

京都府
総合防災情報システム(仮称)構築業務委託
企画提案仕様書

令和2年4月

京 都 府

目次

1	システム基本方針	2
1-1	背景	2
1-2	新システム導入の目的	2
1-3	基本方針	3
2	スケジュール	4
3	システム要件	4
3-1	システム形態	4
3-2	システム化対象範囲	5
3-3	システム概要	6
3-4	業務仕様	7
3-5	機能要件	7
(1)	地図システム	7
(2)	端末	7
(3)	情報発信	8
(4)	外部情報連携	9
(5)	帳票	9
3-6	非機能要件	10
(1)	規模要件	10
(2)	性能	10
(3)	信頼性・継続性	10
(4)	拡張性	12
(5)	移行性	13
3-7	セキュリティ対策	13
(1)	情報セキュリティ対策の基本方針	13
(2)	アクセス制御の対策	13
(3)	ネットワーク保護	14
(4)	ウイルス対策	14
(5)	データの暗号化	14
(6)	監査証跡	15
(7)	ファシリティ対策	15
(8)	監査性	15
4	開発工程及び作業概要	16
4-1	開発工程	16
4-2	開発作業要件	17
4-3	データ移行要件	18
4-4	操作研修要	18
4-5	テスト要件	19
5	運用保守について	20
5-1	運用保守工程	20
5-2	全体管理	21
5-3	運用支援要件	21
(1)	問合せ対応	21
(2)	操作支援	21

(3)	研修・訓練支援	21
5-4	システム保守要件	22
(1)	稼働監視・バックアップ	22
(2)	障害受付及び復旧	22
(3)	データメンテナンス	22
(4)	簡易改修	22
(5)	構成管理	23
(6)	製品予防保守	23
(7)	セキュリティ脆弱性対策	23
(8)	機器保守要件	24
6	その他要件	24
6-1	情報セキュリティと法令順守	24
6-2	システムの継続運用について	24
7	成果物	25
7-1	各工程における成果物及び作成方法	25
7-2	成果物の作成方法	26
(1)	体裁	26
(2)	データファイル形式	26
(3)	部数、媒体	26
7-3	検収方法	26
(1)	受入テスト	26
(2)	ドキュメント等	26
(3)	納入場所	26

1 システム基本方針

1-1 背景

京都府では、災害時に必要な情報の収集・提供を目的とした京都府防災情報コントロール・メール配信システム(平成 26 年度から運用開始)および、京都府災害情報収集共有システム(WebEOC)(平成 26 年度から運用開始)を運営し、関係機関とともに災害対策に従事してきた。

一方で、東日本大震災以降、熊本地震や大阪府北部を震源とする地震や近年の大型台風など、近年の頻出、大規模化する災害状況を受けて、本府の災害対策について強化をする必要がある。

現状調査書に示したように、現行システムには、情報登録の省力化、操作の容易性確保、処理速度の確保、安定性確保、機能の充実、システム間連携の容易性や柔軟性の確保、スマホ等の利用環境整備等、防災業務に影響を与える課題が生じている。

システムの更改時期を迎える中で、これらの課題に対応した刷新を図る必要がある。

1-2 新システム導入の目的

新システムは、以下の4つを目的に導入する。これにより、本府における防災と減災を図る。

図表1-3 新システム導入の目的

1. 災害情報収集の迅速性・正確性確保

外部システムとの連携等により災害情報の自動的な収集を図るとともに、防災機関からの被害情報の収集が容易なシステムとし、情報の収集の迅速性と正確性を確保する。

2. 関係機関の災害対応の円滑化・的確化

収集した情報の一元化と関係機関間での共有を図り、状況把握と対応状況の管理、対外公表等を支援する機能を備え、関係機関の意思決定と対応業務の円滑化、的確化を図る。

3. 災害情報伝達の迅速性と確実性確保

さまざまな立場に置かれた府民、府内滞在者に対して多様な媒体を活用して、災害情報の伝達の迅速性、確実性を確保する。

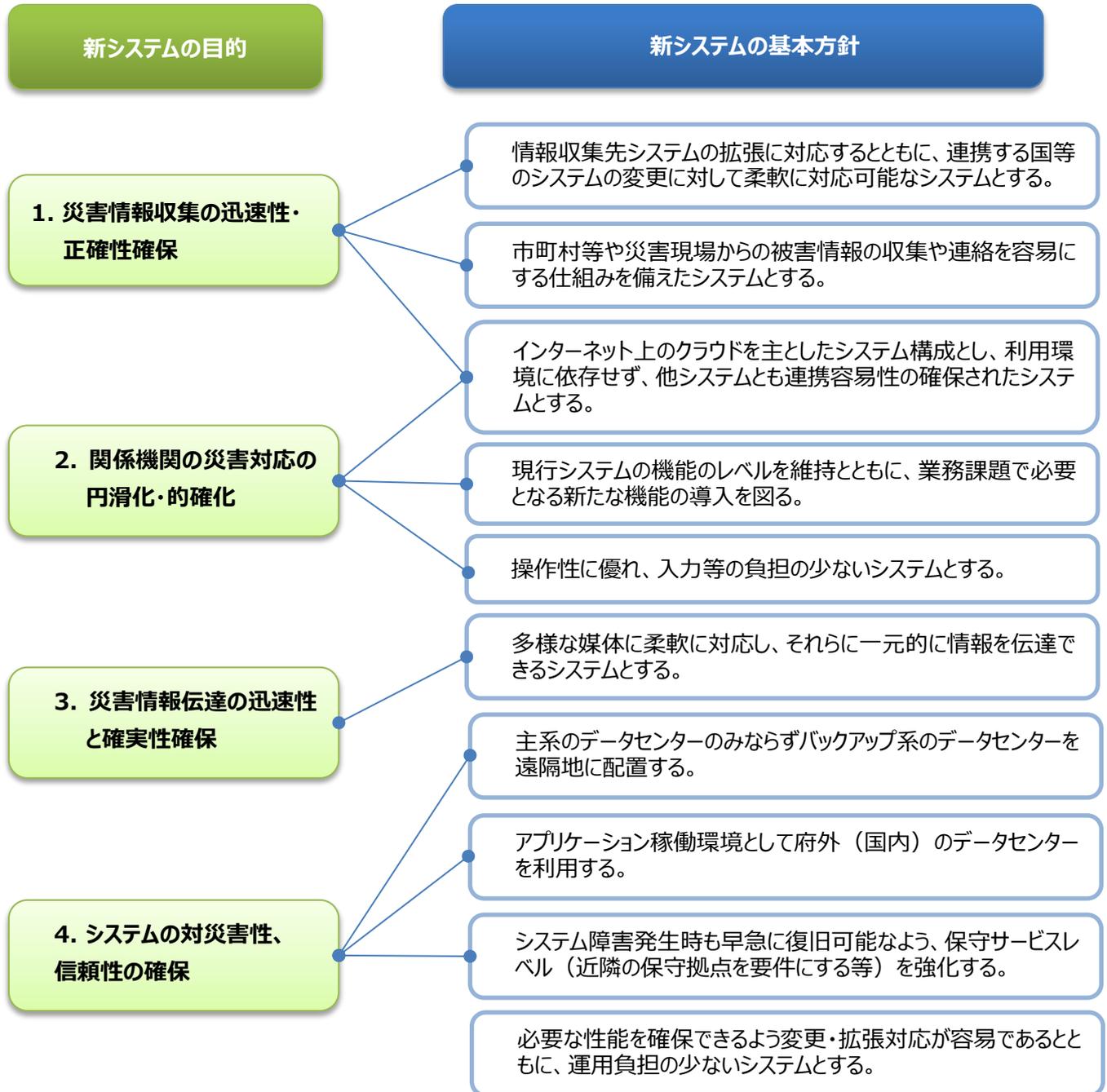
4. システムの対災害性、信頼性の確保

大規模災害発生時にこそ、その効果を発揮できるように、十分なシステムの耐災害性、継続性を確保するとともに、必要な安定性や処理能力を確保する。

1-3 基本方針

先述の目的達成のため、以下を基本方針として新システムを導入する。

図表1-4 新システムの基本方針



2 スケジュール

本府が想定するスケジュールは以下のとおり。なお、詳細スケジュールについては「4. 開発工程および各工程における作業概要」に基づき受託事業者にて適切なスケジュールを策定し、本府の承認を得ること。ただし、令和3年4月1日の稼働開始日については変更しないものとする。

- 令和2年6月中旬:業者選定(公募型プロポーザル方式)
- 令和2年6月下旬:契約締結(システム再構築業務委託契約)
- 令和2年6月下旬～7月下旬:要件定義・基本設計
- 令和2年7月下旬～令和2年12月下旬:詳細設計・開発・テスト
- 令和3年1月上旬～令和3年2月中旬:研修・受入テスト
- 令和3年2月下旬:本番移行
- 令和3年3月上旬～3月下旬:仮運用
- 令和3年4月1日～システム稼働

3 システム要件

3-1 システム形態

新システムは、先述のように、インターネットを利用できる場所であれば地理的な制約を受けずに、職員端末、携帯端末(タブレット/スマートフォン)を用いて利用できるクラウド方式を主とするシステムとする。

また、災害発生時におけるシステムの継続性を確保するため、遠隔地にリカバリーセンターを設け、リアルタイムに同期をとり、万が一メインのシステムが停止した場合にもシステムを継続的に利用できるようにすること。

なお、本調達では、緊急防災・減災事業債(消防庁)の活用を予定しているため、本府の資産となる機器の設置等と一体的に行う必要がある点に留意して提案すること。

本仕様書に記載のない追加事項がある場合は追加提案を受け付ける。ただし、追加提案にあたっては、「京都府総合防災情報システム(仮称)構築業務委託企画提案募集要領」に定める予定価格の範囲内で実現可能なものを記述すること。

端末に関しては、PC の他、タブレット端末やスマートフォンを利用できるようにする、なお、これらの端末は、各組織の既存の端末を利用し、整備対象には含めない。

これらの端末は、本府が整備する防災系ネットワーク上に展開しており、当該防災系ネットワークからは、京都府セキュリティクラウドを経由してインターネットに接続している。

については、利用が想定される端末数等の状況を踏まえ、クラウドシステムに接続する際に必要となるインターネットの帯域を示すこと。

図表3-1. システム形態への要求事項

項目	要求事項
インターネットクラウド方式	インターネットを利用できる場所であれば地理的な制約を受けずに、職員端末、携帯端末(タブレット/スマートフォン)を用いて利用できるシステムとする。
データセンター	本府に大規模な自然災害が発生した際に、システムの機能不全が生じないよう、堅牢な遠隔地(府外かつ国内)に位置するデータセンターを利用する。
災害対策	万が一、データセンターが罹災した際には、速やかに業務を復旧できるよう、必要なバックアップ対策を施すものとする。
運用監視	24時間365日の運用監視を行い、システム障害が発生した場合は、速やかな事象検知を可能とする。
維持保守	職員によるメンテナンスを要することなく、システムの維持保守を可能であるとする。
セキュリティ(ハード面)	物理的なデータセンターの不正侵入を防ぐため、サーバールームへの入室時に入室者確認の認証を行うなど、必要な対策を施すこと。

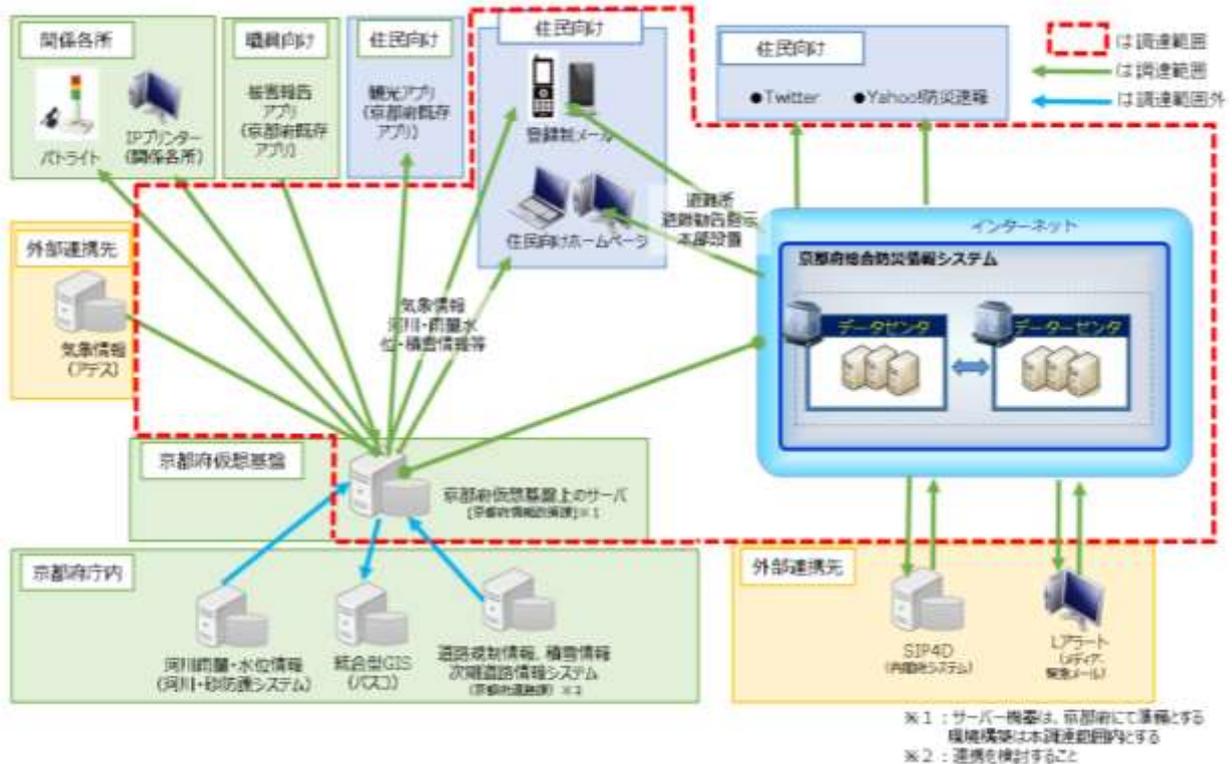
セキュリティ(ソフト面)	ネットワークを経由したサイバー攻撃等を防ぐため、IDS/IPS の導入等、必要な対策を施すこと。
提案機器	令和3年4月の運用開始後、5年間の運用保守が可能な機器とする。

3-2 システム化対象範囲

本調達におけるシステム化の範囲は以下のとおり。ただし、情報収集、状況把握ならびに情報発信等の一連の運用において、中継機器(サーバ、ネットワーク機器等)等を必要とする場合は、これに要する機器又はサービス一式も調達範囲に含めるものとし、具体的内容や目的を提案書に示すこと。

※中継機器(サーバ、ネットワーク機器等)に関しては、本府の仮想基盤上で環境構築すること。

図表3-2. システム化対象



3-3 システム概要

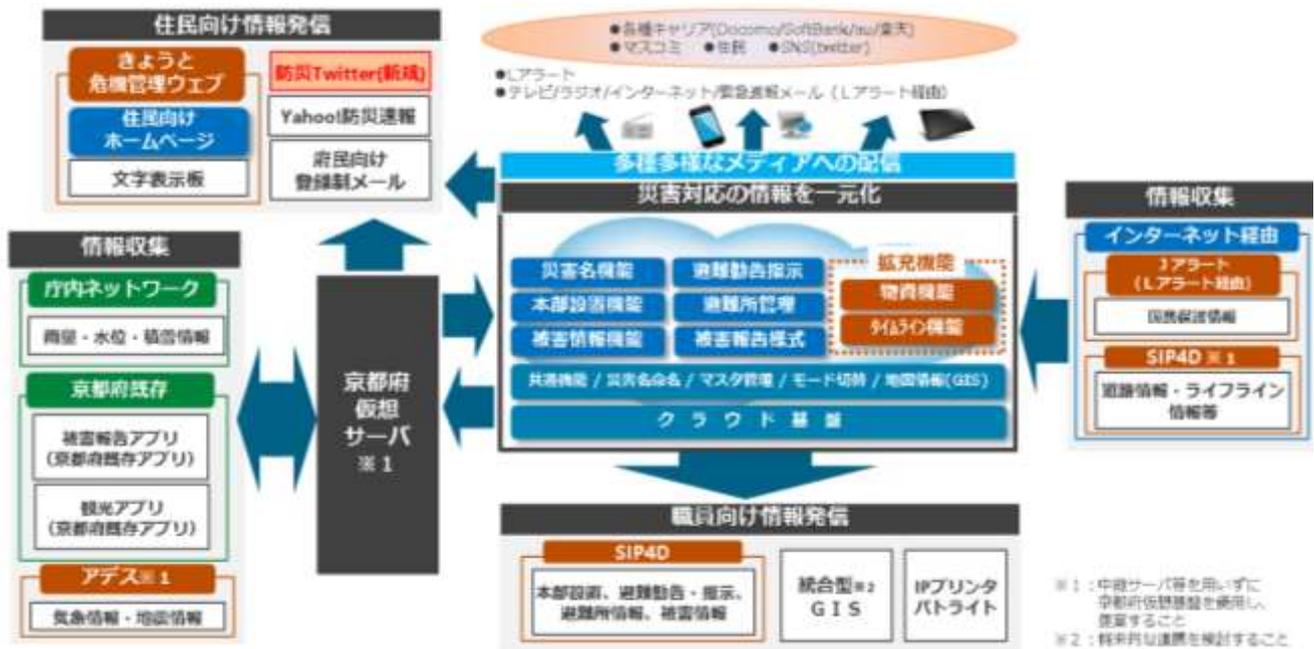
新システムの全体像を図表に示す。

災害情報収集に関し、Lアラート、内閣府 SIP4D 等の外部システム連携を柔軟に図れるようインターフェースを備え、本府の内部のシステムとの連携を図るための中継サーバを整備すること。

収集したデータは一元化し、関係者で共有を図りながら、分析・管理が図れるようにし、迅速な意思決定と円滑な災害対策業務を支援する。具体的には、災害名管理、本部設置管理、被害情報管理、避難勧告指示管理、避難所管理、被害報告等の現行システムで備えていた同様な機能他、物資管理、タイムライン機能等の機能を拡充する。

さらに収集した情報を基に、府民、府内滞在者への迅速な情報提供を可能にするため、住民向けポータルサイト(きょうと危機管理 Web)も一体的に整備し、両システムが有機的に連携したシステムとすること。また、従来提供していたメディアに SNS 等を加えた多様なメディアを通じて配信し、迅速で漏れのない災害情報の伝達を図る。

図表3-3. システム全体概要



3-4 業務仕様

本システムの業務仕様は、「別紙 機能要件一覧」のとおりとする。提案者は「別紙 機能要件一覧」に示す機能要件を満たすこととし、これを満たせない場合は、本企画提案への参加基準に満たないものとする。

提案にあたっては、提案者の持つ専門性、技術力等により、最適な実装方式を提案すること。ただし、本機能要件は本仕様書作成時点の基本要件であり、要件分析及び定義工程から基本設計工程の段階において利用者の意見集約を図りながら、最終的な機能要件を定めること。

3-5 機能要件

本システムの機能要件を以下に示す。提案にあたっては、以下の要件を満たすこと。

(1) 地図システム

地図システムに関する要件を以下に示す。

図表3-5(1). 地図システム要件

項目	要件
地図システム(GIS)	インターネット経由で常に最新の地図情報を確認でき、更新の要らない国土地理院地図などから複数の地図コンテンツを提供すること。 【例】 ・国土地理院地図 ・Google maps ・Open Street Map 等 住宅地図やインターネット障害時用の地図データはサーバ内に格納し地図コンテンツを提供すること。
コンテンツの更新	定期的にコンテンツの最新化が行われること。
その他	インターネット上で利用可能であること。 UTM グリッドに対応しており、該当するグリッド番号を表示できること。 日本国内において地理的な制約なく利用できること。 航空写真を含むこと。

(2) 端末

利用端末に関する要件を以下に示す。

図表3-5(2). 端末要件

端末種別	要件
業務用端末(パソコン) モバイル端末 (タブレット/スマートフォン)	端末機の画面はデスクトップパソコン、ノートパソコン、タブレット、スマートフォンの多様な画面を想定すること。 次に示すWebブラウザであれば、特別なソフトウェアをインストールすることなく、端末機やOSに依存することなく利用できること。また、端末機、OS、Webブラウザのバージョンアップがあった場合もシステムの稼働を保証すること。 ・ Microsoft Internet Explorer 11 以降 (ActiveX 要) ・ Microsoft Edge 8.0 以降 ・ Google Chrome (最新の安定バージョン) ・ Apple Safari 8.0 以降 (iOS は対象外) ・ Android OS 4.4 (chrome ベース) 以降のブラウザ

(3)仮想基盤情報及び調達機器一覧

本府仮想基盤サーバについて以下に示す。

図表3-5(3). 仮想基盤情報

項番	項目	要件
1	仮想基盤	他システム連携に必要なサーバについては、本府が保有する仮想基盤上に用意すること。 当該仮想基盤は、クラスタ構成により冗長化を図るとともに、府庁舎内及び京都市内のデータセンターの2カ所に分散設置し、可用性を高めている。 また、24時間ごとにミラーリングによるバックアップを取得している。

調達機器一覧等の要件を以下に示す。

図表3-5(4). 調達機材一覧

項番	項目	要件
1	仮想サーバ	・他システム連携サーバに必要な OS について、以下のものについては、ウイルス対策ソフトも含めて本府が準備する。については、必要なスペック等について示すこと。 なお、Linuxなど、本府が準備できないOSもあるので留意すること。 WindowsServer2016 standard
2	仮想基盤管理用PC	設置機器及びサーバを管理するためのパソコンを設置すること ・インテル® Corei5-5300U 2.30Ghz 相当の CPU を有すること ・メモリ 8GB 以上を有すること ・内蔵ディスク 500GB 以上を有すること ・LAN インターフェース 10/100/1000 イーサネットポートを 1 ポート以上有すること ・OS は Windows8.1Pro64bit 以降であること ・USB、RJ-45 ポートを 2 つ以上有すること ・19 インチラックにレール等で据付可能であること
3	可動式大型ディスプレイ1台	60V 型以上の可動式の大型ディスプレイを調達すること。 ・HDMI 接続可能 ・バックライト LED 直下型 ・キャスター付とし移動させることが可能であること。 ・電子白板機能を有すること。

情報発信の連携先に関する要件を以下に示す。

図表3-5(5). 情報発信要件

機能	連携先(配信先)	送信トリガー	備考
情報一括配信	Lアラート	手動	—
	緊急速報/エリアメール	手動	Lアラート経由
	防災Webポータル(危機管理専用HP)	自動/手動	気象情報と連動
	防災アプリ/Yahoo!防災速報	自動/手動	Yahoo API連携
	SNS(Twitter)	自動/手動	—
	登録制メール	自動/手動	—
	観光アプリ(本府既存アプリ)	手動	—

(4)外部情報連携

外部情報との連携に関する要件を以下に示す。

図表3-5(6). 外部情報連携要件

種別	内容	要件	
気象情報	気象注意報・警報	・システム上に情報表示	
	地震情報	・システム上に情報表示 ・発表区域を地図上に表示	
	津波情報(大津波・津波情報)	・システム上に情報表示	
	土砂災害警戒情報(判定メッシュ)	・地図上にレイヤー表示	
	大雨情報(浸水害)の危険度分布	・地図上にレイヤー表示	
	洪水警報の危険度分布	・地図上にレイヤー表示	
	降水短時間予報	・地図上にレイヤー表示	
Jアラート	国民保護情報(弾道ミサイル情報等)	・システム上の情報表示	
雨量・河川水位・	雨量・河川水位情報(雨量・水位計)	・システム上に情報表示 ・地図上にレイヤー表示	
道路規制情報等・積雪情報	道路規制情報・道路監視カメラ・異常気象時通行規制情報・積雪情報(予定)	・システム上に情報表示 ・地図上にレイヤー表示	
内閣府 SIP 災害情報ハブ(防災科学技術研究所)	道路規制情報等の道路規制情報 厚生労働省の広域救急医療情報システム(EMIS)の各指定病院の受け入れ可否等の病院情報	・地図上にレイヤー表示	
被害報告アプリ(本府既存アプリ)	現場に駆け付けた職員・団員が撮影した位置情報付写真、およびコメント	・地図上にレイヤー表示	
外部公開サイト(防災情報等)	本府	京都府公式 HP	・リンク連携
		きょうと危機管理 WEB	・リンク連携(本調達範囲)
	国土交通省	川の防災情報	・リンク連携
	気象庁	気象庁 HP	・リンク連携

(5)帳票

本システムで取り扱う帳票の中で、定型かつ出力頻度が高いものを予めシステムに登録し、システムより出力できるものとする。システム内で利用する様式は様式例として本府が受託事業者へ提供する。

図表3-5(7). 帳票要件

帳票名称	想定される対象機能(帳票を呼び出す機能)
災害対策本部設置状況一覧	本部設置機能(配備体制機能)
避難勧告指示状況一覧	発令管理
避難所状況一覧	避難所管理
被害情報管理一覧	被害情報管理
備蓄物資一覧	物資管理
ニーズ管理票	物資管理、各種管理
物資輸送管理票	物資管理
火災・災害等即報要領第4号様式(その2)	被害とりまとめ報告
被害報告とりまとめ	被害とりまとめ報告

3-6 非機能要件

本システムのクラウドサービスの非機能要件を以下に示す。提案にあたっては、以下の要件を満たすこと。

(1)規模要件

システム利用者は以下のとおりである。

図表3-6(1)。「利用者数」

項番	区分	概要	規模(人)
1	システム管理者	管理者機能を利用する、本システムの管理者 ID 管理、閲覧制限の変更、公開可否及びメニューの非表示等の設定を行う。	10 人
2	システム利用者	府職員	2,500 人
3		市町村・外部機関	2,500 人
4		現場職員	2,000 人
5	住民	住民ポータル(公開 HP)へのピーク時の同時アクセスする住民	時間アクセス 1,500,000 人想定

※ システム運用開始時は利用者数を 500 名としている。

※ 利用者 ID 数により維持管理費用が変わる場合は初期導入 ID 数を 500 とすること。

(2)性能

本システムの性能要件を以下に示す。

図表3-6(2)．性能要件

項目	要求事項
システム画面のレスポンス性能	平常時
※ 発災時においても上記条件をクリアし、急激な同時アクセスの増加においても本システムがフリーズしないこと。	1.5 秒以内
※ システム停止等の障害時には、その原因と復旧実施の結果について、本府へ報告すること。	発災時 3.0 秒以内
ただし、利用端末及びネットワークの遅延による影響は考慮しない。	

(3)信頼性・継続性

(ア)システム稼働時間

本システムは防災情報を取り扱うものであり、24 時間 365 日制限なく利用できることを前提とする。維持管理に必要なシステムの停止も、災害対応の状況、天候等の理由により本府がその時期を変更することがあり、対応できることが条件となる。

また、システム障害等を起因とした本システムの機能不全を回避するため、本システムの稼働環境は複数保有・分散設置でのサーバやネットワーク機器等の冗長構成を採用し、複数データセンターによるデータセンターの冗長構成(東日本エリアと西日本エリアへのリアルタイム同期)により、障害の種別に関わらず、単一障害によるシステム停止が発生しない構成とすること。

庁内設置の中継サーバについては法定点検等による庁舎の停電が発生するため、この停電時間は除くものとする。

なお、万が一多重障害が発生し、システムが停止した場合は速やかに復旧を図るものとするが、これに備えた平時のバックアップ方式、障害時のリカバリ方式(データ復旧ポイントを含む)については、企画提案参加者にて提案すること。

図表3-6(3). 稼働時間

項目	要件
システム稼働時間(クラウドサービス)	24 時間 365 日
システム稼働時間(庁内中継サーバ)	24 時間 365 日 ※ただし、庁舎の停電時間を除く
システム稼働時間(外部連携・サービス)	関連システム稼働時間やサービス利用規約に準ずる。

(イ)稼働率

本システムに要求される稼働率を以下に示す。
稼働率は下記の計算式で求める。

$$(\text{年間稼働率} = \text{年間の総稼働時間} - \text{サービス停止時間の累計}) / \text{年間の総稼働時間}$$

図表3-6(4). 年間稼働率

項番	要件
1	システム構成上の受託者の責任分界点範囲における年間稼働率は、99%とする。 ※(年間稼働率=年間の総稼働時間 - サービス停止時間の累計) / 年間の総稼働時間 ※庁内機器(中継サーバ)については、庁舎停電時等の計画停止を除き、95%程度とする。

主なサービス停止時間は下記に示すものとする。

- ・クラウドの障害による運用停止時間
 - ・クラウドの維持管理のために必要なシステム停止時間
- (ただし、クラウドの設定変更など、防災情報システムの運用に影響を与えない機能の保守にかかる停止時間を除く)

なお、下記に示すものはサービス停止時間からは除外する。

- ・府が事前に承諾するシステム停止に関する時間。
- ・インターネットの障害等、クラウド設備以外の障害でありクラウド事業者やシステム構築業者の責によらないシステムが利用できない時間

(ウ)サービスレベル

本システムに要求されるサービスレベルを以下に示す。

稼働環境については、SPOF(システム全体が障害・停止してしまう部位)を回避する構成とすること。
ただし、概要欄に想定施策を記載するが、同等のサービスレベルを確保する施策があれば、この限りではない。

本システムが要求する障害復旧までの所要時間を以下に示す。

図表3-6(5). 障害復旧のサービスレベル

項番	区分	障害種別	復旧時間	概要
1	クラウドサーバ障害(外部環境)	単一コンポーネント障害	即時	単一コンポーネント障害発生に備え、各サーバなどについて N+1 冗長化機能による障害迂回機能を保持し、システム中断を回避すること。
2		障害迂回経路を含む障害	1 時間以内	複数の関連コンポーネントの同時障害又は障害迂回機能自体のいずれかに障害が生じた場合は、稼働停止時間が生じる。復旧所要時間が 1 時間以上を要する判断の場合は、業務データなどを引き継いだスタンバイ環境に切替え、業務を継続させること。
3		データセンター拠点被災	自動切替	メインセンター拠点被災時には、バックアップ拠点への自動切替えにより稼働を継続する。 また、被災したメインセンターが復旧した際は、バックアップセンターから戻すこと。

項番	区分	障害種別	復旧時間	概要
4	庁内環境	サーバ障害	3時間 目安	庁内仮想環境サーバについては冗長化し、障害時の復旧時間をできるだけ短縮すること。 また、災害発生時や平常時などの緊急度合いに応じて、出来る限り稼働継続すること。
5	通信回線	府庁～外部環境	回線事業者の約款に準拠	回線不通時の障害復旧は回線事業者の約款条件に準拠する。

(エ)信頼性要件

本システムが要求する信頼性要件を以下に示す。

図表3-6(6). システム構成の要件

項番	要件
1	稼働環境サーバ構成・設置場所・ネットワーク回線を含めて、本システムの稼働環境はN+1冗長化構成を採用すること。
2	アプリケーションの稼働環境は単一構成ではなく、同様構成の稼働環境をシステム稼働拠点内に複数保有すること。
3	データセンター(サーバ拠点)の被災リスクを踏まえて、データセンター(サーバ拠点)は同一拠点に配置せず外部のバックアップセンタ(バックアップ拠点)との冗長構成とすること。なお、各拠点は東日本エリアと西日本エリアの離れた位置に配置すること。
4	データセンターへ引き込むインターネット回線は、複数回線業者のサービスを利用していること。なお、回線断時の切り替えはシステムにて自動にて行えること。
5	災害対応時のシステム負荷の影響を受けないようにするため、他都道府県の防災情報システムとは独立したシステム構成とすること(データベース含む)

図表3-6(7). データ保全(バックアップ)の要件

項番	要件
1	各サーバ拠点でリアルタイムに複製するなど、複数のストレージにて保管されること。また、本番サーバ拠点とバックアップ拠点間でリアルタイムのデータ複製を実施すること。
2	ディスク複製時のデータの伝送は、暗号化を行い送信されること。
3	日次のバックアップ業務にて、バックアップデータを作成するとともに、稼働拠点が被災した場合に備え、複数の拠点で保管するなど、データの消失を防ぐこと。

図表3-6(8). ファシリティ設備・電源設備の要件

項番	要件
1	自家発電機と燃料貯蔵設備は、冗長構成となっていること。
2	CPS/UPS システム、分電装置(PDU)は、N+1 冗長化構成となっていること。
3	外部サーバ拠点を利用する場合、電源は2回線以上から引き込み自家発電設備を備えること

(4)拡張性

業務仕様の追加、利用者数の増加、蓄積データの増加に対しては、大規模な変更(サーバ機器等の追加、機器交換)を伴うことなく、柔軟に対応できる拡張性を持つこと。

図表3-6(9). 拡張性要件

項番	拡張契機	要件
1	利用者数の増加	導入当初のアカウント数を超える利用者数が必要になった場合も、予備 ID を事前に保持するなど、即日で ID を発行できること。 利用者数を増やすことによりランニングコストの上昇がないこと。

2	アクセス数の増加	アクセス数が増加した場合においても、性能要件で示したレスポンスタイムを維持すること。性能要件が満たせない場合は、スペック拡張等の措置を実施すること。
3	業務機能の追加	業務要件が追加となった場合に、稼働環境の増設を伴うことなく、追加業務のデータベースや機能追加が容易に拡張可能な構成とすること。

図表3-6(10). 上位互換性

項番	要件
1	バージョンアップやパッチ適用が実施された場合は、本システムの機能、設定及び業務データの全てが別途費用を発生させることなく、継続利用できること。

(5)移行性

システム内で取り扱う業務データについては広く一般的に普及している形式で入力・出力できこととし、関連するドキュメントの作成方法についても同様とする。

図表3-6(11). 移行性要件

項目	要件
業務データ	本システムにて取り扱うマスタ情報(職員情報、避難所情報等)については、CSV形式等で出力できること。
ドキュメント成果物	「6-2 成果物の作成方法」に従い、本府が採用するMS-Office2010 (MS-Word 2010及びMS-Excel 2010)で読み書き可能な形式とすること。

3-7 セキュリティ対策

(1) 情報セキュリティ対策の基本方針

本システム内で取り扱う情報の機密性及び外部脅威等を踏まえリスク分析を実施し、網羅的なセキュリティ対策を行うこと。(本府が提示する関連規程を遵守)

図表3-7(1)情報セキュリティの基本方針

項番	要件
1	「京都府情報セキュリティ基本方針」及び「京都府情報セキュリティ対策基準」に基づき、セキュリティ対策に努めること。
2	庁内外からの不正な接続及び侵入、行政情報資産の漏えい、改ざん、消去、破壊、不正利用等を防止するための対策を講じること。継続的にセキュリティが確保されるよう、PDCA サイクルで管理運用し、セキュリティレベルが低減しないように取り組むこと。

(2) アクセス制御の対策

ユーザ認証(ユーザ ID、パスワード)機能を有し、ユーザ認証によって許可された利用者の権限に応じて、本システムで利用できる機能を制御する仕組みとすること。

図表3-7(2)アクセス制御の要件

項番	要件
1	ID/パスワード等により利用者組織の識別を行う機能を設けること。なお、利用者組織に応じてシステムで利用できる機能などのアクセス権限の制御を行うこと。
2	管理者権限を持つユーザはシステム利用者のアカウント管理ならびに利用者のアクセス権限の制御を行えること。

図表3-7(3)パスワードポリシー・ログイン制御の要件

項番	要件
1	パスワードが有効期限切れになるまでの期間を設定できること。
2	パスワード再利用制限にあたり、何回前のパスワードを使用不可にするかを設定できること。

3	パスワードとして許可する最小の長さを設定できること。
4	ログインの失敗が許される回数を制限し、制限を超えた場合はロックできること。
5	文字や数字、記号をくみあわせたログイン ID とパスワードとすること。
6	ロックの解除及びパスワードの変更は管理者側で簡易に行えること。
7	ID ごとに重複ログインを許可するか否かの設定ができること。

図表3-7(4) 伝送とセッション設定の要件

項番	要件
1	何も操作しない状態が何分間続いた場合に自動的にログアウトさせるか設定できること。
2	セッションのタイムアウトによりログアウトするときに、ブラウザから結果を表示できないように設定できること。
3	ログイン可能な IP アドレスを制限できること。
4	すべてのページ要求に対して、TLS1.2 もしくは 1.3 を経由し、暗号化強度が 256bit 以上の SSL サーバ証明書を使用すること。
5	個々のセッションにはログイン時に作成された固有のトークンを使用し、トランザクションごとに識別及び再検証ができること。
6	初回ログインの後、ブラウザにユーザ名とパスワードを保存し、以降のログイン時にオートコンプリートするかの設定ができること。

(3) ネットワーク保護

本システムで使用する通信プロトコル及び通信ポート以外での接続を禁止し、不正な接続等があった場合は、それを検知し、ログを取得する仕組みが提供されること。

図表3-7(5) ネットワーク保護の要件

項番	要件
1	システム構成上の境界部にファイアウォール等を設置し、不要な通信をブロックすること。
2	システム特性に応じ、アンチウイルス、侵入検知、Web フィルタリングなど、外部環境からのアクセスに対してセキュリティを確保すること。

(4) ウイルス対策

マルウェア(ウイルス、ワーム、ボット等)による脅威に備えるため、稼働環境にはウイルス対策ソフトを導入すること。

図表3-7(6) ウイルス対策の要件

項番	要件
1	新たに発見されるマルウェアに対応するため、パターンファイルの自動更新を行い、常に最新のパターンファイルを適用すること。
2	ウイルス感染・検疫・駆除の一元監視機能を有すること。

(5) データの暗号化

本システムからの情報の漏えい等を防止するため、利用者が直接アクセスできないように制限し、機密データ等は暗号化する機能を備えること。また、通信回線に対する盗聴防止のため、通信回線を暗号化する機能を備えること。

図表3-7(7) データの暗号化の要件

項番	要件
1	パスワードは(SHA-256 hash with salt)にて暗号化し、パスワード保有者以外は管理者及び受託者も把握できないこと。
2	システム設定データを保持する場合は、定義情報(メタデータ形式を想定)にて保存し、ログイン成功者以外はシステムに格納されている情報を判読できないこと。

(6) **監査証跡**

ログイン履歴や変更を監視するための監査ログを本府で確認できること。

図表3-7(8)監査証跡の要件

項番	要件
1	運用期間中に行われたログインの成否に関する記録を保存できること。

(7) **ファシリティ対策**

本システムの稼働環境が設置されるサーバ拠点は日本国内の複数拠点に設置されたものとし、以下の物理的セキュリティ対策を満たした設備とすること。

図表3-7(9)サーバ拠点の情報セキュリティ対策

項番	要件
1	有人監視を実施すること。
2	外観は看板や標識がない匿名性を確保していること。
3	入退室(マントラップ)機能をサーバルームの入口に設置し、入退管理を実施すること。
4	サーバ機器はカギ付きケージに格納すること。
5	施設及び周辺を監視カメラにより監視していること。
6	サーバルームは独立した無窓の部屋であり、外部から容易な侵入ができないこと。
7	建物にはクラウド事業者との関連が識別可能な表示を行っていないこと
8	回線設備は専用の設備内にあり施錠されていること。
9	落雷による影響を受けない建物仕様としていること。
10	受電回路の冗長化を施していること。
11	地政学的な影響リスクを低減・回避するため、必ず国内に主および副の環境を備えること。

(8) **監査性**

情報セキュリティ対策の的確性を客観的に判断できるよう、監査認証を実施できること。

図表3-7(10)監査性確保の要件

項番	要件
1	以下の評価を本業務内で定期的に Web アプリケーション診断を実施すること。 アプリケーションコードの脆弱性評価、ネットワークの脆弱性脅威の評価 選定した侵入テストとコードレビュー、セキュリティ管理フレームワークのレビューとテスト
2	関係機関との提携・外部委託により、下記内容を実施すること。 日々発生するセキュリティ脅威の情報収集 セキュリティパッチの情報収集、脆弱性診断
3	データセンター事業者および受託者は情報セキュリティマネジメントシステム(ISMS)の認定を受けていること。
4	収集した脆弱性や不正侵入の手口については随時、本府でも把握できることように周知及び協力すること。

4 開発工程及び作業概要

4-1 開発工程

本府が想定する開発工程及び作業概要は以下のとおり。詳細については、契約締結後にプロジェクトの進捗及び品質について適切に管理するための「プロジェクト計画」を受託事業者にて取り纏め、本府の承認を得ること。本府は、受託事業者が策定した「プロジェクト計画」が適切に遂行されていることを管理し、また、府内部の意見を集約し、要望として受託事業者に対し明確に伝え、受託事業者の成果物を確認、検収するものとする。

なお、本システムの開発は、提案者が保有するパッケージ機能等を可能な限り活用することにより、短期開発、不具合の低減ならびに保守性の向上を図るものとする。本府が示す要件の実現にあたってカスタマイズを要する部分については、要件分析及び設計工程にて十分な協議を行うこと。また、パッケージ製品であることを理由としてカスタマイズ等に制限を設けないこと。

図表4-1(1) 監査性確保の要件

【凡例】◎: 主担当 ○: 支援

工程	概要	役割分担	
		本府	受託事業者
プロジェクト計画策定	プロジェクトについて適切に進行管理、品質管理を行うための実行計画策定	○	◎
機能説明会	本府と受託事業者における開発内容に対するギャップの解消及びカスタマイズ範囲の明確化を目的とした機能説明会の実施、	◎	◎
要件分析及び定義	システム要件・要望等の取り纏め・提示(業務フロー、画面レイアウト、帳票要件等)	◎	
	提示内容及び協議内容に基づく機能・非機能要件の策定		◎
基本設計	要件定義にて定義した要件に基づくアプリケーション機能及びシステム方式の設計、仕様化		◎
	設計、仕様の確認、承認	◎	
詳細設計・開発・テスト	—	—	—
詳細設計	基本設計に基づくアプリケーション機能及びシステム方式、外部インターフェース設計の詳細化		◎
	設計、仕様の確認、承認	◎	
連携システム調整	連携する他システムとの接続に係わる調整等	◎	○
製造・環境構築	稼働環境の設置・工事、サーバ環境の構築、回線敷設、プログラム製造		◎
単体・結合テスト	テスト仕様の作成		◎
	単体・結合テストの実施		◎
総合テスト	テスト仕様の作成		◎
	機能、非機能要件に基づく総合テスト実施		◎
操作研修	研修実施計画の策定	○	◎
	管理者向け操作研修、一般利用者向け操作研修	○	◎
	関係部門向け操作研修	○	◎
受入テスト	テスト仕様の作成	◎	○
	テスト実施	◎	○
本番移行	データ移行、環境の本番化(テスト用設定、一時ファイル削除等)	○	◎

4-2 開発作業要件

各開発工程に共通する作業要件を以下に示す。本作業要件については、受託事業者がプロジェクト遂行に必要なレベルに落とし込み、「プロジェクト計画」へ反映すること。

図表4-2(1)開発作業の要件

管理事項	要件
進捗管理	WBS(Work Breakdown Structure)等により作業工程毎に必要な成果物を明確にすること。
	プロジェクトの進捗状況を管理する進捗管理表及び各作業タスクの進捗状況を可視化し、定期的に報告、提出すること。
	プロジェクト計画で定めたスケジュールに遅延が生じた場合は、原因の調査及び改善策を提示し、本府の承認を得た上で、実施すること。
品質管理	プロジェクト計画にて事前に定めた手法に則って品質管理が実施されていることを継続的に確認すること。
	工程完了判定時に事前に定めた工程完了基準を満たしているかを評価し、本府に報告すること。基準を満たない場合は、対応策について報告すること。
	工程完了判定時に限らず、本府による判断、決定を要する事案については、定期的にレビューを依頼すること。
	仕様や要件の確認及び確定に関しては、必ず書面により行うこと。
課題管理	進捗や品質等の課題が発生しているかどうか、また発生した課題に対して適切に対応が取られているかを、課題一覧を作成し、一元的に管理すること。課題一覧では、検討期限、検討主体、検討状況、検討経過、検討結果等を管理すること。
	定例会議の場において課題の対応状況について棚卸を実施し、迅速な解決に取り組むこと。ただし、急を要するものについては随時報告すること。
リスク管理	プロジェクト遂行上のリスクを管理し、リスクへの対応状況を管理すること。必要に応じて課題化し、解決に取り組むこと。
変更管理	変更要求と対応結果について管理すること。
	各種設計書などのドキュメントについて、変更履歴を適切に管理すること。
	構成管理対象物(ドキュメント、プログラム等)は、改修、製品バージョンアップ、セキュリティパッチ適用等による不具合が万が一発生した場合に備え、変更前の状態に復旧できる仕組みを確立すること。
コミュニケーション管理	作業工程ごとにおける各種協議、成果物レビューのほか、進捗・課題等に関する報告、共有を行う会議を定期的開催すること。
	定例会議、その他会議体(キックオフ、工程終了判定会議等)については、会議体の目的、出席者及び実施頻度等をプロジェクト計画書で明確にすること。
	各種会議体の開催日以降、原則 5 営業日以内に議事録を作成し、本府の承認を得ること。会議議事録には、各会議での決定事項及び検討事項等を明記すること。
体制管理	プロジェクトマネージャ又はプロジェクトリーダーは、システム的设计・開発経験が5年以上あること。
	プロジェクトマネージャ又はプロジェクトリーダーは、原則として、プロジェクト計画策定から本番移行のフェーズまで変更しないこと。止むを得ない理由により人員交代の必要が生じた場合は、本府の承認を得た上で、実施すること。
	作業工程に応じて、適切な知識及び経験を有した要員を配置すること。
	各工程にて生じた事由により、プロジェクト計画書にて定めた体制を変更する場合は、本府の承認を得た上で、実施すること。
	本委託業務に携わる人員については、資格、経歴・実績、経験年数、氏名を明らかにし、業務着手に先立ち本府に提出すること。

管理事項	要件
業務支援	本システムの構築に際して必要となる外部システムとの技術面での連携調整等については必要に応じて支援すること。

4-3 データ移行要件

現在運用中の現行システムや管理ファイルのデータを当システムに移行すること。
 なお、本システムへ移行が必要な現行システムの対象データについては、以下に示す。

図表4-3(1) 移行対象データ

項目	登録情報	データ形式	本府提供
公共施設	主要行政機関／警察・交番／消防署・出張所／病院	CSV 形式	○
ハザードマップ等	土砂災害／津波／浸水・洪水、緊急輸送道路地図	Shape 形式	○
避難所管理	避難所情報等	CSV 形式	○
発令管理	避難情報等	CSV 形式	○
登録制メール情報	登録制メール情報(氏名/メールアドレス等)	CSV 形式	○

4-4 操作研修要件

操作研修に関する要件を以下に示す。

図表4-4(1) 操作研修要件

項目	要件	開催場所
操作研修計画書の作成	本府における操作研修の実施スケジュール作成の支援、および実施内容等を記載した操作研修計画書を作成すること。	-
マニュアルの作成	本システムの操作手順を示した操作マニュアルを作成し、本府の承認を得ること。また、本システムの運用管理及び障害発生時の一次切り分け等を円滑に実施するための運用手順を示した運用マニュアルを作成し、本府の承認を得ること。	-
管理者研修の実施	管理者に対する集合研修を行うこと。実施内容は機能説明に加え、管理者機能に関する研修とし、研修規模は10名程度の規模にて2回程度の実施を想定。	庁舎内
防災担当職員研修の実施	防災担当職員に対する集合研修を行うこと。実施内容は機能説明に加え、実災害を想定したシナリオ型の研修とし、研修規模は20～30名程度の規模にて5～6回程度の実施を想定。	庁舎内
研修結果のフィードバック	操作研修のフィードバックとして、機能、マニュアルの改善を図ること。	-

※研修会場(大型モニタ等表示装置含む)、研修用PC端末、ネットワーク回線は本府にて準備する。

※研修会場は府庁にて行うこととする。

図表4-4(2) 研修対象及び内容等

項番	対象	人数	研修内容	回数	開催場所
1	管理者	約 10 名	<ul style="list-style-type: none"> ・本システムに係る操作方法(実機研修) ・本システムに係る運用管理方法 ・本システムに係る障害時の対応方法 ・円滑な本システム利用に資する事項 	年1回	庁舎内
2	一般利用者	約 200 名	<ul style="list-style-type: none"> ・本システムに係る操作方法 (各回 30～40 名を想定)	年6回	庁舎内

4-5 テスト要件

テストに関する要件を以下に示す。

図表4-5(1) テスト要件

項目	要件
テスト計画策定	総合テスト及び受入テストの実施に先立ち、各テスト工程のテスト計画書及びテスト仕様書を作成すること。
テスト仕様書作成	テスト仕様書には、テスト目的及び項目、テスト方法、テスト環境、テストデータ、テストケース・シナリオ、テスト手順を記載すること。
テスト結果報告	総合テスト及び受入テスト終了後、テスト結果、障害対応、残課題、品質評価結果等をまとめた報告書を作成すること。
品質向上施策の実施	テスト結果報告にて、安定した品質が確保できないと判断される場合は、受託事業者の責任及び費用負担により必要なシステム改修及び追加テスト等の品質向上施策を実施すること。

5 運用保守について

5-1 運用保守工程

本府が想定する保守工程及び作業概要は以下のとおり。詳細については、契約締結後に「運用保守実施計画」を受託事業者にて取り纏め、本府の承認を得ること。

図表5-1(1). 運用保守工程

区分	令和3年度				令和4年度
	第1四半期	第2四半期	第3四半期	第4四半期	第1四半期
運用保守	●契約 				

図表5-1(2). 運用保守工程

項番	工程	概要	実施時間
1	運用支援	問合せ対応	平日業務時間帯 (9:00~17:00)
2		操作支援	平日業務時間帯 (9:00~17:00)
3		研修・訓練支援	平日業務時間帯 (9:00~17:00)
4	システム運用保守 業務	構成管理	24時間 365日
5		稼働状況の監視	24時間 365日
6		データバックアップ	24時間 365日
7		バージョンアップ	24時間 365日
8		セキュリティ対策	24時間 365日
9		予防保守	24時間 365日
10		障害受付対応	24時間 365日
11		障害復旧対応	24時間 365日
12		構成管理	24時間 365日

※上記の運用保守実施前提で、非機能要件に対応できる前提で提案すること。

(1) 非稼働時間のサービスレベル

あらかじめ本府が承諾する、運用保守に係るシステム停止(非稼働時間)については、本システムの停止時間の短縮を図る目的にて、以下のサービスレベルを提案すること。

図表5-1(3). 運用保守工程

項番	種別	要件
1	メジャーリリース	パッケージソフトウェア又はクラウドサービスのバージョンアップ
2	計画メンテナンス	運用上の予防的メンテナンス作業
3	緊急メンテナンス	セキュリティ等事由のメンテナンス作業

※作業頻度や作業時間は別途協議の上定める。

※上記以外のメンテナンスについても、「日時」「メンテナンス内容」「停止時間」等を事前報告すること。

5-2 全体管理

運用保守工程における作業プロセス全体の管理要件を以下に示す。

図表5-2(1). 管理要件

項目	要件
全体管理	受託事業者は、運用保守工程全体の品質及び進捗を管理し、発生したトラブル、課題事項等については、報告書、スケジュール表、課題一覧等に記載し、プロジェクト全体を適切に管理すること。
定例会議	定例会議(2~3回程度/年)を実施し、「運用保守実施計画」の進捗状況について報告し、3月末には年次報告を実施すること。
緊急作業	緊急度の高いセキュリティ脆弱性対策、障害対応等、非定型な運用業務が発生する際は、速やかに本府に報告し、対応を協議すること。

5-3 運用支援要件

本システムの運用支援要件は以下のとおり。受託事業者は、本府がシステムを運用及び活用するにあたり、必要に応じた支援を実施すること。

(1) 問合せ対応

本システムの問合せ対応要件は以下のとおり。

図表5-3(1). 問合せ対応要件

項目	要件
受付方法	受託事業者は、本システムに関する問い合わせの窓口として、代表電話番号及びメールアドレスを用意すること。
履歴管理	過去の問い合わせについては、内容、対処結果等を記録し、ステータスを管理するとともに、年次報告の場にて報告すること。

※本府からの問合せは、整理、集約した上でシステム担当者より行う。(年20件程度を想定)

(2) 操作支援

本システムの操作支援要件は以下のとおり。

図表5-3(2). 操作支援要件

項目	要件
操作支援	本府の依頼に基づき操作支援又は手順提供を行うこと。
アカウント管理	本システムの利用者情報の追加、更新、削除、パスワード初期化、アカウント無効化解除等の作業について、本府からの依頼に基づき実施すること。
データ更新	本システムで利用されるデータの種類・機密度(セキュリティレベル)において、本府と協議の上、運用に合わせて見直すこと。

(3) 研修・訓練支援

本システムの研修・訓練支援要件は以下のとおり。

図表5-3(3). 研修・訓練支援要件

項目	要件
研修支援	管理者及び一般利用者向けに年1回の集合操作研修を対面で実施すること。
訓練支援	図上での防災訓練シナリオ作成に伴う助言、支援を実施すること。

※防災訓練シナリオは本府が主体的に作成し、その実現に向けた技術的な支援を求めることを想定

図表5-3(4). 研修対象及び内容

項番	対象	人数	研修内容	回数	開催場所
1	管理者	約 10 名	<ul style="list-style-type: none"> ・システムに係る操作方法(実機研修とする) ・本システムに係る運用管理方法 ・本システムに係る障害時の対応方法 ・円滑な本システム利用に資する事項 	1回	庁舎内
2	一般利用者	約 200 名	<ul style="list-style-type: none"> ・本システムに係る操作方法(各回 30~40 名を想定) 	6 回	庁舎内

5-4 システム保守要件

本システムのシステム保守要件は以下のとおり。受託事業者は、安定したサービス提供に必要なシステム保守を実施すること。

(1)稼働監視・バックアップ

稼働監視に関する要件を以下に示す。

図表5-4(1). 稼働監視要件

項目	要件
稼働監視	サービスの稼働状況を常時監視し、自動的に稼働環境の負荷上昇や異常を検出し、安定したシステム運用を確保するための処置を施せること。
バックアップ	システムが保有するデータは、複数環境にバックアップし、データ消失を防止した上で、日次(5 世代)での保管を行うこと。

(2)障害受付及び復旧

障害受付及び復旧に関する要件を以下に示す。

図表5-4(2). 障害受付及び復旧要件

項目	要件
障害受付	<p>障害が発生した際には、障害箇所及び原因を調査し、障害の一次切り分けを行い、速やかに本府に連絡すること。</p> <p>障害や災害時には、必要に応じて対応できる保守窓口もしくは保守要員を置くこと。</p>
障害復旧	<p>障害が発生した際には、速やかに本府に連絡し、必要に応じて関連事業者等と連携・協力し、システムの復旧を行うこと。なお、障害の復旧までの所要見込み時間を本府に連絡すること。</p> <p>障害発生原因については、開発保守環境にて再現テストを実施し、原因を特定の上、再発防止策を講ずること。</p> <p>障害内容、原因、復旧対応結果を記載した書面を作成し、本府に提出すること。</p>

(3)データメンテナンス

データメンテナンスに関する要件を以下に示す。

図表5-4(3). データメンテナンス要件

項目	要件
ハザードマップ等	ハザードマップ等の最新版がリリースされた場合に入替を実施する。

※ハザードマップ等の入替は、年次作業として実施を想定

(4)簡易改修

年間 2 人月を上限とした簡易改修に関する要件を以下に示す。

図表5-4(4). 簡易改修要件

項目	要件
パッケージ改修(パッケージ対応業者のみ)	受託事業者が提供する標準パッケージを改修又は機能追加することに伴うシステム改修に対応すること。
法令改正に伴う改修	気象庁電文変更、元号改正等、法令改正に伴うシステム改修に対応すること。
軽微な改修	機能の新規開発や大幅な改修を伴わない配備計画名称の変更、その他表示名称の変更、パラメータ修正等の軽微な改修に対応すること。

※改修要望については、本府にて整理、集約した上で定例会議等に提示することを想定

(5)構成管理

本府が求める構成管理要件を以下に示す。

図表5-4(5). 構成管理要件

項目	要件
ドキュメント管理	運用保守工程において、システム構成等に変更又は追加が生じた場合は関連する設計書、マニュアルを更新すること。
製品バージョン管理	導入するソフトウェア(OS、ミドルウェア、その他製品プログラム等)の製品名、バージョン情報等を台帳として管理し、システム構成等に変更又は追加が生じた場合はこれを更新すること。

(6)製品予防保守

本府が求める製品予防保守要件を以下に示す。

図表5-4(6). 製品予防保守要件

項目	要件
製品予防保守	導入するソフトウェア(OS、ミドルウェア、その他製品プログラム等)に不具合が公開された場合、あるいは製品サポート終了が発表された場合は、事象の影響を評価し、必要に応じたバージョンアップ又はパッチ適用を実施した上で安定した稼働環境を維持すること。

(7)セキュリティ脆弱性対策

本府が求めるセキュリティ脆弱性対策要件を以下に示す。

図表5-4(7). セキュリティ脆弱性対策要件

項番	要件
1	システムのログファイル等からシステムの利用状況(ログイン件数等)を調査し報告すること。また、システムやネットワークに対する不正なアクセス等がないか監視し報告すること。
2	脆弱性を解消するセキュリティパッチの適用作業は、時期を決めた上で本府との協議により実施する。緊急性の高い場合は時期によらず本府との協議によりただちに実施すること。
3	外部セキュリティ関係機関や稼働環境を構成する機器供給先との提携・外部委託により、下記内容を実施すること。 <ul style="list-style-type: none"> ・日々発生するセキュリティ脅威の情報収集 ・セキュリティパッチの情報収集 ・脆弱性診断
4	日々発生するセキュリティ脅威の情報収集結果、対策の具体的な内容、対策の実施状況について、本府が把握できるよう情報の公開サイトを提供すること。
5	コンピュータウイルス対策が正常に稼働し、ウイルス感染が無いことを確認すること。また、常に最新の定義ファイルを適用すること。

(8)機器保守要件

本府が求める機器保守要件を以下に示す。

図表5-4(8). 機器保守要件

項目	要件
運用保守期間中の保守	運用保守期間中(5年間)の保守を行うサービス形態を含んだ形で調達すること。

6 その他要件

6-1 情報セキュリティと法令順守

本システムの開発においては、技術的な対策を施すことはもちろんのこと、防犯対策や入室管理等の物理的対策、規定や情報扱い手順の順守徹底等の人的対策をあわせて行い、網羅的な情報セキュリティ対策を導入すること。

については、本システムで扱う個人情報について明らかにし、その保護手段について明らかにすること。

システムの保守等に伴い、記憶装置等の機器を返却、廃棄する必要がある場合は、本府に報告の上、住民情報等の重要情報が大量に保存されたものは、記憶装置の全ての情報を消去の上、物理的な破壊又は磁気的な破壊の方法により復元不可能な状態にすること。

それ以外の記憶装置については、本府に報告の上、全ての情報を消去した上で、「0」、「1」等の情報で全ての領域を上書きする方法によりデータの抹消を行うこと。

また、民法(明治29年法律第89号)、刑法(明治40年法律第45号)、著作権法、不正アクセス行為の禁止等に関する法律(平成11年法律第128号)、個人情報の保護に関する法律(平成15年法律第57号)等の関係法規を遵守すること。

6-2 システムの継続運用について

本システムは、調達後5年間の利用を見込んでいるが、その後についても継続利用する可能性がある。

この場合、単年度契約となる可能性があるが契約期間が短くなることによりランニングコストの上昇がないようにすること。

7 成果物

7-1 各工程における成果物及び作成方法

各工程における成果物及び納入期限を以下に示す。納入にあたっては、事前に本府の承認を得ること。その他に有効な成果物がある場合は、プロジェクト計画書に記載し、本府の承認を得た上で納入すること。

図表7-1. 成果物及び納入期限

成果物	概要	納入期限
プロジェクト計画書	プロジェクトについて適切に進行管理、品質管理を行うための実行計画を定めたもの (以下、計画に含むもの) ▶ プロジェクト概要 (目的、作業実施方針、対象業務、開発スコープ等) ▶ プロジェクト推進手法 (作業実施方針、工程完了基準等) ▶ スケジュール・体制 ▶ 会議体の定義 ▶ 成果物の定義 ▶ その他プロジェクト管理ルール	契約締結後、10営業日以内
要件定義書	受託事業者の提案内容、本府の提示内容及び協議内容に基づく機能・非機能要件に基づき、システム概要図や機能概要、業務フローを整理したもの	要件分析及び定義工程完了後、10営業日以内
システム設計書	本業務委託に基づき設計したアプリケーション設計(機能要件、画面設計、画面遷移、帳票設計、データ設計、アプリケーション仕様等)、方式設計(ネットワーク構成図、サーバ構成情報、設定パラメータ等)、運用設計、情報セキュリティ設計を整理したもの	令和2年12月末
アプリケーションプログラム等一式	本業務にて開発したアプリケーションプログラム等一式(ただし、受託事業者が従前から有していたプログラム及び第三者が権利を有するソフトに含まれる部分は除く)	令和3年3月末
ライセンス証書	受託事業者が提案するソフトウェアの使用許諾を記載したライセンス証書(必要に応じて)	令和3年3月末
テスト関連資料	テスト計画書、テスト実施報告書	令和3年3月末
操作研修計画書	操作研修の対象職員、実施スケジュール、実施内容等を記載したもの	令和2年12月末
操作マニュアル	管理者および利用者がシステムを利用した業務を遂行する上で、操作手順や機能を示した説明書(管理者、一般職員用にそれぞれ作成することとし、操作研修等でのコメント、改善事項等の取込を行った状態で納品すること。)	令和3年1月末
会議関連資料	本業務委託の遂行に伴い作成した会議資料、進捗管理表、課題一覧、リスク管理一覧、トラブル報告書、議事録等	随時
調達機材	本仕様書の記載事項及び受託事業者と別途締結する委託仕様書の条件を満たすサーバ、サービス等一式(受託事業者にてサービス提供に必要な搬入、設置、工事、回線敷設、構築、テスト等、一連の設定作業が完了していることを納入条件とする。)	令和3年3月末

7-2 成果物の作成方法

(1) 体裁

原則として A4 判とするが、必要に応じて A3 版を可とする。日本語で記載すること。

(2) データファイル形式

データファイル形式は、本府が採用する MS-Office2010 (MS-Word 2010 及び MS-Excel 2010) で読み書き可能な形式とすること。これ以外の形式を利用する際は、本府と相談すること。

(3) 部数、媒体

電子媒体及び紙媒体を納入するものとする。プログラムファイル等、印刷に適さないものについては、電子媒体のみの納入とする。ただし、ソフトウェアのライセンス証書等、複製できないものが含まれる場合は、原本のみの納入とする。

- ① 電子媒体は、CD/DVD-ROM とし、正 1 部、副 1 部を提出すること。
- ② 紙媒体は、バインダーに綴じたうえで、正 1 部、副 1 部を提出すること。必要に応じてインデックスを付与すること。

7-3 検収方法

(1) 受入テスト

テスト仕様書に基づき、本府にて受入テストを実施し、すべての条件を満たすことをもってアプリケーションプログラム等についての検収とする。

(2) ドキュメント等

要件定義書、設計書等は、開発工程の各段階において照査を行うため、受託事業者は、工程完了判定会議にて、ドキュメント等の対応状況を報告すること。最終的には、本府と受注者において別途協議して定める完了届に基づき、検査を行う。検査の結果不合格の場合には、再納入とする。検査の合格をもって、本業務委託に係る委託料の一部または全部を支払うものとする。

(3) 納入場所

〒602-8570 京都市上京区下立売通新町西入藪ノ内町
京都府 危機管理部 災害対策課