次期防災情報システム
要件定義書案

令和 7（2025）年 X 月

栃木県危機管理防災局危機管理課

目次

第１　はじめに

本ドキュメントは、栃木県防災情報システム（以下、「本システム」という。）で実現すべき各種要件について記載したものである。

なお、本文書において、災害対応業務の「関係者」については、警察・消防・自衛隊等の救援機関、インフラ分野をはじめとした民間事業者、国等の関係省庁からのリエゾン職員、対口支援等の県外からの応援職員等の幅広い対象のうちから、各業務・機能に関係する主体を意味している。また、「県民等」については、県内在住者に加え、一時的に県内に滞在している者を含む。

第２　業務要件

２－１ 業務実施手順

２-１-a 業務範囲

本システムは原則として現行システムが対象とする業務範囲を踏襲する。一部業務は業務効率化の観点から機能自体の見直しを想定している。

現行システムが対象とする災害対応業務及び情報システム化の範囲を以下に示す。システム化の範囲に関して、本システムの機能として関連するものは「〇」、職員・組織間での情報共有にシステムが提供する汎用的な情報共有機能を使用するのみの場合は「情報共有機能のみ」としている。

表 2-1　業務の範囲（業務機能とその階層）

階層 1		階層 2		次期システムの対象
項番	名称	項番	名称	
1	災害等の発生覚知・伝達	1-1	危機発生の覚知	〇
		1-2	警報等の伝達	〇
		1-3	警報等の伝達に係る追加対応	情報共有機能のみ
		1-4	異常現象の覚知	―
		1-5	火災・事故災害対策情報の伝達	〇
		1-6	原子力災害情報の伝達	情報共有機能のみ
2	災害対策本部の組織・運営	2-1	取るべき体制の判断・設置	〇
		2-2	本部設置の連絡	〇
		2-3	本部立ち上げ	〇
		2-4	災害対策本部会議の開催	〇
3	通信の確保	3-1	災害発生に向けた準備	―
		3-2	通信の復旧	情報共有機能のみ
		3-3	通信困難時の放送要請	―
		3-4	孤立集落の通信確保	情報共有機能のみ
4	被害情報の収集	4-1	被害情報の収集	〇
		4-2	Ｌアラートを通じた情報発信	〇
		4-3	被害報の作成・確認	〇
		4-4	県消防防災ヘリによる情報収集	〇
		4-5	他機関のヘリによる情報収集	情報共有機能のみ
		4-6	災害時応援協定による情報収集	情報共有機能のみ
		4-7	市町への緊急対策要員の派遣	〇
5	応援の受入	5-1	栃木県広域消防応援－第二次応援体制	―

階層 1		階層 2		次期システムの対象
項番	名称	項番	名称	
			等	
		5-2	消防応援活動調整本部等の設置	情報共有機能のみ
		5-3	応援部隊等の進出拠点及びヘリ離発着陸場の確保	情報共有機能のみ
		5-4	自衛隊の派遣要請	情報共有機能のみ
6	広報活動	6-1	住民向け情報発信	情報共有機能のみ
		6-2	防災ポータルサイトへの掲載	○
		6-3	県ホームページ（防災ポータルサイト以外）への掲載	－
		6-4	メールの発信	○
		6-5	報道機関・記者会見	情報共有機能のみ
7	救助・救急活動	7-1	災害救助法適用の手続き・実施	情報共有機能のみ
		7-2	県消防防災ヘリコプター等の運用	情報共有機能のみ
8	避難所等の被災者の生活対策	8-1	高齢者等避難、避難指示及び緊急安全確保	○
		8-2	避難所の設置、移転又は閉鎖	○
		8-3	避難所の開設	○
9	国民保護関連	9-1	危機事態警戒本部の設置	○
		9-2	県対策本部会議の実施	○
		9-3	消防庁緊急事態調整本部の設置に関する連絡	―
		9-4	危機管理対策本部の設置	○
		9-5	国民保護対策本部の設置	―
		9-6	安否情報報告事務開始の連絡	―
		9-7	対策本部を設置すべき市町への連絡	―
		9-8	武力攻撃事態対処方針の伝達	―
		9-9	国民保護情報の伝達	○
		9-10	国民保護に関する被災情報の収集・報告	―
		9-11	安否情報システムの使用	―

2-1-b 業務フロー

本システムが対象とする業務及び情報システム化の範囲については、「別紙１業務フロー」を参照のこと。以下に記載の凡例とサンプル（別紙１の抜粋）を示す。業務フロー中の赤字箇所は、次期システムにて現行から変更する部分である。

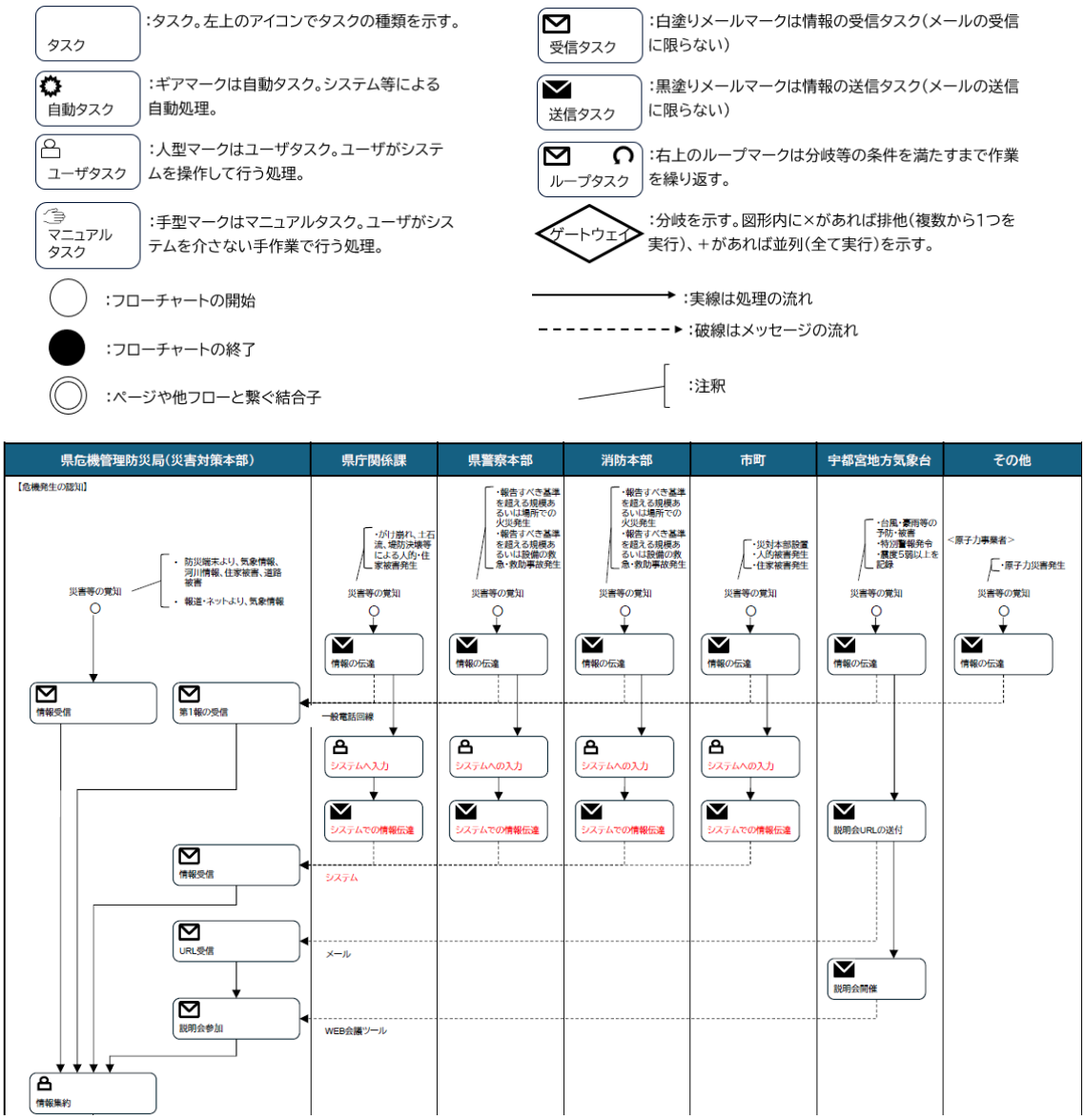

図 2-1　業務フローの凡例及びサンプル

2-1-c 入出力情報項目及び取扱量

本システム運用開始後 1 年間程度の入出力情報及び取扱量に関する現段階における見通しを「別紙 2 入出力情報項目」に示す。SOBO-WEB から入手するデータについては、別紙 2 において他項目とは別の表として記載している。なお、本システム並びに関連するシステムの利用範囲の拡大に伴い、データの範囲と種類、容量が拡大する可能性もあることに留意すること。

入力した事項をもとに、「火災・災害等即報要領」（昭和 59 年 10 月 15 日消防庁長官通知消防災第 267 号）に基づく報告様式など、国等への報告等の各種様式を作成できるよう、適切な入力方式、選択肢等を設定すること。

その他項目については、業務に支障を生じないことを前提に、設計時に主管課の承認を得て変更して差支えない。

2-1-d 管理対象情報一覧

対象業務で管理すべき情報（管理対象情報）を下表に示す。なお、提案するシステムやサービスにおいて既定済みの情報項目等が下記によらない場合は、主管課の承認を得て変更して差支えない。

表 2-2　管理対象情報一覧

項番	管理対象情報名	管理単位	主たる用途	補足
1	被害報告	被害報告 ID	個別の被害報告に関する情報を持つ	被害報告作成時に附番
2	画像映像	画像映像 ID	個別の画像映像ファイルに関する情報を持つ	画像映像ファイルを登録した際に附番
3	本部	本部 ID	県・市町の本部に関する情報を持つ	本部を新規設置した際に附番
4	避難所	避難所 ID	避難所に関する平時／災害時の情報を持つ	避難所を新規に登録した際に附番
5	通行規制	通行規制 ID	通行規制に関する情報を持つ	通行規制報告作成時に附番
6	災害名	災害名 ID	個別の災害に紐づく情報を持つ	災害名を新たに設定した際に附番
7	地図オブジェクト	地図オブジェクト ID	地図上に追記した図形・テキストに関する情報を持つ	地図オブジェクトを新たに追加した際に附番
8	掲示板投稿	投稿 ID	システム内掲示板の投稿に関する情報を持つ	掲示板へ新たに投稿した際に附番

2－2 業務の規模

本システムで実現する業務で想定される規模について、以下に示す。過去の業務実績等に基づく値ではなく、本調達時点の想定に基づく値である点に留意すること。

2-2-a システムの利用者数

本システムの利用者について、下表に示す。

表 2-3　システムの利用者数（想定）

項番	利用者	サービス利用者	主な利用拠点	サービス提供時間帯	利用者数	補足
1	県職員	危機管理課をはじめとする、防災業務に携わる県職員	県災害対策本部	24 時間	100 人	本部事務局員の数
2			県災害対策本部以外の本庁舎執務室	24 時間	200 人	
3			県の出先機関	24 時間	200 人	

項番	利用者	サービス利用者	主な利用拠点	サービス提供時間帯	利用者数	補足
4			市町等の派遣先	24 時間	160 人	緊急対策要員の数
5	市町職員	防災業務に携わる市町職員	各市町拠点	24 時間	3,900 人	14 市×200 人 11 町×100 人
6			災害現場・避難所等	24 時間	—	項番 5 に含む
7	救援機関等（消防、警察、自衛隊、DMAT 等）	防災業務に携わる救援機関等の職員	県災害対策本部	24 時間	200 人	
8			救援機関自らの拠点	24 時間	200 人	
9			災害現場（現場指揮所・活動場所等）	24 時間	50 人	
10	国からのリエゾン等（TEC-FORCE 含む）	防災業務に携わる国等の現地連絡職員	県災害対策本部	24 時間	200 人	
11			機関自らの拠点	24 時間	200 人	
12			災害現場	24 時間	200 人	
13	民間団体・企業等（インフラ企業等）	防災業務に携わる民間団体・企業等の職員	県災害対策本部	24 時間	300 人	協定団体数から想定
14			団体・企業等自らの拠点	24 時間	300 人	協定団体数から想定
15	運用保守事業者	防災情報システムの運用保守を行う担当者	栃木県庁本庁舎又は運用保守を行う事業者の拠点	24 時間	複数名で対応	—

2-2-b 処理件数

次期システムを用いた主な業務の処理件数は下表のとおりである。

表 2-4　主な業務の処理件数

項番	項目	処理件数		補足
		平時（災害発生時以外）	災害発生時	
1	被害報告	0 件	～10,000 件/災害	
2	画像映像登録	0 件	～10,000 件/災害	主に画像ファイルを想定しており、短時間動画（1 分以内）は 100 件以下、長時間動画（数十分程度）は 10 件以下と想定。
3	本部設置	0 件	～30 件/災害	
4	避難所登録・報告	2,000 件/年	～2,000 件/災害	
5	通行規制報告	0 件	～10,000 件/災害	
6	掲示板投稿	0 件	～10,000 件/災害	
7	一斉指令	100 件/年	10～50 件/災害	
8	避難発令	0 件	～300 件/災害	
9	情報発信（L アラート等）	～100 件/年	～500 件/災害	

2－3 業務実施の時期・時間

2-3-a 業務実施時期・時間及び繁忙期

本システムを用いた業務実施時期・時間は、原則として 24 時間 365 日とする。本システムに係る業務の通常時と繁忙期を下表に示す。なお、繁忙期においてもレスポンスの低下等を招かないよう、十分な処理性能を確保すること。

表 2-5 業務の通常期・繁忙期

	実施時期・期間	実施・提供時間	補足
通常期	平時（災害発生時以外）	24 時間 （平常時の業務時間は土日及び祝日、年末年始を除く 9:00-17:00）	通常期においては、災害訓練、運用保守のメンテナンス、過去資料の確認等の業務が想定される。
繁忙期	災害発生時	24 時間	-

2-3-b 業務の実施・提供時間

本システムについては、主管課の責任のもとで運用・保守事業者が運用作業を実施する。なお、本システムの機能提供時間、運用時間、システム障害時の対応については以下のとおりである。

2-3-b-(ア) システム機能提供時間

本システムは計画停止を除き、24 時間 365 日機能提供できること。利用者ごとの提供時間帯は「表 2-3 **システムの利用者数（想定）**」に記載の通り。

2-3-b-(イ) 運用時間

運用・保守業者の運用・保守対応時間は平日（土日及び祝日、年末年始を除く）の 9 時から 17 時までとする。ただし、システムの監視は 24 時間 365 日行うこと。なお、夜間や休日におけるシステム障害時の連絡及び運用・保守対応の実施については、受託者と主管課の間で協議することとする。

運用時間に係る詳細については、「4-1 7-e 主な運用作業一覧」を参照すること。

2-3-b-(ウ) システム障害時の対応

システム障害時は復旧を優先し、一次対応を速やかに実施すること。障害の原因究明・恒久的対策についても速やかに実施し、結果を主管課に報告すること。障害時対応に係る詳細については、「4-1 7-e 主な運用作業一覧」を参照すること。

2-3-c ヘルプデスク業務

ヘルプデスク業務における問合せ対応の受付時間を下表に示す。詳細については、「4-1 7-e 主な運用作業一覧」を参照すること。

表 2-6 ヘルプデスク業務の問合せ対応時間

項番	問い合わせ元	問い合わせ方法	受付時間	回答時間	補足
1	主管課※	電話またはメール	平日（土日及び祝日、年末年始を除く）の 9 時から 17 時	平日（土日及び祝日、年末年始を除く）の 9 時から 17 時	受付時間外に到着した問合せメールは翌実の回答時間に速やかに対応すること。

※各利用者からの直接の問い合せ対応は対象外とする。

2－4 業務の実施等

本システムにおける業務の実施場所に関する要件について、以下に示す。

なお、「**表 4-11　調達ハードウェア一覧**」に記載している調達対象端末以外は、本調達の対象に含まない。

表 2-7　利用者の業務実施場所

項番	場所名	実施体制	所在地	入出力端末※	ネットワーク
1	栃木県庁	県災害対策本部	栃木県宇都宮市塙田 1-1-20	・県の業務用 PC 端末 ・県のタブレット端末　等	県の業務用 PC 端末は、庁内ネットワークからインターネット経由で接続 その他の端末はインターネット経由での接続
2		県災害対策本部以外の栃木県庁本庁舎執務室	同上	・県の業務用 PC 端末	
3		県の出先機関	（各出先機関による）	・県の業務用 PC 端末	
4		市町等の派遣先	（各市町による）	・県の業務用 PC 端末 ・県のタブレット端末 ・県のスマートフォン端末 ・個人のスマートフォン端末	
5	市町職員	各市町拠点	（各市町による）	・市町の業務用 PC 端末　等	インターネット経由での接続
6		災害現場・避難所等	（各災害現場・避難所による）	・市町の業務用 PC 端末 ・県のタブレット端末 ・市町のタブレット端末 ・県のスマートフォン端末 ・市町のスマートフォン端末 ・個人のスマートフォン端末	
7	救援機関等（消防、警察、自衛隊、DMAT 等）	県災害対策本部	栃木県宇都宮市塙田 1-1-20	・県の業務用 PC 端末 ・機関の業務用 PC 端末	県の業務用 PC 端末は、庁内ネットワークからインターネット経由で接続 その他の端末はインターネット経由での接続
8		救援機関自らの拠点	（各救援機関による）	・機関の業務用 PC 端末	
9		災害現場（現場指揮所・活動場所等）	（各災害現場による）	・機関のタブレット端末 ・機関のスマートフォン端末	
10	国からのリエゾ	県災害対策	栃木県宇都宮	・県の業務用 PC 端末	県の業務用 PC

項番	場所名	実施体制	所在地	入出力端末※	ネットワーク
	ン等（TEC-FORCE 含む）	本部	市塙田 1-1-20	・機関の業務用 PC 端末 ・県のタブレット端末 ・機関のスマートフォン端末	端末は、庁内ネットワークからインターネット経由で接続 その他の端末はインターネット経由での接続
11		機関自らの拠点	（各機関による）	・機関の業務用 PC 端末	
12		災害現場	（各災害現場による）	・県のタブレット端末 ・機関のタブレット端末 ・機関のスマートフォン端末	
13	民間団体・企業等（インフラ企業等）	県災害対策本部	栃木県宇都宮市塙田 1-1-20	・県の業務用 PC 端末 ・団体・企業等自らの業務用 PC 端末	県の業務用 PC 端末は、庁内ネットワークからインターネット経由で接続 その他の端末はインターネット経由での接続
14		団体・企業等自らの拠点	（各団体・企業等による）	・団体・企業自らの業務用 PC 端末	インターネット経由での接続
15	運用保守事業者	運用保守を行う事業者の拠点	（各運用保守事業者による）	・運用保守事業者の業務用 PC 端末	インターネット経由で接続

※本システムを利用するための各入出力端末にはセキュリティ等の特別な制約は存在しないが、本システム利用のためのアプリケーション導入や web サイトアクセスに伴う必要な調整、設定変更依頼等については各端末の主管担当と調整をおこなうこと。

2－5 業務観点で管理すべき指標

本システムの利用に係る達成度評価指標（KPI：Key performance Indicator）を下表に示す。なお、本システムの利用動向を踏まえ、必要に応じて更に KPI を追加または変更する場合がある。KPI の追加または変更により「表 3-5　モニタリング対象データ一覧（想定）」および「4-17-e 主な運用作業一覧」に変更があった場合は、対応範囲を主管課と協議の上で決定、対応すること。

表 2-8 達成度評価指標（KPI：Key Performance Indicator）

項番	指標種類	指標名	計算式	単位	目標値	計測方法
1	業務効果指標	被害報告の処理時間	被害報告操作を行う際の 1 件あたりの処理時間	秒	40 秒	被害報告を行うページのユーザー毎の滞在時間に係るログデータ
2	業務効果指標	被害情報の集約時間	市町からの被害報告を締め切ってから被害報が完成するまでの時間	分	30 分	災害対応時の時系列情報を確認
3	業務実施指標	電話以外の情報共有手段の利用状	電話以外の情報共有手段を優先的に利用する職員の割合	%	80%	防災訓練の後のアンケート調査

		況				
4	システム性能指標	稼働率	年間実稼働時間 / 1年間　×100	%	99.9%以上	運用･保守事業者作成の報告資料

2－6 情報システム化の範囲

2-6-a 情報システム化の範囲

本調達の範囲は、下図の赤枠部分に示す範囲である。

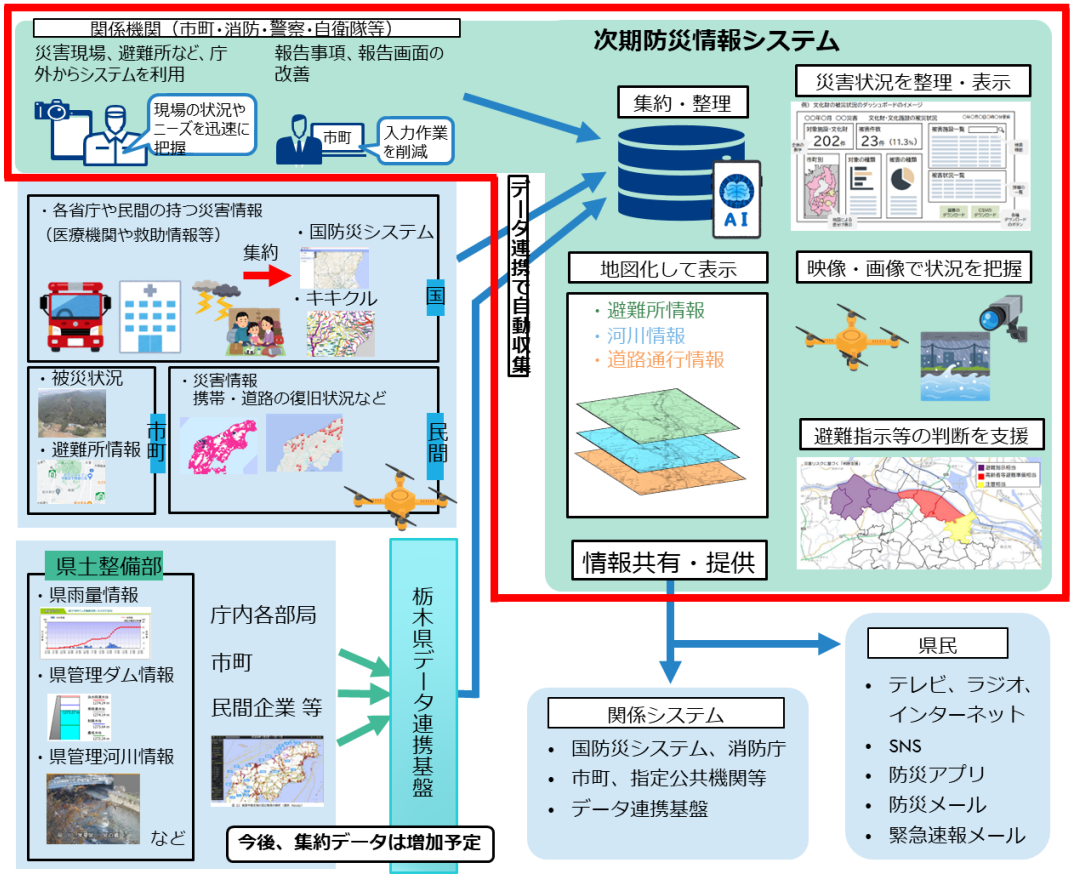

図 2-2　業務概要図

2－7 業務の継続の方針等

システムの継続に関しては「４－９ 継続性に関する事項」に記載する対策を講じること。

2－8 情報セキュリティ対策の方針等

本システムの情報セキュリティ対策に係る具体的な要件は、「４－１０ 情報セキュリティに関する事項」を参照すること。

第３　機能要件

３－１ 機能に関する事項

３-１-a 機能一覧

本調達で要求する主要な機能は「別紙３機能要件一覧」のとおり。詳細な機能構成は、要件定義工程にて主管課と協議の上決定すること。機能の大まかな分類は下記のとおり。

表 3-1 機能の大分類一覧

項番	大分類名	説明
1	情報収集	被害状況や災害対応に必要な情報を収集するための機能。市町等の職員による被害報告機能、災害対策本部管理機能、画像・映像の収集機能などを含む。
2	情報整理・共有	収集した情報を整理分析し、関係者間で共有するための機能。被害情報をダッシュボードへ集約表示する機能、被害報の作成機能、システム内掲示板機能等を含む。
3	情報提供	県民等に対する情報提供を行うための機能。避難発令機能、Ｌアラート発信機能、防災ポータルサイトでの情報提供機能等を含む。
4	共通	システム全般に関連する共通機能。システムへのログイン・認証機能、アカウント管理機能、データ連携機能、訓練機能、運用監視機能等を含む。

３-１-b 機能の主な追加・変更点

本システムでは下表の観点での機能の見直しを行う予定である。

表 3-2 機能の主な追加・変更点

項番	変更区分	主な観点	説明
1	新規追加	業務用端末、携帯端末でのシステム利用	閉域網＋専用端末の構成からインターネット＋クラウドの構成に変更し、業務用端末での利用や庁外での携帯端末の利用を可能とする、
2	変更	被害報告の簡便化	市町による被害報告の入力の手間を減じるため、被害報告1件あたりの操作時間を削減するとともに、市町システムとデータ連携可能な構成にする。
3	変更	画像映像の積極活用	画像映像の積極活用に向け、映像関連の機能強化、使い勝手向上を行う。
4	新規追加	孤立集落に関する情報集約機能	孤立集落に関する情報収集・集約機能を新たに設定する。
5	変更	ダッシュボード機能、地図機能の充実	災害情報をシステム内のダッシュボード、地図を確認するのみで把握できるよう、機能向上、反応速度の向上等を行う。
6	新規追加	判断支援機能の追加	避難発令などの判断に関して、職員の判断に必要な情報を提示することで、経験の浅い職員でも的確に対応可能とする。
7	新規追加	システム内掲示板機能の追加	システム内の掲示板で関係者間のやり取りを完結させ、電話等によるコミュニケーションを削減する。
8	変更	県民向け情報の充実	防災ポータルサイトに掲載する情報を充実させるとともに、引き続き SNS 等の各種手段への情報提供を充実させる。

3-1-c 機能構成概念図

本サービスの機能構成図を以下に示す。

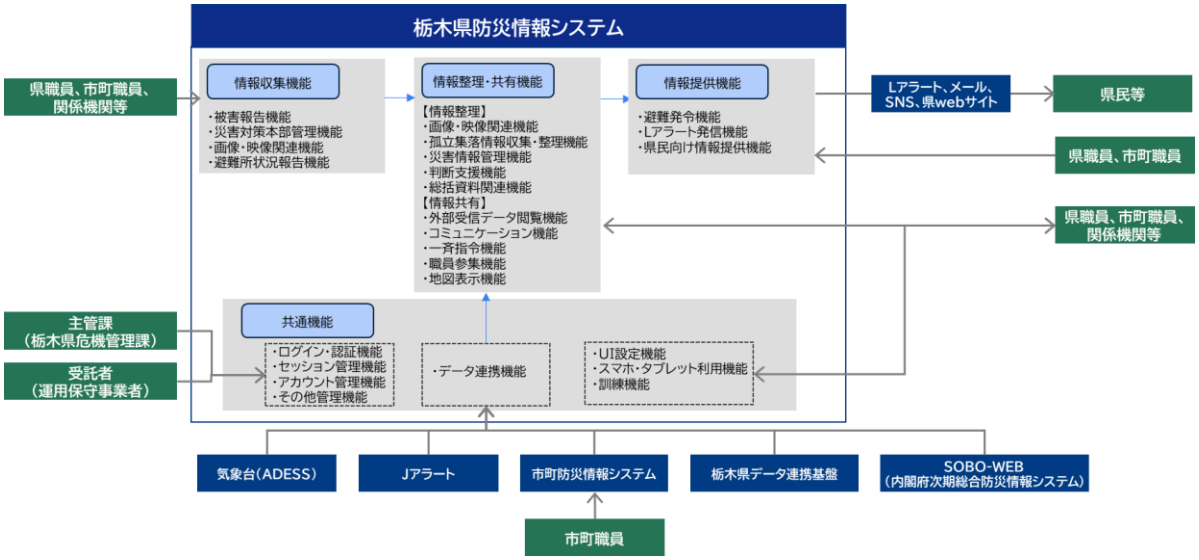

図 3-1 機能構成概念図

3－2 画面に関する事項

前述の「３－１ 機能に関する事項」を実現するために必要な画面については、本システムの受託者の提案を踏まえ、設計時点で決定する。

画面レイアウト等の設計に当たっては、予めワイヤーフレーム（画面の完成イメージを線や枠で表現したもの）などを作成し、主管課の了承を得た上で設計を行うこと。

3-2-a 画面一覧

個別具体のユーザーインタフェースとして実装する際の画面構成、画面レイアウト、画面タイトル等のラベル、画面遷移等の詳細は基本設計工程で定める。本要件定義書では画面設計に当たっての基本的な方針を定める。

3-2-b 画面設計ポリシー

画面設計における要件を以下に示す。

3-2-b-(ア) UX デザイン

UX デザインについては、「４－１ ユーザビリティ及びアクセシビリティに関する事項」の要件を考慮すること。

3-2-b-(ｲ) 画面の表示

画面の表示に関して、利用者に正しく内容を伝達するために、以下の要件を満たすこと。

- 画面の表示にはHTMLを利用し、Webブラウザ上で正常に表示されることを確認すること。また、JavaScript を無効にした状態でも最低限のコンテンツ情報を閲覧可能とすること。
- 画面の表示で使用する Web ブラウザには追加でプラグイン等のインストールを必要としないこと。
- Web ブラウザのバージョン更新があった際は、基本的には更新前のバージョンへの対応を保ちつつ、更新後のバージョンに対応させること。やむを得ず、双方のバージョンへの対応が困難な場合は、対応を優先するバージョンは主管課が判断を行うものとする。
- 利用者が他に起動している Web ブラウザの動作に干渉しないように配慮すること。
- Web ブラウザや利用端末の要件については、「４-１１-h 利用端末の要件」を参照すること。

3-2-b-(ｳ) 入力負荷の軽減

画面での入力操作は以下の要件を満たすこと。

- 画面での入力操作は、本業務の特性も踏まえ、ドロップダウン、ラジオボタン、チェックボックス、カレンダー等既定情報からの選択とする等、入力負荷の軽減及び誤操作防止への配慮をおこなうこと。

3-2-b-(ｴ) 誤操作の防止

利用者認証情報を取り扱う重要性を考慮し、誤操作によるデータの消失や誤った情報の登録等を防止する為、以下の要件を満たすこと。

- Web ブラウザ自体が備えている「戻る」、「更新」等のボタンを押下しても、二重登録などの不具合が発生しないこと。
- Web ブラウザで表示する画面内のボタンを連続で押下しても、二重登録などの不具合が発生しないこと。
- 検索処理中に再度の検索実行が行われないこと。(検索処理中は検索実行ボタンを非活性化する等)。

3-2-b-(ｵ) メニュー

メニューについては、以下の要件を満たすこと。

- 各画面の上部に統一的な操作メニューを表示し、他の画面への遷移を可能とすること。
- 現在の画面のメニュー体系における位置を階層的に表示し、他の画面への遷移を可能とすること。
- 利用用途（情報入力、システム管理等）、利用者（県、市町等）により操作可能な画面が異なるため、権限設定に応じたメニュー表示を可能とすること。

3－3 帳票に関する事項

本システムの帳票に関する要件を「表 3-3　帳票一覧」に示す。法定帳票以外の帳票については、代替手段を積極的に提案して帳票の削減を図ること。

3-3-a 帳票一覧

原則として、各帳票間で基本レイアウトの統一を図ること。なお、帳票の実装方式については、現時点で広く使われている技術を前提として、ユーザビリティや開発効率性の観点から優れた方法を選択するよう特に留意すること。

なお、「種別」の項では、帳票の様式が一意に定まっているものを「確定様式」、システム構築時に主管課と調整して決めるものを「任意様式」としている。

表 3-3 帳票一覧

項番	帳票名	帳票概要	入出力形式	分類	種別
1	栃木県被害報	大規模災害等の際に県が作成する被害報の様式。	以下のいずれか xlsx docx	①情報収集　被害報告	任意様式
2	消防庁第 1 号様式（火災）	消防庁災害即報要領に規定される第1号様式。	xlsx	①情報収集　被害報告	確定様式
3	消防庁第 2 号様式（事故）	消防庁災害即報要領に規定される第2号様式。	xlsx	①情報収集　被害報告	確定様式
4	消防庁第 3 号様式（救急等）	消防庁災害即報要領に規定される第3号様式。	xlsx	①情報収集　被害報告	確定様式
5	消防庁第 4 号様式（災害概況）	消防庁災害即報要領に規定される第4号様式。	xlsx	①情報収集　被害報告	確定様式
6	被害報告一覧	システムへ入力された被害報告の一覧。	csv/xlsx	①情報収集　被害報告	任意様式
7	被害報告集計結果	システムへ入力された被害報告の数値等に集計したもの。	csv/xlsx	①情報収集　被害報告	任意様式
8	通行規制情報一覧	システムへ入力された通行規制情報の一覧。	csv/xlsx	①情報収集　通行規制	任意様式
9	避難所状況一覧	システムへ入力された避難所状況の一覧。	csv/xlsx	①情報収集　避難所	任意様式

項番	帳票名	帳票概要	入出力形式	分類	種別
10	避難所状況集計結果	システムへ入力された避難所状況の数値等を集計したもの。	csv/xlsx	①情報収集　避難所	任意様式
11	本部設置状況一覧	システムへ入力された本部設置状況の一覧。	csv/xlsx	①情報収集　本部	任意様式
12	孤立集落報告一覧	システムへ入力された孤立集落報告の一覧。	csv/xlsx	②情報整理・共有　孤立集落	任意様式
13	災害状況のダッシュボード	ダッシュボードに集約された災害概況情報。	以下のいずれか xlsx docx pptx	②情報整理・共有　ダッシュボード	任意様式
14	時系列情報の一覧	時系列情報として投稿されたデータの一覧。	csv/xlsx	②情報整理・共有　時系列情報	任意様式
15	災害対策本部会議資料（総括資料）	災害対策本部会議資料として使用するための総括資料の様式。	以下のいずれか xlsx docx pptx	②情報整理・共有　総括資料作成	任意様式
16	システム内掲示板投稿一覧	システム内掲示板に投稿されたデータの一覧。	csv/xlsx	②情報整理・共有　システム内掲示板	任意様式
17	一斉指令発信履歴一覧	一斉指令機能によりメール配信を行った履歴の一覧。	csv/xlsx	②情報整理・共有　一斉指令	任意様式
18	受信確認状況一覧	一斉指令機能によるメールを受け取った者の受信確認状況の一覧。	csv/xlsx	②情報整理・共有　一斉指令	任意様式
19	職員参集メール発信履歴一覧	職員参集メールの配信を行った履歴の一覧。	csv/xlsx	②情報整理・共有　職員参集	任意様式
20	職員参集メール回答状況一覧	職員参集メールに付した設問への回答状況の一覧。	csv/xlsx	②情報整理・共有　職員参集	任意様式
21	避難発令状況一覧	システムに入力された避難発令状況の一覧。	csv/xlsx	③情報提供　避難発令	任意様式

3-3-b オープンデーター覧

本システムのオープンデータを下表に示す。

表 3-4　オープンデーター覧

項番	データ名	利用者	概要・目的
1	各種警報等	県民等	防災ポータルサイトに本データを掲載することで、県民等が防災ポータルサイトを閲覧した時点での各種警報等の発令状況を把握できるようにする。
2	避難発令状況	県民等	防災ポータルサイトに本データを掲載することで、県民等が防災ポータルサイトを閲覧した時点での避難発令状況を把握できるようにする。
3	避難所開設状況	県民等	防災ポータルサイトに本データを掲載することで、県民等が防災ポータルサイトを閲覧した時点での避難所開設状況を把握できるようにする。

項番	データ名	利用者	概要・目的
4	映像配信 URL	県民等	河川カメラ、道路カメラなどウェブ上で配信されているライブカメラの URL を、防災ポータルサイトに掲載することで、県民等が防災ポータルサイトを閲覧した際に自身付近のカメラ映像にアクセスできるようにする。
5	通行規制状況	県民等	防災ポータルサイトに本データを掲載することで、県民等が防災ポータルサイトを閲覧した時点での、自身付近の道路の通行規制状況を把握できるようにする。
6	L アラート発信情報	県民等、報道機関、国・他自治体等	L アラートを通じて避難発令、避難所開設状況、お知らせ等の各種情報を送信する。
7	防災メール発信情報	県民等	事前に登録した県民等に対して防災メールを送信し、避難発令、避難所開設状況等の各種情報を提供する。
8	SNS・民間アプリ発信情報	県民等	SNS・民間防災アプリに対してメッセージを投稿し、県民等に対する災害に関する各種呼びかけの情報を提供する。

3-3-c モニタリング対象データー覧

「２－５ 業務観点で管理すべき指標」に記載したプロジェクトの目標について、実績値を適時に確認するデータとして、現時点の案を示す。

表 3-5 モニタリング対象データー覧（想定）

項番	データ名	分析軸となる項目	目的
1	ユーザー毎の本システム web サイトの滞在時間に係るログデータ	アカウント種別、各ページ単位での滞在時間	被害報告操作を行う際の処理時間について、ページ滞在時間を通じて計測・予測できること。
2	システム障害に係る各種情報	システム停止していた時間、システム停止原因	システム稼働率が計測できること。

3－4 外部インタフェースに関する事項

本システムの外部インタフェースに関する要件を以下に示す。なお、一部のインタフェースは機能要件の変更に合わせて修正が必要となることが想定される。新たに追加となった機能への対応を含め、外部インタフェースの修正が必要になる場合については、設計工程で主管課と協議の上で対応すること。

3-4-a 外部インタフェース一覧

本システムは、下表に示す他の情報システム等と連携する。なお、外部インタフェース一覧における記載内容は現在の想定である。設計工程において、連携先システム担当と調整の上、決定すること。

表 3-6　外部インタフェース一覧

項番	外部インタフェース名	外部インタフェース概要	送受信区分	送受信データ種別	プロトコル	文字コード	補足
1	消防庁（被害情報収集ハブ）	L アラートと同じ経路で被害情報等を送信する	送信	XML	HTTP（SOAP）	UTF-8	
2	気象台 ADESS	各種気象・地震・火山等の情報を受信する	受信	XML	TCP/IP ソケット	UTF-8	
3	J アラート	国民保護に関する情報を受信する	受信	J-ALEART 受信機独自データ形式	TCP/IP ソケット	Shift-JIS	
4	市町システム	市町が入力した被害報告を事案毎に連携する	送信／受信	調整中	調整中	調整中	県内市町は 2 社のシステムを利用中
5	栃木県データ連携基盤	県土整備部等からの情報受信、次世代 GIS 等への情報発信を行う	送信／受信	JSON(NGSIv2 形式)（Fiware の API）	HTTPS	UTF－8	構築中であり、今後データ項目が拡充されていく予定
				バイナリ全般（画像データ等）	HTTPS	制約なし	
6	総合防災情報システム（SOBO-WEB）	災害対応に係る各種情報の受信、県からの被害情報などの報告を行う	送信／受信	SIP4D-ZIP	HTTPS/SFTP/FTP	UTF-8	連携するデータ項目は調整中
7	L アラート	L アラートを送信する	送信	XML	HTTP(SOAP)	UTF-8	
8	公開 HP	公開 HP の情報を送信する	送信	XML	HTTP/REST	UTF-8	
9	防災メール	気象台やお知らせ等の情報を送信する	送信	XML	HTTP/POST	UTF-8	
10	緊急速報メール（Softbank）	災害に関する速報メール等を発信する	送信	HTML	HTTPS	Shift-JIS（URL エンコード）	
11	緊急速報メール（au）	災害に関する速報メール等を発信する	送信	HTML	HTTPS	Shift-JIS（URL エンコード）	
12	緊急速報メール（楽天）	災害に関する速報メール等を発信する	送信	HTML	HTTPS	Shift-JIS（URL エンコード）	

項番	外部インタフェース名	外部インタフェース概要	送受信区分	送受信データ種別	プロトコル	文字コード	補足
13	エリアメール（NTT docomo）	災害に関する速報メール等を発信する	送信	HTML	HTTPS	Shift-JIS（URL エンコード）	
14	SNS	災害に関する内容を SNS 投稿する	送信	API	HTTPS	UTF-8	X を想定
15	Yahoo! 防災アプリ	災害に関する内容を発信する	送信	API	HTTPS	UTF-8	

第４　非機能要件

４－１ ユーザビリティ及びアクセシビリティに関する事項

４-１-a 本システムの利用者の種類、特性

本システムの利用者の特性を、目的に応じて以下の表の通り区分する。

表 4-1　利用者の特性

項番	利用者区分	利用者の種類	利用イメージ	利用者の特性
1	県職員	県災害対策本部	• 災害名等の入力や、各種災害情報の閲覧、班・市町等のやり取りや、情報発信を行う。 • 業務用端末、電子黒板を主に利用して業務を実施。 • 情報収集機能のうち分析に係る機能、ならびに情報整理・共有機能を主に利用。	• 災害対応業務に係る知見があり、また、防災情報システムの取り扱いに習熟している。 • タブレット・スマートフォンでの防災情報システムの操作には不慣れであると想定されるため、分かりやすいUIを考慮する必要がある。 • 他利用者と比較して、最も多くの情報を閲覧すると想定されるため、情報整理をしやすい機能・画面にする必要がある。
2		県災害対策本部以外の栃木県庁本庁舎執務室	• 各種情報の入力や、情報の閲覧、災害本部員等とのやり取りを行う。 • 業務用端末からシステムを利用。 • 情報整理・共有機能の中の情報共有関連機能を主に利用。	
3		県の出先機関	• 各種情報の入力や、情報の閲覧、本庁・市町とのやり取りを行う。 • 主に業務用端末、携帯端末からシステムを利用。 • 情報整理・共有機能を主に利用するが、情報収集機能を使用する場合もあり。	
4		市町等の派遣先	• 被害情報の代行入力や、市町の被害状況の把握、本庁とのやり取りを行う。 • 主に業務用端末、携帯端末からシステムを利用。 • 情報収集機能、ならびに情報整理・共有機能の中の情報共有関連機能を主に利用。	
5	市町職員	各市町拠点	• 被害情報の入力や、市町の被害状況の把握、県・関係機関等とのやり取り、市民への情報発信を行う。 • 主に市町の業務用端末からシステムを利用。 • 情報収集機能、情報整理・共有機能、情報提供機能を利用。	• タブレット・スマートフォンでの防災情報システムの操作には不慣れであると考えられるため、分かりやすいUIを考慮する必要がある。 • 災害時において

項番	利用者区分	利用者の種類	利用イメージ	利用者の特性
6		災害現場・避難所等	• 現場からの被害情報の入力や、現場付近の被害状況の把握、市町庁舎等とのやり取りを行う。 • 主に携帯端末からシステムを利用。 • 情報収集機能を主に利用。	は、被害確認や被災者からの問い合わせ対応等、多様な業務により非常に多忙であることが想定されるため、そのような状況下においてもシステム入力が過度な負担とならないよう、簡便かつ迅速に入力できるよう、UI 及び入力必須項目について考慮する必要がある。
7	救援機関等（消防、警察、自衛隊、DMAT 等）	県災害対策本部	• 活動状況等の情報入力、関連する情報閲覧、災害対策本部員、他機関とのやり取りを行う。 • 自機関の端末からシステムを利用。 • 情報整理・共有機能を主に利用。	• 防災情報システムの操作・閲覧には不慣れであると想定されるため、分かりやすいUIを考慮する必要がある。
8		救援機関自らの拠点	• 関連する情報閲覧、リエゾン等とのやり取りを行う。 • 自機関の端末からシステムを利用。 • 情報整理・共有機能を主に利用するが、情報収集機能を利用する場合あり。	
9		災害現場	• 現場からの被害情報の入力や、現場付近の被害状況の把握、他機関等とのやり取りを行う。 • 自機関の端末からシステムを利用。 • 情報整理・共有機能を主に利用するが、情報収集機能を利用する場合あり。	
10	国からのリエゾン等（TEC-FORCE 含む）	県災害対策本部	• 活動状況等の情報入力、関連する情報閲覧、災害対策本部員、他機関とのやり取りを行う。 • 自機関の端末からシステムを利用。 • 主に情報整理・共有機能を利用。	• 防災情報システムの操作・閲覧には不慣れであると想定されるため、分かりやすいUIを考慮する必要がある。

項番	利用者区分	利用者の種類	利用イメージ	利用者の特性
11		機関自らの拠点	• 関連する情報閲覧、災害対策本部員等とやり取りを行う。 • 自機関の端末からシステムを利用。 • 主に情報整理・共有機能を利用。	
12		災害現場	• 現場からの被害情報の入力や、現場付近の被害状況の把握、他機関等とのやり取りを行う。 • 自機関の端末からシステムを利用。 • 主に情報整理・共有機能を利用。	
13	民間団体・企業等（インフラ企業等）	県災害対策本部	• 関連する情報閲覧、災害対策本部員、他機関とのやり取りを行う。 • 自機関の端末からシステムを利用。 • 主に情報整理・共有機能を利用。	• 防災情報システムの操作・閲覧には不慣れであると想定されるため、分かりやすいUIを考慮する必要がある。
14		団体・企業等自らの拠点	• 関連する情報閲覧、リエゾン等とのやり取りを行う。 • 自機関の端末からシステムを利用。 • 主に情報整理・共有機能を利用。	
15	受託者（運用保守実施者）	運用保守を行う受託者の拠点	• 防災情報システムの運用保守を行う。 • 自機関の端末からシステムを利用。 • システム管理者が実施する必要がある各種操作を実施。	• 「4－17 運用に関する事項」及び「4－18 保守に関する事項」を円滑かつ確実に実施する必要がある。

4-1-b ユーザビリティ要件

本システムのユーザビリティ要件を以下に示す。

表 4-2 ユーザビリティ要件

項番	分類	全体方針
1	画面構成	• 利用者が操作方法を直観的に理解できるデザインとすること。 • スマートフォンでの閲覧を考慮し、レスポンシブ対応とすること。 • 画面に表示される各コンテンツの視認性に配慮すること。 • 画面遷移、ボタン機能の操作性は画面表示及び構成に統一性を持たせた配置とすること。
2	画面の構成（フォント及び文字サイズ）	• 十分な視認性のあるフォント及び文字サイズを使用すること。 • 画面サイズや位置を変更できること。 • 一度に膨大な情報を提示して利用者を圧倒しないようにすること。
3	画面の構成（マルチデバイス対応）	• スマートフォン、タブレット端末により本システムを利用する利用者を想定し、これら端末の特性を考慮した画面にすること。 • レスポンシブデザインにより、PC、タブレット端末、スマートフォン等の利用

項番	分類	全体方針
		環境を問わず、同一の情報をグリッドレイアウト等の適切なレイアウトにより表示できるようにすること。
4	画面の構成 （表示/非表示）	• 情報の優先順位をつけ、重要度の低い情報、特定の利用者層に対して提示する情報は、利用者が必要に応じて表示/非表示を切替え可能とする等の工夫をすること。
5	画面の構成（クリックやチェックができる箇所）	• 画面上でクリックやチェックができる箇所とできない箇所の区別を明確にすること。 • タップ操作が可能なタブレット端末やスマートフォンの場合は、タップ操作の結果（どの部分をタップしたのか）を適切にレスポンスできること。
6	画面遷移	• 利用者が次の処理を想像しやすい画面遷移とすること。 • 無駄な画面遷移を排除し、シンプルな操作とすること。
7	画面表示・操作の一貫性（統一）	• 機能、用語、レイアウト、操作方法は統一すること。
8	画面表示・操作の一貫性（視認性）	• 必須入力項目と任意入力項目の表示方法を変えるなど各項目の重要度を利用者が認識できるようにすること。 • 見やすさを考慮し、画面のフォントサイズを決定すること。 • 画面ごとに異なるフォントを使わないこと。
9	操作のわかりやすさ	• 無駄な手順を省き、使いやすく、利用者が効率的に作業できるようにすること。 • 利用者が操作しやすい手順にするため、画面上の情報項目を上から下へ、左から右へ流れる順番に配置すること。 • 利用者の操作を軽減できるよう、画面の初期表示時、入力項目、選択項目等に適切な既定値を設定すること。
10	操作方法のわかりやすさ（操作説明）	• 原則としてマニュアルを参照しなくても操作できるようにすること。
11	操作方法のわかりやすさ（画面遷移）	• 利用者が同じ情報の入力や操作を何度も行う必要がないよう、画面が遷移しても情報がその後の手順に反映されるようにすること。 • 利用者の手間を軽減するため、利用者の手順に即した画面遷移に留意し、可能な限り不要な画面遷移を行わないようにすること。
12	操作方法のわかりやすさ（マルチデバイス対応）	• スマートフォン、タブレット端末等の狭い表示領域、タッチインタフェースでも効率的に作業できる操作性を実現すること。
13	指示や状態のわかりやすさ	• ユーザーインタフェース及び UX に関する一般的に使われているデザイントレンドを取り入れ、アイコン・図表のグラフィック表現を適切に適用すること。 • 本システムが処理している内容や状況を、利用者が把握できるようにすること。
14	指示や状態のわかりやすさ（外部ドメインへの遷移）	• ドメインを異にする他の Web サイトへの遷移を行う際は、離脱メッセージを表示する等、利用者が認識できるようにすること。
15	メッセージ出力	• 利用者に分かりやすいメッセージとすること。 • 必要に応じて、登録・変更・削除等の操作を行う場合には、確認画面等で表示し、利用者の注意を促すこと。 • 処理時間がかかる操作では、処理中であることが分かるようにすること。
16	メッセージ出力 （次の操作）	• 指示メッセージは、次操作が具体的にイメージできるようなメッセージ出力を行うこと。
17	エラーの防止と処理	• 利用者が操作や入力を間違えないデザインや案内を提供すること。

項番	分類	全体方針
18	エラーの防止と処理(エラー防止)	• 利用者の誤操作を想定し、入力チェック機能によりエラーを防止すること。 • 入力値が選択できる場合には、プルダウンメニュー等を活用し、極力キーボード入力操作をなくすこと。
19	エラーの防止と処理(エラーメッセージ)	• エラーメッセージは、その内容が分かりやすく表示されるとともに、利用者が何をすればよいかを示すこと。
20	エラーの防止と処理(エラー表示と解決策)	• 入力内容の形式に問題がある項目については、利用者がその都度該当項目を容易に見つけることができるようにすること。 • エラーが発生した時は、利用者が迷わずに問題解決できるよう、操作の続行に必要な選択肢を利用者が適切に理解できるようわかりやすく提示すること。 • 入力内容の形式に問題がある項目については、それを強調表示する等、利用者がその都度その該当項目を容易に見つけられるようにする。
21	エラーの防止と処理(確認画面)	• 必要に応じて、登録、更新、削除等の処理の前に確認画面を用意し、利用者が行った操作や入力のやり直し、取り消しがその都度できるようにすること。 • 重要な処理については、事前に注意喚起し、利用者の確認を促すこと。
22	エラーの防止と処理(画面遷移)	• 入出力の過誤があった場合、次の画面へ遷移しないこと。
23	エラーの防止と処理(情報保持)	• タブレット端末等、屋外での使用を考慮し、電波受信状況の悪い場所においても操作不能とならないよう工夫すること。
24	ヘルプ	• 利用者が必要とする際に、ヘルプ情報やマニュアル等を容易に参照できるようにすること。 • ヘルプ情報やマニュアル等についても、利用者が必要な情報を容易に検索できるようにすること。
25	画面遷移、操作ログ等の分析	• 運用・保守工程において継続的に UI/UX の改善を検討できるよう、利用者の画面遷移、操作ログ等を分析できる仕組みを整備すること。
26	言語対応	• 本システムで対応する言語は日本語のみとする。ただし、機能要件「F-42 防災ポータルサイト情報提供機能」において情報提供するコンテンツについては、機能要件に記載された各言語に対応すること。

4-1-c アクセシビリティ要件

本システムのアクセシビリティ要件を以下に示す。

表 4-3　アクセシビリティ要件

項番	分類	全体方針
1	基準等への準拠	• 日本産業規格 JIS X8341 シリーズ、「みんなの公共サイト運用ガイドライン」(総務省)に準拠し、以下を前提とすること。 https://www.soumu.go.jp/main_sosiki/joho_tsusin/b_free/guideline.html • JIS X 8341-3:2016「高齢者・障害者等配慮設計指針－情報通信における機器, ソフトウェア及びサービス－第3部:Webコンテンツ」の適合レベル AA に準拠することを目標とする。また、レベル AAA のうち、以下の達成基準についても可能な範囲で適用すること。 ✓ 2.1.3 キーボード(例外なし)の達成基準 ✓ 2.3.2 3 回のせん(閃)光の達成基準 ✓ 2.4.8 現在位置の達成基準 ✓ 3.2.5 要求による状況の変化の達成基準 注記:本仕様書における「準拠」という表記は、情報通信アクセス協議会 Web

項番	分類	全体方針
		アクセシビリティ基盤委員会「Web コンテンツの JIS X 8341-3:2016 対応度表記ガイドライン（令和 3 年 4 月版）」で定められた表記による。 • また、スマートフォン等での操作を行うユーザーが増えていることを踏まえ「Web Content Accessibility Guidelines（WCAG）2.1」で追加された達成基準についても、可能な範囲で適用すること。 ✓ 1.3.4 表示の向き（レベル AA） ✓ 2.5.1 ポインタのジェスチャ（レベル A） ✓ 2.5.2 ポインタのキャンセル（レベル A） ✓ 2.5.4 動きによる起動（レベル A） ✓ 4.1.3 ステータスメッセージ（レベル AA） • デジタル庁が整備する「ウェブアクセシビリティ導入ガイドブック」を参考にすること。
2	指示や状態の分かりやすさ	• 色の違いを識別しにくい利用者（視覚障がいのかた等）を考慮し、利用者への情報伝達や操作指示を促す手段はメッセージを表示する等とし、可能な限り色のみで判断するようなものは用いないこと。ただし、業務の利用用途から、画面色での振り分けを行うことを予定していることから、適用範囲及び配色については主管課と協議し、決定すること。 • Web ブラウザ等の音声読み上げ機能を活用し、視覚障がいの方でも問題なく利用可能な UI とすること。
3	マルチデバイス対応	• 解像度の低い機種、画面サイズの小さい機種でも、業務継続が可能な UI とすること。 • OS の設定でフォントサイズ・表示サイズをそれぞれ最大とした場合でも、業務継続が可能な UI とすること。 • スタイルシートを利用しないユーザーと利用するユーザーにおいて得られる情報に差（表示されない文字や画像がある等）がないこと。レイアウトにおいても大きな差がないことが望ましい。

4－2 システム方式に関する事項

4-2-a システム方式についての全体の方針

本システムの構成に関する全体の方針を以下に示す。なお、安全かつ安定的なサービス提供を前提とし、実現性が十分であることを担保できる場合は、コスト効率を高めることを基本とする。

表 4-4　システム方式についての全体の方針

項番	分類	全体方針
1	システムアーキテクチャ	• 本システムのシステムアーキテクチャはクラウド上に用意される Web アプリケーションから構成される想定である。Web アプリケーションは利用者の端末に追加的なソフトウェアのインストール等を行うことなく、一般に利用されている Web ブラウザで処理を行うものとする。 • 本システムや業務機能等の特性を十分に検討し、クラウドサービスプロバイダが提供するリファレンスアーキテクチャに準拠した形で PaaS、SaaS、IaaS 等の最適なサービスを採用し、システムを構築する。 • クラウドサービスプロバイダが提供するマネージドサービスを最大限活用することを基本とし、アプリケーションの作り込みを削減できる設計とする。特にデータベース、認証、セキュリティ機能や運用管理機能はクラウドサービスが提供する機能を最大限活用すること。 • クラウドサービスが責任共有モデルとして提供されている前提を踏まえ、クラウドサービスを利用するに当たって必要となる考慮事項について検討を

項番	分類	全体方針
		行い、安全かつ効率的に情報システムを構築する。 • 予防的統制と発見的統制を実施すること。また、クラウドサービスを利用するために作成する各種アカウントについては、ガバナンスやセキュリティに係るポリシーを設定の上で、権限管理を確実に行うこと。管理者アカウントについては、多要素認証を必須とすること。 • 全体構成及び利用するクラウドサービスについては、受託者において移行、引き継ぎ、確実なサービス提供等について問題が生じないことをクラウドサービスプロバイダに応札前に確認し、本調達の要件を踏まえ、確認結果と合わせて適切なものを提案する。
2	アプリケーションの設計方針	• マイクロサービスアーキテクチャ、API、クラウドネイティブ、クラウドサービスのマネージドサービスのみによる構成等、モダン技術を前提として構築する。 • クライアントサーバ方式、専用端末のシンクライアント（VDI）等の旧来技術は、高コスト化の要因となるため採用しないこと。 • 原則としてバッチ処理を採用せず、リアルタイム処理を基本とすること。バッチ処理が必要となる場合は、その理由について主管課の承認を得た上で採用すること。 • 本システムを構成する各コンポーネント（ソフトウェアの機能を特定単位で分割したまとまり）間の疎結合、再利用性の確保を基本とする。 • 本システムが取り扱うデータの保管・管理に際して、データの容量、更新頻度、保存期間等を考慮し最適なストレージサービスを選定の上、利用する。またデータの保管・管理方針が変更となった際に、ストレージサービス間でのデータの移行が容易となるよう設計上考慮する。
3	ソフトウェア製品の活用方針	• SaaS については、開発量削減の観点から幅広く優先的に、その利用を検討すること。ただし、ニーズにマッチしているか、開発量削減に貢献するか、セキュリティ対策は十分か、費用対効果は十分に得られるか等を慎重に考慮すること。 • 広く市場に流通し、利用実績を十分に有するソフトウェア製品を活用する。 • アプリケーションの動作、性能等に支障を来たさない範囲において、可能な限りオープンソースソフトウェア（OSS）製品（ソースコードが無償で公開され、改良や再配布を行うことが誰に対しても許可されているソフトウェア製品）の活用を図る。ただし、それらの OSS 製品のサポートが確実に継続されていることを確認しなければならない。 • ノンプログラミングによる画面生成等プロトタイピング用のツール等を利用することにより、システムライフサイクルコストの削減等が見込める場合には、積極的に採用を検討すること。

4-2-b クラウドサービスの選定、利用に関する要件

- セキュリティ確保のため、本システムで用いるクラウドサービスは、原則として ISMAP クラウドサービスリストまたは ISMAP-LIU クラウドサービスリストに登録されているクラウドサービス、またはこれと同等のセキュリティレベルが確保されているクラウドサービスを選定すること。
- 要機密情報を取り扱うクラウドサービスの選定、利用に関しては、「政府機関等のサイバーセキュリティ対策のための統一基準 （令和 5 年度版）」の「4.2.1 クラウドサービスの選定（要機密情報を取り扱う場合）」「4.2.2 クラウドサービスの利用（要機密情報を取り扱う場合）」の内容を遵守すること。
- 情報資産を管理するデータセンターの設置場所に関しては、国内であること

を基本とする。設置場所の考え方についてはクラウド方針を参照すること。

- 契約の解釈が日本法に基づくものであること。
- クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を専属的合意管轄裁判所とするものであること。
- 主管課の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。情報資産を国外に設置されるクラウドサービスに保管する際の考え方についてはクラウド方針を参照すること。なお、利用者がアクセス可能な部分を除き、国外から情報資産へアクセスする場合も日本国外への持ち出しに該当する。
- 障害発生時に縮退運転を行う際にも、情報資産が日本国外のデータセンターに移管されないこと。
- 情報資産の所有権がクラウドサービス事業者に移管されるものではないこと。従って、主管課が要求する任意の時点で情報資産を他の環境に移管させることができること。
- 今後、利用者の拡大が見込まれることから、今後の発行アカウント数の拡大時の安定稼働や運用費用の抑制等の観点から、本調達の趣旨に適したクラウドサービスを利用すること。
- クラウドサービスの可用性を保証するための十分な冗長性、障害時の円滑な切替え等の対策が講じられていること。
- クラウドサービス上で取り扱う情報について、機密性及び完全性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実に行うこと。
- クラウドサービスに係るアクセスログ等の証跡を保存し、主管課からの要求があった場合は提供すること。
- インターネット回線を通じたセキュリティ侵害を防ぐため、インターネット回線とクラウド基盤との接続点の通信を監視すること。
- クラウドサービスの提供に関する次のいずれかの認証を取得していること。

  ISO/IEC 27017:2015

  CS マーク（特定非営利活動法人日本セキュリティ監査協会（JASA）のクラウドセキュリティ推進協議会が定めるもの）

4-2-c 開発方式及び開発手法

本システムの開発方式及び開発手法を以下に示す。

- 本システムの開発方式及び開発手法は、主管課の要求等を取り入れつつ、要求の変更による手戻りを防止できる手法とすること。
- 本調達の開発方式については、特定の方式に制限はしないが、スクラッチ開発／アプリケーションプログラムの移植／ソフトウェア製品のカスタマイズ

等より提案すること。

- 本調達の開発手法（ウォーターフォール、アジャイル等）は、構築・運用保守事業者において、豊富な成功実績を有する確立されたフレームワーク（設計・開発プロセス）を採用すること。なお、主管課による仕様確認及び進捗確認作業実施が容易であること。
- 受託者は開発標準を提案すること。また開発時には、当該開発標準を作業担当者に確実に周知すること。

4-2-d 機器の設置方針

本システムの設置場所及びクラウドサービスの場所は、日本国内（リージョン）とすること。

4－3 規模に関する事項

4-3-a 規模に関する前提条件

以下の取り組みを行うこと。

- 運用期間中において利用予定範囲を超過することがないよう、情報システムの縮退を検討するために必要となる情報収集等の仕組み（クラウドサービスの課金状況やリソースの利用量の監視、一定の閾値を超えた場合のアラート処理等）を設けること。定量的に計測したデータについては、ダッシュボード等による状況の可視化を行うこと。また、リソース利用状況に基づいたリソース見直しを行う点に留意し、情報収集の仕組みについても修正可能とすること。
- クラウドサービスのマネージドサービスを効果的に活用し、コスト削減を継続的に図ること。原則としてサーバレスの構成を取ることとするが、インスタンスを利用してサーバを立てる場合は、サーバのスペック等を適切な範囲に調整してコスト削減を継続的に図ること。（オートスケールを利用する場合の変更条件・上下限値等を含む。）
- リソース確保の方式（リザーブドインスタンス、スポットインスタンス等）についても検討すること。

4-3-b データ量

システムが処理するデータ量について、「2-1-c 入出力情報項目及び取扱量」に記載の各入出力情報項目を扱うことを想定すること。特に、影響が大きい事項として画像・映像データがあると想定しており、それぞれの取扱件数は、画像データが災害あたり最大 10,000 件、短時間映像（1 分以内）が災害あたり最大 100 件、長時間映像（数十分程度）が最大 10 件を想定している。

4-3-c 処理件数

処理件数については、「2-2-b 処理件数」の項を参照すること。

4-3-d 利用者数

本システムで想定する利用者数は、「2-2-a システムの利用者数」の項を参照のこと。

4-3-e 保管データ量・保管期間

本システムに保管するデータ量やデータの保管期間については、要件の整理の中で調査を行い、主管課と協議の上、決定すること。

4－4 性能に関する事項

4-4-a 性能を考慮する対象

「3-1-c 機能構成概念図」における機能の機能群について性能要件を満たすことを、本システムの性能要件とする。

- 情報収集機能
- 情報整理・共有機能
- 情報提供機能
- 共通機能のうち UI 設定機能、スマホ・タブレット利用機能、訓練機能

4-4-a-(ア) 性能目標の設定対象

性能目標の設定対象は本システムの Web サーバにリクエストが到着した時点からレスポンスを返す時点までとする。

4-4-a-(イ) 性能見積もり

本システムのアプリケーション処理時間に係る性能見積りは、以下を考慮する。

- アプリケーション又はコードの起動に要する時間、アプリケーション又はコードの実行時間、データベースアクセスに要する時間に要素分解を行った上で実施すること。
- 各画面・機能等の利用者体験を踏まえた余裕を見込むこと。

4-4-b 応答時間

本システムの応答時間に関する目標値は以下の通りとする。

参照処理・更新処理・検索処理は利用者の環境に依存しないレスポンスタイム（サーバ側でリクエストを受け付けてからレスポンスを返し始めるまで）を指標とする。

地図表示・帳票出力は各々初期表示までの時間、帳票を作成するまでの時間を指標として設定する。ただし、これらは利用者の環境に依存するため目安の値とする。

表 4-5　目標応答時間

項番	設定対象	指標名	目標値	遵守率
1	参照処理	レスポンスタイム	定常時:1 秒以内 ピーク時:3 秒以内	90%以上
2	更新処理	レスポンスタイム	定常時:1 秒以内 ピーク時:3 秒以内	90%以上
3	検索処理	レスポンスタイム	定常時:1 秒以内 ピーク時:5 秒以内	90%以上
4	地図表示	初期表示までの時間	3 秒以内(目安)	90%以上
5	帳票出力	生成までの時間	7 秒以内(目安)	90%以上

バッチ処理を行う場合は、ピーク時であってもオンラインレスポンスに著しい影響を与えないようにすること。

4-4-c スループット

本システムのスループットについて、以下の動作を円滑に行えるだけの性能を確保すること。

表 4-6　スループットを検討する際の観点

項番	観点	推定値	説明
1	ユーザーからのアクセス数	380,000 回／時間	発災から数時間程度の間、多数のユーザーがシステムに頻繁にアクセスする見込み。1 人が 1 分あたり 1 回アクセスすると想定し推計。
2	画像・映像データの入力・出力	38,000 回／時間	画像・映像データの収集と閲覧を多数行うと想定される。ピーク時には、職員の 10 人に 1 人(被害報告・収集担当者)が 1 分に 1 回実施すると想定し推計。
3	初回起動時のアクセス	6,300 回／時間	平日昼間の大規模地震発生時など、関係職員が一斉にシステムを立ち上げ、GIS の地図情報の読込を含むシステムへのアクセスを行う状況が想定される。1 時間以内に利用者全員がシステムに初回アクセスを行うと想定し推計。
4	帳票出力・ダウンロード	—	帳票出力やファイルダウンロードなどは、システムのスループットに影響するほどの頻度では実施されないと想定。

4－5 信頼性に関する事項

4-5-a 可用性要件

本システムにおける可用性に関する要件を以下に示す。なお、単一障害点（SPOF）を極力排除するとともに、サーキットブレーカーパターンなども検討し、

一律ではなく機能又はセグメントの特性に応じた合理的な提案を示すこと。また、SPOF の発生が避けられない場合においてそれら稼働状況を管理する仕組みを準備すること。

4-5-a-(ア) 可用性に係る目標値

4-5-a-7-① サービス提供時間

- 本システムのサービス提供時間（利用者が使用可能な時間）は、24 時間 365 日とする。
- 保守作業を実行する場合も、サービス提供を極力可能にすること。計画停止を行う場合は、停止時間を極力短縮すること。

4-5-a-7-② 稼働率

本システムの稼働率は、99.9%を満たすこと。

なお、稼働率は、稼働予定時間に対して実際に稼働した時間の割合であり、下記の算式により算出する。

稼働率（%）＝（1－1 年間の停止時間÷1 年間の稼働予定時間）×100

稼働予定時間とは、稼働すべき時間を指し、計画停電及び定期保守等の事前に計画した停止時間を除く。ここで、定期的なコンテンツ更新に関しては原則として「事前に計画した提示時間」には含めないものとする。コンテンツ更新はシステム停止なしで実施すること。

停止時間とは、計画外でシステムが停止していた時間、あるいは多数の利用者が使用できない状態にあった時間を指し、待機系システム等への切り替えのために発生した停止時間、障害発生から復旧のために必要となった停止時間及び人為的なミスにより発生した停止時間を含む。

その他、採用するクラウドサービスにおいてアップデート対応のために計画停止等の時間が必要な場合には、当該期間がどの程度事前に把握できるのか、変更等の調整は可能なのか等についても提案書で明示すること。

4-5-a-(イ) 可用性に係る対策

本システムの可用性要件の実現方法に関する要件を以下に示す。

- 本システムを構成するサーバ、ネットワーク機器及びネットワーク経路を冗長化し、単一障害点（SPOF）を回避すること。
- フェールソフトの観点から、障害が発生したコンポーネントを切り離すことによりサービス全体を停止せずに運用可能とすることを考慮する。そのために各種障害発生時の影響を回避又は局所化し、原則として自動縮退運用に対応すること。

- 本システムに係る運用・保守上の人的ミスに起因する障害が本システムの可用性に影響を与える事態を未然に防止するため、「４－１７ 運用に関する事項」及び「４－１８ 保守に関する事項」を踏まえ、適切な手順書を整備すること。また、定型的なオペレーションは自動化すること。

４-５-b 完全性要件

本システムにおける完全性に関する要件を以下に示す。

- 以下の対策を講ずること。
  ―コンポーネントの故障に起因するデータの減失や改変を防止する。
  ―異常な入力や処理を検出しデータの減失や改変を防止する。
- システム運用中に障害・トラブル等が発生した際に原因追求が可能となるよう、操作ログやアクセスログ等のシステムログ、例外事象の発生に関するログ等を取得・保管し、必要な時に出力可能とすること。ログの出力に当たっては、環境（本番環境、検証環境等）別に出力するログのレベル（ERROR、WARNING、INFO、DEBUG 等）の設定を可能とすること。

４－６ 拡張性に関する事項

本システムの性能及び機能に対する拡張性に関する要件を以下に示す。

４-６-a 基本方針

本システムの利用率の増加、データ量の増加等により、利用資源の規模・性能を拡張する必要が生じた場合に備え、可能な限り性能の拡張を柔軟に行えるよう、設計・開発を行うこと。また、将来の制度改正等により機能を拡張する必要が生じた場合に備え、容易に機能追加・変更を行えるよう、設計・開発を行うこと。

４-６-b マネージドサービスなどの活用

本システムの構築に当たってはマネージドサービスなどを可能な限り活用することにより、処理能力等の動的調整を実現すること。

４-６-c 機能の追加

運用開始後、機能の追加や外部システムとの接続インタフェースの追加等の必要が生じることが想定されることから、既存機能やインタフェースと追加機能間の連携が十分に図られるようにすること。

４-６-d コンポーネントの再利用性・拡張性

アプリケーションやインフラの設計に当たっては、将来の拡張時に効率良く対応ができるように、設定情報の外部化や一元化、機能の共通化等に努めること。特に本システム利用者が使用する本システムのスマホアプリについては、様々な利用者

が広く利用することが想定されるため、特定の端末、OS のバージョン、ミドルウェア等に可能な限り依存しない設計とすること。

４-６-e モニタリングと定期的な報告

本システムの運用に当たっては、定期的な運用報告において定期的にサーバコア数やディスク、メモリ、ネットワークの帯域などの使用状況等を確認すること。またリソースの増加の必要性が見込まれる場合は、リソースの増強の必要性の有無を判断できるような形で主管課に報告を行うこと。

４-６-f 割り当て変更

業務量の増加減に伴い、これらリソースの割り当てを動的に行えること。

４－７ 上位互換性に関する事項

本システムの上位互換性に関する要件を以下に示す。

４-７-a クラウドサービスのバージョンアップ

システムの構成にクラウドサービスのマネージドサービスを採用する場合、軽微なバージョンアップについては自動適用を前提とする。大規模なバージョンアップについては、アプリケーションへの影響を事前に精査し、適用を検討すること。

４-７-b OS 等への依存

原則特定バージョンへの依存は避けること。なお、やむを得ず OS、ミドルウェア等の特定バージョンに依存する場合は、その利用を最低限とすること。

４-７-c クライアント端末の更新

クライアント端末が更新され、OS や Web ブラウザとして新しいバージョンのものを利用する場合も、業務運営に極力支障が生じないよう計画されたシステム構成とすること。

４－８ 中立性に関する事項

本システムの中立性に関する要件を以下に示す。

４-８-a オープンな標準的技術又は製品の採用

本システムを構成するサーバ、ソフトウェア、アプリケーションとして、市場で広く利用されている製品群及びクラウドサービスが提供する標準的なサービスを除き、原則として特定事業者の技術に依存しないオープンな技術仕様に基づくものを選択すること。

４-８-a-(ｱ) データの可搬性の担保

- 本システム内のデータについては、原則として XML や CSV 等の標準的な形式で取り出すことができるものとすること。

- パッケージ製品から抽出されたデータであっても、移行データフォーマットや移行データの権利は主管課に所属すること。
- 技術的な理由により、提供することが難しいデータ項目がある場合には、代替案を提示することが可能であること。
- 移行用データが満たすべき制約（移行データのデータフォーマットやスキーマなどの要件も含む）をドキュメントに取りまとめること。ドキュメントについては、本システムの業務要件を理解しているユーザーであれば理解できるように記述すること。なお、システム運用期間中に該当ドキュメントの内容に変更が生じる場合は継続して改定を行い最新化できること。
- 移行データに関する文字コード等は以下に従うこと。
  ―取り扱う日本語文字集合の範囲： JIS X 0213
  ―文字コード： ISO/IEC 10646
  ―文字の符号化形式： UTF-8

4-8-a-(イ) オープンソースソフトウェア（OSS）活用

- ソフトウェア又はアプリケーションについてフレームワークを活用する場合は、可能な限りオープンソースソフトウェアとして提供されているフレームワークを選定すること。

4-8-a-(ウ) オープンソースソフトウェア（OSS）活用

- 本システムを構成するサーバ、ソフトウェア等は、原則として仕様が公開された API 等のインタフェースを選定すること。

4－9 継続性に関する事項

4-9-a 継続性に係る目標値

4-9-a-(ア) 予測可能な障害発生時

予測できる障害（一時的な過負荷等）については、あらかじめ業務停止を回避するための対策を講ずること。また、単一障害発生時は業務停止せずに処理継続可能であること。

4-9-a-(イ) 業務停止を伴う障害発生時（大規模災害発生時を含む）

大規模災害を含む、予測困難な事象により業務停止を伴う障害が発生した場合の目標復旧時間（RTO）、目標復旧レベル（RLO）及び目標復旧時点（RPO）を示す。なお、大規模災害時においては、インターネット等本システム管理外の通信インフラが被災していない前提とした目標値とする。

表 4-7　継続性に関する目標値（業務停止を伴う障害発生時）

項番	指標名	指標の定義	目標値
1	目標復旧時間	本システムに障害が発生した時刻から障害が復旧した時刻までに要した時間	24 時間前
2	目標復旧レベル	本システムを用いた業務のサービスレベルをどの程度まで復旧させるか	100%（全機能の復旧）
3	目標復旧時点	バックアップからデータを復元する際、過去のどの時点まで遡ることを許容するか	8 時間以内

4-9-b 継続性に係る対策

本システムの継続性要件の実現方法に関する要件を以下に示す。

4-9-b-(ｱ) 冗長化

各構成要素について、故障等を検知した際、自動的に予備の環境へ切替える等、適切に冗長化を行い、特定の部分の障害によりシステム全体が停止してしまうような SPOF（単一障害点）を極力排除するよう、設計時に配慮すること。

4-9-b-(ｲ) 災害対策

システム上の対策及び非常時の運用体制や切替え手順の整備等による運用上の対策を行うことで、業務継続を可能とすること。

災害発生後に本番環境が正常に稼働できる場合は、災害対策環境から切り戻しができるよう連携先システムと調整しておくこと。

4-9-b-(ｳ) データバックアップ

4-9-b-ｳ-① バックアップ対象

- データバックアップに当たっては、本システムの稼働に必要な全データを復旧可能とすることを前提として、外部組織から再入手可能なデータの有無を含め、保全対象を精査し、復旧時に必要となるデータを過不足なく保全対象に含めることができるようにすること。なお、クラウドサービスのマネージドサービスを利用することで自動的にバックアップを取得できる部分はあるが、オペレーションミスやアプリケーションのバグ等に起因するデータ破壊に対しても破壊前の時点まで遡れるように、バックアップの実施方法について配慮すること。

4-9-b-ｳ-② バックアップ頻度

- バックアップの取得間隔は、原則日次とする。ただし、障害発生時点への復旧が必要なデータについては、復旧に用いる PITR : Point In Time Recovery/Restore を保存する等の対応を行うこと。

4-9-b-ｳ-③ 保存期間

- 万一の障害発生に備え本システムの稼働に必要な全データを復旧可能とするとともに、過去のシステム処理に問題が発生した場合に原因分析を可能とすることを目的として、日次のバックアップについては、30 日分のデータをバックアップとして保持すること。

4-9-b-ｳ-④ アクセス制限

- バックアップしたデータの保管場所にはアクセス権限を付与し、管理者以外がアクセスできないようにすること。

4-9-b-ｳ-⑤ データの隔地保管

- 「3-2-1 ルール」（2012 年に US-CERT（米国のコンピュータ緊急対応チーム）が提唱）に示されている「データはコピーして３つ保有（プライマリー1 つ、バックアップ 2 つ)、2 種類の異なる記録媒体に保管、コピーのうち１つは遠隔地に保存」という方針を十分に理解した上で、データのバックアップについて万全を期した対応を行うこと。クラウドサービス上のスナップショットやレプリカだけではこの要件に十分対応できないので、暗号化を行った上で、別リージョンのオフサイトに隔地保管すること。

4-9-b-ｳ-⑥ バックアップツール

- バックアップ対象、頻度、バックアップデータへのアクセス権限及び保存期間といったバックアップポリシーを一元的に管理できる機能を持った、クラウドサービスプロバイダが提供するバックアップサービスをできるだけ利用すること。なお、個別データの復旧にはデータベース等の PITR：Point In Time Recovery/Restore を実現できることが望ましい。

4-9-b-(ｴ) システムバックアップ

- クラウドサービスのマネージドサービスにおけるバックアップ機能を有効に活用すること。
- 「4-9-a 継続性に係る目標値」に示す RTO、RLO、RPO を満たすようにすること。

4－10 情報セキュリティに関する事項

4-10-a セキュリティ対応方針

セキュリティ要件を決定するためのシステム特性や特に対処すべきセキュリティリスク、セキュリティ対応方針を示す。

表 4-8　本システムにおけるセキュリティ対応方針

項番	分類	概要
1	原則	• 「政府機関等のサイバーセキュリティ対策のための統一基準」、「栃木県情報セキュリティ基本方針」に準拠した情報セキュリティ対策を講ずること。 • セキュリティ対策については、高度化/大規模化するサイバー攻撃等に対応するため、多層防御やサイバーレジリエンス強化といった原則に基づいて要件を定義する。
2	システム特性	【システムの利用者】 • 本システムで想定する利用者数は、業務要件「2-2-a システムの利用者数」の項を参照のこと。 【システムで取り扱う情報】 • 特定個人情報は取り扱われない。 【利用環境・ネットワーク構成】 • 利用者はブラウザ（PC 及びスマートフォン）及びスマートフォンアプリからインターネットを介して本システムにアクセスし各種機能を使用する。 • システム管理者はインターネット VPN を介して当該システムにアクセスし、システム管理を実施する。 • 閉域網及びインターネットを介し外部システムと接続する。接続先及び接続構成は「４－１１ 情報システム稼動環境に関する事項」の項を参照のこと。 【その他】 • 本システムは自然災害発生時に利用するシステムであり、特に大規模災害発生時において本システムの停止が発生した場合、行政関係者間の適時かつ正確な情報共有が困難となり、ひいては災害救助等人命にかかわる事案が発生する可能性があることから、平時と同等の可用性確保及び完全性担保をおこなう必要がある。
3	優先的に対処すべきセキュリティリスク	• 第三者が不正にログインし、情報を窃取される、情報を書き換えられる等が行われる。 • マルウェアを展開される、システムを乗っ取られる等の事態が発生する。 • サービス妨害を目的とした攻撃等によりシステムが長時間停止する。

項番	分類	概要
4	セキュリティ対応方針	【セキュリティ要件のベースライン】 • 本システムにおいては、セキュリティ要件を過不足なく導出するため、NISC の提供する SBD マニュアルをセキュリティベースラインとして利用する 。SBD マニュアルに基づき、「4-10-b 情報セキュリティ対策要件」のとおり具体的な情報セキュリティ要件を列挙している。 【優先的に対処すべきセキュリティリスクへの対応方針】 • 上記の優先的に対処すべきセキュリティリスクについては、多層防御の観点で発生確率を抑えるとともに、発生時の範囲を極小化するような対策を実施する。 • 外部からの不正アクセス対策として不正ログイン対策、脆弱性対策を徹底するともに、攻撃やインシデントの兆候を早期検知できるような仕組みを導入する。 • サービス妨害を目的とした攻撃対策については、L3～L7 層で対策可能な仕組みを導入する。 【その他セキュリティリスクへの対応方針】 • 上記以外のセキュリティリスク（内部不正や人為的ミス等に起因するもの、サプライチェーンに起因するもの等）についても発生時影響は看過できないことから、予防的な対策だけでなく早期検知するための対策を実施し、リスクを低減する。

4-10-b 情報セキュリティ対策要件

本システムに求める情報セキュリティに関する要件を以下に示す。

なお、受諾者は開発の各工程において、本セキュリティ要件に則ってセキュリティ対策がもれなく実装されていることを検証する方法を定め、要件のトレーサビリティを確保することが求められる。開発工程以降、セキュリティ対策を具体化する過程でセキュリティ上の懸念が発生した場合は、本要件のみに縛られず、必要に応じて追加のセキュリティ対策を講じること。

また、デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」の記載内容（要求事項、実施内容、重要なセキュリティ対策の考え方）に従い、各工程でのセキュリティ対応状況について抜け漏れを確認して是正すること。加えて、デジタル庁「政府情報システムにおける脆弱性診断導入ガイドライン」の 4 付録 A を参考に情報システムの脆弱性が作りこまれないように留意すること。

表 4-9　情報セキュリティに関する要件

項番	大項目	小項目	対策に係る要件
1	侵害対策	通信回線対策	• 外部システム等とのネットワーク接続は必要最低限に設定すること。 • 不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離するとともに、業務目的、所属部局等の情報の管理体制に応じて内部のネットワークを通信回線上で分離すること。 • 通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルやアプリケーションの通信を通信回線上にて遮断する機能を備えること。 • 本システムのなりすましを防止するために、サーバの正当性を確認できる機能を備えるとともに、許可されていない端末、サーバ装置、通信回線装置等の接続を防止する機能を備えること。 • サービスの継続性を確保するため、本システムの負荷がしきい値を超えた場合に、通信遮断や処理量の抑制等によってサービス停止の脅威を軽減する機能を備えること。 • フィルタリング及びルーティングについて、設定の不整合が発生しないようにファイアウォール、ルータ等の通信ソフトウェア等を設定すること。 • 外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保すること。また、情報セキュリティ対策について、定期的な確認により見直すこと。 • 必要なポート、プロトコル及びサービスだけを有効とすること。また、これらに加え、マルウェア対策やログ取得等がクラウドサービス事業者側でされているかを事前に確認すること。 • 受託者拠点等よりアクセスを行う場合は、利用者の ID、パスワード及び他要素認証に加え、通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じること。
		不正プログラム対策	• 不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染や感染拡大を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。 • システム全体として不正プログラムの感染防止機能を確実に動作させるため、当該機能の動作状況及び更新状況を一元管理する機能を備えること。 • システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講じること。 • 不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、主管課が許可したユーザー以外に当該権限を付与しないこと。

項番	大項目	小項目	対策に係る要件
2	不正監視・追跡	ログ管理	• 本システムに対する不正行為の検知、発生原因の特定に用いるために、本システムの利用記録、例外的事象の発生に関するログを蓄積し 5 年間保管するとともに、不正の検知、原因特定に有効な管理機能（ログの検索機能、ログの蓄積不能時の対処機能、様々なログを組み合わせた相関分析に有効な管理機能、等）を備えること。 • ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能及び消去や改ざんの事実を検出する機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざんの脅威の軽減）のための措置を含む設計とすること。 • 情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。 • ログが取得できなくなった場合の記録・監視方法について検討し、主管課と協議すること。 • クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護について、ログ管理等に関する対策や機能に関する情報を確認し、適切に保護が実施されていることを確認すること。
		不正監視	• 不正行為に迅速に対処するため、送受信される通信内容の監視及びサーバ装置のセキュリティ状態の監視等によって、不正アクセスや不正侵入を検知及び通知する機能を備えること。 • サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。 • ネットワーク機器を使用する場合は、機器の固有情報等によって端末とネットワークとの接続の可否が自動的に識別されるようにすること。
3	アクセス・利用制限	主体認証	• 本システムによるサービスを許可された者のみに提供するため、管理者権限については他要素認証方式を採用すること。 • ログイン成功時、自身がどのアカウントでログインしたのかを分かるようにすること。 • 短期間に多数のログイン失敗が見られた場合、一定期間アカウントをロックすること。 • セッションを 24 時間等の適切な間隔にてリセットすること。

項番	大項目	小項目	対策に係る要件
		アカウント管理	• 主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。 • 本システムの利用範囲を利用者の職務や信用情報に応じて制限するため、本システムのアクセス権を職務や信用情報に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。 • 特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。 • コミュニケーションツールを用いてのチャット・通話等はアカウントを所有する者のみが参加可能とすること。 • 管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理すること。また、主管課から指示を受けた場合を除き、栃木県システム管理者（主管課）の ID 及びパスワードの変更を行わないこと。 • システム管理者の ID 及びパスワードについて、人事異動の際のパスワードの変更、入力回数制限等のセキュリティ機能を強化すること。 • システム管理者の ID を初期設定以外のものに変更すること。 • 認証情報設定のセキュリティ強化機能等、認証情報ファイルを不正利用を防止するための措置を講じ、認証情報を厳重に管理すること。 • ユーザーの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させること。 • ユーザー以外の者がパスワードを知り得ないよう、また不十分な長さ及び複雑さのパスワードを用いることができないよう必要な措置を講じること。 • 開発完了後、開発用に作成したアカウント等は削除すること。 • アクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認すること。 • パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、管理手順等が、栃木県のセキュリティポリシーを満たすことを確認すること。

項番	大項目	小項目	対策に係る要件
4	データ保護	機密性・完全性の確保	• 通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信回線を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズム及び鍵長については、「電子政府推奨暗号リスト」を参照し決定すること。 • 本システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、保護すべき情報を利用者が直接アクセス可能な機器に保存しないことに加えて、保存された情報を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズム及び鍵長については、「電子政府推奨暗号リスト」を参照し決定すること。 • 情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。 • 暗号化された通信データを監視のために復号可能する場合に備え、当該通信データを復号する機能及び再暗号化すること。
5	障害対策（事業継続対応）	構成管理	• 情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の本システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに文書どおりの構成とし、加えて本システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。
6	サプライチェーン・リスク対策	機器等の調達における対策	• 機器等の製造工程において、県が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。
7	利用者保護	情報セキュリティ水準低下の防止	• 本システムの利用者の情報セキュリティ水準を低下させないように配慮した上でアプリケーションプログラムやウェブコンテンツ等を提供すること。
		プライバシー保護	• 本システムにアクセスする利用者のアクセス履歴、入力情報等を当該利用者が意図しない形で第三者に送信されないようにすること。

4－11 情報システム稼動環境に関する事項

4-11-a システム環境

本システムにおいて提供するシステム環境を以下に示す。

表 4-10　システム環境一覧

項番	環境	利用用途	備考
1	本番環境	• 業務実施のための利用 • システム開発時の総合テスト、受入テストの実施	• 本番環境と開発／検証環境における各サーバは、それぞれ論理的に独立して構築すること。

項番	環境	利用用途	備考
2	開発/ 検証環境	• 開発 • 単体テスト及び結合テストの実施 • 業務アプリケーション、バージョンアップ、設定変更の更新等によるシステム影響の確認 • セキュリティパッチの適用に関するシステム影響の確認 • 運用ツール、自動化ツール等、調達対象システムに導入しているツール類のバージョンアップや設定変更によりシステム影響の確認 • ミドルウェア等のバージョンアップによるシステム影響の確認 • 機能追加時の システム利用者によるユーザー検証 • 運用・保守におけるデータ更新に伴うユーザー検証	• 開発/検証環境は合わせて 1 環境を想定しているが、分離してもよい。 • 開発／検証環境の利用に伴い、本番環境の性能、機能、データ管理に影響を与えないこと。 • 開発／検証環境について、利用用途を満たせれば、可用性や性能等の要件を満たさなくともよい。

4-１１-b システム全体構成

本システムの全体構成図を以下に示す。以下図は参考情報として扱い、想定される構成図は提案書に明示すること。

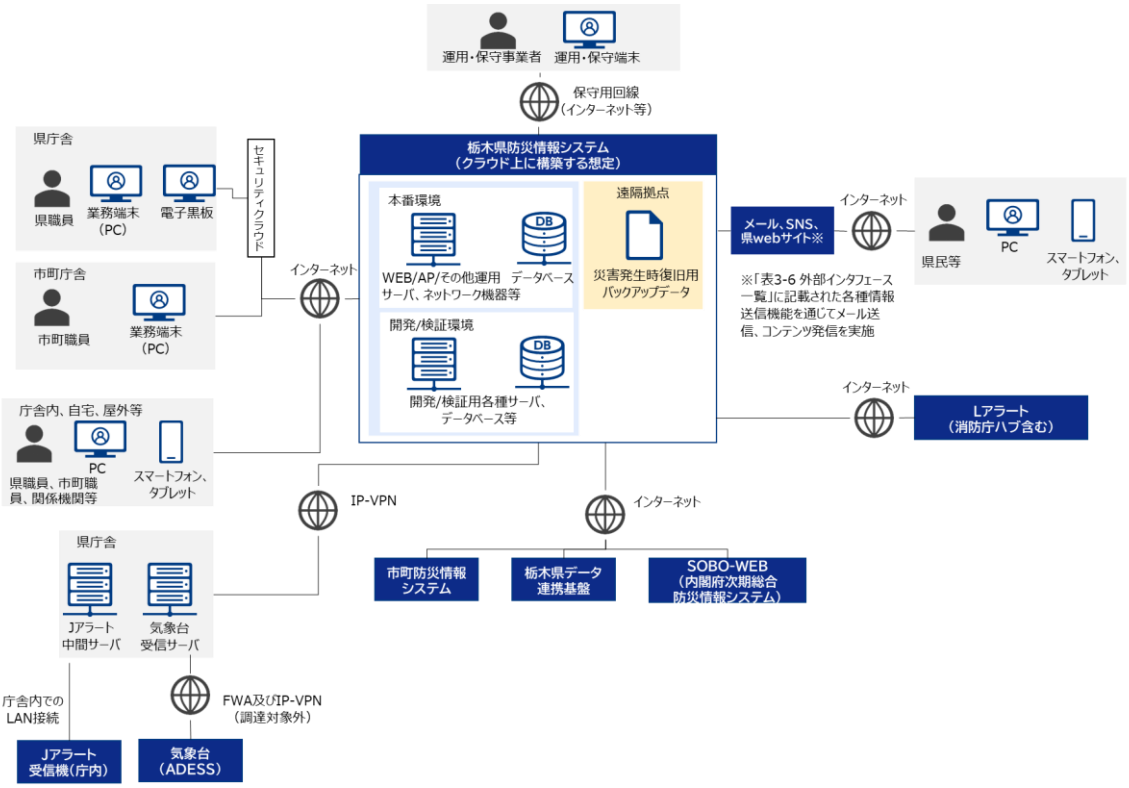

図 4-1　全体構成図

4-11-c クラウドサービスの構成

「4-2-b クラウドサービスの選定、利用に関する要件」を参照のこと。

4-11-d ハードウェア構成

クラウドサービス外に準備するハードウェアを以下に示す。なお、特定の装置への依存により、将来的なシステムの拡張及び更新や事業者間での引継ぎが妨げられることがないよう十分に配慮すること。また、機器選定にあたっては、事前に主管課の承認を得ること。

表 4-11　調達ハードウェア一覧

項番	機器種別	利用用途及び機器要件	配備箇所	調達数
1	PC 端末	• インターネット回線を通じ web ブラウザにて本システムを利用する。 • 機器要件は「4-11-h 利用端末の要件」を参照のこと。	栃木県庁本庁舎 ※	リエゾン利用 10 台（なお、市町庁舎、消防本部、その他県事業所においては別調達にて設置利用中の PC 端末を用いる）
2	電子黒板	• 大画面のタッチパネル式スクリーンを持ち、一般的な PC 端末と同様の操作が可能な端末を想定している。 • インターネット回線を通じ webブラウザにて本システムを利用する。 • 機器要件は、「4-11-h 利用端末の要件」を参照のこと。	栃木県庁本庁舎	4 台
3	映像関連機器	• 機能要件「F-26 リアルタイム配信基盤機能」に必要な機器一式。リアルタイム配信基盤機能はクラウド上に配置することを想定しており、本項の機器としては、映像スイッチャから出力された映像をクラウド基盤に対して送信するためのエンコーダ、送信機等を想定している。	栃木県庁本庁舎	1 式
4	外部連携用中間サーバ	• 気象情報伝送処理システム（ADESS）と閉域網で接続し気象情報を取得のうえ、本システム（クラウドサービス）にデータ転送する。	栃木県庁本庁舎	1 式
5	外部連携用中間ネットワーク機器		栃木県庁 本庁舎	1 式

※市町庁舎、消防本部、その他県事業所においては別調達にて設置利用中の PC 端末を用いて本システムを利用する。

4-11-e ソフトウェア構成

本調達においてソフトウェア（クラウドサービス含む）場合の要件を以下に示す。

- 提案するソフトウェア（クラウドサービス含む）は、本システム供用開始時点で販売、サポートされており、かつ、その後 5 年間は販売元によるサポートが得られるものであること。なお、サポートとは、技術情報の提供に加えて、脆弱性の修正やパッチ提供がされるものでなければならない。
- 汎用的な複数の製品（サーバ、OS 等）でソフトウェアが動作できること。
- ソフトウェアのバージョンは、基本的に提案時点で最新バージョンを選定するとともに、供用開始時点において最新バージョンへ更新すること。
- ソフトウェアライセンス違反を犯さないよう、受託者の責任においてライセンスを購入すること。
- セキュリティホール等への対応として、ソフトウェアプログラムの修正モジュール及びパッチファイルが公開された場合は、主管課にその影響度合いを報告し、必要な対策を実施すること。
- 特定のソフトウェアへの依存により将来的なシステムの拡張及び更新や事業者間での引継ぎが妨げられることがないよう十分に配慮すること。
- 本システムの構築及び運用・保守に最適なプログラミング言語を採用すること。

4-11-f ネットワーク構成

本システムのネットワークに求める要件を以下に示す。

表 4-12 ネットワーク構成

項番	名称	用途	回線種別	ネットワーク要件
1	システム用回線	本システムを各利用者端末がインターネット経由で利用するためのクラウドサーバ側回線	インターネット回線	• 通信プロトコルは、HTTPS を採用すること。 • IPv6 及び IPv4 に対応すること。 • 「4-4-c スループット」に示す性能要件を満たすことのできる回線帯域を用意すること。
2	運用監視用回線	本システムの遠隔監視及びリモート保守	インターネット回線を想定	• 各利用者への機能提供するための本システムとインターネットとの接続回線については、運用監視及びリモート保守用途を兼ねることを可とする。その際、「4-10-b 情報セキュリティ対策要件」の要求事項を満たすこと。また、「4－17 運用に関する事項」及び「4－18 保守に関する事項」に示す各業務が安定的に実施できること。

項番	名称	用途	回線種別	ネットワーク要件
3	利用者端末用バックアップ衛星回線	利用者端末側のインターネットが停止した際においても本システムを利用継続するための衛星インターネット回線	衛星通信インターネット回線	• 低軌道衛星によるインターネット通信サービスであること。 • ベストエフォート型の回線とし、期待される速度として下り 50Mbps 以上。上り 10Mbps 以上を得られること。 • 通信プロトコルは、HTTPS を採用すること。 • IPv6 及び IPv4 に対応すること。
4	外部情報提供元との接続回線	気象情報伝送処理システム（ADESS）及び J-ALERT から緊急情報及び気象情報を受信するための回線	VPN 網（通信キャリアの閉域網）	• L3VPN 方式による閉域網接続であり、通信事業者が提供するマネージドサービスであること。 • 帯域確保型（ベストエフォート型）の回線とし、1Mbps 以上の通信帯域を提供すること。 • 99.9%以上の稼働率を確保すること。
5	情報発信及びデータ連携基盤接続用回線	SNS、エリアメール、L アラートにて情報を発信するための回線 栃木県データ連携基盤とデータを送受信するための回線	インターネット回線	• 通信プロトコルは、HTTPS を採用すること。 • IPv6 及び IPv4 に対応すること。

4-11-g 施設・設備要件

本システムが設置される施設・設備に求める要件を以下に示す。

- 情報資産を管理するデータセンターの物理的所在地が日本国内であること。
- 主管課の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。

4-11-h 利用端末の要件

本システムの運用開始時点で動作保証の対象とする PC・スマートフォン・OS・ブラウザの考え方について、以下に示す。

ア：本システムの運用開始時点で動作保証の対象とする PC・スマートフォン・OS の機種やバージョンを示す。

表 4-13 動作保証対象とする利用端末

項番	端末	OS	バージョン
1	PC、電子黒板	Windows	10/11
2	スマートフォン	Android	●●●
3	スマートフォン（iPhone）	iOS	●●●

イ：本システムの運用開始時点で動作保証の対象とするブラウザは以下とする。

- PC 及び電子黒板（Windows）: Microsoft Edge/Mozilla Firefox/Google Chrome の最新バージョン
- Android ：Google Chrome の最新バージョン
- iOS　　：Safari の最新バージョン

4－12 データマネジメントに関する事項

本システムのライフサイクル全般を通じて、保有するデータ品質の維持・向上やデータの適正な利活用等を実現するため、以下に示す要件を踏まえ本システムのデータマネジメントを実施すること。

4-12-a データ管理体制の明確化

本システムで扱うデータの種別ごとに管理主体（管理する組織、担当者等）や役割の設定を主管課と共に行い、データ毎の管理責任を明確化すること。

4-12-b データの標準化

データの相互運用性を高めるため、以下の点に留意すること。

- マスターデータは、広範囲に共通利用できるデータから選定すること。マスターデータを独自に作成する場合は、関連する分野でも共通利用できるように設計上の配慮を行うこと。
- コード値については、国際標準、業界標準など、広範囲に共通利用されているものを採用すること。コード値の標準化については、「コード（分類体系）導入実践ガイドブック」（デジタル社会推進標準ガイドライン DS-463-1）を参考とすること。
- 本システムだけでなく、関連分野全体でのデータ流通を促進するという大局的な視点も踏まえて、ステークホルダーとの連携、調整を主管課と共に行うこと。

4-12-c データに関するドキュメントの一元的管理

本システムの運用・保守にあたってデータに関する一元的管理が行えるように、データに関する各種設計書等のドキュメントを内容的に独立した構成とすること。

4-12-d オープンデータ化を容易にする設計

本システムが扱うデータのうち、オープンデータとして対外的に公開することが有意義と考えられるものについては、公開要否を主管課が検討することを支援する。また、オープンデータとして公開するデータについては、オープンデータ・バイ・デザインの考え方に基づき、機械判読性の高いデータにする、Web-API により処理できるようにする、データを抽出しやすいデータベース構造にする等の対応を設計段階から十分に検討し、実装すること。

４-１２-e データに関する運用情報の管理

システム障害等が発生した際に迅速な原因分析が行えるように、データに関するログ機能を充実させること。

また、サービス・業務の運営状況に関する指標や本システムの利用状況等のデータを適時に把握できる機能を組み込み、取得したデータに基づいて本システムの継続的な改善を行うとともに、サービス・業務改革（BPR）が行えるようにすること。

４-１２-f データの機密性定義に応じた設計

データの機密性に応じたセキュリティを確保するため、データ配置やアクセス管理方法について設計段階から十分に検討し、実装すること。

４-１２-g データ品質の継続的改善

データ品質に起因するシステム障害や不具合を防止し、データの利活用を推進するため、データ品質の定期的な棚卸と不備・不具合の改善を行うこと。

４－13 テストに関する事項

本システムのテストに関する要件を示す。

表 4-14 テスト要件

項番	分類	要件
1	テスト工程の定義	• 本システムでは調達仕様書に記載の通り、以下のテストを実施する。 • 単体テスト • 結合テスト • 総合テスト • 受入テスト
2	テスト環境	• 本番環境に加え、テストを実施するための環境（開発環境・検証環境等）を整備すること。 • テスト環境については、連携先と接続して行う外部連動テストが実施可能な環境として整備すること。 • 開発スケジュールを踏まえ、効率化を考え、各環境を流用するなど検討すること。
3	テスト計画書	• 各テスト工程の開始時に、以下の内容を定義したテスト計画書を作成し、主管課の承認を得ること。 テスト計画書の目的と位置づけ テストの目的、概要 対象範囲 テストスケジュール テストの観点 テスト実施体制、役割分担 テスト実施手順 テスト環境 テストシナリオの概要 工程開始条件、工程終了条件 使用するテスト自動化ツール

項番	分類	要件
		成果物一覧 テスト結果に係る定性・定量評価の方法（テスト密度、バグ検出密度等） 進捗管理、品質管理、不具合管理 • 受託者は、本業務を実施する各過程においてテスト計画書の内容に変更が生じる場合、変更箇所及び内容について主管課の承認を得ることを条件として、テスト計画書を適切に更新すること。 • 情報セキュリティの観点から必要なテストがある場合には、テスト項目及びテスト方法を定め、これに基づいてテストを実施し、その実施記録を保存すること。 • 受託者は、テストに係る管理要領を共通化し、各テスト工程において、原則として同一の管理要領を適用するようにすること。各テスト工程に応じて部分的に異なる管理要領の適用を必要とする場合は、その適用差分のみ「テスト計画書」に記載すること。
4	テスト 仕様書	• 本システムの各テスト工程の開始前に、テストシナリオ、テスト項目等を記載したテスト仕様書を作成すること。 • 各テスト工程のテスト項目は、設計書等の記述内容を網羅的に確認できるよう作成すること。 • 各テスト工程に応じたテスト技法を適用すること。 • テスト項目は、品質を確保するために十分なテスト項目を定義すること。また、テスト計画の策定時に定めた定性・定量評価方法を満たすよう作成すること。 • 受託者においてレビューを徹底し、上記要件を満たしたテスト仕様書となっているかを確認すること。
5	テストの実施	• 作成したテスト項目に基づきテストを実施すること。 • テストを実施する際は証跡を取得すること。証跡の納品対象については、別途主管課と協議の上、決定すること。 • 受託者は証跡等に代表されるテストの成果物のレビューを徹底し、テスト項目に基づきテストを実施しているか確認する。想定外のテスト結果となった場合は、システムの欠陥であるか、想定結果が誤りであるか等、原因を明らかにした上で必要な対応を行うこと。 • 欠陥を検知した場合は、その原因を明らかにした上で、原因を解消すること。 • 検知した欠陥について修正を行った場合は、修正対象機能について回帰テストを実施すること。 • 主管課において、再テストが必要と判断した場合、受託者は再テストの計画を作成し、主管課の承認を得た上で、定められた期限内に再テストを実施すること。また、類似バグを抽出するため、必要に応じて強化テストを実施すること。
6	テストデータ	• 総合テスト及び受入テストにおいて実データを使用する必要がある場合は、実データの取得申請を条件として、実データの使用を許可する。なお、疑似データの作成に当たり、実データの匿名化、符号化等を行う必要がある場合は受託者の作業とする。 • 取得した実データは、適切に保管・管理すること。 • 受入テストにおいて作成したテストデータは、システム切替え実施前までに、検証環境等のデータも含め削除すること。 • 機密性の高いデータ項目は、マスキングした上で使用すること。
7	対応状況の報告	• テストの進捗について、テスト実施済項目数や信頼度成長曲線等の定量的なメトリクスの推移を示すことにより、テスト進捗状況、不具合検出状況及び不具合対応状況を報告すること。 • 受託者は、主管課からのテストの進捗状況や品質等に対する指摘に対し確実に修正すること。 • 受託者は、各テスト工程に応じたテスト計画内容について主管課に説明し、各テスト工程における最初のテスト開始予定日の遅くとも 1 週間前までに主管課の承認を得ること。
8	テスト完了報告書	• 各テスト工程の完了に当たっては、テスト完了報告書を作成し、主管課の承認を得ること。また、完了に当たっては以下をすべて満たすこと。 • すべてのテスト項目が完了していること。

項番	分類	要件
		• テスト結果について、定性評価及び定量評価（テスト密度、バグ検出密度等）により評価を行うこと。 • テストで発生したすべての障害が、当該テスト工程内で解消されていること。 • 外的要因等により次工程への申し送り事項が発生した場合は、対応方針、対応時期等を明確にした上で、主管課の承認を得ること。
9	テストの自動化	• 各テスト項目のうち、反復的にテストを実施するものについては、自動化することを原則とする。そのために、必要となるテストツールについては、新規に作成するか、既存のツールを活用すること。 • UI のテスト、受入テスト等、テストの自動化に馴染まないものについては、自動化対象外とする。ただし、自動化対象外とすることについて、主管課の承認を得ること。

4-13-a 単体テスト

現時点で想定する単体テストの要件を以下に示す。

- 本システムにおける最小の実装構成要素の動作を検証するために必要となるテストコードを作成し、コードベースの単体テストを実行すること。また、テストコードは、テスト対象とする実装構成要素に関するソースコードを記述する前に記述するようにすること。
- 単体テストの結果は、必要に応じて数値的指標等（ステップ数あたりの試験項目数、試験消化率等）をもって報告すること。以下に示す事項については、あらかじめ主管課に提示すること。
- 単体テストのスケジュール
- テスト環境（テストを実施するハードウェア、ソフトウェアの構成、テストツール等）の概要
- 合否判定基準 等
- 単体テスト実施時は、テスト結果を検証するための証跡を採取すること。
- 単体テストは、原則として開発環境において実施すること。

4-13-b 結合テスト

現時点で想定する結合テストの要件を以下に示す。

- 結合テストの観点として以下を想定する。

表 4-15 結合テストの主なテスト観点

項番	テスト種別	概要
1	システム基盤テスト	構築した本番環境及び検証環境の確認を行う。 • 環境設計において作成したリソース定義コードを実行し、サービスのインフラストラクチャを構成する環境及び仮想資源を構築すること。 • 構築した環境及び仮想資源が正しく動作するか、動作確認テストを実施すること。 • クラウドサービスが提供するツールによって実行可能なテストコードを作成すること。 • 動作確認テストの結果、何らかの異常またはエラーを確認した場合、実行し

項番	テスト種別	概要
		たリソース定義コードに原因が作り込まれていないか、必要な見直しを行うこと。 • 問題修正後、該当する環境または仮想資源について、再構築と動作テストを再度実施すること。
2	外部連携テスト	外部システムとの連携部分の確認を行うため、以下を実施する。 • 疎通テスト：本システムと外部連携システム間で必要な通信の疎通が通ることを確認する。 • 異常系テスト：想定しうるエラーを発生させ、エラーメッセージ等の確認をする。また必要な対処を行うように修正する。 • バリエーションテスト：インタフェースによる動作と必要なバリエーションの確認を行う。 • 運用観点テスト：正常時、異常時の運用に関する動作を確認する。異常時の対応として、エラーメッセージやログ等を基に、運用事業者が運用業務を行えることを確認すること。

- テスト対象機能について同値分析、境界値分析、原因結果分析を行い、その結果を踏まえてテストケース、テスト項目を設定し、アプリケーション機能相互間の接合に不具合が無いことを検証すること。
- 状態遷移マトリクスを踏まえ、本システムに備えるユーザーインタフェースについて、仕様どおりに操作可能か、誤った操作をした場合も適切なエラーメッセージが表示されるか等の操作確認を行うこと。
- 状態遷移マトリクスを踏まえ、アプリケーションコンポーネントが備えるAPIに対して境界値テストを行い、境界及び状態遷移を網羅すること。
- 結合テストに用いるテストデータには、テストケース、テスト項目を踏まえた疑似データを作成して使用すること。
- 結合テスト実施時は、テスト結果を検証するための証跡を採取すること。
- 結合テストは、原則として開発環境または検証環境において実施すること。

4-13-c 総合テスト

現時点で想定する総合テストの要件を以下に示す。

- 総合テストの観点として以下を想定する。

表 4-16　総合テストの主なテスト観点

項番	テスト種別	概要
1	業務運用テスト	業務の実施手順や業務で取り扱うデータを基に様々なシナリオ・データのバリエーションを作成し、本システムを用いて業務、機能を確認する。 • シナリオ・データには、日常的に実施する業務や日常的に取り扱うデータだけではなく、月次や年次等の特定のタイミングでしか発生しない業務やイレギュラデータも含めること。 • ユーザーの誤操作や予期しない現象を契機としたシステム障害が発生しないことを確認することを目的として異常系のテストケースも含めること。
3	性能・拡張性テスト	ユーザー数、データ量、リクエスト数、レスポンス等の性能要件を本システムが満たしているか検証する。検証に当たっては、現在の想定だけではなく、今後の予想される増加量も含めて確認する。

項番	テスト種別	概要
		短時間で本システムに重い負荷をかけ、本システムが処理量や長時間稼働等のシステム限界に関する性能や拡張の要件を満たしているか確認する。
4	可用性（障害）テスト	疑似的に障害を発生させる等の方法により、本システムのコンポーネントに障害が発生した場合に、どの程度許容して安定動作するか検証する。また、システム障害及びエラー発生時の回復機能等が適切に動作することを確認する。
5	完全性テスト	疑似的に障害を発生させる等の方法により、本システムのコンポーネントに障害が発生した場合に、データの滅失や改変がないことを検証する。また、操作ログやアクセスログ等のシステムログが出力されることを検証すること。
6	セキュリティテスト	不正侵入や Web 特有の攻撃への対策、データベースへの不正アクセスなどに対する対策、データの持ち出しに対する対策、マルウェア（ウィルス）対策等のセキュリティ要件を満たしているか脆弱性検査、インシデントレスポンステスト等を実施し確認する。
7	運用・保守テスト	運用・保守作業全般を通して、運用・保守事業者が円滑に日々の業務を実施できることを確認する。 運用・保守における正常時、異常時の運用に関する動作を確認し、特に異常時の対応として、エラーメッセージやログ等を基に、運用・保守事業者が業務を行えることを確認すること。

- 総合テストに用いるテストデータには、本番運用を想定した疑似データを作成して使用すること。
- キーワード駆動テストの適用により、総合テストの効率化を図ること。
- システム停止に伴うシステムバックアップやシステム停止、リストア、システム起動等については、受託者が主体的に実施すること。
- 総合テスト実施時は、テスト結果を検証するための証跡を採取すること。
- 総合テストは、原則として検証環境または本番環境において実施すること。

4-１３-d 受入テスト

受託者は調達仕様書にある通り以下の支援を行うこと。

- 受託者は、主管課が実施する受入テスト計画書作成作業を支援するために、受入テスト計画書（案）を作成すること。主管課は受入テスト計画書（案）を基にして受入テスト計画書を作成する。なお、受入テストの実施期間を十分に確保したスケジュールとすること。
- 受託者は、主管課が実施する受入テスト仕様書作成作業を支援するために、テスト項目、使用するテストデータ、合格判定基準等を示した受入テスト仕様書（案）を作成すること。主管課は受入テスト仕様書（案）を基にして受入テスト仕様書を作成する。
- 受託者は、主管課及びプロジェクト関係者が受入テスト計画書及び受入テスト仕様書に基づき実施する受入テストの実施支援を行う。
- 受入テストは、原則として検証環境または本番環境において実施すること。受入テストの実施に当たり、必要に応じて本システムの運転スケジュール、環境設定、テストデータ等の変更を行うこと。

- 受入テストの実施に当たり、主管課からの質問に対する問合せ対応を行うこと。
- 受入テストで発生したすべての障害が解消されている、または問題を特定した上で対応策について主管課の承認を得ていること。

4－14 移行に関する事項

4-14-a 移行に関する前提条件

- 現行システムから本システムへの移行にあたっては、現行システムの運用・保守事業者と協力し、調整の上で確実に実施すること。なお、移行実施体制と役割分担については以下を想定している。

表 4-17 移行に向けた作業手順及び役割分担

項番	作業名	主管課	現行システム運用・保守事業者	本システム設計・開発事業者（受託者）
1	移行計画の作成	■	△	◎
2	移行データ準備・提供	◎、■	◎	△
3	移行データ分析	■	△	◎
4	移行設計	■	—	◎
5	データ移行実施	■	△	◎
6	移行リハーサル	■	△	◎
7	移行判定	◎、■	—	◎
8	本番移行	■	△	◎
9	稼働判定	◎、■	—	◎

◎：主体者、●：確認者、■：確認及び承認者、△：支援者

- 移行時期については、令和 9 年 6 月末を想定する。具体的な移行時期については、本システムの設計・開発着手後に別途定める。
- 移行作業中に障害が発生する場合も想定し、連絡体制・現場対応体制を確保すること。

4-14-b 移行計画の作成

移行等に関しての計画をまとめた「移行計画書」を作成し、主管課の承認を得ること。「移行計画書」には、下記を含めること。なお、移行計画は本プロジェクト関係者以外の第三者にも容易に理解可能でかつ継承可能な形式で作成すること。

表 4-18 移行計画書の記載内容

項番	項目	補足
1	主管課及び各事業者の移行実施体制と役割	• 移行作業は、受託者が主体となり実施するものとする。
2	移行に係る詳細な作業及びスケジュール	• 受託者は、主管課に最終的な移行スケジュールを提示し、確定した内容を移行計画に反映させること。
4	移行環境／移行方法／移行ツール	• 移行可能期間の制約も踏まえた上で、一括移行、差分連携等の手法を組み合わせて、円滑に移行が行えるように留意すること。 • 業務停止に当たっては、主管課に対して移行に係る時間や制約条件等を報告し、事前に十分な調整を行うこと。

項番	項目	補足
		• 移行方式は、原則として一括移行とする。
5	移行作業、移行に伴い発生する各種設定を行うための各種手順書・マニュアル	• 移行する際の移行手順を作成し、主管課の承認を得ること。具体的な移行方法や手順は、主管課との協議の上で確定し、必要に応じて手順やツールを用いる際の操作方法等に関するマニュアル等を受託者が作成すること。 • 移行手順は、本システムと連携する外部情報提供元（気象情報伝送処理システム（ADESS）及び J-ALERT）からのデータ受信に係る新旧切替えが必要であることを踏まえ、主管課経由で調整等を実施した上で作成すること。
6	切り戻し基準、切り戻し手順書	• 令和 9 年 7 月～令和 10 年 3 月（9ヶ月間）は、現行システムをバックアップシステムとして並行稼働させる予定である。 • 本システムの不具合等により現行システムへの切り戻しが必要となった場合に対応できるよう、切り戻し基準や切り戻し手順書をあらかじめ定めること。切り戻し手順書には、切り戻した後の両システムの運用方法、再度本システムに切り替える際の移行手順等も含めること。
7	移行判定基準	• 移行開始時に満たすべき移行判定基準を定めること。なお、移行判定基準には以下を含め詳細は主管課と協議の上決定すること。 • 計画した全てのテストケースを消化し、摘出された全ての障害（バグ、不具合等を含む）が除去されていること。仮に除去されていない障害がある場合は、その対処方針が明確となっていること。 • 移行計画書及び移行リハーサルの結果が適正であること。 • 切り戻し基準や切り戻し手順書を定めており、主管課の承認を得ていること。 • 稼働後の運用準備が整っていること。
8	連携先の外部システム	• システム移行に当たっては、各種外部システムとの連携の現状を把握し、新システム移行に伴うテスト計画を作成し、テストに向けた事前合意、進捗管理、テスト結果取りまとめを行うこと。
9	移行リハーサルの実施場所（システム環境）	• 移行リハーサルについては、検証環境または本番環境で実施すること。本番環境を利用しない場合は、可能な限り本番環境に近い環境を準備した上で移行リハーサルを実施すること。

移行計画書に加えて下表の計画も作成すること。

表 4-19 計画の種類

項番	計画の種類	概要
1	移行リハーサル計画	• 移行の設計内容、移行リハーサルにおける方針、スケジュール、実施体制、実施手順、検証方法等を定めたもの
2	移行（本番）計画	• 本番移行時の方針、連携先外部システムとの接続切替え方法、スケジュール、実施体制、実施手順、作業結果判定方法、移行作業時のセキュリティ対策等を定めたもの

4-14-c 移行データ準備・提供

主管課は、現行システム運用・保守事業者の支援を受けつつ移行対象となるデータを整理し受託者に提供する。

移行対象となるデータは以下である。受託者は、移行対象データを受領し内容を確認すること

表 4-20 移行対象データ

項番	データ名	概要
1	栃木県防災メール送信先アドレス一覧	•「機能番号 F-39 防災メール発信機能」により配信される栃木県防災メールの送信先メールアドレス一覧情報

4-１４-d 移行データ分析

受託者は、移行対象データを分析し、データ・クレンジング等の加工作業が必要であるか確認の上、結果について主管課に報告すること。

4-１４-e データ移行実施

受託者は、移行対象データ（栃木県防災メール送信先アドレス一覧）を本システムに取り込むことによりデータ移行を実施すること。移行対象データに差分が発生する際は、主管課と調整のうえ、本システム運用・保守業務の開始時点の最新情報を取り込むこと。

4-１４-f 移行設計

受託者は、「移行計画書」を踏まえ、以下の点に留意して移行設計書を作成の上、主管課の承認を得ること。また、本システム利用者が本システムを利用するために必要となる準備事項について、提案や支援を行うこと。

- システム移行の方式を設計すること。
- 本番移行等、各移行作業に関しての見込み時間を算出すること。
- 現行システムから本システムへ接続切替えを実施する方法に関する設計を行うこと。なお、接続切替えを実施するために、他の情報システム等に設定変更等を依頼する場合には、依頼内容を整理した上で、主管課を通じて現行システム運用保守事業者との調整を行うこと。
- システム移行フローを組み立て、タイムスケジュール化等を行うこと。

4-１４-g 移行リハーサル

システム移行、データ移行のリハーサルでは以下の点に留意すること。

- 移行リハーサル設計書及び移行リハーサル手順書の内容を最終確認し、主管課と最終的な意識合わせを行うこと。
- 移行計画書及び移行手順書に問題がないことを検証するため、最低１回以上移行リハーサルを実施すること。なお、移行リハーサル実施後における使用データの扱い（移行リハーサル後に使用データを削除等）についても検討すること。
- 受託者は、移行リハーサルの実施後、移行に係る作業手順、作業時間見積もり等を評価し、「移行リハーサル結果報告書」を作成すること。また、その

内容について主管課に説明し、承認を得ること。

- 受託者は、移行リハーサルの結果として移行リハーサルの結果を分析し、本番移行に向けた課題などを明確にすること。
- 作業品質に改善及び再検証を要する問題点を確認した場合、必要に応じて移行リハーサルの再実行を検討すること。
- 受託者は、主管課の指示がある場合、修正した移行リハーサル計画書及び移行リハーサル手順書を基準として移行リハーサルを再実行すること。

4-14-h 移行判定

主管課は、「4-14-b 移行計画の作成」にて定めた移行判定基準を満たしているか確認した上で、移行判定を行う。

受託者は、主管課が移行判定を適切に実施できるよう、報告には移行計画にて定めた移行判定基準を満たしていることが分かるようにすること。

4-14-i 本番移行

本番移行では以下の点に留意すること。

- 本番移行に向けて、移行リハーサルの実施結果を元に移行計画書及び移行手順書を修正すること。また、その内容について主管課に説明し、承認を得ること。
- 移行計画書には、チェックポイントを設定し、作業の進捗度と経過時間などを元に、切り戻しの判断基準を設けること。
- 受託者は、本番移行及び稼働に係る作業過程において作成する提出物及び成果物の内容について、主管課に説明を行い、承認を得ること。
- 受託者は、本番移行に伴う作業状況についてチェックポイントに基づき適切なタイミングで主管課に報告すること。万一、作業の実施中に不具合等を生じた場合は、速やかに主管課に報告するとともに、必要な対応を行うこと。
- 受託者は、本番移行開始判断を受け、稼働のための作業を実施し、本番稼働を開始すること。
- 受託者は、稼働関連作業の完了後、本システムの稼働状況を確認すること。また、稼働以降安定運用までの3か月間において、QA対応を主体とした運用支援を行うこと。
- 令和9年7月～令和10年3月（9ヶ月間）は、本システムの不具合等により、現行システムへの切り戻しが必要となった場合には、移行設計書内の並行稼働実施計画に記載する対応方針に基づき切替え処理を行うこと。
- 本番移行の実施結果を「移行結果報告書」として取りまとめ、主管課の承認を得ること。

4-14-j 稼働判定

主管課は、サービスインを判断（稼働判定）する。受託者は、本番環境への移行の実施結果が適正であり、現行システムから本システムへ切り替えても業務に支障が生じないことを主管課が判断するための資料を提出すること。

4－15 引継ぎに関する事項

本システムの運用・保守は設計・構築を実施した受託者自身が、別途主管課と契約の上、実施することから引継ぎ業務は発生しない。ただし、受託者は設計・開発工程及び運用・保守工程における設計書、作業経緯、残存課題等を文書化し、将来的な他事業者によるシステム改修や運用・保守事業者変更等の事態発生に備えること。

4－16 教育に関する事項

4-16-a 教育計画の策定

教育訓練の対象者、スケジュール、実施内容、実施方法、教材等に関する教育訓練実施計画書を作成し主管課からの承認を得ること。

4-16-b 教育対象者

本システムの教育対象者を示す。詳細は本システムの開発時点で決定する。

表 4-21 教育対象者

項番	教育対象者	教育内容	教育対象者数
1	本システム管理部門職員（栃木県危機管理課）	運用業務の全体概要、当該職員において管理者権限で実施可能な業務・機能の手順等	約 50 名
2	県システム利用者（県職員）	県職員の業務に関する本システムの操作手順等	約 60 名
3	市町システム利用者（市町職員）	市町職員の業務に関する本システムの操作手順等	約 50 名
4	その他システム利用者（消防・警察等救援機関等）	救援機関及びリエゾンの業務に関する本システムの操作手順等	約 50 名

4-16-c 教育の実施時期

教育訓練の実施スケジュールについては、主管課を介した調整により、受講対象者と事前に調整した上で確定すること。ただし、遅くとも本システム運用開始の 4 週間前までに教育を完了し、本システムを利用した業務開始前までに十分な習熟期間を確保できるようにすること。

4-16-d 教育の方法

教育訓練の実施方法は、主に講義形式又はマニュアル配布を想定している。以下に、各教育訓練方法についての要件を示す。

- 講義における講師は、受託者が実施すること。
- 講義に必要な教材については、受託者が準備すること。必要な機材（プロジェクタ等）は、主管課と協議の上、必要に応じて受託者が準備すること。
- 講義会場及びWeb会議環境は、主管課側で準備するものとする。詳細については主管課と協議の上、決定とする。
- 講義は録画を行い、必要に応じて掲載等を行うこと。また、録画データは納品の上、主管課が再利用することを妨げないこと。
- 講義開催日数及び講義開催時間は、主管課と協議の上決定すること。
- 講義参加予定人数分の教育教材を用意すること。紙媒体または電子データいずれにするかについては主管課と協議の上決定すること。
- 講義終了後、質疑応答の時間を設けること。
- 講義では受講者がシステム操作を実体験できるようにすること。本番環境以外に研修用の環境を構築するなどし、本番稼働に影響を与えずに研修を実施できるよう主管課と調整すること。

4-16-e 教材の作成

- 教育対象者に対して、操作マニュアル、教育資料（本システムの概要資料、操作動画、FAQ等を想定）を作成すること。詳細は教育実施計画書の策定時に主管課と協議の上決定する。

表 4-22 教育資料の概要

項番	教材	教材の概要	対象者	補足
1	本システムの概要資料	本システムの概要を取りまとめた資料	本システム管理部門職員 県システム利用者 市町システム利用者 その他システム利用者	• 必要に応じ、対象者ごとの役割に沿った記載内容とすること
2	操作マニュアル	本システムの操作方法について手順をまとめたもの	本システム管理部門職員 県システム利用者 市町システム利用者 その他システム利用者	• 対象者ごとにマニュアルを作成すること • 必要に応じ、操作動画を作成し配布すること
3	FAQ	よくある質問や回答を取りまとめた資料	県システム利用者 市町システム利用者 その他システム利用者	• 必要に応じ、対象者の役割に沿った記載内容とすること

- 教育資料の作成に当たっては、情報システムやスマートフォンの操作に不慣れな者でも分かりやすいような構成、内容とすること。
- 教育資料については、主管課のレビューを経て承認を得ること。

4-16-f 教育訓練実施結果報告

教育訓練の実施結果を教育訓練実施結果報告書にて主管課に報告し、承認を得ること。

4－17 運用に関する事項

4-17-a 運用・保守計画

運用・保守の設計で検討した内容を踏まえて、以下の要件を含む運用・保守計画書及び運用・保守実施要領の確定版を作成すること。

表 4-23 運用・保守計画書の記載内容

項番	項目	補足
1	作業概要	• 監視、運用・保守作業の対象範囲、管理対象、作業概要等を記載する。
2	作業体制に関する事項	• 運用・保守業務を実施するための体制について、管理体制図、本件受託者の要員（責任者、作業者、役割分担）、連絡手段等について記載し、全体的な運用管理体制を明確にすること。
3	スケジュールに関する事項	• プロジェクト計画書及び調達仕様書に基づき、運用・保守を行う上で基本とする作業内容、関係するほかの作業工程、そのスケジュール等について記載すること。 • 日次、週次、月次等の定型的な業務について、作業内容を記載すること。また、複数回発生した非定型業務の報告及びその定形業務化（手順書の作成等）の提案を含めること。 • 年次の作業内容には、運用業務の中で発生した運用上の課題、作業量の多い作業等について整理報告し、自動化等の改善提案を行う作業、本システム運用継続計画の見直し作業、運用・保守計画書の見直し作業を含めること。
4	成果物に関する事項	• 運用・保守業務にて納品する成果物の内容、担当者、納品期限、納品方法、納品部数等について記載する。
5	運用・保守形態、運用・保守環境等	• 運用において採用する運用形態（オンサイト、リモート等）、運用にて利用する環境（本番環境、検証環境、研修用の環境等の有無）等を記載すること。
6	管理対象	• 受託者は本業務で運用・保守を実施する対象機能、システム範囲等を明確化すること。
7	クラウドサービスの利用	• 運用作業、運用手順及び運用管理用のソフトウェアも含め、可能な限り統一化を図るとともに、自動化された機能及びクラウドサービスが提供する機能等を利用し、運用に係る役務を可能な限り効率化すること。 • 利用しているクラウドサービスの機能や性能等に変更が発生した場合、受託者側でクラウドサービスの変更に伴う開発中システムへの影響を確認し、本システムの改修が必要な場合は、原則対応すること。ただし、改修規模が大きい又は影響範囲が広い場合は主管課と協議の上対応を検討・実施すること。
8	サービスレベル	• 運用・保守業務で達成目標とするサービスレベル項目及びサービスレベルを主管課が協議の上、決定すること。 • 運用におけるリソース使用状況に基づき、毎年のリソース計画を策定する。月間の運用実績を評価し、達成状況が目標に満たない場合はその要因の分析を行うとともに、サービスレベル達成状況の改善に向けた対応策を提案すること。
9	その他	• 上記に掲げる事項のほか、運用・保守を行う上での前提条件、時間、予算、品質等の制約条件等について記載する。

表 4-24　運用・保守実施要領の記載内容

項番	項目	補足
1	コミュニケーション管理	• 運用・保守業務を実施する上で必要となるコミュニケーション手段について、会議体（会議体名称、開催目的、開催スケジュール、出席者、報告内容等）、インシデント発生時の報告ルート等について記載し、効率的かつ円滑なコミュニケーションを実現すること。
2	体制管理	• 運用・保守に携わる事業者における作業体制の管理手法等について記載する。
3	作業管理	• 運用・保守作業及びその品質の管理手法等について記載する。
4	リスク管理	• 運用・保守における作業を阻害する可能性のあるリスクを適切に管理するため、リスク認識の手法、リスクの管理手法、顕在時の対応手順等について記載すること。
5	課題管理	• 運用・保守において解決すべき問題について、発生時の対応手順、管理手法等について記載すること。
6	システム構成管理	• 運用・保守における本システムの構成（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、施設・区域、公開ドメイン等）の管理手法等について記載すること。
7	変更管理	• 運用・保守により発生する変更内容について、管理対象、変更手順、管理手法等について記載すること。
8	情報セキュリティ対策	• 運用・保守における情報漏えい対策等について記載すること。平常時のセキュリティ運用として、継続的な脆弱性管理、構成管理及び変更管理を行い、不正アクセス等のセキュリティ脅威に対する監視運用を行うための具体的な方法を記載すること。 • セキュリティインシデント発生に備えた体制や手順、発生時の被害極小化、速やかなサービス復旧を行うための具体的な方法を記載すること。

4-17-b 運用・保守準備

運用・保守に当たって、以下の準備作業を行うこと。

4-17-b-(ア) バックアップ

システムの故障復旧に必要なデータのバックアップを定期的に取得すること。また、故障復旧時における必要なデータのリストア作業の手順、役割分担等を事前に決定し、故障発生時には実施すること。

4-17-b-(イ) 運用・保守手順書

運用・保守実施要領及び運用・保守計画書に基づき、運用・保守手順書を作成すること。

4-17-c 共通的な要件

4-17-c-(ア) 運用・保守期間

本システムは令和 9 年 7 月に稼働後、別途主管課と契約の上、令和 15 年 3 月 31 日まで運用・保守を行うこと。なお、当該期間後も本システムの運用・保守を延長する可能性があるため、長期的な運用・保守を前提とした運用・保守の体制及び仕組みとすることが望ましい。

4-17-c-(ｲ) 運用・保守報告書の作成

運用・保守業務の実施結果を運用・保守報告書として取りまとめ、主管課が指定した日時までに納品すること。

4-17-c-(ｳ) 情報セキュリティ対策の実施

「４－１０ 情報セキュリティに関する事項」を踏まえて実施した情報セキュリティ対策の対応結果を情報セキュリティ対策実施報告書に取りまとめ、主管課が指定した日時までに納品すること。

4-１７-d システム稼働要件

本システムの本番稼働に係る要件は「２－３　業務実施の時期・時間」を参照すること。

4-１７-e 主な運用作業一覧

現時点で想定する主な運用作業の一覧について以下に示す。以下の内容を基に、本システムの設計及び開発時に、運用・保守計画書、運用・保守設計書及び運用・保守マニュアルの案を作成すること。

表 4-25 主な運用作業一覧

項番	運用作業の分類	主な運用作業の内容
1	パッチ適用	• 保守におけるパッチ適用要否の判断結果に基づき、パッチを適用の上、適用後の稼働確認を行う。
2	ログ管理業務	• 操作ログやアクセスログ等のシステムログ、例外事象の発生に関するログを取得すること。 • ログ解析機能の活用を前提として、適切なキャパシティ管理を行うこと。キャパシティの改善が必要と判断された場合、キャパシティ改善提案を行うこと。 • 収集したログを一元的に管理し、不正侵入や不正行為の有無の点検・分析を効率的に実施すること。 • ログの正確性を担保するため、適切なアクセス制御を行い、ログの改ざんを防止すること。
3	ジョブ管理業務	• ジョブの登録・更新、ジョブの起動スケジュール（カレンダー）を登録し、ジョブの実施結果を確認、報告する。 • 主管課が必要性を認めた際は、主管課の指示に従い、ジョブの手動実行を行う。
4	システム 監視	• 本システムの運用状況を監視し、障害の発生またはその兆候を検知するとともに、障害を検知した際には重要性等で分類した上で、メールなどにより自動で通知する仕組みを構築すること。 • セキュリティ監視に当たっては、取得ログやセキュリティ製品のアラート等を用いて、不正アクセスやマルウェア感染等のセキュリティ脅威により引き起こされる異常な状態の監視等を行い、セキュリティインシデントやその兆候を早期に検知すること。 • 各種監視結果を定期的に集計・分析し、監視方法や閾値、通知の見直し等が必要な場合は、主管課の承認を得た上でこれに係る設計を行い、対応を実施すること。システムサイジングについても定期的に分析を行い、主管課の承認を得た上で見直すこと。
5	問題管理	• 本システムに対し、重大な影響を与えるインシデントや将来的に重大なインシデントに発展する可能性がある問題について影響評価を行った上で、緊急度及び優先度を定め、根本原因の調査及び解決策の立案を行うこと。

項番	運用作業の分類	主な運用作業の内容
6	変更管理	• 課題管理機能の活用を前提として、適切な変更管理を実施すること。 • 構成要素を追加、変更又は廃棄する場合は、変更依頼書を起票すること。 • 機密情報の不要な公開等の意図しないセキュリティインシデントを防止するため、本システムの設定変更等に当たっては、情報セキュリティ関連の設定に影響しないことを確認すること。
7	リリース管理	• 主管課とリリース作業の日程、作業内容、依頼事項等の調整を行い、実施の計画をリリース計画書に記載すること。 • リリースを実施した際、リリースに関する情報を「リリース管理台帳」にて管理すること。 • 「リリース管理台帳」には以下の項目を管理し、履歴を確認することとし、その管理が必要な項目についても管理する仕組みとすること。 実施計画の内容 リリーステストの実施有無及び結果 リリース時期 各種レビューの実施有無及び結果 リリース内容 • リリース計画書については、リリース予定日より十分な期間を確保の上、前もって主管課の承認をもって提出すること。なお、緊急なリリースを要する場合は主管課と協議すること。
8	システム構成管理	• 本システムに係る全ての構成品目について、適切な構成管理を実施すること。 • システム構成管理対象を特定し、管理レベルを定めること。なお、システム構成管理対象は、本システムを構成するクラウドサービス、ソフトウェア（製品名、開発元、バージョン、ライセンス、依存関係等）、アプリケーション、通信回線、公開ドメインのほか、本システムの運用・保守に係る全てのドキュメント及びデータとすること。ただし、本システムの外部から提供を受けるものであり、運用・保守において変更を行わないものは、システム構成管理の対象外とする。 • システム構成管理対象の変更について、変更履歴を追跡可能であること。 • 本番環境・検証環境の維持管理を行うこと。 • アプリケーションは CI ツールの活用等により標準化・自動化された管理を実現すること。
9	バックアップ	• システムバックアップ、データバックアップを取得すること。 • 必要に応じてシステムリストア、データリストアを実施すること。
10	業務支援	• 主管課の指示に基づき、利用者の利用状況のデータを集計し、主管課に定期的に報告すること。 • 必要に応じて、データベースやディレクトリ等に施されるアクセス制御の設定変更を実施すること。 • 運用に必要な端末は受託者が用意すること。 • 栃木県内において災害対策本部が設置されるほどの大規模災害が発生した場合には、遠隔でシステムの運用支援を行うとともに、必要に応じて栃木県庁本庁舎においてオンサイトで支援を行うこと。具体的な支援内容としては、アカウント発行等のシステム管理に関する事項、データの取込など情報整理・共有に関する事項、軽微な機能・UI 改修などを想定している。
11	障害対応	• 障害発生時は、発生から解決までの一連の作業（受付、問題判別、業者間調整、調査解析、修復方法の検討、障害原因アプリケーションの再設計・製造・試験、再発防止・品質向上作業、報告書作成・報告実施、環境（本番環境・検証環境等）反映）を行うこと。 • 運用・保守の対応時間は、土・日・祝日・年末年始（12/29～1/3）を除く平日の 9:00～17:00（以下、「営業時間」という）とすること。障害発生の検知が営業時間帯以外となった場合は、翌営業時間より運用・保守業務を開始できること。なお、当該範囲以外に運用・保守業務を実施する必要がある場合に

項番	運用作業の分類	主な運用作業の内容
		は、受託者と主管課の間で協議することとする。また、提案において営業時間帯を拡大することは問題ない。 • 監視アラートや問い合わせ窓口への申告等により障害を検知した場合は、速やかに切り分け及びサービス継続のための一次対応を行うこと。一次対応時間は営業時間内において 2 時間以内とすること。 • 障害検知した際は、主管課に 30 分以内に事前に合意した方法にて一報を行うこと。 • 本システムの連携先システムにおいて障害が発生し、本ステム側の機能提供への営業が発生した場合においても、連携先システム担当が実施する原因調査、代替策、解決策の検討及び処置を必要に応じて支援すること。 • システム障害と想定される連絡を受け付けた際、別途、主管課より指示する担当者へ速やかにエスカレーションすること。 • 応答内容の記録を残すこと。
12	ヘルプデスク業務	• 本システムの利用方法に関する問合せの受付からクローズまでを一元管理するヘルプデスクを設け、主管課からの本システムに関する問合せを受け付けること。受付時間及び方法は「２－３　業務実施の時期・時間」を参照のこと • ヘルプデスク担当者のスケジューリング等の運営を適切に行うこと。 • 受け付けた問合せは、質問、インシデント、サービス要求、作業依頼等に分類した上で、対応日時、問合せ元、内容、回答状況等とともに記録すること。なお、具体的な運用方法については、本システムの設計開始以降に改めて検討する。 • 運用･保守の計画及び実施状況について、主管課の定める報告様式に従って取りまとめ、主管課に月次にて報告を行うこと。
13	インシデント管理	• 情報セキュリティインシデントが発生した場合は、「運用・保守実施要領」等に定めた手順に従ってインシデント対応を行うこと。対応に当たっては、主管課、関係事業者と適宜調整の上で対応を行うこと。 • インシデント対応手順の実効性を担保するため、定期的にインシデント対応手順の見直しやインシデント対応訓練を実施すること。
14	バージョンアップ対応	• 保守におけるバージョンアップ対応要否の判断結果に基づき、バージョンアップ対応を実施し、稼働後の動作確認を行うこと。
15	大規模災害等対応訓練	• 年 1 回主管課にて実施している防災図上総合訓練に立ち会い、訓練中の本システム利用における各種サポートを実施すること。立ち合い場所は栃木県庁内訓練実施会場とする。 • 訓練の事前準備期間において、主管課に対し訓練における本システム利用の場面設定等に係る助言等をおこなうこと。訓練当日においては、システム利用における利用者からの操作方法等に対する問合せに迅速に対応すること。
16	運用改善	• 受託者は、システムの状況を主管課が定期的に把握できるように仕組みを整えること。 • プロジェクトの目標とする指標、システムの利用者の利用状況 • クラウドのリソース等、システムの利用状況・コストの発生状況 • システムの利用状況については、少なくとも以下の項目および「3-3-c モニタリング対象データー覧」に記載した項目を実施し、利用状況の分析とその後の改善策に資する項目を含めること。 • 運用管理・保守業務の作業別の所要時間 • 自動化や効率化が可能と思われる作業の洗い出し • システム及び運用・保守業務の改善提案 • 受託者は、システムの利用拡大や利便性向上のため、実績に基づいた定量的なデータや利用者からの問合せ内容等を分析し、多くの利用者が操作方法に迷う部分や誤操作を誘発する部分を把握した上でシステムの改善策を検討すること。また主管課と協議の上、システムの改善を実施すること。
17	サービスオペレー	• 本システムが動作するに当たり、必要となるデータベースの各種マスタ情報

項番	運用作業の分類	主な運用作業の内容
	ション支援	を維持管理すること。 • 計画停止、保守作業、障害対応等により利用者への影響が生じる場合、トップ画面等にお知らせを掲載するなどの方法により周知連絡を行うこと。 • 作業影響を生じる範囲について、不測の運用障害を回避する観点から、メンテナンス機能を利用してサービス閉塞・閉塞解除運用を実施すること。
18	情報セキュリティ監査	• 主管課が情報セキュリティ監査を実施する場合がある。その際はセキュリティ監査事業者との調整・ヒアリングへの協力を行うこと。
19	アカウント管理	• アカウントの利用状況の棚卸しを実施すること。実施するタイミングは、年 1 回程度を想定しているが、具体的な時期については主管課と協議の上、決定すること。
20	その他業務	• サーバ証明書の更新、ドメインの管理等を行うこと。

4－18 保守に関する事項

4-18-a 保守業務の実施

保守業務として以下を実施すること。

- 問合せの受付時間は、「２－３ 業務実施の時期・時間」に記載の通りとする。ただし、主管課が緊急かつ業務に支障を来すと判断した場合はこの限りではない。
- 受け付けた問い合わせをインシデントとして管理し、インシデントのクローズまで、対応を継続すること。
- 障害について対応したときは、障害報告書を作成し、主管課に報告すること。

4-18-b 保守設計

保守設計として以下を実施すること。

4-18-b-(ア) 役割分担の整理

役割分担を行う際に以下の点に留意すること。

- 保守業務の設計に際し、受託者の責任範囲及びクラウドサービスを含めた関連事業者間の役割分担を整理すること。
- 新システムがクラウドサービス上で稼働することを踏まえ、各業者間の役割分担を考慮した上で、保守設計を行うこと。

4-18-b-(イ) クラウドサービスの利用

クラウドサービスを利用する際に以下の点に留意すること。

- 保守設計を実施する上で、クラウドサービスの標準機能を可能な限り活用すること。
- クラウドサービスによる自動化等により、省力化を実施すること。

- 運用・保守実施要領、運用・保守計画書及び運用・保守手順書については、クラウドサービスが提供する各サービスを活用することにより、作業のみならずドキュメント類についても効率的に作成すること。
- 利用するクラウドサービスにおいて、提供サービスの仕様上必要となるアップデートパッチの適用やメンテナンス等の対応に際して、システムへの影響度に鑑み、主管課と協議の上対応を行うこと。または、自動適用を行う等の対応が可能となるよう、必要な仕組み（検知、適用、等）を準備すること。

4-１８-c アプリケーションの保守

アプリケーションの保守として以下を実施すること。

4-18-c-(ｱ) インシデント管理

運用管理・監視等作業におけるインシデント管理と適切な連携を図ること。

4-18-c-(ｲ) 是正保守

アプリケーションに起因した障害発生時、監査指摘事項への対応時等、アプリケーションの是正が必要な場合に、是正保守を行うこと。

4-18-c-(ｳ) 適応保守

OS、ブラウザ、ミドルウェア等のバージョンアップ対応等、利用環境の変更への対応が必要な場合、アプリケーションに係る適応保守を行うこと。

4-18-c-(ｴ) 予防保守

本システムのアプリケーションに潜在的な問題が発見され、当該問題除去を目的とした変更が必要な場合又はアプリケーションコンポーネントについて新たに脆弱性が報告された場合に、予防保守を行うこと。

4-18-c-(ｵ) 改善措置

改善措置を実施する際には以下の点に留意すること。

- 利用者に影響がある保守作業を実施する場合は、アプリケーション保守の実施効果、現在及び将来の利用者に対する影響の分析を行うこと。
- アプリケーションに係る機能性、信頼性、使用性、効率性、保守性、移植性等の改善が必要な場合に、対処を行うこと。
- Web 解析結果に基づき、本システムのユーザーインタフェースについて、ユーザビリティ又は UX に関する課題を識別した場合、課題解決に資する是正保守、予防保守を行うこと。

- Web サーバ、データベース等について、「表 4-25 項番 16.運用改善」の結果を踏まえ、必要に応じて稼働環境の改善等に伴う設定変更を実施すること。

4-18-c-(ｶ) 根本原因の分析

是正保守及び予防保守の実施に当たり、障害、監査指摘、潜在する問題等に係る根本原因の分析を行うこと。

4-18-c-(ｷ) 検証

修正したアプリケーションを本番環境へ展開（デブロイ）する前に、修正が適切に実施されているか否かについて検証環境において検証すること。

4-18-c-(ｸ) ドキュメントの修正

アプリケーション保守に伴い、ドキュメント（設計書、マニュアル等）の修正を要する場合は、速やかに修正を行うこと。なお、改修等に伴い画面等に発生する変更が軽微な場合は、ドキュメントの更新方針等について別途主管課と協議すること。

4-18-d クラウドサービスの保守

クラウドサービスの保守として以下を実施すること。

- 利用しているクラウドサービスにおいて脆弱性及び不具合が確認された場合は、その対応について主管課と協議し、パッチ適用要否を判断すること。
- クラウドサービスにおいてバージョンアップ等の情報が公開された場合には、バージョンアップに伴う影響調査を実施した上で、主管課と協議し、適用等の可否を決定すること。なお、実施することとなったバージョンアップに伴う機器・サービス等の停止は計画停止に準ずるものとして扱う。また、バージョンアップに起因して改修が必要な場合には、対応について別途主管課と協議すること。
- クラウドサービスで利用している環境の最新化や更新は、原則として IaC（Infrastructure as Code）を活用しコードを変更し、変更後のコードを実行することにより実施すること。
- 修正パッチ適用やバージョンアップ等を行う場合には、事前に検証環境において本システムの運用に影響が生じないことを十分に検証し、環境更新の事前評価を実施すること。

4-18-e ソフトウェア保守

ソフトウェアの保守として以下を実施すること。

4-18-e-(ア) ソフトウェア最新化

本システムを構成する全てのソフトウェアについて、製品不具合や情報セキュリティに関する脆弱性を修正するため、主管課と協議の上、ソフトウェアを最新化すること。なお、ソフトウェアの最新化に当たっては、本システムのシステム構成等に考慮すること。

4-18-e-(イ) 修正プログラムの適用

修正プログラム適用の際は以下の点に留意すること。

- 情報セキュリティや安定稼働の観点から緊急性が高いと考えられる修正プログラムについては、緊急適用を計画すること。緊急性が低い修正プログラムについては、定期保守作業の中での適用を計画すること。
- 使用しているクラウドサービスの内容に変更が発生する際には、クラウドサービスより提供する情報を元にシステムへの影響範囲を調査の上、修正プログラムの適用可否を主管課へ報告すること。適用が必要と判断された場合、クラウドサービスより提供されるソフトウェアに対する修正プログラムの適用作業を実施すること。

4-18-e-(ウ) 検証・デプロイ

検証・デプロイを行う際は以下の点に留意すること。

- ソフトウェア保守に当たっては、事前に検証環境で本システムの運用に影響が生じないことを十分に検証すること。
- ソフトウェア保守に伴い、本システムの安定稼働に影響が生じる事態が予測される場合、主管課の指示に基づいてデプロイ実施の是非を判断すること。

4-18-e-(エ) 設計書への反映

ソフトウェア保守によりソフトウェア構成に変更が生じた場合、設計書等へ変更内容を反映すること。

4-18-e-(オ) 保守条件の決定

保守条件は、「製品の導入や使用方法」、「製品の互換性や相互操作性」、「製品資料の解釈」、「構成サンプルの提供」、「修正策の情報提供」、「製品プログラム、製品コードに起因する障害」等の保守が提供されることを想定しているが、最終的な保守条件は、主管課と調整の上、保守設計において決定すること。

4-18-e-(カ) 脆弱性管理

ソフトウェアに関する脆弱性に対処するために、以下の対応を行うこと。

４-１８-e-ｶ-① 脆弱性管理基準の作成と運用

脆弱性管理の方針を定めた脆弱性管理基準を、保守設計において主管課と調整の上で作成し、運用すること。脆弱性管理基準には、以下の項目を含めること。

- 個別対応の要否判断の基準
  情報システムの「脅威」、「脆弱性」、「重要度」からの観点からのリスクの評価基準と対応優先度、個別対応または定期保守でのどちらで対応するかの方針、目標とする脆弱性対処の対応期限を取り決めたもの。
- 定期アップデート規則
  ソフトウェアの定期アップデートを実施する頻度、実施条件、回帰テストの範囲を取り決めたもの。
- ソフトウェア採用判断の基準
  提供元の信頼性やサポート条件、脆弱性の情報開示やパッチ提供など、脆弱性対応を円滑に行うための基準を取り決めたもの。
- 脆弱性管理の対象と管理方式
  クラウドの責任共有モデルを含む情報システムの脆弱性管理の対象と、ソフトウェア構成や脆弱性を管理するツールやサービスなどの管理方式を取り決めたもの。

４-１８-e-ｶ-② 脆弱性管理の手順と運用

脆弱性に対処する手順を定めた脆弱性管理手順を、保守設計において主管課と調整の上で作成し運用すること。脆弱性管理手順には以下の項目を含めること。

- ソフトウェア構成の管理
  情報システムで使用するソフトウェアの製品名、開発元、バージョン、ライセンス、依存関係などを容易に参照できるよう構成管理及び変更管理を行うこと。
- 脅威情報の収集、自システムへの影響分析
  日々出現するセキュリティ脅威や脆弱性に対処するため、定常的に脅威情報や脆弱性情報を収集し、情報システムへの影響含めてリスク分析を行うこと。
- リスクに応じた脆弱性対応及び定期アップデート
  情報セキュリティや安定稼働の観点からリスク評価を行い、即時もしくは優先的な対応が望ましいと判断される脆弱性については、緊急対応を

計画すること。即時対応が不要もしくは対応の必要性が低い脆弱性については、定期保守作業の中での対応を計画すること。

4-18-f 保守実績の評価及び改善

保守実績の評価及び改善として以下を実施すること。

- 本システムの運営に関わる関係者間で本システムの保守に係る情報や問題認識を共有し、保守業務の品質を継続的に維持・向上させること。
- 本システムが使用するアプリケーション、クラウドサービス、ソフトウェア等の保守実施状況について、日々の保守業務の中で収集する定量的な管理指標を定め、主管課と合意すること。
- ログ解析機能等を活用し、指標値の収集、評価及び管理を効率的に行うこと。
- 管理指標の達成状況を評価し、未達の場合は原因分析を行い、改善措置を検討すること。また、これらの実績、評価、改善措置について、定期報告すること。
- ログ解析機能、Web 解析機能の活用を前提として、モニタリング及び運用過程を通じて得られた利用状況を分析することにより、ライフサイクルコスト低減の観点から、利用するクラウドサービスの所要量及びソフトウェアライセンスの削減可能性を検討すること。また、利用状況の実績、評価、コスト削減可能性について、定期報告すること。

4-18-g ドキュメントの保守

設計・開発関連ドキュメント及び運用・保守関連ドキュメントが、受託者の契約期間において、最新の状態であるよう維持・更新等を行う。

4-18-h 軽微な改修

運用・保守の期間中に必要となる軽微な改修として以下を実施すること。

- 調達仕様書「●●●●（スケジュール関連の項を想定)」（※現時点では別紙スケジュールを参照）のとおり、本システムのリリース後の利用者の操作運用実態を踏まえた画面、UI の改善、改修実施を予定している。本対応を保守作業として見込むこと。
- 「3-4-a 外部インタフェース一覧」について、本システムのリリース後にデータ送受信に係るインタフェース改修（新規接続先追加、既存接続先への送受信データ増減等）を予定している。本対応を保守作業として見込むこと。

- 上述に加え、運用・保守期間中に、利用者からの要望対応、不具合の改善、環境変化への対応等の目的で軽微な改修を行う可能性がある。改修への対応工数として、合計 20 人日／年の作業を見込むこと。
- 個々の改修に当たっては、改修範囲、影響範囲等を分析して必要工数を事前に見積もった上で、主管課の承認を得た上で作業を実施すること。
- 月次の定期報告において、個々の改修の実施状況（工数の消化状況等）について報告すること。また、改修が必要と考えられる事項が受託者においてある場合は積極的な提案を行うこと。
- 個々の改修が完了した後に、工数実績を提示すること。また、計画工数と実績工数の差異を分析した上で、その後の改修案件のおける見積精度向上と改修生産性向上に努めること。

以上