非機能要件一覧

（別紙４）

項番	大項目	中項目	小項目	メトリクス（指標）	要求目標
1	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、県・市町の管理者・担当者の要望を踏まえ、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 PDFビューア：Microsoft Edge、Acrobat Reader
2	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。
3	可用性	継続性	運用スケジュール	運用時間	システムの運用時間は、24時間365日を前提とすること。
4				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。
5			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を活用した情報のカテゴリ分け・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・運用および県・市町担当者への問い合わせ対応とする）とすること。
6				サービス切替時間	1日程度の中断とすること。
7				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。
8			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。
9				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。
10				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。
11			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。
12			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。
13		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。
14			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。
15				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。
16	性能・拡張性	業務処理量	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。
17				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。
18				APIクライアント数	APIが送受信をするクライアントは、情報発信事業者等のシステムであり、最大10程度を想定する。
19				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。 なお、バッチ処理件数および保管期間（1年間）を踏まえて見積もること。
20				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・カテゴリ分け・出力する頻度は、1日1回程度を想定する。
21				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。
22				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300～700ページ程度を想定する。
23				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。
24			保管期間	保管期間	保管期間は、1年とすること。
25		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・カテゴリ分け・XML形式に出力するタイムは、最大180分間を想定する。システムとしては、毎日17時頃に取得したデータを1～2時間後に情報発信事業者向けに発信することを想定する。
26				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。
27				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。
28	運用・保守性	基盤運用	バックアップ	バックアップ利用範囲	障害発生時に、システム全体を目標復旧地点（RPO）へ回復すること。
29				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、ベンダーによる提案事項とすること。
30				バックアップ取得間隔	バックアップ取得間隔は、1日1回以上とすること。
31				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。
32			運用監視	死活監視	システムを構成するハードウェア、OS、ミドルウェアおよびアプリケーションについて、死活監視を含む稼働監視を行い、異常を検知した場合に速やかに通知される仕組みを備えること。監視間隔は、リアルタイム（概ね数分間隔）とすること。
33				エラー監視	システムの処理が正しく実行されない（クローリングが実施できない、生成AIによるカテゴリ分け・抽出ができない、データの出力が実施できない、システムにログインできない等）場合に速やかに障害対応できるような監視を行うこと。監視間隔は、1時間ごととすること。
34		運用保守	システム保守	保守業務の範囲	システムの正常な動作を確保するための一切の保守業務を実施すること。

項番	大項目	中項目	小項目	メトリクス (指標)	要求目標
35				モジュールの使用有無	システムで使用するソフトウェアにおいて、修正等のモジュールが提供された場合は、モジュールの適用の必要性を判断し、県の承認を得た上で実施すること。
36				情報取得対象ウェブサイトの追加・更新	県からクローリング対象のウェブサイト追加や更新の連絡を受けた際には、速やかに対象のウェブサイトの新着情報欄から正しくクローリングができるよう、設定等の更新作業を実施すること。
37				ソフトウェアの脆弱性に対する対応	システムで使用するソフトウェアに対する脆弱性情報が各メーカーより報告された場合は、全体への影響度を考慮に入れ、対策プログラムの適応の必要性を判断し、県の承認を得た上で、対策を実施すること。
38				ウイルスの検出等に対する対応	ウイルスの検出や不正アクセス等の事案が発生した場合は、県・市町等と協力し、対応および原因究明を行うこと。
39			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。
40		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。
41			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。
42			マニュアル準備レベル	マニュアル準備レベル	県・市町の管理者・担当者用の操作マニュアルおよび運用保守計画書（基本的ベンダーが保守作業を実施するが、緊急時に県が補助的に実施する設定変更・簡易復旧作業等に必要な内容も含む ）を提供すること。
43			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APIにより接続する。API が同一環境内の他の API やソフトウェアとリソース（ポート・CPU・メモリ・ストレージ等）や設定を奪い合わず、干渉や性能低下を起こさないようにすること。他のシステムやコンポーネントと正しくデータやサービスを利用できるようにすること。
44			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（次回のシステム更改までの期間）は、5年とすること。
45		問い合わせ対応等	通常時	連絡窓口の設置（県・市町）	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る連絡窓口を設置すること。希望する対応時間および連絡方法については次に示す。なお、さらに効果的・効率的な体制が整えられる場合は提案すること。 ・電話での問い合わせ：平日の午前９時から午後５時００分まで ・メールでの問い合わせ：同上（受信は24時間365日可能とする。）
46				連絡窓口の設置（情報発信事業者）	情報発信事業者からの、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窓口を設置すること。希望する対応時間および連絡方法については、県・市町の連絡窓口と同様とする。
47				県への報告等	問い合わせ内容・改善内容の記録・管理を行い、定期報告会で報告を行うこと。
48			障害時	連絡窓口の設置	通常時の問合せ対応の時間帯以外においても対応できる障害等緊急時用の連絡窓口を設置すること。障害等緊急で対応すべき事象が発生した場合は、速やかに必要な対応を行うこと。なお、障害など緊急時の対応手順等はあらかじめ作成し、県へ提示すること。
49				県への報告等	障害発生の際は、その障害原因を特定し、県へ報告すること。重大障害の際には、対策会議等を開催し、経過等を取りまとめて報告するとともに、改善策を県へ提示すること。
50		その他の運用管理方針	定期報告会等	定期報告会の開催 （四半期に1回程度）	県・市町および情報発信事業者からの問い合わせ内容、障害対応・システム保守内容、生成AIの処理精度の確認結果、システムおよび運用方法の改善に関する検討・実施内容、県・市町による情報取得対象ウェブサイトの運用の見直しに向けた課題・改善点等について定期報告会資料としてとりまとめ、県に報告すること。
51				定期連絡会の開催 （1年に1回程度）	住民への効果的な情報発信に向けて情報発信事業者（県が指定する1～2者程度）と住民目線でのプッシュ型情報発信の利用体験向上を目的とした、システムおよび運用方法の改善を検討し、その結果を定期連絡会資料としてとりまとめ、県に報告すること。
52				利用者へのアンケートの実施 （1年に1回程度）	利用者目線からの意見・要望を把握するため、当該情報発信事業者と連携して利用者へのアンケートを行い、利用者のニーズやシステムの改善点等を把握すること。
53			改善の検討・実施	システムおよび運用方法等の改善検討	システムの目指す姿（仕様書1.3後段を参照）の実現に向けて、県との協議、県・市町の管理者および担当者からの問い合わせ対応、利用者アンケート等に基づき、システムおよび運用方法等の改善を検討すること。改善点については定期報告会資料に取りまとめ、県に報告すること。
54			改修等における対応	関連資料の改版	システム改修または設定変更により設計書や操作マニュアル等の関連資料に改版が必要になる場合は当該資料の改版を行い、県へ提出すること。
55	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）
56		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。
57		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。
58			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。
59			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。
60			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。
61		APIセキュリティ	不正アクセス対策	不正アクセスのリスク対策	外部システムと連携するAPIについて、許可されていない利用者が情報にアクセスできないようにすること。リクエストやレスポンスの通信途中の第三者による改ざんを防ぐこと。
62			トレーサビリティの確保	API利用のログ取得	送信者や受信者が後から関与を否定できないようにすること。監査やトラブルシューティング時に追跡可能にすること。やり取りする情報や利用者が正しいものであることを保証すること。
63		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。
64				Web診断実施の有無	Web診断は、実施すること。
65		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。
66		データの秘匿	データ暗号化	伝送データの暗号化の有無	伝送データについては、認証情報のみ暗号化すること。
67				蓄積データの暗号化の有無	蓄積データについては、認証情報のみ暗号化すること。
68		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。
69				ログ保管期間	ログ保管期間は、6ヶ月とすること。

項番	大項目	中項目	小項目	メトリクス (指標)	要求目標
70				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。
71				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。
72				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。
73		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。
74			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。
75			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）。
76		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。
77		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。
78	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	構築時の制約条件	システム構築時には制約無しを想定するが、考慮すべき条件があればベンダーから提案すること。
79			運用時の制約条件	運用時の制約条件	システム運用時には制約無しを想定するが、考慮すべき条件があればベンダーから提案すること。
80			クライアント数	クライアント数	クライアント数は、上限が決まっているものとする（100アカウント程度）。
81			拠点数	拠点数	拠点数は福井県および県内全市町の計18自治体を基本として18以上とすることを想定する。
82			地域的広がり	地域的広がり	アクセス範囲は国内とすること。
83			特定製品指定	特定製品の採用有無	特定製品の指定はないものとする。