	セキュリティホールや不正プログラム等の、セキュリティリスクに関する情報を収集し、必要に応じ、委託者へ共有すること。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、情報セキュリティ侵害を未然に防止するための対策を速やかに講じること。
21	セキュリティ	アクセス・利用制限	システム上の対策における操作制限	システムへのセキュリティソフトウェアのインストールやプログラム実行等については、不正なソフトウェアがインストールされたり、不要なアクセス経路を利用されることが無いよう、必要最小限の操作のみ許可するように設定すること。
22	セキュリティ	アクセス・利用制限	アクセス制御	不正アクセスを防止するため、ネットワークに適正なアクセス制御（境界にファイアウォールを設置し通過する通信のプロトコルを必要最小限に限定する等）を施すこと。
23	セキュリティ	アクセス・利用制限	アクセス制御	通信プロトコルを必要最小限に限定するため、使用されていないポートを閉鎖すること。
24	セキュリティ	アクセス・利用制限	アクセス制御	不要なサービスについて、機能を削除又は停止すること。
25	セキュリティ	アクセス・利用制限	外部ネットワークとの接続制限	外部ネットワークに係るネットワーク構成、機器構成、情報セキュリティ技術等を詳細に調査し、庁内の情報資産に影響が生じないように対応すること。
26	セキュリティ	アクセス・利用制限	利用者IDの管理・取扱い	IDの登録、変更、抹消等の情報管理や、職員の異動、出向、退職者に伴うIDの取扱い等の方法に従うこと
27	セキュリティ	アクセス・利用制限	利用者IDの管理・取扱い	利用者IDは個人単位で設定すること。管理者IDを利用する者は必要最小限としてID/PASSを厳重に管理する他、特定個人情報を取り扱う場合は必要に応じて当該ファイルへのアクセス制限を実施すること

28	セキュリティ	アクセス・利用制限	認証情報	認証情報ファイルを不正利用から保護するため、情報システムで認証情報設定の情報セキュリティ強化機能がある場合は、これを有効に活用すること
29	セキュリティ	アクセス・利用制限	認証情報	職員に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更すること（ただし、認証基盤の取組により、文書管理システムでのID/PASS保持が不要であることが確定した場合、本要件は取り下げとする）
30	セキュリティ	データの秘匿	伝送・蓄積データの暗号化の有無	伝送・蓄積データの秘匿性を維持するため、ファイル・フォルダまたはDBの暗号化を実施すること。
31	セキュリティ	不正追跡・監視	ログの取得	不正を検知するために、監視のための記録（アクセスログ）を取得すること。ログは、閲覧可能な形式で１年、アーカイブ形式で５年間保管すること。
32	セキュリティ	不正追跡・監視	ログの保存	取得したログは、改ざんや消失が起こらないよう適切に保存し、また、必要に応じて、情報システムから出力したログを記録媒体にバックアップすること。
33	セキュリティ	不正追跡・監視	不正監視対象（装置）	重要度が高い資産（サーバ、ストレージ、ネットワーク機器、端末）への不正を検知するためのログの提供を実施すること。
34	セキュリティ	不正追跡・監視	改ざん・漏洩の検出と防止	故意又は過失により情報が改ざんされる又は漏えいする恐れがある場合に、これを検出及び防止する手段を講じること。
35	セキュリティ	不正追跡・監視	改ざん・漏洩の検出と防止	不正アクセスによる情報システムの改ざんを防止するために、必要に応じてデータの書換えを検出し、通報するよう、設定すること。
36	セキュリティ	不正追跡・監視	改ざん・漏洩の検出と防止	重要なシステムの設定を行ったファイル等について、必要に応じて定期的に当該ファイルの改ざんの有無を検査すること。
37	セキュリティ	不正追跡・監視	不正侵入、不正操作等の点検と分析	必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。
38	セキュリティ	セキュリティ診断	Webアプリケーション診断実施の有無	内部ネットワーク経由での攻撃への対応策のため、Webアプリケーションへのセキュリティ診断を、構築時に1回、以降、年1回程度実施すること。（実施方法については、外部ツールを使った診断を想定している。）
39	運用・保守性	保守運用	OS等パッチ適用タイミング	OS等パッチ適用の際には、脆弱性に対するセキュリティパッチなどの緊急性の高いものは即時に適用し、それ以外は定期保守時に適用すること。
40	運用・保守性	通常運用	運用時間（平日）	運用時間（平日）は、7:00-22:00で稼働すること。時間外に決裁業務が行われることもあるため、バックアップやメンテナンスの実施時期・時間については、市が指定する時期・時間を避けて実施すること。
41	運用・保守性	通常運用	運用時間（休日等）	運用時間（休日）は、平日の開庁時間（8:45-17:30）で稼働すること。バックアップやメンテナンスの実施時期・時間については、市が指定する時期・時間を避けて実施すること。
42	運用・保守性	通常運用	バックアップ取得間隔	全体バックアップ：週次で取得する。 差分バックアップ：6時間おきに取得する。
43	運用・保守性	通常運用	バックアップ世代管理	バックアップ世代管理を実施すること。 世代管理方法はバックアップの手法やシステムの特性を鑑みて委託者へ提案し、委託者と合意した内容を基に実施すること。
44	運用・保守性	通常運用	監視情報	システム全体の監視については、以下の項目を実施し、異常が発生した場合は随時報告を実施すること。 ・死活監視 ・エラー監視 ・リソース監視 ・パフォーマンス監視
45	運用・保守性	通常運用	監視間隔	障害検知のため、システム全体の常時（リアルタイム）監視を行うこと。
46	運用・保守性	通常運用	データ復旧の対応範囲	障害発生時のみならず、ユーザーにより誤って大量のデータを削除等の操作が行われ、かつ、システムの仕組みにより復旧が困難なケースにおいて、削除時の復帰時点（RPO）へデータを回復できるようにすること。
47	運用・保守性	運用環境	マニュアル準備レベル	各ユーザーに合わせたマニュアルを提供すること。 例： ・一般ユーザー向けマニュアル ・システム管理者向けマニュアル
48	運用・保守性	運用環境	外部システムとの接続有無	本市の他業務システムとの連携を実現すること。対象システムは外部「別紙4_1_外部インターフェース一覧」に、また、連携方法は「別紙4_3_システム間連携要件標準仕様書」記載の通り。 ただし、データ連携基盤を利用しないシステムについては、独自で連携を行うこと。
49	運用・保守性	サポート体制	保守契約（ソフトウェア）の種類	ソフトウェア等の保守（アプリケーション領域におけるバグやトラブルといった問題の解決、OSのアップデートに伴う不具合の修正、通信障害の潜在的な原因究明や復旧作業）を実施すること。
50	運用・保守性	サポート体制	定期報告会実施頻度	運用・保守に関する定期報告会を月に一回実施すること。
51	運用・保守性	サポート体制	報告内容のレベル	定期報告会において、通常運用状況や障害の報告に加え、改善提案を実施すること。
52	運用・保守性	サポート体制	ライセンスの管理	ソフトウェアのライセンス管理を行うこと
53	運用・保守性	その他の運用管理方針	問い合わせ対応窓口の設置有無	ユーザーからの問い合わせ窓口を開設、または既存の窓口を利用し対応する。対応時間は以下の通り。 ・平日開庁時間（8:45-17:30）
54	運用・保守性	その他の運用管理方針	トレーニング	システムリリース前に、職員向けのトレーニングを3カ月間（令和8年9月～12月を予定）実施すること。 また、システム稼働後3カ月はヘルプデスクにて問い合わせ等に対応すること。
55	運用・保守性	その他の運用管理方針	インシデント管理の実施有無	ITILに準拠し、「インシデント」を定義の上で管理・運用を行うこと。

56	運用・保守性	その他の運用管理方針	問題管理の実施有無	ITILに準拠し、「問題管理」を定義の上で管理・運用を行うこと。
57	運用・保守性	その他の運用管理方針	構成管理の実施有無	ITILに準拠し、「構成管理」を定義の上で管理・運用を行うこと。
58	運用・保守性	その他の運用管理方針	変更管理の実施有無	ITILに準拠し、「変更管理」を定義の上で管理・運用を行うこと。
59	運用・保守性	その他の運用管理方針	リリース管理の実施有無	ITILに準拠し、「リリース管理」を定義の上で管理・運用を行うこと。
60	運用・保守性	その他の運用管理方針	情報システムの開発・保守に関連する資料等の整備・保管	システム開発・テスト・保守に関連する資料、システム関連文書、情報システムに係るソースコードを適正に整備・保管すること
61	運用・保守性	その他の運用管理方針	情報システムの更新又は統合時の検証	システム更新・統合を行う場合は、伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行うこと
62	移行性	移行時期	システム移行期間	「次期文書管理システム_調達仕様書」（p.7）で記載した想定スケジュールを基に、システムの移行作業開始から本稼働までの移行期間における具体的な作業スケジュールを提案し実行すること。
63	移行性	移行時期	システム停止可能日時	現システムから新システム本稼働までのシステム停止可能時間は年末（2026/12/29-2027/1/3）とする。
64	移行性	移行対象（データ）	移行データ量	現システムが保有する約7,000GBの文書データやその他移行対象となるデータを含め、移行計画実施スケジュールを提案し、移行作業を実施すること。
65	移行性	移行計画	移行のユーザ/ベンダー作業分担	移行作業に係る役割分担は、下記を想定している。 事業者：データ移行作業、動作確認 市：データ移行確認、動作確認
66	他システム連携	電子署名サービスとの連携	電子署名事業者の認証	電子署名は、電子署名及び認証業務に関する法律（平成十二年法律第百二号、以下、「電子署名法」という。）第２条第１項に該当するものであること。また、当該電子署名が電子署名及び認証業務に関する法律施行規則（平成十三年総務省・法務省・経済産業省令第二号、以下「電子署名法施行規則」という。）第２条に該当するものであること。
67	他システム連携	電子署名サービスとの連携	電子署名事業者の認証	電子署名は、時刻認証業務の認定に関する規程（令和３年 総務省告示第 146 号）第 13 条の指定を受けている日本データ通信協会が認定する時刻認証業務認定事業者（TSA）のタイムスタンプ等を使用し、最低 10年間有効性を検証できるものであること。また、上記タイムスタンプ以外を使用する場合は、同等以上の有効性を示すこと。
68	他システム連携	電子署名サービスとの連携	電子署名規格	電子署名（長期署名）規格は、PAdES（PDF Advanced Electronic Signatures）を採用すること。
69	他システム連携	電子署名サービスとの連携	電子署名規格	Adobe Acrobat Readerにより、電子署名の検証ができること。
70	他システム連携	電子署名サービスとの連携	電子署名サービス上のデータ保管について	電子署名サービス上で保有しているデータを廃棄の際は、削除またはアクセス権のはく奪により実行すること。
71	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	市が指定する以下の条例・ガイドライン等に準拠したセキュリティ対策を実施すること。 ・情報取扱注意項目 ・名古屋市情報あんしん条例 ・名古屋市情報あんしん条例施行細則 ・名古屋市個人情報保護条例 ・愛知県障碍者差別解消推進条例 ・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 ・電子署名及び認証業務に関する法律 ・ISO/IEC27000系
72	システム環境・エコロジー	システム制約/前提条件	運用時の制約条件	市が指定する以下の条例・ガイドライン等に準拠したセキュリティ対策を実施すること。 ・情報取扱注意項目 ・名古屋市情報あんしん条例 ・名古屋市情報あんしん条例施行細則 ・名古屋市個人情報保護条例 ・愛知県障碍者差別解消推進条例 ・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 ・電子署名及び認証業務に関する法律 ・ISO/IEC27000系
73	ユーザビリティ要件	－	－	業務上不要な情報やデザインを排し、できる限り美的かつシンプルな画面構成とすること
74	ユーザビリティ要件	－	－	何をすればよいかが見て直ちに分かるような画面構成にすること
75	ユーザビリティ要件	－	－	クリックしやすい大きさのボタンや十分な視認性のある文字とすること
76	ユーザビリティ要件	－	－	画面や文字の大きさを自由かつ容易に拡大・縮小でき、画面の位置の変更ができること
77	ユーザビリティ要件	－	－	最小限の操作や入力等（ワンクリック、キーボード入力、ショートカット、ドラッグ＆ドロップ等）で作業ができるようにすること
78	ユーザビリティ要件	－	－	ユーザが自ら行った操作を容易に取消し、ユーザが戻りたい状態まで戻ることができること
79	ユーザビリティ要件	－	－	言葉や状況、アクションの表現・デザインをシステム内で統一すること
80	ユーザビリティ要件	－	－	迷わずに操作ができるよう人の視線の動きに沿ったボタンやタブの配置とし、業務手順を考慮した画面構成とすること
81	ユーザビリティ要件	－	－	直接入力形式やプルダウン形式などユーザにとって手間のかからない最適な入力方式を選択可能とすること

82	ユーザビリティ要件	−	−	操作の指示、説明、メニュー等には、ユーザが正確にその内容を理解できるよう地方自治体の文書事務と一致した用語を使用すること
83	ユーザビリティ要件	−	−	一連の業務の中での処理状況及び処理にかかる説明を一目で端的に理解できるよう表示すること（カーソルを合わせると各処理の説明がポップアップ表示される等）
84	ユーザビリティ要件	−	−	システムの処理時の状態を端的に理解できるよう表示すること
85	ユーザビリティ要件	−	−	各文書や項目の優先度をユーザが一目で認識できるようにすること
86	ユーザビリティ要件	−	−	ユーザが操作、入力等を間違えないようなデザインや案内を提供すること
87	ユーザビリティ要件	−	−	エラー発生前に適切なタイミングで予防となるメッセージ等を表示すること
88	ユーザビリティ要件	−	−	エラー発生時のエラーの発生箇所・発生理由・対応策をユーザが容易に理解できるよう表示すること
89	ユーザビリティ要件	−	−	ヘルプ情報やマニュアル等を参照できるようにすること
90	ユーザビリティ要件	−	−	関連するヘルプ情報やマニュアルが一目で把握できる場所に配置されていること