事業者名：

回答選択　○　標準機能
△　カスタマイズ
×　対応不可

仕様書要件確認表（業務内容の的確性）

前提条件

No	評価項目	回答	備考
1	アプリケーションサービス、また同サービスが稼働する仮想化サーバ及びデータベース等は、本書の非機能要件が示す第三者認証を取得したSaaS又はIaaSで保守・管理すること。		
2	アプリケーションサービスは、APIを有し、APIを介して本市が本事業に先行して構築したデータ連携基盤と相互接続すること。		
3	大規模災害(日向灘地震等)発生時、データ連携基盤との情報連携が実施できない場合をセキュリティリスクとして考慮し、レジリエンス設計を具備すること。		
4	データ連携基盤と連携し、情報資産の相互接続を実現するAPIが設計・実装されること。		
5	APIは、基本的にREST形式、メッセージはJSON形式とすること。		
6	アプリケーションサービスは、アクセスする全ての利用者をマイナンバーの信頼で支える認証により本人認証すること。		
7	利用者のＩＤとしては、利用者が保有するマイナンバーのほかに利用者が保有するスマートフォン等汎用端末に対応すること。		
8	マイナンバーの信頼で支える認証により本人認証された医療関係者が市役所職員の代理として医療機関に不足する物資を発注することを可能とする拡張性を担保すること。		
9	外部システムが保有する非パーソナルデータに属性分類される情報資産が別途事業において構築されるデータ連携基盤とのAPI経由で提供され、利用できること。		
10	非パーソナルデータを有する外部システムとデータ連携基盤間、データ連携基盤と本事業で構築するアプリケーション間のAPIは、当該外部システムとデータ連携基盤の連携に基づき提供されること。		

※機能向上に関する提案がある場合、項目を明らかにして記入ください。

事業者名：

回答選択　○　標準機能
　　△　カスタマイズ
　　×　対応不可

仕様書要件確認表（システムの要件）
機能に関する要件

	評価項目（災害時物資支援統合情報サービス領域）	回答	備考
1	避難所情報・物資支援情報を一元管理し、民間含めた災害支援者で情報共有できること。		
2	災害時運営を支援・マイナンバーをトラストアンカーとしたデジタルIDを活用し、民間含めた許可を得た災害支援者が、本人確認済で取引真正性確保のもと、自治体と共に支援業務を実施できること。		
3	避難者数に応じた必要物資品目・数量を把握できること。		
4	備蓄在庫/流通在庫から物資提供するため、民間事業者と情報連携・協業・指示を一元化できること。		
5	物資不足分を避難所からの要求により民間事業者に発注できること。		
6	物資提供状況を見える化し避難所運営者・避難者に情報提供できること。		
7	民間企業と協業した通常時の業務に準じた強力な物資提供力を活用できること。		
8	市職員だけだはなく、地区管理者／協定事業者など民間資源を活用し、同一情報を活用した物資支援の実施できること。		
9	支援物資情報(品目・数量・場所など)／避難所情報(開設／混雑等情報、住民属性ごとの避難者数など)を一元管理できること。		
10	避難所から物資要求を発信、民間物資支援企業への発注処理～納品までは、民間企業の日常使いの仕組みによって実現すること。		
11	収集した物資提供に関わるデータは、避難所で参照可能とし、必要に応じて市民に公開できる形態とすること。		
12	避難所支援者に対する情報提供手段である「災害支援アプリ」との情報連携を行うこと。		
13	本市の災害対策を担う利用者が本事業が構築するデジタルＩＤ認証が付与するアクセス権に基づき、同じ情報を参照することができること。意思決定・指示・指示結果の共有を行うことができること。		
14	指示実施時の本人確認済/取引真正性を本事業が構築するデジタルIDにて担保すること。		
15	マイナンバーをトラストアンカーとしたスマートデバイス上のデジタルIDを使用し、デジタル・コックピットへのログイン、アクセス管理ができること。		
16	重要処理(物資在庫更新、物資発注依頼、物資配送予定など)の取引証明での活用を実現すること。		
17	「防災のべおか」アプリへの情報提供を目的としたURLリンクを設計・運用すること。		

※機能向上に関する提案がある場合、項目を明らかにして記入ください。

	評価項目（地域防災情報サービス領域）	回答	備考
18	災害発生情報や災害時支援情報などの収集・共有すること。		
19	データ一括表示を支援者に提供し、支援実施時の各種判断の効率化／適正化につなげること。		
20	通常時は、道路情報、河川情報や防災情報や気象情報などを主に地域に関するデータをデータ連携基盤経由で取得し提供すること。		
21	発災時は、避難所開設・物資提供情報などの情報や外部提供の河川氾濫/道路不通などの災害情報を、デジタル地図上に統合表示すること。		
22	収集してきた各種情報は、市が所有するＧＩＳクラウド上に表示できるようにすること。		
23	災害支援者・市職員は、デジタル地図を参照可能とすること。地図上のアイコンをクリックすることで、避難所状況や物資支援情報など、災害時物資支援統合情報サービスの情報にアクセスすることができること。		
24	災害支援者・市職員は、ハザードマップ／避難所情報／物資情報などの災害支援情報なども合わせてデジタル地図上で視覚的に把握できること。		
25	通常時は災害時の行動検討のための情報として活用でき市民の防災意識向上に寄与し、災害時は道路不通など災害状況に合わせた迅速な行動を判断できること。		
26	市職員および支援者が、地域の災害情報を踏まえた、適切かつ迅速な物資支援計画の策定に活用できること。		
27	物資支援者の地域物流事業者は、デジタル地図上に統合表示された河川氾濫や土砂災害等で発生した道路不通情報などを確認した上で避難所への適切な避難物資配送シナリオの作成が可能となること。		
28	災害対策本部には、他サービスからの情報と合わせて、情報の一元管理と判断／指示を実施することができるデジタル・コックピットが構築されること。		
29	デジタル地図上に表示された避難所アイコンの色などから避難所の状況（開設/混雑、物資提供、要請有無など）を把握でき、迅速な対応に繋げること、道路情報なども重ねて判断することで、孤立させない避難所／避難者支援、優先度を間違えない支援に貢献できること。		

※機能向上に関する提案がある場合、項目を明らかにして記入ください。

事業者名：

回答選択肢　○　標準機能
△　カスタマイズ
×　対応不可

仕様書要件確認表（システムの要件）

非機能機能に関する要件

非機能要件については、独立行政法人情報処理推進機構が作成した「非機能要求グレード」を地方公共団体情報システム機構が地方公共団体向けに一部変更したものを基に、本市が一部変更したものである。機能選定やシステム構成の設計等を実施するにあたり、遵守すること。

No	項目	メトリクス(指標/要素)	要件	回答	LV記入	備考
1	継続性	稼働率	レベル２(年間のシステム稼働率は、99%とすること)			
2		RPO(目標復旧地点) (業務停止時)	レベル1(業務停止を伴う障害が発生した際には、5営業日前の時点（週次バックアップからの復旧)			
3		RTO(目標復旧時間) (業務停止時)	レベル1(業務停止を伴う障害が発生した際には、1営業日以内でのシステム復旧を目標とすること)			
4		RLO(目標復旧レベル) (業務停止時)	レベル1(業務停止を伴う障害が発生した際には、一部システム機能の復旧を目標とすること)			
5		システム再開目標 (大規模災害時)	レベル5(1日以内に再開することを目標とすること)			
6	耐障害性	冗長性(サーバ機器)	レベル＊			事業者による提案事項とすること
7		冗長化(ストレージ機器)	レベル＊			事業者による提案事項とすること
8		冗長化(ストレージのディスク)	レベル＊			事業者による提案事項とすること
9	災害対策	復旧方式	レベル１(限定された構成で情報システムを再構築すること)			
10		保管場所分散度 (外部保管データ)	レベル＊(地震、水害、テロ、火災などの大規模災害時の業務継続性を担保するためのデータ保管先は、事業者の提案事項とすること)			事業者による提案事項とすること
11		保管方法 (外部保管データ)	レベル＊(地震、水害、テロ、火災などの大規模災害発生により被災した場合に備えたデータ保管方法は、事業者の提案事項とすること)			事業者による提案事項とすること
12	業務処理量	ユーザ数(利用者数)	レベル０(特定ユーザーのみとすること)			
13		ユーザ数増大率	レベル3(2倍でサービス開始時より増えることはない)			
14		同時アクセス数	レベル１(特定利用者の限られたアクセスのみとすること)			
15		同時アクセス数増大率	レベル3(2倍でサービス開始時より増えることはない)			
16		データ量(項目・件数)	レベル１(主要なデータ量のみが明確である)			
17		データ量増大率	レベル3(増大率2倍とすること)			
18		オンラインリクエスト件数及び増大	レベル＊(同時アクセス数に平均通信間隔を乗じた数値。事業者の提案事項とすること)			事業者による提案事項とすること
19		バッジ処理件数	レベル＊(本サービスでバッジ処理を行う場合は、その処理件数増大率は、本仕様書掲載の情報に基づき、事業者の提案事項とすること)			事業者による提案事項とすること
20		保管期間(データ)	レベル１(１年とすること)			
21	性能目標値	通常時オンラインレスポンスタイム	レベル０(オンラインレスポンスタイムは、10秒以内とすること)			
22		アクセス集中時のオンラインレスポンスタイム	レベル＊			事業者による提案事項とすること
23		通常時バッジレスポンス遵守度合い	レベル＊			事業者による提案事項とすること
24		アクセス集中時のバッジレスポンス遵守度合い	レベル＊			事業者による提案事項とすること
25	通常運用	運用時間【平日】	レベル３(24時間運用とすること)			
26		運用時間【休日等】	レベル３(24時間運用とすること)			
27		バックアップ取得時間	レベル＊			事業者による提案事項とすること
28		外部データの利用可否	レベル０(全データの復旧に利用できる)			
29		データ復旧の対応範囲	レベル１(障害発生時に決められた復旧時点（RPO）へデータを回復できれば良い。障害発生時のデータ損			
30		バックアップ自動化の範囲	レベル＊(バックアップ自動化の範囲は、事業者の提案事項とすること)			事業者による提案事項とすること
31		監視情報	レベル２(エラー監視を行うこと)			

No	項目	メトリクス(指標/要素)	要件	回答	LV 記入	備考
32	保守運用	OS等パッチ適用タイミング	レベル４(緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行うこと)			
33	障害時運用	対応可能時間	レベル0(事業者の営業時間内【例：9時～17時】で対応を行うこと)			
34		駆けつけ到着時間	レベル0(保守員の駆けつけ無し)			
35		障害検知時間	レベル1(障害の発生を検知した場合、利用者に通知するまでの時間は、24時間以内とすること)			
36	運用環境	マニュアル準備レベル	レベル2(情報システムの通常運用と保守運用のマニュアルを提供すること)			
37		外部システムとの接続有無	レベル3(庁外の外部システムと接続する)			
38	リモートオペレーション	リモート監視地点	レベル＊			事業者による提案事項とすること
39		リモート操作時の接続方法	レベル＊			事業者による提案事項とすること
40	サポート体制	保守契約(ハードウェア)の種類	レベル2(定額保守:センドバック)			
41		保守契約(ソフトウェア)の種類	レベル＊(保守契約内容は、事業者の提案事項とすること)			事業者による提案事項とすること
42		ライフサイクル期間	レベル2(アップデート)			
43		一次対応役割分担	レベル1(一部ユーザが実施)			
44		事業者側対応時間帯	レベル＊(事業者側対応時間は、事業者の提案事項とすること)			事業者による提案事項とすること
45		定期報告会実施頻度	レベル3(四半期に１回開催すること)			
46		報告内容のレベル	レベル2(障害報告に加えて運用状況報告を行うこと)			
47	その他の運用管理方針	問い合わせ対応窓口の設置有無	レベル１(事業者の既設コールセンターを利用すること)			
48	移行時期	システム停止可能日時	レベル-(仕様の対象としない)			
49	移行対象(機器)	設備・機器の移行内容	レベル0(移行対象無し)			
50	移行対象(データ)	移行データ量	レベル0(移行対象無し)			
51	前提条件・制約条件	遵守すべき規定、ルール、法令、ガイドライン等の有無	レベル１(有り。総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（最新版）」を参照すること)			
52	セキリュティリスク分析	リスク分析範囲	レベル1(重要度が高い資産を扱う範囲、あるいは、外接部分)			
53	セキュリティ診断	Web診断実施の有無	レベル＊(Webサイトに対して行うWebサーバやWebアプリケーションに対するセキュリティ診断の実施有無は、事業者の提案事項とすること)			事業者による提案事項とすること
54	セキュリティリスク管理	ウィルス定義ファイル適用タイミング	レベル２(システム脆弱性等に対応するためのウィルス定義ファイルの適用は、定義ファイルリリース時に実施すること)			
55	アクセス・利用制限	管理権限を持つ主体の認証	レベル３(複数回、異なる方式による認証を行うこと。但しそのうち一つはマイナンバーの信頼で支える認証と準じるスマホ利用の公的個人認証基盤)			
56		システム上の対策における操作制限	レベル＊(システム上の対策における操作制限度は、事業者の提案事項とすること)			事業者による提案事項とすること
57	データの秘匿	伝送データの暗号化の有無	レベル３(すべてのデータを暗号化すること)			
58		蓄積データの暗号化の有無	レベル１(認証情報のみ暗号化に準じること)			
59	不正追跡・監視	ログの取得	レベル１(必要なログを取得すること)			
60		不正環視対象(装置)	レベル１(重要度が高い資産を扱う範囲及び外接部分)			
61	Web対策	セキュアコーディング、Webサーバの設定等による対策の強化	レベル1(対策の強化。Webアプリケーション特有の脅威、脆弱性への対策を行うこと。対策内容は、本書5.2.8項IaaS領域に準拠すること)			
62		WAFの導入の有無	レベル＊			事業者による提案事項とすること
63	システム制約前提条件	構築時の制約条件	レベル2(制約有り。すべての制約【事業者は情報セキリュティマネジメントシステムに関する国際規格［ISO27001］を取得している、IaaS部分はクラウド型IT サービスに関する国際規格［ISO/IEC27017］を取得している】、延岡市情報セキュリティポリシー事本方針を適用すること)			
64		運用時の制約条件	レベル2(制約有り。すべての制約【情報セキリュティマネジメントシステムに関する国際規格［ISO27001］を取得している、IaaS部分はクラウド型IT サービスに関する国際規格［ISO/IEC27017］を取得している】、延岡市情報セキュリティポリシー事本方針を適用すること)			
65	システム特性	クライアント(端末)数	レベル１(上限が決まっている)			
66		特定製品の仕様有無	レベル１(一部に特定製品の指定【利用者端末のOSは Windows 10以降上＋ブラウザはMicrosoft Edge 最新版、Android 12以降＋Chrome最新版、iOS15以上＋Safari最新版】がある)			

No	項目	メトリクス(指標/要素)	要件	回答	LV記入	備考
67	適合規格	規格取得の有無(安全性)	レベル１(規格取得の必要有り。すべての制約【情報セキュリティマネジメントシステムに関する国際規格［ISO27001］を取得している、IaaS部分はクラウド型IT サービスに関する国際規格［ISO/IEC27017］を取得している】を適用すること)			
68		規格取得の有無(有害物質)	レベル＊(提供するサービスに使用する製品について、RoHS指令※などの特定有害物質の使用制限についての規格の取得は、事業者の提案事項とすること)			事業者による提案事項とすること
69	環境マネージメント	グリーン購入法対応	レベル＊(グリーン購入法対応は、事業者の提案事項とすること)			事業者による提案事項とすること

No	評価項目		回答	備考
71	アプリケーション領域	サービスに関連するデータ管理は、日本国内法の適用を受けること。		
72		利用者端末と災害物流DX間の通信SSL/TLS 通信により接続が可能な環境とすること。		
73		蓄積データは、暗号化を基本とすること。蓄積データの暗号化ができない事情がある場合は、暗号化対策に準じた対策を行い、当該内容を事業者による提案事項とする。尚、その場合においては、認証情報は暗号化した上で保管すること。		
74		リバースプロキシ、WAF(Web Application Firewall)機能等を有し、 外部端末からWebサーバに向けて送信されるデータ及び入力のチェックを行い、不正な入力がWebサーバに渡されないようにすること。		
75	IaaS領域	クラウドサービス及び保管データは、日本国内法の適用を受けること。		
76		外部から接続する際には、インターネット回線が利用できることとし、通信速度1Gbpsベストエフォートに対応できること。		
77		デジタルID機能を運用できること。		
78		外部接続環境との間でのSSL通信（https）に対応すること。		
79		ネットワークファイヤウォール、IPS（Intrusion Prevention System)機能等を有し、仮想化サーバ・ネットワークと外部・内部通信を監視し、特定の IP アドレスからのトラフィックを拒否（ブラックリスト化）、外部アクセスの接続数を制限するといった方法によって、分散型サービス拒否（DDoS）攻撃、不正な通信の侵入を防止すること。		
80		ネットワークファイヤウォール、IPS等において通過させなかった通信のIPアドレスのログの取得ができること。		
81		機器、部品及びネットワーク経路は冗長化されており、機器部品の単一障害によってサービスが停止しないこと。		
82		物理サーバの障害発生を検知した場合は対象の物理サーバ上で稼働していた仮想サーバは自動的に別のサーバで再起動すること。		
83		複数の仮想サーバを異なる物理サーバ上で稼働させ、単一の物理サーバ障害の影響範囲を限定すること。		
84		自動火災報知設備、消火設備（サーバ室においてはガス系消火施設）が設置されていること。		
85		停電時にシステムを運用するため十分な電源容量を持つ非常用自家発電装置を備えていること。また、非常用発電装置は72 時間運転が可能なこと。災害時に優先的に燃料が供給可能な場合で、72 時間対応できる時は、非常用発電装置は24 時間の運転が可能なこと。		
86		汎用的なOS(具体的には、Windows, RedHatEnterpriseLinux等Linux、Solaris(SunOS)等Unix)が利用可能であること。		
87		運用期間中に発生するサーバOSやパッケージソフトのアップグレードやセキュリティパッチ適用は、サービス提供に必要とされる業務として実施すること。		

※機能向上に関する提案がある場合、項目を明らかにして記入ください。