

インフラマネジメント基盤(DoboX)運用保守業務(その2)仕様書

目次

1. 業務の目的	3
2. 業務の場所	3
3. 業務対象項目	3
4. 前提条件及び留意事項	4
4.1. 前提条件等	4
4.2. 業務工程	4
4.3. 運用保守対象の構成	5
4.4. 運用保守体制	6
4.5. 問い合わせ・障害対応体制	6
4.6. 情報の管理	7
4.7. その他	7
5. 業務内容	8
5.1. 運用作業	8
5.1.1. システム稼働監視	8
5.1.2. バックアップ	8
5.1.3. セキュリティ対策	8
5.1.4. 運用支援	8
5.1.5. 問い合わせ対応	8
5.1.6. 月次報告	8
5.2. 保守作業	9
5.2.1. データ保守作業	9
5.2.2. 基盤保守作業	9
5.2.3. ドキュメント保守作業	9
5.2.4. 障害対応	9
5.3. 管理作業	9
5.3.1. 計画準備	9
5.3.2. コミュニケーション管理	9
5.3.3. 体制管理	9
5.3.4. 作業管理	9
5.3.5. リスク管理	9
5.3.6. 課題管理	9
5.3.7. 構成管理	9
5.3.8. 変更管理	9

5.3.9. 情報セキュリティ管理.....	10
5.4. その他	10
5.4.1. 監査対応	10
6. 提出物	100

1. 業務の目的

広島県インフラマネジメント基盤(DoboX)(以下「DoboX」という。)は、インフラに係る県保有データ等を一元化し、県民や民間企業等が閲覧・ダウンロードできるオープンデータとして広く公開するシステムである。

本県では県民の安全・安心や利便性、建設分野の生産性向上を目的として、公共土木施設等に関する情報を一元化・オープンデータ化し、インフラ事業者や国・市町等のシステムとDoboXを連携することで、インフラデータの利活用を推進し、官民の枠を超えた業務の効率化やインフラ維持管理の高度化等を進めている。また、オープンデータを活用した民間企業等におけるアプリケーション開発の促進などにより、新たなサービス・付加価値の創出を目指している。

本業務では、令和4年度に運用を開始したDoboXの運用・保守を行い、引き続きデータ利活用の促進や、新たな県民サービス・付加価値創出の推進に向けたデータ提供のための安定した運用環境を確保することを目的とする。

2. 業務の場所

電話、e-mail、Web 会議による受付が可能な場所

3. 業務対象項目

本業務の対象項目を次表に示す。

表1 業務対象項目

No	業務対象項目
1	運用作業
1-1	システム稼働監視
1-2	バックアップ
1-3	セキュリティ対策
1-4	運用支援
1-5	問い合わせ対応
1-6	月次報告
2	保守作業
2-1	データ保守作業
2-2	基盤保守作業
2-3	ドキュメント保守作業
2-4	障害対応
3	管理作業
3-1	計画準備
3-2	コミュニケーション管理
3-3	体制管理
3-4	作業管理
3-5	リスク管理
3-6	課題、アクション管理
3-7	構成管理
3-8	変更管理
3-9	情報セキュリティ対策管理
4	その他
4-1	監査対応

4. 前提条件及び留意事項

4.1. 前提条件等

DoboX の運用保守は、「運用保守作業計画書」「運用保守作業手順書」に従い実施すること。なお「運用保守作業計画書」「運用保守作業手順書」は、閲覧可能である。

- (1) クラウド環境は、建設DX担当にて別途調達し、月額清算している。ウイルス対策ソフトウェアの利用料は本業務の費用に含め、受注者側で契約をすること。
- (2) 建設DX担当からクラウド環境の仕様を提示する。
- (3) クラウド環境は、AWS(Amazon Web Services)を利用している。
- (4) クラウド環境における DoboX の仮想サーバ、ネットワーク、ロードバランサ、バックアップ、セキュリティ対策、保守用のリモート接続等に関する運用を、本業務の対象とする。
- (5) クラウド環境の仮想サーバは、以下のネットワーク通信が可能な状態で、建設DX担当より提供する。

表 1 仮想サーバのネットワーク通信

No.	項目	備考
1	県庁からの通信	
2	仮想サーバ間の通信	
3	保守業者リモートメンテナンス用の通信	
4	その他の通信	ウイルス対策ソフトウェア、庁内システムとの接続／データ連携環境、等

- (6) DoboX の運用環境を本業務対象のとし、DoboX が連携する対象のシステム及び運用環境は本業務の対象外とする。
- (7) 次表の項目を含むネットワーク通信に関する仕様は、建設DX担当より提示する。仕様の不足や変更が必要な場合は、その内容を提示すること。

表 2 ネットワーク通信に関する仕様

No.	項目	備考
1	仮想サーバの IP アドレス	
2	仮想サーバ間の通信制御	

- (8) クラウド環境の仮想サーバへのリモート接続手順書は、建設DX担当より提示する。

4.2. 業務工程

本業務の履行に当たっては、以下に示すとおり実施すること。

運用保守 令和 7(西暦 2025)年 7 月 1 日～令和 8(西暦 2026)年 3 月 31 日

本業務の対象環境(場所及び、ハードウェア)は広島県 AWS 本番環境、検証環境であり、DoboX のシステム構成について以下図 1 に示す。対象環境(ソフトウェア)について表 4 に示す。

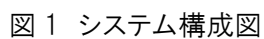


表 4 対象環境(ソフトウェア)

サーバ／ クライアント	種類		名称・バージョン
サーバ	オペレーティング システム	OS	AmazonLinux2
	ミドルソフト	Web サーバ	Apache
		DB	MariaDB
		PROXY	Squid
	アプリケーション	開発言語	Laravel(PHP フレームワーク)

4.4. 運用保守体制

保守運用作業の実施体制を記述する。

表 5 運用保守作業の実施体制

役割	作業内容
運用管理者	・運用保守作業を管理する。運用保守事業者への作業指示、作業結果の確認及び承認を行う。
運用保守事業者	・運用管理者の作業指示及び、手順書に従い、運用保守作業を実施する。

受注者は、次の事項に係る知識、技術、実務経験を保有し、DoboX の円滑な運用保守が履行できること。

- (1) 「4.3 運用保守対象の構成」記載のシステム構成、対象環境における同等の開発経験を有し、DoboX の円滑な運用保守業務が履行できること。
- (2) パブリッククラウドによるサービス/システムの運用実績があること。
- (3) 機能拡張や基盤連携に係る協議への同席、問合せ等に対応できること。
- (4) オープンデータの活用、情報発信、国・地方自治体の動向調査について、発注者を支援できること。

4.5. 問い合わせ・障害対応体制

問い合わせ・障害対応体制については以下とする。

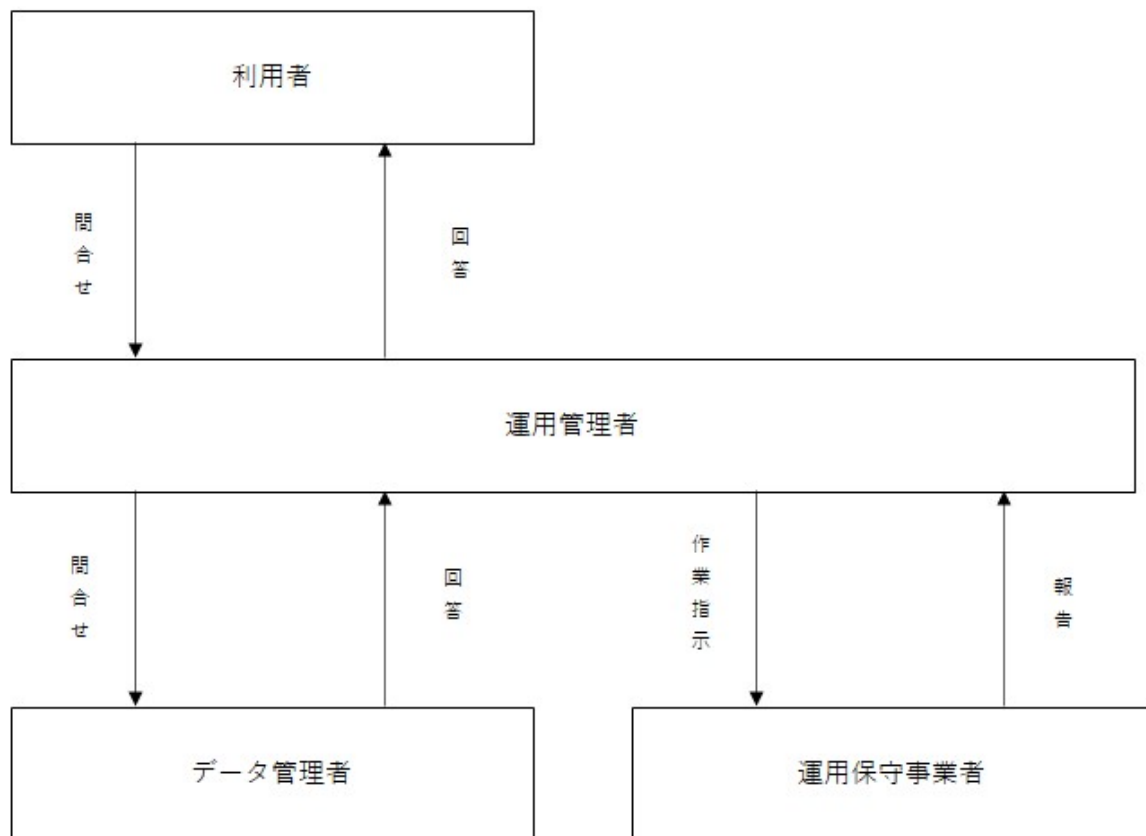


図 2 障害発生時等の連絡体制

4.6. 情報の管理

本委託業務の遂行にあたっての情報管理については、次の点に留意すること。

- (1) 本業務に携わる者は、個人情報の管理を適正かつ厳格に行うこと。
- (2) 本業務に携わる者は、事業の遂行を通じて知り得た情報を漏らしてはならないこと。その職務を退いた後も同様とすること。
- (3) 「広島県情報セキュリティポリシー」を遵守すること。なお、「広島県情報セキュリティポリシー」は、閲覧可能である。

4.7. その他

- (1) 計画停止は、事前連絡し発注者と相談のうえ対応すること。
- (2) 運用、保守の過程で重大な問題、障害、その他発注者へ緊急に報告する必要がある場合には、速やかに連絡すること。
- (3) 問い合わせの受付時間は、営業日の 9:00 から 17:00 までとすること。それ以降の時間のメールへの一次対応は翌営業日に行うこととする。

5. 業務内容

5.1. 運用作業

5.1.1. システム稼働監視

- (1) システムの稼働状況を確認すること。自動で監視を行い、アラートが発信された際は調査、解決策を提示し、対応を行うこと。
- (2) 項目としては、稼働状況確認(死活監視、ポート監視、URL 監視、Deep Security 監視)、リソース状況確認(CPU 使用状況、メモリ使用状況、ディスク使用状況)、連携状況確認を実施すること。
- (3) 作業は日次で実施すること。

5.1.2. バックアップ

- (1) リソースのバックアップを取得すること。
- (2) 対象は、仮想マシンと DB とすること。
- (3) 日次で自動バックアップを実施すること。

5.1.3. セキュリティ対策

- (1) 脆弱性公開情報確認を日次で実施すること。
- (2) ログ確認、Deep Security IPS/IDS 確認を月次で実施すること。確認結果に問題がある場合は調査、解決策を提示し、対応すること。
- (3) 情報セキュリティインシデントが発生した際には発注者の指示の下、受注者はセキュリティインシデントの調査、報告を実施すること。

5.1.4. 運用支援

- (1) 発注者が対応するよりも受注者が対応する方が望ましい場合、データの追加と削除を随時実施すること。
- (2) API に関する設定・管理を随時実施すること。
- (3) メタデータ、利用規約、プライバシーポリシー翻訳・適用を随時実施すること。メタデータ、利用規約、プライバシーポリシーの記載内容は発注者側で更新し、庁内利用者への更新版の周知は発注者より実施するものとする。
- (4) 別調達で行う OS アップデート業務等の問い合わせに対応すること。DB データ抽出、環境設定等の質問対応を想定している。

5.1.5. 問い合わせ対応

- (1) 問い合わせ対応を随時実施すること。原因調査が必要な場合は随時行うこと。問い合わせの受付時間は営業日の 9:00 から 17:00 までとし、それ以降の時間のメールへの一次対応は翌営業日に行うこと。対応時の連絡ルート「4.5 問合せ・障害対応体制」のとおりとする。

5.1.6. 月次報告

- (1) 運用・保守計画に則り実施した運用保守作業の実施状況について、月次で作業報告書に取りまとめ、発注者へ報告すること。
- (2) 各作業の実績、工数等を定期的に報告すること。また、ハードウェア、ソフトウェアを含むシステム機能としての障害実績を整理し報告すること。

5.2. 保守作業

5.2.1. データ保守作業

- (1) システムの設定データ、マスタデータ、オープンデータの更新作業を必要に応じて随時実施すること。手動連携等の更新作業も想定すること。

5.2.2. 基盤保守作業

- (1) アプリケーションリリース(データカタログ、可視化コンテンツ、API)を必要に応じて随時実施すること。
- (2) リソースのスケールアップ、スケールダウンを必要に応じて随時実施すること。
- (3) 障害発生時には仮想サーバ/DB リストア、再起動等の障害復旧作業を実施すること。
- (4) 検証環境のグローバル IP アドレス接続許可変更を必要に応じて随時実施すること。
- (5) 基盤の設定変更、パッチ適用を必要に応じて随時実施すること

5.2.3. ドキュメント保守作業

- (1) 運用保守作業内で変更があった場合に、ドキュメントの更新を実施すること。別調達で行う OS アップデート業務等でドキュメント変更が発生した場合、ドキュメントの更新を実施すること。

5.2.4. 障害対応

- (1) 障害発生時は障害記録一覧に記載し、必要なインシデント管理及び障害復旧対応を実施すること。別調達で行う OS アップデート業務等でリリース後に障害発生した場合も障害記録一覧に記載し、必要なインシデント管理及び障害復旧対応を実施すること。対応時の連絡ルートは「4.5 問合せ・障害対応体制」のとおりとする。

5.3. 管理作業

5.3.1. 計画準備

- (1) 作業計画については発注者と受注者で都度協議の上決定すること。

5.3.2. コミュニケーション管理

- (1) 月に 1 回会議体を設け、サービス稼働状況、運用保守作業状況、保守作業実績を報告すること。
- (2) その他、運用保守作業が円滑に行えるように、協議の上必要に応じて会議体を開催すること。

5.3.3. 体制管理

- (1) 運用保守作業が円滑に行える体制を整備すること。責任者を明らかにし、体制図を提示すること。
- (2) 受注者は、作業体制に変更がある場合は、速やかに県に報告すること。

5.3.4. 作業管理

- (1) 運用保守作業が円滑に行えるように作業を管理すること。

5.3.5. リスク管理

- (1) 受注者は、本作業の実施に悪影響のあるリスクが顕在化した際に適切な対応がとれるようリスク管理を行い、発注者と共有すること。

5.3.6. 課題管理

- (1) 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整備すること。受注者は既存の課題についても引継ぎ、対応すること。

5.3.7. 構成管理

- (1) システム構成に係る文書の整備及び更新を行うこと。別調達で行う OS アップデート業務等で変更が発生した場合についても更新を行うこと。

- (2)ソフトウェアのライブラリ管理を適切に行うこと。別調達で行う OS アップデート業務等で変更が発生した場合についても更新を行うこと。
- (3)作業手順に係る文書を整備し、適宜更新すること。別調達で行う OS アップデート業務等で変更が発生した場合についても更新を行うこと。
- (4)DoboX を構成するプログラムのバージョン履歴を適切に管理すること。別調達で行う OS アップデート業務等で変更が発生した場合についても管理を行うこと。

5.3.8. 変更管理

- (1)プロジェクトの進捗により発生する変更について、管理対象、変更手順、管理手法等を協議する。

5.3.9. 情報セキュリティ管理

- (1)受注者は、発注者から「情報セキュリティポリシー」等の説明を受け、これらの事項を遵守すること。
- (2)受注者は、事業者組織全体のセキュリティを確保するとともに、発注者から求められた当該業務の実施において情報セキュリティを確保するための体制を整備すること。

5.4. その他

5.4.1. 監査対応

- (1)システム監査対象に指定された場合や外部事業者によるセキュリティ診断を受ける場合、ヒアリングや情報提供等の協力を行うこと。

6. 提出物

作業報告書 1 部 電子納品