【別紙３】非機能要件一覧

項番	大項目	中項目	小項目	メトリクス (指標)	要求目標
－	県・市町のシステム環境				県・市町の管理者・担当者が使用できるパソコンのOSとブラウザは、以下の代表的なものにおいて、正常に表示し、動作すること。なお、以下に該当しないものについても適宜柔軟に対応すること。 また、バージョンアップした場合は3か月以内に対応可能なシステムとすること。 ＝＝＝ OS：Windows11以上 ブラウザ：Microsoft Edge、Google Chrome、Safari ウイルス対策ソフト：Windows Defender オフィスソフト：Microsoft 365 PDFビューア：Microsoft Edge、Acrobat Reader
－	サーバ環境				ISMAPに準拠したクラウドサーバを前提とすること。県との協議の上、ガバメントクラウドの利用も検討すること。
A.1.1.1	可用性	継続性	運用スケジュール	運用時間（通常）	システムの平日運用時間は、24時間利用を前提とすること。
A.1.1.2				運用時間（特定日）	システムの特定日運用時間は、24時間利用を前提とすること。
A.1.1.3				計画停止の有無	事前の合意に基づく計画停止有り（運用スケジュールの変更可）とすること。
A.1.2.1			業務継続性	対象業務範囲	対象業務範囲は、全ての業務（県・市町のウェブサイトからの自動的な情報取得、生成AIを活用した情報の分類・テキスト作成による配信データの作成、情報発信事業者への配信データの提供、システムの保守・運用及び県・市町担当者への問い合わせ対応とする）とすること。
A.1.2.2				サービス切替時間	1日程度の中断とすること。
A.1.2.3				業務継続の要求度	障害時の業務停止を許容することとする。
A.1.3.1			目標復旧水準 （業務停止時）	RPO（目標復旧地点）	平常時、業務停止を伴う障害が発生した際には、1営業日前の時点までのデータ復旧を目標とすること。
A.1.3.2				RTO（目標復旧時間）	平常時、業務停止を伴う障害が発生した際には、1営業日以内でのシステム復旧を目標とすること。
A.1.3.3				RLO（目標復旧レベル）	平常時、業務停止を伴う障害が発生した際には、システム機能の復旧を実施すること。

項番	大項目	中項目	小項目	メトリクス (指標)	要求目標
A.1.4.1			目標復旧水準 （大規模災害時）	システム再開目標（大規模災害時）	大規模災害時、情報システムに甚大な被害が生じた場合、情報システムは、１ヶ月以内に再開することを目標とすること。
A.1.5.1			稼働率	稼働率	年間のシステム稼働率は、99.5%を目標とすること。
A.3.1.1		災害対策	システム	復旧方針	同一の構成でシステムを再構築すること。
A.3.2.1			外部保管データ	保管場所分散度	遠隔地へのデータ保管は、インフラの仕様等を踏まえ、ベンダーによる提案事項とすること。
A.3.2.2				保管方法	大規模災害時のデータ保管方法は、インフラの仕様等を踏まえ、ベンダーによる提案事項とすること。
B.1.1.1	性能・拡張性	業務処理量	通常時の業務量	ユーザ数	プッシュ型情報発信システム（管理機能）にアクセスする利用者は、事前に登録された県・市町の管理者・担当者最大100名程度を想定すること。
B.1.1.2				同時アクセス数	同時アクセス数は、最大100アカウント程度を想定する。
B.1.1.3				データ量	データ量は、ベンダーによる提案事項とすること。
－				バッチ処理頻度①	取得対象ウェブサイトに掲載されるお知らせを取得・分類・出力する頻度は、毎日9-20時で12回を想定する。
－				バッチ処理頻度②	福井県に関連するLアラート情報を取得・出力する頻度は、24時間即時に実施することを想定する。
－				バッチ処理件数①	取得対象ウェブサイトに掲載されるお知らせの合計数は週当たり300～500ページを想定する。
－				バッチ処理件数②	県・市町担当者による直接入力の件数は、週当たり最大100件程度を想定する。
B.1.3.1			保管期間	保管期間	保管期間は、1年とすること。
－		性能目標値	オンラインレスポンス	バッチ処理時間	情報取得対象ウェブサイトに掲載されるお知らせを取得・分類・XML形式に出力するタイムは、最大10分間を想定する。システムとしては、毎時取得したデータを1時間後に発信することを想定する。（例：9時にクローリングした情報を、10時に情報発信事業者向けに発信する。）
－				レスポンス①	県・市町の管理者・担当者により直接入力されてからXML形式に出力・情報発信事業者向けに発信するタイムは、最大10分間を想定する。
－				レスポンス②	その他の単純な画面操作（アカウント管理、マスタ登録等）へのレスポンスタイムは最大10秒を想定する。

項番	大項目	中項目	小項目	メトリクス (指標)	要求目標
C.1.1.1	運用・保守性	通常運用	運用時間	運用時間（通常）	システムの平日運用時間は、24時間利用を前提とすること。
C.1.1.2				運用時間（特定日）	システムの特定日運用時間は、24時間利用を前提とすること。
C.1.2.3			バックアップ	バックアップ利用範囲	バックアップ利用範囲は、障害発生時のデータ損失防止とすること。
C.1.2.4				バックアップ自動化の範囲	バックアップ自動化の範囲は、仕様の対象としない。
C.1.2.5				バックアップ取得間隔	バックアップ取得間隔は、ベンダーによる提案事項とすること。
C.1.2.6				バックアップ保存期間	バックアップ保存期間は、1年とすること。
C.1.3.1			運用監視	監視情報	システムの監視は、エラー監視を行うこと。
C.1.3.2				監視間隔	監視間隔は、9-20時の間で1時間ごととすること。
C.2.1.1		保守運用	計画停止	計画停止の有無	計画停止有り（運用スケジュールの変更可）とすること。
C.2.2.1			運用負荷削減	保守作業自動化の範囲	保守作業自動化の範囲は、ベンダーによる提案事項とすること。
C.4.1.1		運用環境	開発用環境の設置	開発用環境の設置有無	開発用環境の設置方法・設置環境について、ベンダーによる提案事項とすること。
C.4.2.1			試験用環境の設置	試験用環境の設置有無	試験用環境の設置方法・設置方法・設置環境について、ベンダーによる提案事項とすること。
C.4.3.1			マニュアル準備レベル	マニュアル準備レベル	システムの通常運用と保守運用のマニュアルを提供すること。
C.4.5.1			外部システム接続	外部システムとの接続有無	情報発信事業者のシステム・アプリ等とのAPI連携（オープンAPI）を検討すること。
C.5.3.1		サポート体制	ライフサイクル期間	ライフサイクル期間	システムのライフサイクル期間は、5年とすること。
C.5.9.1			定期報告会	定期報告会実施頻度	運用の定期報告は、四半期に1回程度実施すること。
C.5.9.2				報告内容のレベル	障害報告に加えて運用状況報告を行うこと。

項番	大項目	中項目	小項目	メトリクス (指標)	要求目標
C.6.2.1		その他の運用管理方針	問い合わせ対応	問い合わせ対応の有無	県・市町の管理者・担当者からの、システム利用方法や、情報取得元ウェブサイトの追加・変更等の問い合わせを受け付け、回答すること。 情報発信事業者からの、プッシュ型情報発信システムへの新規接続依頼や、システムの活用方法に関する問い合わせを受け付け、回答すること。 問い合わせ方法は、電話・メールもしくは問い合わせフォームを想定する。
E.1.1.1	セキュリティ	前提条件・制約条件	情報セキュリティに関するコンプライアンス	順守すべき社内規程、ルール、法令、ガイドライン等の有無	有り（福井県セキュリティポリシー）
E.2.1.1		セキュリティリスク分析	セキュリティリスク分析	リスク分析範囲	リスク分析範囲は、開発範囲とすること。
–		AIセキュリティ	不正入力対策	不正入力のリスク対策	プロンプトインジェクション等の攻撃を想定し、不正な入力（個人情報や隠し命令文を含む）を受け付けない、あるいは無害化する仕組みを実装すること。
–			出力コンテンツの安全性確保	不適切な出力のリスク対策	AIの生成結果に、意図しない有害な情報（差別的、暴力的内容など）や機密情報が含まれないよう、出力内容を監視・フィルタリングする仕組みを実装すること。
–			攻撃リスクへの対策	LLMサーバのアクセス先の制限	LLMサーバのアクセス先を制限し、攻撃者のサーバにアクセスできないようにすること。
–			トレーサビリティの確保	AI利用のログ取得	AIへの入力（プロンプト）とAIからの出力（レスポンス）に関するログを取得し、不正利用の追跡や監査に利用できるようにすること。
E.3.1.1		セキュリティ診断	セキュリティ診断	ネットワーク診断実施の有無	ネットワーク診断は、実施すること。
E.3.1.2				Web診断実施の有無	Web診断は、実施すること。
E.5.1.1		アクセス・利用制限	認証機能	管理権限を持つ主体の認証	ユーザ（県・市町職員）がシステムにアクセスする際の認証方法は、2要素以上の認証とすること。
E.7.1.1		不正追跡・監視	不正監視	ログの取得	ログの取得については必要なログを取得すること。
E.7.1.2				ログ保管期間	ログ保管期間は、6ヶ月とすること。
E.7.1.3				不正監視対象（装置）	不正監視対象は、重要度が高い資産を扱う範囲、あるいは、外接部分とすること。
E.7.1.4				不正監視対象（ネットワーク）	不正監視対象（ネットワーク）は、重要度が高い資産を扱う範囲、あるいは、外接部分とすること。
E.7.1.5				不正監視対象（侵入者・不正操作等）	不正監視対象（侵入者・不正操作等）は、重要度が高い資産を扱う範囲、あるいは、外接部分とすること。

項番	大項目	中項目	小項目	メトリクス (指標)	要求目標
E.8.1.1		ネットワーク対策	ネットワーク制御	通信制御	踏み台攻撃等の脅威や、情報の持ち出しを抑止するために、不正な通信を遮断等のネットワーク制御を実施すること。
E.8.2.1			不正検知	不正通信の検知範囲	不正通信の検知範囲は、システム全体とすること。
E.8.3.1			サービス停止攻撃の回避	ネットワークの輻輳対策	ネットワークの輻輳対策は行わないこと（DoS/DDoS攻撃については、可用性対策にてある程度の対策を実施し、それ以上は許容する）。
E.9.1.1		マルウェア対策	マルウェア対策	マルウェア対策実施範囲	マルウェア対策実施範囲は、システム全体とすること。
E.10.1.2		Web対策	Web実装対策	WAFの導入の有無	WAF等ネットワークセキュリティ対策は、実施すること。