徳島県安否確認アプリ構築業務
仕様書

令和８年５月　徳島県

目　次

別紙

1　業務概要

1.1　業務名

徳島県安否確認アプリ構築業務

1.2　業務目的

徳島県（以下、「本県」という。）は、南海トラフ地震で甚大な被害が想定される地域であることから、県民の命と財産を守るための対策は待ったなしの状況である。そうした中、大規模災害発生時に地域を支える医療機関や社会福祉協議会、企業等（以下、「事業者」という。）において、職員や従業員の参集可否を判断する「安否確認手段」の確保が必須となる。また、災害時の通信輻輳により状況把握に時間を要することが懸念されるため、電話やメール以外での連絡手段を確保する必要がある。

本業務は、これらを具現化するための仕組みとして、スマートフォン等で利用できる「徳島県安否確認アプリ（以下、「アプリ」という。）」を開発し、大規模災害発生時に地域を支える関係者間の安否状況の把握をデジタル化することで、地域の災害対応力を強化するものとする。

1.3　業務委託期間

契約締結の日から令和９年３月３１日（水）まで

1.4　業務概要

業務の実施に当たっては、1.6 に掲げる業務内容に加え、「別紙１　安否確認アプリ機能一覧」を十分理解し、適切な実施体制でこれに臨むこととし、その具体的手法は受託者が自らの知見を最大限活用して実施するものとする。

また、本事業は地域未来交付金（デジタル実装型 TYPEA）の交付を受けて実施するものであるため、地域未来交付金制度要綱等、国の通知や随時発出される国からの指示に沿って業務を実施すること。

1.5　スケジュール

以下のスケジュールを想定しており、受託者はこれを参考とした詳細なスケジュールを策定の上、業務を実施すること。

＜想定スケジュール＞

・令和８年６月：事業者選定
・令和８年６月～１２月：設計、庁内プロトタイプ作製・運用、構築完了
・令和８年１２月～３月：移行期間
・令和９年４月１日～：本格運用開始

1.6　調達範囲

本仕様書に定める業務（以下、「本業務」という。）の調達範囲は下記のとおりとし、業務遂行上必要な費用は受託者にて負担すること。

なお、次の各号に掲げる業務内容について、過不足やその他対応すべきと考えられるものがあれば追加提案し、本県と協議の上、実現すること。

ア） アプリ構築に係るプロジェクト管理

受託者は、本業務の遂行を確実とする実施体制を確保した上で、本業務全体について、実施内容やスケジュール等を整理したプロジェクト計画書を作成すること。

また、システムの仕様及び運用方法の調整や、プロジェクトの進捗状況管理を行うこと。

イ） アプリの初期構築作業

・本アプリの設計、開発及び安定して稼働する環境の構築

・防災情報の自動取得に必要な外部基盤（L アラート等）との連携設定

・テストの実施及び本県職員によるテスト実施への支援

なお、運用に必要な機能についても設計開発を実施すること。

また、本業務委託期間中において、本アプリの構築、テスト、稼働等に必要となるクラウドサービス利用料については本調達範囲に含め、受託者の負担とする。

ウ） 本アプリを県民が利用できるように各プラットフォームで公開する業務

また、仕様に記載がない事項であっても協議中発生する事項については検討し、可能な限り実現に向けて対応すること。

なお、安否確認アプリは 10 年程度運用することを想定している。令和９年度以降の運用保守業務については、各年度における予算の成立を前提条件として別途契約する。

2 機能要件

2.1 本アプリに必要な機能

本アプリが備えるべき業務機能の要件は、「別紙１ 安否確認アプリ機能一覧」に記載のとおりであり、これらの機能の実現は必須とする。機能の実現にあたって、受託者が提案する代替手段による場合には、県に申し出て、承諾を得ること。

2.2 運用保守機能

本アプリのシステムの障害対応や稼働環境の運用保守等に対して、費用を抑制でき、適切な維持管理ができる機能を実装すること。具体的な機能については以下を想定している。

- ✓ 監視機能（障害検知、イベント検知、リソース監視等）
- ✓ メンテナンス機能（システムメンテナンス等を想定）
- ✓ バージョンアップ更新機能（サーバ側、アプリ側）
- ✓ 県民からの問合せ機能（Q&A 集含む）

3 非機能要件

3.1 稼働環境

本システムは、インターネット上のクラウドサービスを利用することとし、安定的に常時運用が可能で、かつ耐災性の高いシステムとする。

3.1.1利用環境

ユーザインターフェース（ネイティブアプリ、Web アプリ等）については、本サービスにおいて最も有用だと考えられる方針及び当該方針におけるメリットとデメリットを提案の上、提供を行うこと。またデメリットに対する対応策についても提案すること。

3.1.2対象 OS、ブラウザについて

スマートフォン・タブレット・パソコンのいずれでも対応可能なものとすること。(細部は以下のとおり)

3.1.2.1スマートフォン・タブレット

① OS は、iOS 及び Android に対応し、国内の主要な通信回線で利用できるとともに、国内で一般的に流通している機種で正常に動作すること。

② Web アプリとして提供する場合のブラウザは、Google Chrome、Safari 等、対象 OS の標準ブラウザで利用可能であること。

③ OS 及びブラウザのバージョンは稼働開始時点で過去５年以内に正式リリースされたバージョンにて追加費用なしで稼働を保証できること。なお、運用保守期間内においては、稼働開始後５年間に新たに正式リリースされるバージョンに対しても、追加費用なしで稼働を保証できるように対応を行う想定であること。

④ 受託者においてあらかじめ動作検証を実施し、特定の機種において機能制限等の問題が判明した場合は、速やかに本県へ報告し、対応方針を協議すること。なお、事前検証の対象とする具体的な機種については、本県と協議の上決定する。

⑤ レスポンシブデザインに対応すること。

3.1.2.2パソコン

① OS は、Windows、MacOS 及び ChromeOS で利用可能であること。

② Web アプリとして提供する場合のブラウザは、Edge、Safari 及び Google Chrome で利用可能であること。

③ OS 及びブラウザのバージョンは稼働開始時点で過去５年以内に正式リリースされたバージョンにて追加費用なしで稼働を保証できること。なお、運用保守期間内においては、稼働開始後５年間に新たに正式リリースされたバージョンに対しても、追加費用なしで稼働を保証できるように対応を行う想定であること。

④ 専用ソフトウェアやプラグインのインストール、及び事前の設定作業等を一切必要とせず利用可能であること。

3.1.3サーバ環境

本アプリを管理するサーバ環境を構築すること。クラウド環境を利用する場合は、「別紙２外部サービス要件」に基づく県の審査を受ける必要があるため、本条項及び別紙２の内容を十分に確認し、遵守すること。当該審査にあたっては、受託者はクラウドサービス提供者の資本関係・役員等の情報、クラウドサービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報を書面にて報告すること。

また、利用するクラウドサービス及びサーバを設置するデータセンターについては以下の要件を満たすこと。

・政府情報システムのためのセキュリティ評価制度（ISMAP）クラウドサービスリストに登録されたサービスであること。
・首都直下地震、南海トラフ地震などを想定し、当該被害の影響を受けない遠隔地（「南海トラフ地震防災対策推進地域」に該当しない地域）にメインサーバを設置していること。
・物理的なデータの保管場所が国内であること。
・日本国内法に準拠していること。
・システムを運用するオペレーションが国内で実施されていること。

3.2　使用性・操作性

本アプリの使用性・操作性について、基本的な事項は下記のとおりとする。なお、受託者が実現するアプリにおいて、下記と異なる内容がある場合には、県に申し出て、説明すること。

要素	要件
インターフェース設計	システム全体が、一貫性のある画面構成・画面遷移・入出力操作方法であること。
画面構成・画面設計	アプリの操作にあたり、何をすればよいかが分かるよう、ボタンを集約して配置する等、業務を効率的に行えるように配慮した画面構成・画面遷移・入出力操作方法を工夫すること。
	簡潔で分かりやすさを考慮した画面構成とすること。
	視線移動に配慮したレイアウトを考慮すること。
	入力ミス等入力内容に問題がある項目については、強調表示する等、利用者がその都度該当項目を容易に見つけられるようにすること。
入力負荷の軽減	安否状況や参集可否等の集計対象項目については選択式とし、選択肢が多い場合や使用頻度が高い項目については、入力欄の初期表示、プルダウンメニュー等を活用する等、利用者の操作負担を低減する対応を講じること。ただし、自由記述欄には直接入力も対応可能とすること。
	入力項目の文字属性に応じて、自動的に文字入力モードが切り替わるようにすること。
操作性の向上	事業者内管理者が事業者内従業員アカウント登録時に所属を特定・紐付けできる機能を備える等により利用者負担の軽減を図る機能について工夫すること。その際、事業者内管理者の承認ステップを簡略化する仕組みについても工夫すること。
	アイコン等を適切に使用することで、簡易な操作となるように工夫すること。
	処理の重要度に応じ、適宜メッセージを表示しながら画面遷移するように配慮すること。データ削除等の操作については、必ず確認画面を表示する等、誤操作のないよう考慮すること。
	キーボードや画面タッチ等での項目間移動を実現し、マウスレスで基本的な操作を可能とすること。
	システム内で適切なデータ連携を図り、同一項目を別画面から複数回入力することがないように配慮すること。
エラーの防止と処理	エラー及び警告のメッセージは、システム全体で統一し、容易にエラー内容、解決方法等を利用者が見つけられ、問題を解決できるよう分かりやすく情報提供すること。
	複雑な操作が必要なものについては、ガイダンス機能、操作ミス対策及び

要素	要件
	操作訓練機能を設ける等、操作性の向上を考慮すること。

3.3　性能要件

3.3.1画面遷移

通信環境に問題がない場合の画面遷移はアプリで２秒以内、ブラウザで３秒以内とする。

3.3.2高負荷時の対応

システムは、初期ユーザーを５万人とし、台風接近時や地震発生時などにおいて、同時アクセスによる高負荷が発生した場合も動作が遅くなる等の支障がなく運用できる容量と性能を確保し、オートスケール機能などを可能とすること。

また、将来の利用者の増加を想定した作りとすること。

3.4　保守性要件

受託者が、受託者以外から購入して導入する製品については、稼働開始から５年間は製造元のサポートやセキュリティパッチの適用等の保障が受けられる製品を導入すること。製造元の都合で保障がなされない場合は、県の承諾を得た上で、受託者の責任において必要となる措置を講じること。

3.5　中立性要件

継続的に安定した品質保証を目的に、可能な限り、受託者の技術に依存しないオープンな技術仕様、オープンなインターフェースを利用し、特定の技術や製品に依存しない業界標準又は国際標準に準拠した技術を採用すること。なお、クローズドな技術を採用する場合には、受託者の責任で、継続的に安定した品質保証が可能であることについて、県に申し出て、内容を説明すること。

3.6　上位互換性要件

本調達範囲だけでなく、関連する環境（例：端末等）においてバージョンアップを実施する際に影響範囲を最小化するとともに、影響調査、対応が容易になる仕組みを導入すること。

3.7　セキュリティ

以下のセキュリティ要件について対策を実施すること。

分類	チェック項目	チェックする観点
前提条件・制約条件	セキュリティポリシーの遵守	業務の遂行にあたっては、徳島県情報セキュリティポリシーを遵守すること。
脆弱性対策	開発環境のセキュリティ	開発を行う端末や環境において、マルウェア対策や不正アクセス対策を徹底し、開発環境経由の汚染や情報漏洩を防止すること。
	脆弱性対策の実装	SQL インジェクション､クロスサイトスクリプティング(XSS)、クロスサイトリクエストフォージェリ（CSRF）等の既知の脆弱性に対する対策を実装すること。
	サプライチェーン・セキュリテ	システムに使用する OSS（オープンソースソフトウェア）やライブラリ等は、脆弱性情報やサポート状況を確認し、安全性

分類	チェック項目	チェックする観点
	ィ	が確認されたバージョンを使用すること。
	耐タンパ性対策	アプリの解析や改ざんを防ぐため、難読化ツール等を用いてリバースエンジニアリングを困難にする対策（難読化等）を実装すること。
	セキュリティ診断の実施	本番稼働前に、アプリケーション及びプラットフォームに対するセキュリティ診断（脆弱性診断）を実施し、検出された脆弱性（中リスク以上）については、サービス開始までに修正を行うこと。
アクセス制御	システム認証	利用者認証においては、推測されにくいパスワードポリシーの設定や、総当たり攻撃（ブルートフォースアタック）への対策（アカウントロック機能等）を講じること。
	セッション管理	セッション管理を適切に行い、セッションハイジャックやなりすましを防止するとともに、一定時間操作がない場合のタイムアウト機能を実装すること。
	アクセス権限	利用者ごとの適切なアクセス権限管理を行い、権限のないデータへのアクセスや操作ができない設計とすること。
データの秘匿	通信の暗号化	データ通信を行う際、暗号化通信方式（SSL 通信等）を使用した伝送データの暗号化がなされること。
	蓄積データの暗号化	サーバ上に保存される個人情報及び安否確認データ等の重要情報は、暗号化して保存すること。スマートフォン等のアプリ内（ローカルストレージ等）には、極力、機微な個人情報を保存しない設計とすること。保存が必要な場合は、適切に暗号化を行うこと。
不正追跡・監視	バックアップ制御	OS のバックアップ機能等により、意図せず機密情報が外部に保存されないよう制御すること。
	ログの取得	不正を検知するために、監視のための記録（ログ）の取得に対応していること。
	不正監視対象（装置）	不正行為を検知するために、サーバ、ストレージ等への不正アクセス等を監視すること。

3.8　ライフサイクルコスト

システム運用後のコストを安価にし、かつ機器更新や利用環境変更への対応等、極力追加コストが発生しないシステムとすること。

3.9　省電力化の工夫

災害時の利用を目的とするため、次の事項を考慮した開発とすること。

ア）アプリの起動や動作を軽くする工夫

イ）バッテリー消耗を最小限にする工夫

ダウンロードや通信量をできるだけ削減させ、アプリそのものの処理を工夫し消費電力を最小限に抑えること。

ウ）GPS 機能の位置情報による工夫

アプリを起動していない時は、GPS 機能を最小限に抑えたバックグラウンド機能などを実装すること。

なお、この他に効果的と思われる対策があれば提案し開発に組み込むこと。

4　業務委託要件

4.1　本業務実施体制における要員と役割

本業務実施体制における各要員の役割は下記のとおりとする。

組織	要員	本業務における役割
担当部署	―	本アプリの管理組織として、本業務の進捗等を管理する。
本業務受託者	―	担当部署を通じて、本アプリの設計・開発業務を担う。
	プロジェクト管理者（業務遂行責任者）	・本業務全体を統括し、必要な意思決定を行う。また、各関連する組織・部門とのコミュニケーション窓口を担う。 ・原則として全ての進捗に関連する会議に出席する。
	品質管理者	・成果物（設計書、システム等）に係る品質管理を行う。 ・工程完了判定においては、品質面の責任を負う。
	チームリーダー	本アプリの設計・開発において、作業状況の監視・監督を担うとともに、チーム間の調整を図る。
	業務担当者	本アプリの設計・開発を担う。
	その他要員	本業務受託者は、上記以外に業務遂行上必要となる要員（施行管理者等）がある場合は追加で配置すること。

4.2　業務体制

4.2.1受託者に求める要件（プロジェクト体制）

業務実施にあたり受託者は本業務を確実に履行できるプロジェクト体制を設け、下記の内容を遵守すること。

（ア） SE 等、設計及び製造に携わる者は、日本語での打合せが可能であること。なお、打合せが可能なレベルとは、日常会話だけでなく、システム開発を行う上で必要な会話が可能なレベルとする。

（イ） 本業務を遂行するにあたり、本業務仕様書が示す要件を満たし、一貫性をもって本業務の実施が可能な体制を構築すること。

（ウ） プロジェクト管理者及びチームリーダーについては、プロジェクト期間中は、原則として同一人物が継続して対応すること。

（エ）作業に先立ち、受託者の体制、責任者及び連絡体制、担当者について書面で県に提出すること。なお、プロジェクト発足時からの従事者の変更に当たっては、県に変更後の体制を書面で提出するとともに、変更後の従事者のスキルが前任者と同等以上であることを担保すること。

（オ） 本業務に関わる要員を管理監督する第三者的な立場の要員を、受託者内部で確保し、必要に応じて県とプロジェクト実施について協議すること。

4.2.2担当者に求める要件

本業務の担当者に求める要件は下記のとおりとする。

担当者	要求する能力・経験	要件
プロジェクト管理者（業務遂行責任者）	プロジェクト管理能力	プロジェクト実施計画を策定し、プロジェクト全体を統括・運営管理するとともに、全てにおいて責任を有する者。 ・システムの設計・開発、テスト、システムの評価、

担当者	要求する能力・経験	要件
		プロジェクト間の調整を行い、生産性及び品質の向上に資する管理能力を有すること。
品質管理者	品質管理能力	受託者の品質管理基準に従い、プロジェクトを離れて第三者的かつ客観的に、プロジェクト全般の品質状況を監査し、評価・改善する能力を有すること。
チームリーダー	調整能力	・開発・構築整備及びテストにおいて、県担当部署と調整を行うこと。 ・県との協議において、良好かつ円滑なコミュニケーションを維持できること。
開発・構築整備業務従事者全体	導入サービスに関する専門知識	・導入するソフトウェア（OS、ミドルウェア含む。）に関する専門知識と、本県の要求事項を理解した上で、最適なシステム構成の設計・構築・運用に係る技術及び技術コンサルティング能力を有すること。
	システム導入業務に関する知識	・他自治体事例等を提供し、業務改善及びカスタマイズ抑制、品質向上に資する能力を有すること。
	アプリ開発の実務経験	・スマートフォン向けアプリ開発の実務経験を有すること。なお、担当技術者においては氏名、経歴等を書面により通知し、担当技術者がその職務の執行につき著しく不適当と認められるときは、本県は受託者に対して必要な処置をとるべきことを請求できるものとする。

4.3　作業場所

受託者は、本業務の役務に関する作業場所について、下記に示す要件を遵守すること。

(1) 受託者は、本業務の役務に関する作業場所として、県施設を使用する場合、担当部署と協議の上、担当部署及び各関係機関が指定する必要な手続を実施し、承認を得ること。

(2) 本アプリの開発スペースは、受託者にて準備すること。

5　開発業務実施要件

5.1　プロジェクト管理要件

5.1.1プロジェクト計画書の策定

契約締結後２週間を目途に、本アプリの構築における具体的な体制、作業工程を明確に示すスケジュール、プロジェクト管理方針、プロジェクト管理方法、各プロセスの実施手順等を定義した管理要領を網羅したプロジェクト計画書を作成し、県に提出すること。なお、受託者内部でこれに代わる管理手法や書面がある場合には、県に申し出て、内容を説明すること。プロジェクト計画書について、本業務の途中段階で修正や見直しが必要になった場合には、速やかに再提出し、県の承諾を得ること。

プロジェクト計画書の作成に当たっては、下記の内容に留意すること。

（ア）プロジェクト計画書には、委託業務の内容、実施体制及び役割、委託業務のプロジェクト管理方法（コミュニケーション管理・体制管理・作業管理・品質管理・リスク管理・課題管理・情報セキュリティ管理等）、スケジュール、納入成果物一覧に関する記載を含めること。

（イ）スケジュールの策定については、設計・開発に加え、テスト等、所要の実施期間を十分に考慮すること。
（ウ） 品質管理において本プロジェクトに適用する定量的な品質管理基準を設定すること。
（エ）効率的・効果的な人的計画を行い、万全な体制とすること。
（オ）開発の手戻り等の際に、必要機能の漏れを防ぐための対策を、リスク管理・課題管理の一環として、計画に含めること。

5.1.2プロジェクト管理

受託者は監督職員と協議・調整の上、下記内容に基づき、本アプリ構築業務を管理すること。

なお、新型コロナウィルス等をはじめとする各種感染症拡大時には、作業場所等における感染予防策を講じるとともに、プロジェクト遂行に大きな支障が出ないよう方策を講じること。

管理項目	管理内容
進捗管理	プロジェクト計画書策定時に定義したスケジュールに基づく進捗管理を実施すること。受託者は、実施スケジュールと状況の差を把握し、進捗の自己評価を実施し、定例報告会において進捗状況について本県に報告すること。進捗及び進捗管理に是正の必要がある場合は、その原因及び対応策を明らかにし、速やかに是正すること。なお、受託者内部で確立した進捗管理方法がある場合には、本県に申し出て、内容を説明すること。
品質管理	プロジェクト計画に基づいた品質管理を実施すること。品質基準と状況の差は受託者内部で把握し、結果について定量的・定性的な判断結果を本県に報告すること。品質及び品質管理に是正の必要がある場合は、その原因と対応策を策定し、速やかに本県に報告すること。
課題・リスク管理	リスクや障害が顕在化した場合や協議事項が生じた場合は、課題として管理すること。受託者は、リスクの発生を監視し、リスクが発生した場合には、本県に報告すること。課題への対応策について、本県と協議の上、対応方法を確定し、解決するまで継続的に管理すること。
変更管理	仕様確定後に仕様変更の必要が生じた場合には、受託者は、その影響範囲及び対応に必要な工数等を識別した上で、変更管理ミーティングを開催し、本県と調整の上、対応方針を確定すること。

5.1.1プロジェクト会議

受託者は、定期報告の会議体として、定例報告会、工程完了報告会、作業部会等を設置することとし、必要な報告書類を会議開催までに県に共有すること。各会議終了後、会議内容に係る議事録は書面で会議開催後５開庁日以内に県に提出すること。なお、会議体の実施方法については、Web 会議等を利用する想定であるが、詳細は本県と調整の上、決定すること。

規定以外の会議が必要な場合は、適宜開催すること。

会議体	実施内容
定例報告会	【目的】 プロジェクト計画策定時に定義したプロジェクト管理方法に基づき、プロジェクト管理を実施すること。 【参加者】 県、受託者（プロジェクト管理者、チームリーダー等、その他必要な者）

会議体	実施内容
	【開催サイクル】 少なくとも月１回程度、当月の進捗状況をまとめた定例報告会を開催すること。その他定期的な開催が必要な場合、詳細は県と協議すること。 【報告書類】 進捗状況、品質管理及び課題・リスクに関する報告書等、必要な報告資料
各工程完了会議	【目的】 各工程の終了状況を確認すること。 【参加者】 県、受託者（プロジェクト管理者、チームリーダー等、その他必要な者） 【開催サイクル】 下記の各工程及び主要なマイルストーンの完了時等（定例報告会と同時開催で構わない。） 要件定義・基本設計 テスト システム仮稼働 安定稼働判定 本稼働 【主要報告書類】 各工程の実施結果報告書等
各作業部会	【目的】 各所管課や他受託者（関連システム事業者）との要件・仕様の調整、進捗管理、課題管理等に関する方策・作業内容の検討・調整等を行うこと。 【参加者】 県、受託者（プロジェクト管理者、チームリーダー、業務担当者）、他受託者担当者等 【開催サイクル】 必要に応じて開催することを基本とし、詳細は県と協議すること。 【報告書類】 進捗・課題管理表、変更管理表等、その他必要な報告資料等

5.2　開発・構築整備体制

5.2.1基本的な要件

- ✓ 受託者は、本システム開発に係る各種問題、問合せが生じた場合に対応できる体制を構築すること。
- ✓ 対応窓口は土曜日、日曜日、国民の祝日に関する法律（昭和２３年７月２０日法律第１７８号）に規定する祝日及び１２月２９日から１月３日までを除く平日で、午前８時３０分から午後６時１５分までとする。ただし、緊急時等において、上記以外の時間で利用が必要になった場合は、あらかじめ県の緊急連絡先に連絡の上、必要な支援を的確に行うこと。
- ✓ 受託者は、システム運用試験の際に発生した課題事項について、書面を作成し、管理すること。
- ✓ 受託者は、システム運用試験の際に障害対応等、非定型な業務が発生する際は、都度、県に報告すること。

5.2.2システム環境

システムに必要な環境として、開発環境、保守・検証環境、本番環境等、区分した環境を設定すること。本県が想定する各環境の詳細は下記のとおりとする。なお、受託者が異なる内容で設定することを妨げない。

環境	各環境の詳細
開発環境	開発作業に必要な設備（サーバ、開発用ソフトウェア等）について、受託者の責任の下で準備すること。
保守・検証環境	本番環境に適用する前に動作検証するため、本番環境と論理的に分離された環境を構築すること。
本番環境	本番環境に必要な機器等については、本業務の委託範囲とする。

5.2.3要件定義・基本設計

本仕様書に示す要件及びシステム開発・構築整備に必要な要件を対象に、下記の項目について設計作業を実施し、要件定義・基本設計書にまとめ、本県に提出すること。なお、異なる名称で作成して構わない。

（ア）要求差異確認作業
（イ）システム機能設計（システム内の業務フローを説明する図書を含む）
（ウ）帳票設計
（エ）画面設計（画面遷移図策定作業を含む）
（オ）データ設計（論理データ設計、ファイル定義等を指す）
（カ）システム方式設計（ソフトウェア構成及び機器構成等の技術基盤の設計）
（キ）障害対策設計
（ク）ネットワーク設計（ネットワーク構成図策定作業を含む）
（ケ）情報セキュリティ対策設計

5.3　テスト要件

5.3.1基本事項

受託者は、本アプリの開発・構築整備において、下記の基本事項を遵守すること。

5.3.2テストの実施

受託者がテストを実施するに当たっては、5.3.5 以降に定める各テストについて、テスト環境、作業内容、作業スケジュール、合否判定基準等を記載したテスト計画書を作成し、本県に提出すること。

なお、受託者内部の所定のテストによる場合は、本県に申し出て、内容を説明すること。また、最終結果について本県に報告すること。

ただし、運用テストについては、5.3.7 の規定によること。

5.3.3テスト結果報告書

テスト終了後、テスト結果の実績、障害対応、残課題、品質評価結果及びその後の見通し等について、テスト結果報告書にまとめ、本県に提出すること。修正や追加テスト等が必要な場合には、受託者の責任により実施した上で、当該修正及び追加テストの結果を提出し、

本県に報告すること。

5.3.4テスト時の障害対応

運用テストにおいて発生した障害は、必要に応じて本県に報告した後、復旧作業及び原因の解明、対策を行うこと。また、性能面での問題が発生した場合には、チューニングを施すこと。

5.3.5単体テスト

受託者は、開発した個々のプログラム等について、各機能のモジュール単位又はモジュール単体結合において動作検証を行うこと。なお、受託者内部の基準により代替する場合、受託者は本県に申し出て、内容を説明すること。

5.3.6結合テスト

受託者は、前項のテストにて機能の実装が確認できたプログラム等を相互に結合し、プログラム等間のインターフェースが正しく実装されていることについて、確認するための結合テストを実施すること。

5.3.7総合テスト

5.3.7.1 基本事項

受託者は、本アプリを構成する装置等をそれぞれ適切な場所に据付け・設置し調整を行った後、ソフトウェアを実装した状態で、業務の流れを想定した一連の機能の動作確認、性能評価及び障害時切替の試験を、総合テストとして行うこと。なお、性能評価は、県と事前に合意した内容についてテストを実施すること。

また、総合テストにおいて、運用制限事項が発生する場合には、あらかじめ本県に説明すること。

5.3.7.2 本番環境での実施

総合テストでは、本アプリの各機能が機能要件を満たし、県、各事業者において、業務遂行及びシステム運用が可能であること、適切にセキュリティが確保されていること及び業務ピーク時を想定した状況下での性能要件を満たしていること等を、本番環境（実際の業務環境と同じ状態）で確認すること。

5.3.8運用テスト

5.3.8.1 基本事項

受託者は、県参加職員が操作する運用テストを実施すること。なお、受託者は、県が作成するシナリオに基づき、県と協議の上、運用テスト計画書を作成し、県に提出すること。

運用テストにおいては、実際の運用に合わせたシステム全体の機能及び性能の確認、県職員による操作マニュアルの検証、運用担当者による運用訓練、エンドユーザによる総合的な機能検証を実施すること。

5.3.8.2 テスト結果の取扱い

受託者は、運用テスト終了後、ユーザ検証により抽出された課題及び問題点について問題解決を図り、運用テスト結果報告書に記載し、本県に提出すること。

また、運用テストの結果及び本県の指示を基に操作マニュアルを修正し、本県に提出すること。

5.3.9テストデータ

各テストで使用するテストデータに関しては、受託者が準備すること。なお、実データが必要な場合には、別途県と協議すること。受託者の開発環境内における実データによるテスト実施は認めない。

5.4　操作マニュアルの作成

5.4.1事業者内従事者向けマニュアル

本システムを利用する事業者内従業者による各画面の操作方法・操作手順を示した操作マニュアル及びこれらを分かりやすく解説する動画又は質問ＡＩ等を作成し、本県に提出すること。

本アプリを初めて操作する者に説明を行う場面を想定し、各画面の説明や機能、説明等を実際の操作画面を挿絵として利用するなど、分かりやすいものとすること。

5.4.2管理者向けマニュアル

操作する上で必要となる事項を全て記載したマニュアル及びこれらを分かりやすく解説する動画又は質問ＡＩ等を作成し、本県に提出すること。

マニュアルは管理者が業務の際に利用することを想定し、実際の操作画面を挿絵として利用するなど、専門的な知識が無い人にも分かりやすいものとすること。

5.5　完成検査

(ア) 令和８年度末までに本稼働可能な状態を県が確認する検査であり、原則この検査をもって本業務を完了し、完成とする。

(イ) 本県及び受託者立合いのもと実施する。

(ウ) 受託者は、検査前に完成検査手順書を作成し、本県に提出すること。

(エ) 完成検査手順書には、本仕様書、要件定義・基本設計書等を基に、総合的な動作試験等を含む検査項目、合否判定基準、その他必要な事項を記載するものとする。

(オ) 受託者は、完成検査における本県の指摘事項等を記録して完成検査報告書にまとめ、本県の承認を得て提出すること。

(カ)完成検査において本仕様書及び要件定義・基本設計書等の記載により完成していない場合、受託者は改修を行い、再検査を受けるものとし、改修に要した費用は受託者が負担すること。

6　アプリ展開業務

提案するユーザインターフェースがストア登録必要な場合、App Store 及び Google Play（以下、「配布用ストア」という。）へのアプリケーション登録申請のための手続きを行い、iPhone 版は App Store から、Android 版は Google Play から無料でダウンロードできるアプリケーションとして登録するための申請を行うこと。

受託者は、Apple Developer Program の登録に必要なメンバーシップ登録料を免除とする公的機関申請のための手続きを行うこと。

申請に当たっては、申請者を徳島県として登録すること。

なお、配布用ストアへの公開申請時、Apple 及び Google の審査方針変更等により、申請が却下される場合がある。このとき、本県及び受託者にて公開スケジュール等について協議し、双方合意の上で修正版の公開申請を行うものとする。

7　成果物

7.1　成果物

各開発工程における成果物とその納入時期については、下記のとおりとする。ただし、「納入時期」は目安であり、原則として次工程着手前に現工程の成果物について作成し、県に提出すること。

また、納入後 1 年間は、媒体破損、データ及びプログラム不良による納入物の再作成及び修正を保証できるように、受託者の責任において納入成果物の複製物を保管すること。

工程	作成ドキュメント	内容	納入時期
プロジェクト計画	開発・構築体制図	本業務実施における受託者内部の組織・業務遂行・推進体制を示すもの（4.2.1 参照）	契約締結後 2 週間以内
	技術資格証明書又は工事経歴書等	本業務の担当者に求める要件を証明するもの	
	プロジェクト計画書	5.1.1 記載のとおり	
要件定義・基本設計	要件定義・基本設計書インターフェース仕様書等	5.2.3 記載のとおり	要件定義及び基本設計終了後
テスト（単体、結合、総合）	テスト実施計画書	5.3.2 記載のとおり	総合テスト実施前
	テスト結果報告書	5.3.3 記載のとおり	総合テスト実施後
運用テスト	運用設計書	システム構成図やジョブ運用、バックアップ運用、ログ運用、監視運用（プロセス監視、リソース監視等）、障害時運用等の運用設計をまとめたもの	運用テスト実施前
	運用テスト計画書	5.3.8.1 記載のとおり	
	運用テスト結果報告書	5.3.8.2 記載のとおり	運用テスト実施後
資料作成	操作マニュアル	5.4 記載のとおり（動画又は質問ＡＩ等を含む）	運用テスト実施前・運用テスト実施後
検査	完成検査手順書・報告書	5.5 記載のとおり	完成検査前・完成検査後
アプリ展開	ストア公開証明書	配布用ストアでの公開を証する書類	配布用ストアでの公開後

工程	作成ドキュメント	内容	納入時期
プロジェクト管理	議事録	プロジェクトを管理するための各種書類	各種会議終了後 5 開庁日内
	進捗管理表		定例会時
	課題･障害･リスク等管理表		定例会時
	変更要求管理表		随時
その他	業務完了報告書	業務完了時に提出する書類	本業務完了時
	その他	その他作業上作成した資料等	随時

7.2 納品形態及び部数

書面及び電子でそれぞれ 1 部納入すること。なお、電子データ提出時には、県が指定する納品書を併せて提出するものとする。

また、成果品完成時点で最新のウイルスに対応したウイルス対策ソフトによりチェックを行い、使用したウイルス対策ソフト、チェックを実施した日付を明示した上で納品すること。

7.3 成果品の提出先

徳島県危機管理部防災対策推進課　防災企画担当

住　所：徳島県徳島市万代町 1 丁目 1 番地　徳島県庁 4 階

電　話：088-621-2297

e-mail：bousaitaisakusuishinka@pref.tokushima.lg.jp

8 運用保守

運用保守作業は本調達の対象外だが、以下の運用保守要件を踏まえた運用が可能となる機能を構築すること。

8.1 運用・保守体制

(1) 本アプリの運用時間帯は 24 時間 365 日である。ただし、計画停止による業務停止を許容する。

(2) 本アプリは、10 年程度の利用を予定しており、利用中の運用・保守において発生する障害や問題に対して、責任を持って解決できる体制であること。

(3) 本県職員による問合せ等に対応する窓口を設けること。希望する対応時間及び連絡方法については、次に示す。

・電話での問合せ：開庁日の 8 時 30 分から 18 時 15 分まで

・メールでの問合せ：常時

（また、アプリ利用者からの問合せ窓口を準備できることが望ましい。）

(4) 問合せ対応の時間帯以外においても対応できる障害等緊急時の連絡窓口を設置すること。また、障害等緊急で対応すべき事象が発生した場合に対応が必要となる受託者の技術者やその他関係する事業者等との連絡体制を整備すること。

(5) 本システムに対する障害などの連絡受付時間帯は、24 時間 365 日とする。障害復旧対応に当たっては、ハードウェア障害及びソフトウェア障害のいずれにも対応できる担当者が連絡受付後、下記の時間内に作業を開始するものとする。作業開始時間は、現地到着時間ではな

く、障害に対応するための何らかの作業を開始した時間とする。なお、遠隔地からのリモート操作による障害復旧が可能な場合には、リモート操作の開始時間を作業開始時間とする。

・平常時対応時間帯（開庁日の 8 時 30 分から 18 時 15 分まで）：4 時間

・上記以外の時間帯：8 時間

(6) 運用・保守体制として、通常及び緊急時の連絡先及び連絡方法を提示すること。

8.2 運用保守業務の範囲

現時点において県の想定する運用保守業務は次のとおりである。なお、運用保守の詳細な作業内容は、本アプリ開発の設計にて決定する。

(1) 問合せ対応

・職員からの運用に関する問合せに対して、速やかに回答を行うこと。必要に応じて現地に来庁し、運用支援を行うこと。

・問合せ窓口に寄せられた内容などから、機能改善要求及び追加機能要求を把握すること。

・問合せ対応で把握したニーズは、その対応について検討するとともに、対応を行った場合は定期バージョンアップ等での反映を検討すること。

(2) 稼働環境の監視

・本システムの稼働状況を常時監視し、過去の障害履歴や経験から問題発生の兆候を自動的に事前に検知する監視環境・体制を確立すること。

(3) データバックアップ

・本システムが保有するデータ（アプリケーションプログラム、設定、業務データ等の全て）について、定期的にバックアップの上、適切な保管を行うこと。

(4) システムのバージョンアップ

・本システムの稼働に係るソフトウェアやアプリケーション等について、適宜、バージョンアップを実施し、上位互換が確保された形で常に最新のバージョンを維持すること。バージョンアップは、自動又は手動で対応を実施し、アプリケーションの移行作業が発生することなく最新の稼働環境を維持できること。

(5) セキュリティ対策

・本システムを稼働させているクラウドサービスのセキュリティ対策に準ずること。

(6) 予防保守

・本システムの稼動状況分析を行い、必要に応じて、データベースや業務アプリケーションのチューニング、リソース追加の改善計画を立案し、本県と協議の上、対策を実施すること。

① システムリソース（CPU、メモリ、ディスク等）の使用状況、ネットワークのトラフィック及びオンライン処理時間（レスポンスタイム）を常時モニタリングすること。

② 過去の障害やパフォーマンス劣化の兆候に合致する事象を検知した場合は、本県の承諾を待たずにチューニング等の対応を図ること。なお、対応後は、速やかに県に報告すること。

(7) 障害対応

・障害を受け付けた際には、障害箇所及び原因を調査し、障害の一次切り分けを行い、速やかに本県に連絡すること。

・障害が発生した際には、速やかに県に連絡し、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県に連絡すること。
・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。
・障害内容、原因、復旧対応結果等を記載した書面を作成し、県に提出すること。

(8)クラウドサービス利用料等の負担

・運用保守期間中の発生する本アプリのクラウドサービス利用料（データ通信料等、インフラ環境の維持に必要な費用を含む）及び外部サービス（L アラート等）連携の維持管理は、運用保守業務受託者の負担とすること。

8.3 サービスレベル（SLA）

受託者は、以下の水準（案）を満たすサービスレベル合意（SLA）の締結が可能となるよう、可用性や耐障害性を考慮したシステムの設計・構築を行うこと。なお、具体的な指標及び目標値については、要件定義及び設計工程において本県と協議の上、決定するものとする。

項目	定義	目標値（案）
稼働率	運用保守業務受託者の提供するサービスに起因し、一部又は全体的にサービスの提供が困難な状態の時間を障害時間と定義し、下記の計算式により得られる数値。 （月間稼働率＝月間累計稼働時間÷（月間累計稼働時間＋月間累計障害時間）×100） ただし、事前に告知し県が承認する計画的な停止時間は除く。	99.9%以上
目標復旧時点（RPO）	障害等の発生によりシステムが停止した際、過去のどの時点のデータ状態に復旧させるかを示す指標	障害発生時点の最大１時間前（可能な限りデータ損失がゼロに近づくような構成とすること）
目標復旧時間（RTO）	障害発生からシステム復旧までに要する時間	４時間以内（時間外の場合、８時間以内）を 90%
オンライン対応時間	端末からのリクエストに対するサーバ応答時間	アプリ：２秒以内 ブラウザ：３秒以内
障害対応着手時間	障害検知又は連絡受付後、調査・復旧作業を開始するまでの時間	２時間以内（時間外の場合、３時間以内）を 95%

9 留意事項

業務の施行上の留意事項は次のとおりとする。

9.1 資料等の提供

ア）受託者から本県に対し、本業務遂行に必要な資料等の提供の要請があった場合、本県と受託者が協議の上、本県は受託者に対し、無償でこれらの提供を行う。

イ）受託者は、本県から提供された本業務に関する資料等を善良なる管理者の注意をもって管

理し、保管し、かつ、本業務以外の用途に使用し、又は第三者に提供してはならない。

ウ）受託者は、本契約が満了し、若しくは解除されたとき、又は資料等が本業務遂行上不要となった場合、遅滞なく資料等を本県に返還し、又は本県の指示に従った処置を行うものとする。

9.2　人員配置等

ア）受託者は、本業務に精通した担当者を配置し、受託者の窓口として本県と直接調整を行うこと。

イ）受託者は、本業務の実施にあたり、必ず２名以上の人員体制で臨むこととし、緊急の資料作成等、対応が図れるよう体制を整えるものとする。

ウ）本県は、受託者が配置する担当者に問題等があるときは、担当者の変更を要求できるものとし、受託者はこれに応じるものとする。

9.3　その他の注意事項

ア）本仕様書に記載がない事項にあっても、本システムに必要と認められる事項に関しては、本県と協議の上、行うこと。

イ）法令、条例及び規則等を遵守し、本県が最適な成果を得られるよう本業務の履行を遂行すること。また、必要事項については、積極的に本県に提案すること。

ウ）本業務の履行の際は、上記の指示事項及びその他要件について、本県と十分に協議を行うとともに、本県の指示を受けること。また、作業内容に疑義が生じた場合は、速やかに本県と協議の上、対応すること。

エ）受託者が本業務の履行のために作業する環境は、受託者の負担によることとし、本県では一切提供しない。ただし、本県と受託者との会議、打合せ及び運用テストに係る場所については、本県にて提供する。

オ）受託者は、本業務終了後においても、本業務納入成果物に関する照会に応じること。

カ）納入成果物を含め、全ての図書類、会話・文書・メール等のコミュニケーションは日本語を用いること。

以上

【別紙1】安否確認アプリ機能一覧

NO.	機能分類体系			機能概要
	大項目	中項目	小項目	
1	基本事項	データ登録	—	事業者内管理者が事業者内従業員アカウント登録時に所属を特定・紐付けできる機能を備える等により利用者負担の軽減を図る機能について工夫すること。その際、事業者内管理者の承認ステップを簡略化する仕組みについても工夫すること。
2		データ管理	—	アプリユーザの端末故障時や機種変更時にデータ引継ぎができること。
3		対応言語	—	日本語、英語、中国語（繁体・簡体）、韓国語の各言語で表示できること。（多言語の追加が可能）
4		利用規約等	利用規約への同意	サービスの初回利用時やサービスに重要な変更を行った際には、ユーザに利用規約の内容を提示し、確認（同意）を求めることができること。
5			プライバシーポリシー	プライバシーポリシーを表示すること。
6		訓練機能	—	訓練機能を搭載し、災害時以外にも、ユーザが自身の安否を登録（回答）できること。 災害時は必要な情報を分かりやすく、訓練時と区別ができるように災害時モードで表示すること。
7	事業者内従事者向け機能	アカウント管理	アカウント登録・設定	アカウントやユーザ情報を登録・設定・変更・削除できること。 ユーザアカウントを所属する事業者に紐づけできること。
8			パスワードリセット	ユーザ自身がパスワードを忘れた場合の手続きを行えること。
9		安否情報の登録	—	安否情報（本人、家族）、現在地、出勤可否、交通手段、連絡事項を登録できること。
10			オフライン時への対応	OSの許容する範囲内で、オフライン時でも安否情報を入力できること。
11			再送信	OSの許容する範囲内で、安否情報の送信が完了するまでバックグラウンドで再試行を繰り返すこと。 安否情報の送信に失敗した場合、電波回復時や一定時間経過後に未送信データがある旨のローカル通知を出すこと。
12		プッシュ通知	通知方法	OSの許容する範囲内で、ユーザのスマートフォン、タブレット等がマナーモードであっても、通知音を鳴らすこと。 視認性と誘目性の高いデザインでポップアップ通知されること。
13			位置情報の活用	プッシュ通知先の出し分けは、下記の通りとする。 ・ユーザ属性に対応する地域（所属している事業者の拠点の自治体及びユーザの住所地） ・ユーザ現在地（スマートフォン等のGPS機能を利用） GPS機能はユーザ側でON/OFFを設定できること。
14			自動配信トリガー	安否確認の通知は、ユーザ属性に対応する地域、又はユーザ現在地（GPS機能有効時のみ）のいずれかにおいて、以下の防災情報が発表された場合にプッシュ通知されること。なお、防災情報の取得は、外部基盤（Lアラート等）から自動取得することとする。 ・地震：震度5弱以上 ・津波：津波注意報、津波警報、大津波警報 ・気象警報：氾濫特別警報、大雨特別警報、土砂災害特別警報、大雪特別警報、暴風特別警報、暴風雪特別警報、波浪特別警報、高潮特別警報 なお、安否未回答のユーザには、1時間ごとに繰返しプッシュ通知されること。
15			再送信	OSの許容する範囲内で、端末への到達を確認できるまで再試行を繰り返すこと。

16	管理者向け機能	管理者登録	アカウント登録・設定	管理者アカウントの登録・変更・停止・削除ができること。 管理者ユーザの所属する事業者に紐づく機能のみが利用可能なこと。 ただし、ログインユーザが、県管理者の場合、全事業者に紐づく機能が利用可能なこと。
17			ロール設定	管理アカウントごとのロール設定ができること。
18		ユーザ管理	事業者内従事者アカウント	事業者内従事者のアカウント情報を確認・停止（削除）できること。 CSV形式等により事業者内従事者の一括登録・更新・削除ができること。 事業者の下部組織に事業者内従事者を登録・変更できること。
19			下部組織	事業者の下部組織（拠点、事業所、部署等。3階層程度を想定。）を作成・変更・削除できること。
20		安否情報の確認	—	事業者内従事者が回答した安否情報を確認できること。 安否回答人数を安否種別ごとに表示できること。
21		利用状況把握	—	県及び各事業者がユーザ数、利用状況等の把握・分析が行える環境を提供すること。 ユーザ情報、安否回答内容等のデータをCSV形式等によりダウンロードできること。
22		安否確認の実施	—	管理者ユーザの所属する事業者の従事者に対して、手動で安否確認（実災害・訓練）を実施できること。
23	その他機能	リンク集	—	インフラ、災害用伝言サービス、県ホームページ及びSNS、災害関連リンク等のリンク集を表示できること。 リンク集はアプリをバージョンアップすることなく、運用管理システムで作成、保存、更新を可能とすること。
24		問合せ	Q&A・マニュアル	アプリ操作に関するQ&A集や操作マニュアルを掲載できること。 Q&A集や操作マニュアルはアプリをバージョンアップすることなく、運用管理システムで作成、保存、更新を可能とすること。
25			管理者への問合せ	アプリ管理者（本県担当者・運用保守業者）へ問合せできること。

別紙2 外部サービス要件

クラウドサービスセキュリティ対策確認チェックリスト（構築時）

サービス名		
サービス提供者名		
提案社	職	

1.不正なアクセスを防止するためのアクセス制御

項番	セキュリティ対策	確認内容
1	クラウドサービスを利用する際にクラウドサービス提供者が付与又はクラウドサービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管理方法を確認する。 ※ 特に、以下の項目に留意すること。 ・シングルサインオンを行う場合の連携方式 ・より強力な認証方式の採用（多要素主体認証方式等） ・管理者特権をもつ識別コードの取扱い	【クラウドサービスを利用する際の識別コード】 （クラウドサービス提供者等にクラウドサービスを利用する際の識別コードを確認し、記入する。） 識別コードの生成者　：（生成者を記入する。） 識別コードの保管方法：（保管方法を記入する。） 識別コードの廃棄方法：（廃棄方法を記入する。）
2	クラウドサービスを利用する際に使用するネットワークに対するサービスごとのアクセス制御方法を確認する。 ※ 同一のクラウドサービス提供者が提供するクラウドサービスであっても、そのサービス内容によってはアクセス方法を限定する必要がある。例えば、機密性の高い情報を扱うサービスの場合、インターネットからの直接のアクセスは認めずに県からのアクセスに限定するなどの対策が考えられる。	・管理者機能へのアクセス方法（システム管理者） （クラウドサービス提供者等にシステム管理者のアクセス制御方法を確認し、確認結果を記入する。） ・機密性が高い情報へのアクセス方法（システム運用者） （クラウドサービス提供者等にシステム運用者のアクセス制御方法を確認し、確認結果を記入する。） ・それ以外の情報へのアクセス方法（一般利用者） （クラウドサービス提供者等に一般利用者のアクセス制御方法を確認し、確認結果を記入する。） ・運用・保守機能へのアクセス方法（委託業者） （クラウドサービス提供者等に委託業者のアクセス制御方法を確認し、確認結果を記入する。）
3	クラウドサービスを利用する情報システムの管理者特権を保有するクラウドサービス利用者に対する強固な認証技術の利用方法を確認する。 ※ クラウドサービスを利用する情報システムの管理者特権を保有するクラウドサービス利用者の主体認証情報が漏えいした場合、インターネットから直接管理権限を要する操作が可能となるため、十分に強固な認証技術（例えば、多要素主体認証方式）を利用すること。管理用のインタフェースがインターネットに公開されることを避けることと不正アクセスの検知・防御の観点から踏み台サーバを用意し、操作は踏み台サーバからのアクセスのみに限定するなどの対策も考えられる。なお、踏み台サーバへのアクセスにはSSHと公開鍵認証によるアクセスのみを許可すると良い。	・管理者特権を保有するクラウドサービス利用者の認証方式（多要素主体認証方式） （クラウドサービス提供者等に管理者特権を保有するクラウドサービス利用者の認証方式を確認し、確認結果を記入する。）
4	クラウドサービス提供者が提供する主体認証情報の管理機能が要求事項を満たすことを確認する。 ※ 例えば、パスワード等の主体認証情報に係る規定（パスワード長など）に対し、クラウドサービス提供者が提供する機能等が十分かどうか確認を行うこと。	*（クラウドサービス提供者等に県が指定するパスワードに係る要件を満たさない値が設定できないようになっているか確認し、確認結果を記入する。）*
5	クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御できることを確認する。 ※ クラウドサービス利用者がクラウドサービスにおける情報やクラウドサービスの機能へのアクセスを制限できること及びそのような制限を実現することを確実にする仕組みを整備できることを確認する必要がある。	・システム管理者がアクセスできる情報 （クラウドサービス提供者等にシステム管理者がアクセスできる情報を確認し、確認結果を記入する。） ・システム運用者がアクセスできる情報 （クラウドサービス提供者等にシステム運用者がアクセスできる情報を確認し、確認結果を記入する。） ・一般利用者がアクセスできる情報 （クラウドサービス提供者等に一般利用者がアクセスできる情報を確認し、確認結果を記入する。） ・委託業者がアクセスできる情報 （クラウドサービス提供者等に委託業者がアクセスできる情報を確認し、確認結果を記入する。）
6	クラウドサービス利用者によるクラウドサービスに多大な影響を与える操作の特定と誤操作の抑制 ※ クラウドサービス管理者は、クラウドサービス利用者（システム運用者）に対してクラウドサービスに対するユーティリティプログラムの利用を許可する場合は、そのプログラムの機能を特定し、クラウドサービスの管理策を妨げないようにすること。（ユーティリティプログラムとは、設定の自動化ツールなど実行が容易ではあるがその影響がシステム全体に影響するようなものを指す。）	・ユーティリティプログラム （クラウドサービス提供者等にクラウドサービス利用者に利用許可しているユーティリティプログラムを確認し、確認結果を記入する。） ・ユーティリティプログラムによるクラウドサービスの運用を妨げないようにする方策 （クラウドサービス利用者に利用許可しているユーティリティプログラムがある場合、クラウドサービス提供者等にクラウドサービスの運用を妨げないようにする対策等を確認し、確認結果を記入する。）
7	クラウドサービス上で構成される仮想マシンに対する適切なセキュリティ対策の実施 ※ クラウドサービス上に構成される仮想マシンは、展開直後はセキュリティ設定が何もされていないことがあるにも関わらず、外部のネットワークへ接続が可能となっていることがあるため、サービスを実行するのに必要なポート、プロトコル及びサービスのみを有効にするなどのセキュリティ対策をすぐに行い、マルウェア対策やログ取得などのセキュリティ管理策を実施することが求められる。	（クラウドサービス提供者等に以下の点を確認し、確認結果を記入する。） ・必要なプロトコル、ポートのみ有効になっているか。 ・必要なサービスのみ有効になっているか。 ・ウィルス対策ソフトが導入されており、定期的にパターンファイルの更新、スキャン設定が行われる設定となっているか。また、ウィルスを検知した際にクラウドサービス提供者にメール等で通知される設定となっているか。 ・ログの取得が行われる設定となっているか。
8	インターネット等の外部の通信回線から庁内通信回線を経由せずにクラウドサービス上に構築した情報システムにログインすることの要否の判断と認める場合の適切なセキュリティ対策の実施 ※ 職員については、原則として、庁内通信回線を経由せずにクラウドサービス上の情報システムへのログインは認められない。また、委託業者については、接続元のグローバルIPアドレスを特定する等の強固なアクセスコントロールを行うこと。	クラウドサービスへの接続元ネットワーク及び技術的制限 ・システム管理者 （システム管理者としてクラウドサービスにアクセスする際の接続元ネットワークと技術的制限対策を記入する。） ・システム運用者 （システム運用者としてクラウドサービスにアクセスする際の接続元ネットワークと技術的制限対策を記入する。） ・一般利用者 （一般利用者がクラウドサービスにアクセスする際の接続元ネットワークと技術的制限対策を記入する。） ・委託業者 （委託業者がクラウドサービスにアクセスする際の接続元ネットワークと技術的制限対策を記入する。）

2.取り扱う情報の機密性保護のための暗号化

項番	セキュリティ対策	確認内容
1	クラウドサービス内及び通信経路全般における暗号化を確認する。 ※ 通信経路全般において暗号化されていることを確認すること。特に、クラウドサービスにおいて利用可能な暗号機能にはサーバサイド暗号化とクライアントサイド暗号化があり、両者には鍵管理を含めた暗号機能の実装と運用に関わる責任分界に大きな相違があるため注意が必要である。	・通信経路の暗号化 （クラウドサービス提供者等に通信経路の暗号化方式を確認し、確認結果を記入する。） ・データの暗号化 （クラウドサービス提供者等に当該サービス内のデータの暗号化方式を確認し、確認結果を記入する。）
2	利用する情報システムに係る法令や規則に対する暗号化方式の遵守度合い ※ 適用する暗号による一連の管理策が、関連する協定、法令及び規制を順守していることを確認することが求められる。	*（クラウドサービス提供者等に当該サービスの暗号化方式が関連する協定、法令及び規制を順守しているかを確認し、確認結果を記入する。）*

3.開発時におけるセキュリティ対策

項番	セキュリティ対策	確認内容
1	情報システムの構築においてクラウドサービスを利用する場合のクラウドサービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用 ※ クラウドサービスを利用する場合、クラウドサービス特有の手法等が存在するため、その情報をクラウドサービス提供者に要求し利用することが求められる。	*（情報システム構築業者にクラウドサービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用について確認し、確認結果を記入する。）*
2	情報システムの構築において、クラウドサービス上に他ベンダが提供するソフトウェア（CMS、データベースソフト）等を導入する場合、そのソフトウェアを利用するに当たりライセンス違反とならないか確認する。 ※ クラウドサービス（特にクラウドサービス）において、その仮想基盤は容易にスケールアウト、スケールインが可能であり、CPU数によるライセンス価格が決定するソフトウェアなどの場合、オンプレミスで利用していた場合よりもはるかに高いライセンス費用が必要になる場合があるため、利用するソフトウェアをクラウドサービスにインストールする前に、クラウド固有の使用許諾に関する要求事項を特定しなければならない。	・クラウドサービス上に導入する予定の他ベンダが提供するソフトウェア （情報システム構築業者にクラウドサービス上に導入する予定の他ベンダが提供するソフトウェアを確認し、列挙する。） ・ライセンスの種類及び数量とライセンス違反とならないことの確認 （クラウドサービス上に導入する予定の他ベンダが提供するソフトウェアについて、ライセンスの種類及び数量とクラウドサービス上で運用する上でライセンス違反とならないことを確認したことについて記入する。）

4.設計・設定時の誤りの防止

項番	セキュリティ対策	確認内容
1	クラウドサービス上に情報システムを構築する際のクラウドサービス提供者への設計、構築における知見等の情報の要求とその活用 ※ クラウドサービスにおける情報システムの設計・構築はオンプレミスと同じ手法で十分とは限らない。また、クラウドサービスは提供者によって同様なシステムであってもその設計手法、対策が異なる。よって、クラウドサービスを利用して情報システムを構築する場合、その情報システムのセキュリティの最適化に資する設計、構築に係る情報をクラウドサービス提供者に要求し、不足している知見を補う必要がある。	*（情報システム構築業者にクラウドサービス提供者への設計、構築における知見等の情報の要求等を行っているか確認し、確認結果を記入する。）*
2	クラウドサービス上に情報システムを構築する際の設定の誤りを見いだすための対策 ※ クラウドサービスにおいて、クラウドサービスの構成要素（リソース）の設定変更はオンプレミスにおける物理機器に対する変更と比べはるかに容易である。また、設定する内容はオンプレミスと似たものが多いが、クラウドサービス特有の対応（ネットワーク全般における設定等）が必要な場合もある。誤った設定や設定漏れに起因するインシデントを減らすために、例えば次のような対策を行うこと。 ・設定内容のレビュー ・クラウドサービス提供者が提供するセキュリティ設定・監視ツールの利用 ・設定権限を与えるクラウドサービス利用者の限定 ・責任共有モデルにおけるクラウドサービス利用者側の責任範囲の明確化 ・開発プロセスへのセキュリティ対策の組み込み	*（情報システム構築業者に左記対策を講じているか確認し、確認結果を記入する。）*
3	クラウドサービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視 ※ クラウドサービス上のネットワークは、セキュリティ要件が異なるネットワークどうしの接続が存在するため、これらの間の通信（トラフィック）を監視・制御することは重要であり、通常はこの位置にファイアウォールを構成し、トラフィックの制御を実施する。クラウドサービスによっては、ファイアウォールを細かく設置できるものもあるため、設計時にその設置箇所等を十分に検討して決める必要がある。また、これらの間の通信を監視して異常の検知を行うとともに、設定は定期的な見直しを行うことが推奨される。	*（情報システム構築業者（又はクラウドサービス提供業者）に、ネットワーク間の通信の監視方法について確認し、確認結果を記入する。）*
4	利用するクラウドサービス上の情報システムが利用するデータ容量や稼働性能についての監視と将来の予測 ※ クラウドサービスはオンプレミス環境と異なり、要求するデータ容量や性能等のリソースに増減が発生した場合、スケールアウト、スケールイン等によりリソースを柔軟に増減させることが可能なだけでなく、利用実績に応じて自動的にリソースを増減させるサービスも存在するため、リソース不足によるサービス停止とならないよう適切に監視を行う必要がある。また、監視のほかにリソースの現在の利用状況や将来の利用予測を行い設計当初の要求と比較することも重要である。クラウドサービス提供者側で監視のためのサービスが用意されていない場合は、手動で定期的に確認する等の対策が求められる。	*（情報システム構築業者（又はクラウドサービス提供業者）に、リソース不足によりサービス停止とならないための対策について確認し、確認結果を記入する。）*
5	利用するクラウドサービス上で可用性2の情報を取り扱う場合の可用性を考慮した設計 ※ クラウドサービスを利用して可用性2の情報を取り扱う場合は、構築時に可用性を考慮して設計を行う必要がある。可用性の設計には、システムの地理的・電源的な独立性を踏まえた冗長化などのオンプレミスで行う対策と同じものも含まれるが、クラウドサービス特有の機能もあるためクラウドサービス提供者に当該サービスの可用性に係る機能等の詳細な情報を要求し、設計に反映させることが求められる。利用するクラウドサービス全体の利用停止に至る障害に対しては、マルチクラウドやオンプレミスを含む代替サービスによる冗長化も検討する必要がある。	*（情報システム構築業者（又はクラウドサービス提供業者）に、可用性確保のための対策について確認し、確認結果を記入する。）*
6	クラウドサービス内における時刻同期の方法の確認 ※ クラウドサービス内において時刻が同期していないと記録されたログ等の時刻の信頼性が下がり、インシデント発生時の原因解析等に影響を及ぼすため、構築時に当該クラウドサービスにおける時刻同期の方法を確認し、確実に時刻が同期するように設計する必要がある。	*（情報システム構築業者（又はクラウドサービス提供業者）に、時刻同期方法について確認し、確認結果を記入する。）*

別紙2 外部サービス要件

クラウドサービスセキュリティ対策確認チェックリスト（運用中）

サービス名		
サービス提供者名		
提案社	職	

1.クラウドサービス利用方針の規定

項番	セキュリティ対策	
1	責任分界点を意識したクラウドサービスの利用 ※ クラウドサービス提供者との間で協力して情報システム全体の責任を担うことを認識する必要がある。また、その分界点は契約するサービスによって変わるため、契約時に交わされた合意内容を把握する必要がある。これら責任分界点を踏まえた上で運用時における規定や手順等を作成することが求められる。	*（情報システム、サービスごとに担当業者と責任範囲を記入すること。）*
2	利用承認を受けていないクラウドサービスの利用禁止 ※ 利用承認を得ずに職員等がクラウドサービスを利用することは「シャドーIT」と呼ばれるが、シャドーITは監視が不十分になりやすく、セキュリティリスクが高まる等の問題がある。	*（利用しているクラウドサービスを洗い出し、すべての外部システムについて、統括情報セキュリティ管理者から承認を得ていることを確認し、確認結果を記入すること。）*
3	クラウドサービス提供者に対する定期的なサービスの提供状態の確認 ※ クラウドサービスは、クラウドサービス提供者の都合によりそのサービス内容は容易に変更されてしまうため、クラウドサービス利用の当初に想定したセキュリティ対策が利用期間中に正しく機能しなくなることが想定される。クラウドサービスについては、例えば次のような項目や契約時に同意した項目について、定期的にクラウドサービス提供者に確認することが求められる。 ・情報の保存方法、保存場所、伝送経路 ・情報の廃棄 ・ログ情報の収集と保存状況 ・時刻同期の状況 ・バックアップの実施 ・不正アクセスの監視	*（左記確認結果を記入すること。）*
4	利用するクラウドサービスに係る情報セキュリティインシデント発生時の連絡体制 ※ 利用するクラウドサービスにおいて情報セキュリティインシデントの発生を検知した場合に、連絡する体制をあらかじめ規定しておく必要がある。また、連絡先にはクラウドサービス提供者も含むように規定すること。	*（連絡体制が整備されており、内容が最新かどうか確認し、確認結果を記入すること。）*

2.クラウドサービス利用に必要な教育

項番	セキュリティ対策	確認内容
1	※ クラウドサービスの利用はオンプレミスの情報システムと異なり、クラウドサービスごとに知識が必要となる。多くのクラウドサービス利用者は初めて当該サービスを利用することが多く、そのクラウドサービス特有の知識や経験を習得するのに時間を要する。また、クラウドサービスの多くがオンプレミスの情報システムと比較して開発頻度が高く、同一のサービスでも数か月でその仕様が変わるものも少なくない。このような状況に対応するには機関等内での教育だけでは不足することが予想されるため、積極的にクラウドサービス提供者が提供するトレーニングへの参加等を支援し、クラウドサービス利用者の当該クラウドサービスに対する理解を深めることも必要である。 ・クラウドサービス利用のための規定及び手順 ・クラウドサービス利用に係る情報セキュリティリスクとリスク対応	*（クラウドサービス利用に係る教育・研修内容（実施日、対象者、研修内容、スケジュール等）を記入すること。）*

3.取り扱う資産の管理

項番	セキュリティ対策	確認内容
1	クラウドサービス上で利用するIT資産の適切な管理 ※ クラウドサービス利用において、そのサービス内容の設定等を容易に変更できるため、手動でIT資産を管理することは困難である。また、クラウドサービスによっては利用状況により提供するCPUやバックアップストレージ等のリソースを自動的に拡張するなどの機能を有しているため、オンプレミスで利用していたソフトウェアを導入する際にはライセンスの注意も必要となる。オンプレミスにおいてもIT資産管理ソフトウェアの利用が推奨されるが、多くのクラウドサービス提供者はサービスの利用料を従量課金としており、その対象となるリソースの管理ツールが用意されていることがほとんどであるため、その管理ツールを利用し適切に管理することが求められる。	*（リソース管理を行う者に対して、クラウドサービスを利用する上で必要十分なリソースが用意されているか、ライセンス違反は発生していないか確認し、確認結果を記入すること。）*
2	クラウドサービス上に保存する情報に対する適切な格付・取扱制限の明示 ※ クラウドサービスを利用する職員等は、クラウドサービス上で取り扱う情報について格付が分かるように保存する必要がある。クラウドサービス提供者により格付操作を支援する機能が提供されている場合は、それを利用することが推奨される。	*（クラウドサービス利用開始時に想定していた情報以外が、当該サービスで取扱われていないことを確認し、確認結果を記入すること。）*

3	クラウドサービスの機能に対する脆弱性対策について、クラウドサービス利用者の責任範囲の明確化と対策の実施 ※ 例えば、仮想化技術を用いたマルチテナントの環境において、OS等の脆弱性に加えてハイパーバイザーを経由して他の利用者が享受するサービスを阻害する脆弱性はクラウドサービスに対するリスクであり、対策を講ずる必要がある。責任分界点がクラウドサービス提供者側の実施する範囲にある場合はクラウドサービス提供者に対策の実施を求め、結果の報告を要求する必要がある。	*（クラウドサービスを運用しているOS、ミドルウェア、情報機器のセキュリティ対策が適切に実施されているか確認し、確認結果を記入すること。）*

4.不正アクセスを防止するためのアクセス制御

項番	セキュリティ対策	確認内容
1	管理者権限をクラウドサービス利用者へ割り当てる場合のアクセス管理と操作の確実な記録 ※ クラウドサービスにはインターネット等から操作するための管理コンソールが用意されている場合が多いが、この管理コンソールに全体の管理者権限を有する利用者の識別コードでログインすると利用中の情報システムをすべて削除できるなど重大な影響を及ぼすため、当該識別コードのアクセス管理は非常に重要となる。対策としては、通常の管理業務は役割を細かく分割し、役割ごとに管理者を設定することなどが考えられる。（全体の管理者権限を持つ利用者の識別コードは通常の運用では利用しない）。また、管理者権限を有する識別コードの運用を支援する管理製品の利用も検討すると良い。 ※ また、クラウドサービスに対する管理者権限を持つ者の操作等について、すべて記録され保存されることを確認することが求められ、また、異動等により管理者権限を持つ者が交代する場合などは権限設定の変更が遅れることのないように注意することが求められる。 ※ クラウドサービスを利用し、情報システムが構築されている場合に限る。	*（管理コンソールが用意されている場合、委託者に管理コンソールの機能と管理業務ごとに利用するアカウントが分割されており、操作記録が残されているかを確認し、確認結果を記入すること。）*
2	クラウドサービス利用者に割り当てたアクセス権限に対する定期的な見直し ※ クラウドサービス利用者に割り当てたクラウドサービスへのアクセス権限について、定期的に見直すことが推奨される。見直す対象としては、クラウドサービス利用の目的及び必要性、対象者の妥当性、対象期間、権限の範囲等が挙げられる。	*（クラウドサービスに登録されているすべてのアカウントについて、現在利用されていないアカウントがないか確認し、確認結果を記入すること。）*
3	クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の機能の確認と利用者の制限 ※ クラウドサービスのリソース（ネットワーク、仮想マシン等）の設定を変更するユーティリティプログラムを使用する場合は、その機能の確認と利用者を制限する必要がある。 ※ クラウドサービスを利用し、情報システムが構築されている場合に限る。	*（ユーティリティプログラムが用意されている場合、委託者に当該プログラムの機能と利用者を確認し、確認結果を記入すること。）*
4	利用するクラウドサービスの不正利用の監視 ※ クラウドサービスへの不正利用を検知することが可能な監視機能をクラウドサービス提供者に要求し、監視を行うことが求められる。クラウドサービスの利用者の識別コードを含むクラウドサービス内に保持されるクラウドサービス利用者の情報に対して、クラウドサービス提供者がアクセスするものについてはあらかじめ両者で確認し、サービス利用開始後に当該情報へのアクセス履歴をクラウドサービス利用者が常に監視・確認できることが求められる。	*（委託者及びクラウドサービス提供者がアクセスできるクラウドサービス内の情報とクラウドサービス利用者以外が当該情報にアクセスした際のアクセス履歴を確認し、確認結果を記入すること。）*

5.取り扱う情報の機密性保護のための暗号化

項番	セキュリティ対策	確認内容
1	※ クラウドサービスにおいて機密性を保護するためには情報の流通経路全般において対策が必要となるが、クラウドサービスの個々の構成要素において対策を採ることは容易ではないため、暗号化機能を利用して対応することが推奨される。特に、鍵の管理をクラウドサービス提供者が行う場合は注意が必要である。基本的に鍵の管理はクラウドサービス利用者側で行う必要があるが、鍵の管理をクラウドサービス提供者が提供するサービスを利用せざるを得ない場合は、詳細な情報をクラウドサービス提供者に要求し、リスク評価を行った上で使用する必要がある。 ・暗号化に用いる鍵の管理者と鍵の保管場所 ・鍵管理機能をクラウドサービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価 ・鍵管理機能をクラウドサービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価	*・サーバ証明書発行機関* *（サーバ証明書を利用したSSL暗号通信を行っている場合、委託業者等に確認し、サーバ証明書発行機関を記入すること。）* *・暗号化に用いる鍵の管理者と鍵の保管場所* *・鍵管理機能をクラウドサービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価* *・鍵管理機能をクラウドサービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価* *（委託業者又はクラウドサービス提供業者自らがサーバ証明書の発行を行っている場合は、上記内容を確認し、確認結果を記入すること。）*

6.クラウドサービス内の通信の制御

項番	セキュリティ対策	確認内容
1	利用するクラウドサービスのネットワーク基盤が他のネットワークと分離されていることの確認 ※ クラウドサービス基盤内における自身の利用するネットワークが他のテナント及びクラウドサービス提供者が利用するネットワークと分離され、論理的に独立していることを確認することが求められる。	・クラウドサービスのネットワークの共用状況 （他のテナント及び委託者等が利用する保守用ネットワークと分離されているかどうか確認し、確認結果を記入すること。） ・分離方法 （論理的に分離 or 物理的に分離）

7.設計・設定時の誤りの防止

項番	セキュリティ対策	確認内容
1	クラウドサービスの設定を変更する場合の設定の誤りを防止するための対策 ※ クラウドサービスの設定を変更する場合の設定誤りはサービス自体の停止などの広範囲な障害につながる可能性があり、それを避けるための対策は重要である。設定の誤りや設定漏れを防止するため、例えば次のような対策を行うこと。 ・定期的な設定の確認 ・クラウドサービス提供者が提供するセキュリティ設定・監視ツールの利用 ・設定権限を与えるクラウドサービス利用者の限定 ・責任共有モデルにおけるクラウドサービス利用者側の責任範囲の明確化 ・開発プロセスへのセキュリティ対策の組み込み ・クラウドサービスの機能追加に係る設定の見直し	・クラウドサービスの設定項目及び設定者 （設定者ごとに設定項目を列挙すること。） ・左記セキュリティ対策 （設定者ごとに実施している左記セキュリティ対策（該当するものに限る。）を記入すること。）
2	クラウドサービス利用者が行う可能性のある重要操作の手順書の作成と監督者の指導の下での実施 ※ クラウドサービス利用者の操作により利用中のクラウドサービスに重大な障害をもたらすことが予想される操作については、その操作手順を文書化し、実施の際はクラウドサービス管理者が指名した監督者の監視の下、実施することが求められる。	・重要操作の手順書の有無 *（手順書名を記入すること。）* ・管理者の指導の下で実施するなどの誤りを防止する対策 *（誤り防止対策を記入すること。）*

8.クラウドサービスを利用した情報システムの事業継続

項番	セキュリティ対策	確認内容
1	不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施（クラウドサービス提供者が提供する機能を利用する場合は、その実施の確認） ※ クラウドサービス提供者が提供するバックアップ機能を利用する場合、クラウドサービス提供者にその仕様を要求し要求事項を満たすことを確認する必要がある。また、取得したバックアップが有効であることを定期的に確認することも求められる。	・バックアップ実施者 ・バックアップ頻度 ・バックアップファイルの世代数 ・バックアップ保管場所 ・バックアップされていることの定期的な確認方法（誰が、どのように）
2	可用性2の情報をクラウドサービスで取り扱う場合の十分な可用性の担保、復旧に係る手順の策定と定期的な訓練の実施 ※ クラウドサービスを利用して可用性2の情報を取り扱う場合、十分な可用性を担保するために当該情報システムに係る情報のバックアップからの復旧手順を文書化し、定期的に訓練を実施することが求められる。また、遠隔地クラスタなどの冗長化構成を採用した場合もフェールオーバー及びフェールバックの検証を定期的に行う必要がある。	・クラウドサービス復旧に係る手順書の有無 （クラウドサービス復旧に係る手順書の有無を記入する。） ・定期的な訓練 （訓練の実施状況を記入する。）
3	クラウドサービス提供者からの変更通知の内容確認と復旧手順の確認 ※ クラウドサービス提供者によるサービス内容の変更が行われる際の事前通知を受けた場合、その影響範囲・影響度を確認し、サービス停止等が発生した場合の復旧手順を確認することが求められる。	・クラウドサービスの変更等の有無 （当該期間内にクラウドサービスの変更等が発生したかどうかを記入する。） ・クラウドサービスの変更等の内容 （変更等が生じた場合、その変更等の内容を記入する。） ・影響範囲・影響度及び復旧手順の確認有無 （変更等の前に、事前に実施した対策を記入する。）
4	クラウドサービスで利用しているデータ容量、性能等の監視 ※ クラウドサービス管理者は、利用するクラウドサービスで使用済みのデータ容量やサービスの性能について監視を行い、想定された容量・性能内で運用可能であることを確認する必要がある。想定を超える利用が予想される場合は、対策を検討することが求められる。	・確認内容 *（CPU、メモリ、HDD、ネットワーク帯域等の利用状況、今後1年間の利用に対して運用可能かどうかを確認し、確認内容を記入すること。）*

別紙2 外部サービス要件

クラウドサービスセキュリティ対策確認チェックリスト（終了時）

サービス名		
サービス提供者名		
提案社	職	

1.クラウドサービスの利用終了時における対策

項番	セキュリティ対策	確認内容
1	クラウドサービスの利用を終了する際に移行・終了計画書を作成し、統括情報セキュリティ管理者の承認を得る。 ※ クラウドサービスの利用終了において、クラウドサービス利用者への影響を考慮して移行計画書又は終了計画書を作成し、統括情報セキュリティ管理者に承認を得た上でクラウドサービス利用者に提示することが求められる。いずれの計画書にも以下を例とする内容が記載されていることが求められる。 ・当該クラウドサービス名 ・サービスの利用終了日時 ・情報の廃棄日時 ＜以下は、他のクラウドサービスへの移行を行う場合＞ ・移行先のクラウドサービス名 ・移行手順	*（クラウドサービスの利用を終了する場合の移行・終了計画書の作成及び承認までの過程を記入すること。）*
2	移行計画書又は終了計画書のクラウドサービス利用者への事前通知 ※ 作成した移行計画書又は終了計画書を当該サービス利用者に対して十分な余裕をもって通知することが求められる。	*（関係者ごとに、通知日及び合意日を記入すること。）*

2.クラウドサービスで取り扱った情報の返却・廃棄

項番	セキュリティ対策	確認内容
1	情報の廃棄/返却方法 必要に応じたデータの返却 ※ クラウドサービスの利用終了時に、取り扱った全ての情報が、クラウドサービス基盤上から確実に削除されていることを確認する必要があり、クラウドサービス提供者に対し、契約時に同意した情報の廃棄手順に基づく廃棄実施報告書を提出させ確認を行うこと。また、対象はバックアップ等により複製された物にも及ぶ点に注意が必要である。資産管理ツール等に記録された情報等を使用し、サービス終了時から時期を逸せずに廃棄/返却を漏れなく完了しなければならない。暗号化された情報の廃棄/返却は、復号に用いる鍵に対してそのバックアップを含め確実な廃棄/返却が求められる。なお、クラウドサービス利用終了時に廃棄/返却すべき情報は、例えば次のようなものがある。 ・仮想リソース（仮想マシン、仮想ストレージ、仮想ネットワーク機器など） ・ファイル（ストレージサービスに格納したファイル、各サービスのログ、開発関連ファイル、設定ファイルなど） ・暗号化された情報の復号に用いる鍵 ・ドメイン情報	・廃棄/返却者 *（廃棄を行った者を記入すること。）* ・廃棄/返却日 （廃棄を行った日を記入すること。） ・廃棄/返却方法 *（廃棄方法を記入すること。）* ・廃棄/返却したことの確認手段 *（廃棄した証拠書類を記入すること。）* ・廃棄/返却した情報 *（廃棄した情報を列挙すること。）*
2	基盤となる物理機器の廃棄 ※ クラウドサービス提供者が行う、クラウドサービスの基盤となる装置等のセキュリティを保った処分又は再利用のための方針・手順の確実な実施について確認する必要がある。	*（情報機器の廃棄又は再利用を伴う場合は、廃棄・消去の方針・手順等によりデータの復元が不可能であることを確認し、確認結果を記入すること。）*

3.クラウドサービスの利用のために作成したアカウントの廃棄

項番	セキュリティ対策	確認内容
1	作成されたクラウドサービス利用者アカウントの削除 ※ クラウドサービス利用終了時に作成されたクラウドサービス利用者アカウントを全て削除すること。	*（クラウドサービス利用者アカウントの削除日、作業者、作業内容等を記入すること。）*
2	利用したクラウドサービス管理者アカウントの削除・返却と再利用の確認 ※ 作成したクラウドサービス利用者アカウントが全て削除されていることを確認した上で可能であればクラウドサービス管理者アカウントを削除し、クラウドサービス提供者に返却すること。また、クラウドサービス管理者アカウントについては再利用されないことをクラウドサービス提供者に確認すること。	*（クラウドサービス管理者アカウントの削除日、作業者、作業内容等を記入すること。）*
3	クラウドサービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄 ※ クラウドサービス利用者アカウント以外の特殊なアカウント（ストレージアカウントなど）を作成した場合は、サービス利用終了時に確実に削除すること。また、当該アカウントを利用して作成された情報についても廃棄されていることを確認すること。	*（特殊なアカウントがある場合は、削除日、作業者、削除したアカウント情報、作業内容等を記入すること。）*