情報閲覧システムの賃貸借　仕様書（案）

１　目的

県政全般及び全国の諸政策等に係る各種情報を集積し、検索・閲覧・管理できる「情報閲覧システム」（以下、「システム」という。）を導入し、行政施策の調査や全国知事会等の業務遂行に活用するもの。

２　賃貸借の期間等

令和６年６月１日から令和１１年３月３１日まで。

なお、令和６年５月３１日までに本システムを下記に掲げる場所に設置し、動作確認等を行うこと。

３　システムの設置場所

福島県庁本庁舎　総務部政策調査課内の県の指定する場所に設置すること。

４　システムの機能要件

本システムは、政策調査課担当職員（８名）が利用することを想定しており、その機能要件は以下のとおりである。

（１）文書登録機能

ネットワークに接続されたスキャナから読み込まれた紙文書を DocuWorks 形式に変換し、システムに自動的に格納できること（想定する年間のデータ登録件数は約２万５千件)。CSV ファイルを用いた一括登録も可能とすること。

（２）文書検索・閲覧・管理機能

本システムに登録された文書情報を一覧から選択、あるいはキーワードによる検索を行い、Web ブラウザ上に表示できるようにすること。具体的には以下の機能を有するものとする。

・Web ブラウザを介した文書の登録・閲覧
・ワード、一太郎、PDF、DocuWorks 文書の日本語による全文検索
・登録文書の履歴管理
・階層構造による文書管理

（３）アクセス制御機能

本システムの管理担当者が、フォルダ単位、あるいはドキュメント単位でアクセスの制御設定を行うことで、適切な利用者のみが閲覧できるようにすること。具体的には以下の機能を有するものとする。

・文書及びフォルダ単位のアクセス権限管理

・文書登録、履歴変更時のメール通知

5　システムの運用・保守要件

（1）本システムを運用するに当たり、現行システムにおける既存データ（DocuShare7.0内のDocuWorksデータ等）を移行し、検索・閲覧・管理できるようにすること。

（2）県の指示に従い、本システムの設置を行うとともに、利用者（クライアント）側の環境設定及び操作支援等を行うこと。

（3）本システムの導入に係る関連図書及び操作手順書（管理者用・利用者用）を作成し、納品すること。

（4）本システムのハードウェアの保守管理を行うこと。

（5）本システムの不正使用や情報漏洩等を未然に防止するため、必要なセキュリティ管理を行うこと。

（6）本システムを運用するために必要な県側の保有する機器（スキャナ等）に変更が生じた場合は、必要な調整等を行うこと。

（7）本システムを運用する上で必要な情報の提供に努め、県からの問い合わせや助言要求に対し、速やかに対応すること。

（8）契約終了時は、機器の撤去及びデータ消去（物理破壊）を行うこと。

6　システムの構成及び機器要件

別紙１及び２のとおり。

7　その他

（1）本システムに必要な機器の管理、変更作業等について、責任を持って行うこと。

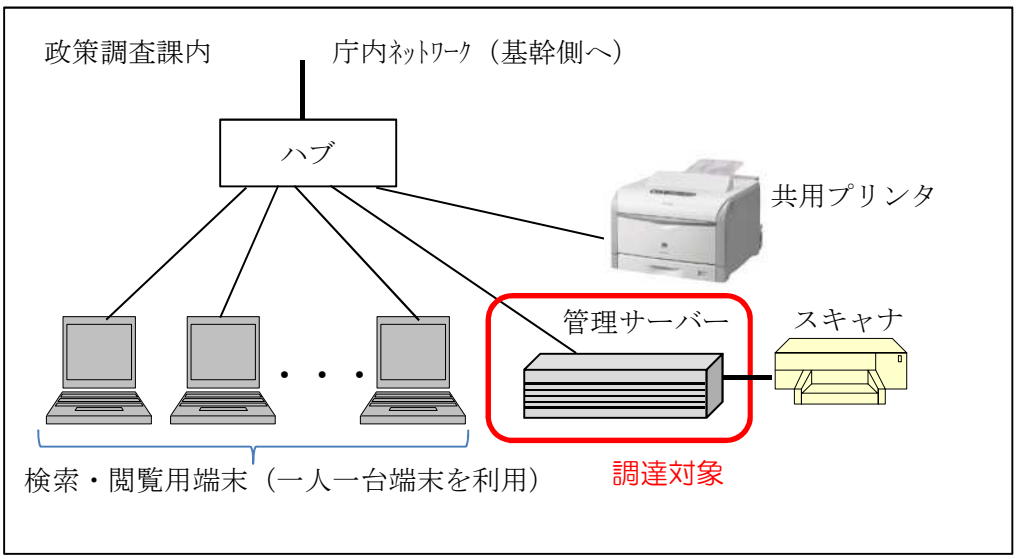
（2）本システムに格納された情報等について、県の許可なく持ち出し等を行ってはならない。また、システムの運用に必要となる関連データ等についても、漏洩、滅失、その他の事故等の予防に十分注意し、信頼性・安全性の確保に努めること。

（3）本仕様書に記載のないものや疑義が生じた場合は、県と協議の上、決定するものとする。

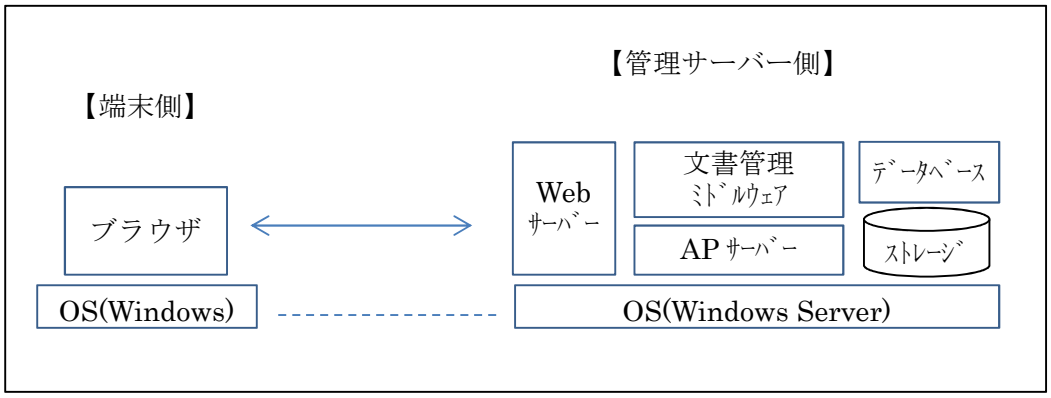
別紙１

システム構成図、ネットワーク構成図

１　システム構成図（ネットワーク構成図・ハードウェア構成図）



２　ソフトウェア構成図（概略）



別紙2

項目			仕様・要件	数量
ハードウェア	サーバー本体 (富士通 PRIMERGY TX1320 M5モデル)同等以上	サーバーの形態	タワー型	１式
		ＣＰＵ	Intel Xeon プロセッサー E-2324 (3.1GHz/4コア/8MB)　相当以上。	
		メインメモリ	１６ＧＢ以上。	
		内蔵ハードディスク	ＳＡＳに対応し、物理容量６００ＧＢ以上ドライブ２台でＲＡＩＤ１構成であること。	
		ネットワークカード	オンボード型で、１０Ｂａｓｅ－Ｔ／１００Ｂａｓｅ－ＴＸ／１０００Ｂａｓｅ－Ｔを自動認識可能なポートを１個以上有すること。	
		光学ドライブ	本体内蔵型　DVD-ROMドライブ相当以上。	
		インターフェースポート	ディスプレイ×2〈DisplayPort×1［背面］、VGAポート×1［背面］、シリアルポート（D-SUB9ピン）×１、USB×10［USB3.2（Gen2x2 Type C：前面×1/Gen1x1 Type A：前面×1/Gen2x1 Type A：背面×2/Gen1x1：内部×2）、USB2.0 Type A：背面×４］	
		ＯＳ	Microsoft® Windows Server® 2022 Standard Edition (64bit)日本語版 ※併せて１０台分のデバイスＣＡＬも付属すること。（Ｗｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　デバイスＣＡＬ　追加）	
	データのバックアップ媒体		バックアップ用装置として、外付け型ハードディスク装置を有しＲＡＩＤ1で冗長化されていること。 装置はＵＳＢ２．０接続とし、物理容量が２ＴＢドライブ２台で構成であること。	1
	データのバックアップソフト （Arcserve UDP 9.x Advanced Edition）又は同等品		上記媒体にイメージバックアップ用のソフトを用意すること。	1
	サーバー本体の保証内容 （富士通　５年ハードウェア保守パック）又は同等		５年間の部品保証・作業員の当日オンサイト対応が可能な内容とすること。	1
			祝祭日および年末年始　（１２／３０～１／３）を除き、平日（月～金）の対応が可能であること。	
			サーバー本体に内蔵される機器は全て、この保証内容にて対応可能なこと。	
	モニタ		１７インチ以上ＴＦＴ液晶モニタ	1
	無停電電源装置 (UPS)		停電時に、サーバのシャットダウンが可能な容量を有すること。	１式
			メーカー保証が２年以上であること。	
			停電時にサーバーを自動シャットダウンすることが可能なオプションを含むこと。	

別紙2

項目		仕様・要件	数量
システムソフトウェア	情報閲覧システムソフトウェア （ゼロックス社 Xerox DocuShare7.6） （富士フイルムビジネスイノベーション DocuWorks9.1以上）	Xerox DocuShare7.6と連携するDocuWorks9.1以上を用意すること。現在運用システムのファイル形式がDocuWorks（XDW）のため、引き続き同じファイル形式の運用とすること。	１式
		文書登録時に1日分(４０文書程度)を一括登録し、かつ全文検索時にダイレクトに１文書１ページ表示ができるようにすること。及び、複数日の複数ファイル登録時もドラックアンドドロップにより、複数ファイルを同時に登録可能なこと。	
		複数の文書を統一フォーマットで、1つに束ねる、ばらす、ページ順の変更、追加、取り出しを縮小表示(サムネール)された文書を確認しながらマウス操作で自在に行える機能を有すること。	
		ファイル名を修正する場合、専用アプリケーションで開かずに簡易ビューアで内容を確認しながら連続して修正が可能なこと。	
		３０万文書まで格納可能なWebベースのソフトウェアであること。	
		Web上で検索/表示/登録/移動/フォルダ操作/アクセス権設定/文書更新が可能なこと。	
		登録する記事はOCR処理し全文検索可能なデータファイル単位での登録であること。	
		Web画面レイアウトをユーザーごとに設定可能なこと。	
		Webブラウザ上でDocuWorksサムネイル表示が可能なこと。	
		運用に当っては現状の複合機のスキャナ機能とプリント機能での運用が可能なこと。また、将来的に機器が入れ替わっても柔軟に対応できるソフト構成であること。複合機の変更があった際の文書取り込み変更作業費用も含むこと。	
		全文検索可能な画像ファイルをシステム上から別の記憶媒体に取り出し可能なこと。	
		登録される文書の版管理機能を有すること。	
		登録においてWindows上のファイル・フォルダを複数一括して登録が可能なこと。	
		ライセンスについて、登録者は１０名を対象とすること。匿名ユーザー（アカウント登録されていないユーザ/Guestユーザー）でも閲覧ができるよう設定することが可能なこと。	
		登録・閲覧するクライアントはMicrosoft® Windows® 10,11。閲覧ブラウザはMicrosoft Edge(Chromium),Google Chromeで動作可能であること。	
		Active Directory環境で利用可能なこと。	

情報セキュリティ関連特記仕様書
目次

本特記仕様書は、福島県が導入する「情報閲覧システム」仕様書に加え、追加で求めるセキュリティ要件を記載するものである。受注者は本書に従わなくてはならない。

(1) ＩＤ共有の禁止

利用者のアカウントの発行単位は個人とし、組織へのアカウント発行はしない。

また、１利用者に付き１アカウント発行するものとし、アカウントの共有は認めない。

(2) 管理者用の ID の共有

管理者のアカウントの発行単位は個人とし、組織へのアカウント発行はしない。

また、１管理者に付き１アカウント発行するものとし、アカウントの共有は認めない。

(3) 管理用接続の自動タイムアウト

自動ログアウトを有効にする

(4) パスワードの強制変更

管理用アカウントのパスワードは、年に１回強制的に変更を行うシステムとする

(5) パスワードの文字数制限、単語制限

管理用アカウントのパスワードは、最低 8 文字となるようにシステムを設定する。

(6) サーバに保存されたパスワードの暗号化等

アカウントのパスワードは、サーバには平文（元テキストのまま）又は単純な暗号化したものでは保存せず、運用管理者がそのパスワードの暗号化キーを知ることができない、十分な強度の暗号化又はハッシュ化を行い保存すること。

第２章　物理的対策関連

(1) サーバ多重化

多重化を行わず運用による回避策を行う。

（詳細：修理している間は稼働させない。）

(2) データ多重化

RAID(ミラー(RAID1))

(3) 予備電源
UPS(既設)

(4) 雷対策
UPS

(5) 転倒防止
免震ジェル等を使用

(6) 盗難防止
セキュリティワイヤーによる固定

(7) 断線防止、引っ掛け防止
既設配線収納管の利用

(8) 火災対策
火災防止策は行わず運用による回避策による
（詳細：情報システムのための火災防止策は行わず、執務室等の通常の防火対策を行う。）

(9) 水害対策
水害防止策は行わず運用による回避策を行う
（詳細：水害が予想される警報が発令された場合は、上階等安全な階へ退避する。）

(10) 埃対策
埃対策は行わず運用による回避策を行う
（詳細：政策調査課は、特段の防塵対策がなされているわけではないが、サーバの稼働に問題があるほどではない。半年に一度、ファン付近の埃について目視でチェックし、付着しているようであれば掃除する。）

(11) 異常温度湿度、静電気対策
異常温度湿度、静電気防止策を行わず運用による回避策による
（詳細：故障した場合は、運用を停止し修理する。）

(12) 漏水対策
天井等の水道管、スプリンクラーを回避して機器を設置

(13) 入室制限
入室制限策は行わず運用による回避策を行う
（詳細：執務室内に設置するため、職員による目視監視を行う。）

(14) 入退室管理
入退室管理は行わず運用により管理する
（詳細：執務室内に設置するため、職員による目視監視を行う。）

(15) 定期保守
定期保守は行わない。

第３章　ネットワーク関連

(1) アクセス制御
情報政策課によるパケットフィルター

(2) 外部のネットワークと接続時の認証方法
外部ネットワークとは直接接続しない

(3) 機密性の低いネットワークの使用
機密性の低いネットワークは使用しない

(4) プロトコル制限
外部ネットワークとは直接接続しない

(5) 外部のネットワークと接続時の回線の選択
外部ネットワークとは直接接続しない

(6) 外部ネットワーク由来の業務への影響
外部ネットワークとは直接接続しない

第４章　サイバー攻撃対策

(1) 不正データの入出力の除外
その他の影響対策（詳細：外部には公開しない）

(2) ウィルス対策の実施
情報通信システムネットワークシステムのウィルス対策ソフトを使用

(3) ウィルス対策ソフトのパターンアップデート間隔
概ね１時間毎

(4) Web コンテンツ納品時の改ざんチェック
インターネット向け Web コンテンツを運用しない

(5) Web コンテンツ運用時の改ざんチェック
インターネット向け Web コンテンツを運用しない

(6) 脆弱性又は改ざん等のチェックの間隔
インターネット向け Web コンテンツを運用しない

(7) システムの設定ファイルの改ざんチェック
改ざん等のチェックは行わないが、運用で回避策を行う
（詳細：システム使用時に確認する　）

(8) システムの設定ファイルの改ざんチェックの間隔
改ざん等のチェックは行わない

(9) 脆弱性対応パッチ情報の取得
その他の脆弱性の解消方法
（詳細：OS については庁内の WSUS を適用する。パッケージソフトについては、賃貸借契約の範囲で必要に応じて更新等を実施する。）

(10) 脆弱性対応パッチの適用
その他
（詳細：OS については庁内の WSUS を適用する。パッケージソフトについては、賃貸借契約の範囲で必要に応じて更新等を実施する。）

(11) 脆弱性対応パッチの適用時期
1 ヶ月から 3 ヶ月未満に一度

第５章　障害対策

(1) データベースのバックアップ
3 世代以上

(2) データベースのバックアップの間隔
その他（詳細：土曜日にフルバックアップ、月～金曜日は増分バックアップ）

(3) データ領域（データベース以外)のバックアップ（
3 世代以上

(4) データ領域（データベース以外)のバックアップの間隔
その他（詳細：土曜日にフルバックアップ、月～金曜日は増分バックアップ）

(5) システム領域のバックアップ
　3世代以上

(6) システム領域のバックアップの間隔
　その他（詳細：土曜日にフルバックアップ、月～金曜日は増分バックアップ）

(7) ログのバックアップ
　毎日

(8) 死活確認
　その他（詳細：　使用時に確認するため行わない　）

第６章　検出、事故対応

(1) アクセス記録の取得
　取得する

(2) ログの分析
　システムの不正アクセス監視は行わない。

(3) 時刻の同期
　情報通信ネットワークシステムのNTPサーバ

第７章　その他の契約事項

(1) 資格の確認
　プライバシーマークまたはISO/IEC27001

(2) 外部委託における契約項目
　ア　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
　イ　委託先の責任者、委託内容、作業者及び作業場所の特定
　ウ　提供されるサービスレベルの保証
　エ　従業員に対する教育の実施
　オ　提供された情報の目的外利用及び受託者以外の者への提供の禁止
　カ　業務上知り得た情報の守秘義務
　キ　再委託に関する制限事項の遵守
　ク　委託業務終了時の情報資産の返還、廃棄等
　ケ　委託業務の定期報告及び緊急時報告義務
　コ　情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

(3) クラウドの利用におけるサービスレベル

クラウドは使用しない

(4) クラウドの利用における第三者提供サービス
クラウドは使用しない

(5) パブリッククラウドの利用におけるデータの第三者利用
パブリッククラウドは使用しない