令和５年度　基幹水利施設保全管理対策　農業水利ストック情報データベースシステム運用保守・改修及びクラウドサービス提供業務　仕様書（令和４年９月 20 日付け公告）新旧対照表

修　正　後	現　行
第 2-3 作業項目 作業項目は次のとおりであり、実施内容の詳細は第 5 章に示すとおりである。 【Ⅰ－１　ＢＩツールの導入に伴う基盤改修】 (1) 設計 (2) 基盤改修 (3) プログラム修正 (4) プログラムテスト (5) 受入テスト 【Ⅰ－２　通信設定変更、セキュリティ対策に伴う基盤改修】 (6) 設計 (7) 基盤改修 【Ⅱ　システム運用及び保守】 (8) クラウドサービスの引継ぎ及び提供 (9) システム模擬環境構築 (10) サービスデスク (11) 障害管理及びデータ修正 (12) セキュリティ管理 (13) システム監視 (14) 稼働状況管理 (15) 構成管理 (16) プログラム修正 (17) 業務進捗状況報告	第 2-3 作業項目 作業項目は次のとおりであり、実施内容の詳細は第 5 章に示すとおりである。 (1) 設計 (2) 基盤改修 (3) プログラム修正 (4) プログラムテスト (5) 受入テスト (6) クラウドサービスの引継ぎ及び提供 (7) システム模擬環境構築 (8) サービスデスク (9) 障害管理及びデータ修正 (10) セキュリティ管理 (11) システム監視 (12) 稼働状況管理 (13) 構成管理 (14) プログラム修正 (15) 業務進捗状況報告

令和５年度　基幹水利施設保全管理対策　農業水利ストック情報データベースシステム運用保守・改修及びクラウドサービス提供業務　仕様書（令和４年９月 20 日付け公告）新旧対照表

修　正　後	現　行
第 4-4 情報セキュリティ (1)～(10)　略 (11)本業務の遂行に当たり、以下の内容を含む情報セキュリティ対策を実施し、情報セキュリティ水準の低下を招かないこと。 1)提供するアプリケーション・コンテンツに不正プログラムを含めないこと。 2)提供するアプリケーションに脆弱性を含めないこと。 3)実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。 4)電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。 5)提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのＯＳやソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、ＯＳやソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。 6)サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。 7)「.go.jp」で終わるドメインを使用してアプリケーション・コンテンツを提供すること。 8)詳細については、担当部署から「アプリケーション・コンテンツの作成及び提供に関する規程」の説明を受けるとともに、それに基づきアプリケーション・コンテンツの作成及び提供を行うこと。 9)以下のセキュリティ対策要件を参照し、本システムのセキュリティ対策要件を点検すること。 ・AWS 設定確認リスト（別紙４） ・OWASP チェックリスト【Web システム／Web アプリケーションセキュリティ要件書】（別紙５）	**第 4-4 情報セキュリティ** (1)～(10)　略 (11)本業務の遂行に当たり、以下の内容を含む情報セキュリティ対策を実施し、情報セキュリティ水準の低下を招かないこと。 1)提供するアプリケーション・コンテンツに不正プログラムを含めないこと。 2)提供するアプリケーションに脆弱性を含めないこと。 3)実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。 4)電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。 5)提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのＯＳやソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、ＯＳやソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。 6)サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。 7)「.go.jp」で終わるドメインを使用してアプリケーション・コンテンツを提供すること。 8)詳細については、担当部署から「アプリケーション・コンテンツの作成及び提供に関する規程」の説明を受けるとともに、それに基づきアプリケーション・コンテンツの作成及び提供を行うこと。

令和５年度　基幹水利施設保全管理対策　農業水利ストック情報データベースシステム運用保守・改修及びクラウドサービス提供業務　仕様書（令和４年９月 20 日付け公告）新旧対照表

修　正　後	現　行
第 5 章　業務実施内容 **第 5-1 業務内容** 第 2-3 作業項目に示す事項に対する業務内容は別紙６のとおりである。 **第 5-2 業務実施に当たっての留意点** 業務実施にあたっては、次の点に留意すること。 (1)～(20)　略 (21)プロジェクトの推進体制及び本件受注者に求める作業実施体制は別紙７のとおりである。なお、受注者内のチーム編成については想定であり、受注者決定後に協議の上、見直しを行う。また、受注者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成すること。 (22)受注者は、担当部署が承認した設計・開発計画書の作業体制、スケジュール、開発形態、開発手法、開発環境、開発ツール等に従い、記載された成果物を作成すること。その際、設計・開発実施要領に従い、コミュニケーション管理、体制管理、工程管理、品質管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。 (23)設計・開発を行う担当者には、次に掲げる試験の合格者を１名以上必要な人数含むこと。 ・AWS 認定ソリューションアーキテクト-アソシエイト試験 (24)本システムのソフトウェア情報については、「別紙８　ソフトウェア構成」を参照すること。ソフトウェア情報に記載するソフトウェアの内、「OpenSSL」「PostgreSQL」については、2023 年にサポート期限を迎えることから、本調達において指定するバージョンとするとともに、アプリケーションソフトウェアの改修を実施すること。 (25)過年度ディスク増加量は、別紙９のとおりである。	**第 5 章　業務実施内容** **第 5-1 業務内容** 第 2-3 作業項目に示す事項に対する業務内容は別紙４のとおりである。 **第 5-2 業務実施に当たっての留意点** 業務実施にあたっては、次の点に留意すること。 (1)～(20)　略 (21)プロジェクトの推進体制及び本件受注者に求める作業実施体制は別紙５のとおりである。なお、受注者内のチーム編成については想定であり、受注者決定後に協議の上、見直しを行う。また、受注者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成すること。 (22)受注者は、担当部署が承認した設計・開発計画書の作業体制、スケジュール、開発形態、開発手法、開発環境、開発ツール等に従い、記載された成果物を作成すること。その際、設計・開発実施要領に従い、コミュニケーション管理、体制管理、工程管理、品質管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。 (23)設計・開発を行う担当者には、次に掲げる試験の合格者を１名以上必要な人数含むこと。 ・AWS 認定ソリューションアーキテクト-アソシエイト試験 (24)本システムのソフトウェア情報については、「別紙６　ソフトウェア構成」を参照すること。ソフトウェア情報に記載するソフトウェアの内、「OpenSSL」「PostgreSQL」については、2023 年にサポート期限を迎えることから、本調達において指定するバージョンとするとともに、アプリケーションソフトウェアの改修を実施すること。 (25)過年度ディスク増加量は、別紙７のとおりである。

令和５年度　基幹水利施設保全管理対策　農業水利ストック情報データベースシステム運用保守・改修及びクラウドサービス提供業務　仕様書（令和４年９月 20 日付け公告）新旧対照表

修　正　後	現　行

別紙４

AWS設定確認リスト　　凡例：〇：責任者、△：サポート

【PaaS/IaaS】基本的な設定すべきセキュリティ対策（AWS）	担当		役割分担に関する補足
	MAFFクラウド管理者(PMO)	PJMO／業者	
IDおよびアクセス管理			
組織が許可したアカウントの管理		〇	
管理者アカウントに対する多要素認証の利用	△	〇	多要素認証を設定していない限りあらゆるAWSリソースの操作が出来ないよう設定
管理者アカウントに紐づく最新の連絡先の登録と定期的な見直し	△	〇	MAFFクラウド管理者が、年度末に実施
必要最低限の管理者権限の割当て	△	〇	AWS Configを利用して実施、MAFFクラウド利用ガイドラインにて規定。
グループを利用した権限の設定		〇	
管理者アカウントに関する復旧手段の確保		〇	
すべてのアカウントへのパスワードポリシーの適用	△	〇	AWS Configを利用して実施、MAFFクラウド利用ガイドラインにて規定。
アクセスキー、サービスアカウントキー等の適切な管理		〇	
管理者アカウントと日常的に使用するアカウントの分離		〇	利用システムのIAMユーザーの払い出しは、PJMO管理
アカウント・権限・認証情報の定期的な見直し		〇	MAFFクラウド管理者が、年度末に実施
AWSにおいて考慮すべき設定			
AWS サポートセンターへのアクセス設定		〇	
IAMに保存されているサーバ証明書の管理		〇	
IAM Access analyzerの有効化		〇	
ログの記録と監視			
ログの有効化及び取得	△	〇	MAFFクラウド管理者で有効化の為の手順を作成し、PJMOに配布
ログの一元管理	△	〇	MAFFクラウド利用ガイドラインにて規定。
ログの保護	△	〇	管理者アカウントで保管
ログの監視/通知の設定	△	〇	アクセスログなどは管理者アカウントでGuardDutyを用いて対応。、MAFFクラウド利用ガイドラインにて規定。そのほかのログについてはPJMOに一任。
ネットワーク			
ロードバランサの接続設定		〇	
仮想マシン			
最新のOSパッチの適用確認		〇	
不正プログラム対策ソフトウェアの導入		〇	
攻撃対象となるネットワークポートへのアクセス制限		〇	
ストレージ			
匿名/公開アクセスの禁止	△	〇	不適切設定を有効化し、管理者アカウントで監視
ストレージアクセスの通信設定	△	〇	不適切設定を有効化し、管理者アカウントで監視
AWSにおいて考慮すべき設定			
Amazon RDSの暗号化	△	〇	不適切設定を有効化し、管理者アカウントで監視
MFA Deleteの有効化	△	〇	不適切設定を有効化し、管理者アカウントで監視
Amazon EBSの暗号化	△	〇	不適切設定を有効化し、管理者アカウントで監視

【新規追加】

令和５年度　基幹水利施設保全管理対策　農業水利ストック情報データベースシステム運用保守・改修及びクラウドサービス提供業務　仕様書（令和４年９月 20 日付け公告）新旧対照表

修　正　後

別紙５

OWASP チェックリスト【Webシステム／Webアプリケーションセキュリティ要件書】

項目		見出し		要件		備考	必須可否
1	認証・認可	1.1	ユーザー認証	1.1.1	特定のユーザーや管理者のみに表示・実行を許可すべき画面や機能、APIでは、ユーザー認証を実施すること	特定のユーザーや管理者のみにアクセスを許可したいWebシステムでは、ユーザー認証を行う必要があります。また、ユーザー認証が成功した後にはアクセス権限を確認する必要があります。そのため、認証済みユーザーのみがアクセス可能な箇所を明示しておくことが望ましいでしょう。 リスクベース認証や二要素認証など認証をより強固にする仕組みもあります。不特定多数がアクセスする必要がない場合には、IPアドレスなどによるアクセス制限も効果があります。 OpenIDなどIdP(ID Provider)を利用する場合には信頼できるプロバイダであるかを確認する必要があります。IdPを使った認証・認可を行う場合も他の認証・認可に関する要件を満たすものを利用することが望ましいです。	必須
				1.1.2	上記画面や機能に含まれる画像やファイルなどの個別のコンテンツ（非公開にすべきデータは直接URLで指定できる公開ディレクトリに配置しない）では、ユーザー認証を実施すること		必須
				1.1.3	多要素認証を実施すること	多要素認証（Multi Factor Authentication: MFA）とは、例えばパスワードによる認証に加え、TOTP (Time-Based One-Time Password：時間ベースのワンタイムパスワード）やデジタル証明書など二つ以上の要素を利用した認証方式です。手法については NIST Special Publication 800-63B などを参照してください。	推奨
		1.2	ユーザーの再認証	1.2.1	個人情報や機微情報を表示するページに遷移する際には、再認証を実施すること	ユーザー認証はセッションにおいて最初の一度だけ実施するのではなく、重要な情報や機能へアクセスする際には再認証を行うことが望ましいでしょう。	推奨
				1.2.2	パスワード変更や決済処理などの重要な機能を実行する際には、再認証を実施すること		推奨
		1.3	パスワード	1.3.1	ユーザー自身が設定するパスワード文字列は最低 8文字以上であること	認証を必要とするWebシステムの多くは、パスワードを本人確認の手段として認証処理を行います。そのためパスワードを盗聴や盗難などから守ることが重要になります。	必須
				1.3.2	登録可能なパスワード文字列の最大文字数は64文字以上であること	パスワードを処理する関数の中には最大文字数が少ないものもあるので注意する必要があります。	必須
				1.3.3	パスワード文字列として使用可能な文字種は制限しないこと	任意の大小英字、数字、記号、空白、Unicode文字など任意の文字が利用可能である必要があります。	必須
				1.3.4	パスワード文字列の入力フォームはinput type="password"で指定すること	基本的にinputタグのtype属性には「password」を指定しますが、パスワードを一時的に表示する可視化機能を実装する場合にはこの限りではありません。	必須
				1.3.5	ユーザーが入力したパスワード文字列を次画面以降で表示しないこと（hiddenフィールドなどのHTMLソース内やメールも含む）		必須
				1.3.6	パスワードを保存する際には、平文で保存せず、Webアプリケーションフレームワークなどが提供するハッシュ化とsaltを使用して保存する関数を使用すること	関数が存在しない場合にはパスワードは「パスワード文字列＋salt（ユーザー毎に異なるランダムな文字列）」をハッシュ化したものとsaltのみを保存する必要があります。（saltは20文字以上であることが望ましい） パスワード文字列のハッシュ化をさらに安全にする手法としてストレッチングがあります。	必須
				1.3.7	ユーザー自身がパスワードを変更できる機能を用意すること		必須
				1.3.8	パスワードはユーザー自身に設定させること システムが仮パスワードを発行する場合はランダムな文字列を設定し、安全な経路でユーザーに通知すること		推奨
				1.3.9	パスワードの入力欄でペースト機能を禁止しないこと	長いパスワードをユーザーが利用出来るようにするためにペースト機能を禁止しないようにする必要があります。	推奨
				1.3.10	パスワード強度チェッカーを実装すること	使用する文字種や文字数を確認し、ユーザー自身にパスワードの強度を示せるようにします。またユーザーIDと同じ文字列や漏洩したパスワードなどのリストとの突合を行う必要があります。手法については NIST Special Publication 800-63B などを参照してください。	推奨

表については、以下省略

現　行

【新規追加】

令和５年度　基幹水利施設保全管理対策　農業水利ストック情報データベースシステム運用保守・改修及びクラウドサービス提供業務　仕様書（令和４年９月20日付け公告）新旧対照表

修　正　後

作業項目に対する業務内容　別紙6

項目	作業内容	対応頻度	適用
【Ｉ-1 BIツールの導入に伴う基盤改修】 BIツールを利用し、ストックDBデータの利活用を行うため、BIツール導入作業計画を作成し、監督職員の承認を得ること。 監督職員の承認を受けたBIツール導入作業計画に基づき、BIツールの導入に向けた設計、基盤改修、プログラム改修、プログラムテスト、受入テストを実施すること。 テストの実施に当たってはテスト計画書を作成し、計画書に基づき、テストを実施すること。			
１．設計	BIツールの導入に必要となるサーバやネットワーク設定等の基盤設計、及び、アプリケーションの画面設計やデータベース設計を実施し、BIツール導入設計書を作成する。 なお、BIツールは、ストックDBが稼働するAWS内に新規サーバを構築し、構築したサーバ上に導入すること。また、AWSサービスの設計にあたっては、MAFFクラウド命名規約に基づき実施すること。	実施回数1回	
２．基盤改修	BIツール導入設計書に基づき、BIツールを導入し、アプリケーションからのアクセスやBIツールからストックDBデータベースへの疎通確認を実施する。 なお、BIツールは、「受入テスト」が完了するまでの期間、発注者拠点及び受注者拠点以外からのアクセスを制限するものとする。	実施回数1回	
３．プログラム修正	BIツール導入設計書に基づき、ストックDBからBIツールへの遷移及び各画面の構築・集計設定を実施する。なお、BIツールの画面や集計設定については、監督職員と協議のうえ実施するものとする。	実施回数1回	
４．プログラムテスト	構築したBIツールの動作確認を実施する。 テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載したテスト計画書を作成し、監督職員の承認を受けること。 また、テスト計画書に基づき、テストを実施し、テストの実施状況を監督職員に報告すること。	実施回数1回	
５．受入テスト	監督職員によるBIツールの動作確認を実施する。 なお、受注者は、監督職員の作業実施にあたって必要な支援を行うこと。 動作確認の結果、成果物等に不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点について監督職員に説明を行った上で、再度指定する期日までに納品すること。 また、本工程完了後に指定した利用者に公開するため、ネットワークのアクセス制限設定を解除すること。	実施回数1回	
【Ｉ-2 通信設定変更、セキュリティ対策に伴う基盤改修】 CloudFrontを利用する通信設定への変更及びAWS WAFマネージドルールを活用したストックDBのセキュリティ対策を行うため、通信基盤改修作業計画を作成し、監督職員の承認を得ること。 監督職員の承認を受けた通信基盤改修作業計画に基づき、CloudFrontとAWS WAFマネージドルールの導入に向けた設計、基盤設計、実装を実施すること。			
６．設計	ストックＤＢの通信設定変更及びＡＷＳ ＷＡＦマネージドルールに必要となる設定事項等を検討する。 なお、設定事項及び手順については、貸与資料「NWHBE-001_クラウド基盤設定書及び構築手順書」に追記すること。また、AWSサービスの設計にあたっては、MAFFクラウド命名規約に基づき実施すること。	実施回数1回	
７．基盤改修	貸与資料「NWHBE-001_クラウド基盤設定書及び構築手順書」に追記した設定事項に従い、CloudFrontとAWS WAFへのマネージドルールの導入を実施する。 なお、導入後にストックDB利用者がアクセス可能となるようにドメイン申請を実施する。	実施回数1回	
【Ⅱ システム運用及び保守】 ストックDBにおける運用計画及び保守作業計画を作成し、監督職員の承認を得ること。 監督職員の承認を受けた運用計画及び保守作業計画に従い、下記に示す運用、保守作業を実施すること。 運用作業については、クラウドサービス環境のサービス内容等を踏まえ、下記の要件を満たす範囲で、可能な限りクラウドサービス環境のサービスを用いて実施することとし、難しい場合は代替案の提案を許容するものとする。 なお、死活監視、性能監視、稼働状況監視、ログ管理、バックアップ管理、構成管理についてはクラウドサービス環境のサービスを利用して運用作業を実施することを想定しているが、その他の運用作業項目についても、クラウドサービス環境のサービスを用いて運用作業を実施できる場合は提案すること。			
8.クラウドサービスの引継ぎ及び提供	IaaS型のクラウドサービスを利用し、ストックDBが稼働する基盤を提供すること。詳細は、別紙2のとおりである。 ・採用するクラウドサービスは、現行の基盤を引継ぐことを前提とするが、受注者は、前年度の運用・保守業務の事業者からパブリッククラウド上に構築された情報システムの引継ぎを受け、アカウントの契約の移管を行い、環境を維持すること。なお、AWS以外を提案し基盤を再構築する場合は、そのメリットを明確に示すこと。	実施回数1回	
９．システム模擬環境構築	受注者拠点内にストックＤＢが稼働するシステム運用及び保守作業に利用する模擬環境を構築する。ストックＤＢシステム及びデータは発注者が貸与する。 本作業で構築する環境は【MAFFクラウド参入に伴う基盤改修作業】で実施する環境とは別に構築すること。 ＯＳ、ミドルウェア、ソフトウェア及び機器等は受注者の負担によるものとする。なお、模擬環境のストックＤＢシステム、ＯＳ、ミドルウェア、ソフトウェア等のバージョンは本番環境と同一となるよう期間中も更新を行うこと。模擬環境には、内部ネットワークにより接続する関連システムは含めないこととする。 また、本番環境の更新に伴い、ＯＳ、ミドルウェア、ソフトウェア、ハードウェア等の種類を変更する場合は、監督職員と協議するものとする。 業務完了後は模擬環境のシステム及びデータの消去を行い、監督職員に報告するものとする。	構築回数1回	業務開始後14日以内
１０．サービスデスク	監督職員からの質問及び作業依頼への対応を行う。 （1）質問の受付 質問（動作検証、データ調査等）を受付け、回答を行う。内容が障害の場合は障害管理として対応する。 （2）データ調査 依頼により、データ調査、データ抽出、データ整理を行う。	質問、依頼毎に対応する。 (1)(2)の対応件数は30件まで。	様式１ Q&Aシート

表については、以下省略

現　行

作業項目に対する業務内容　別紙4

項目	作業内容	対応頻度	適用
【Ｉ-1 BIツールの導入に伴う基盤改修】 BIツールを利用し、ストックDBデータの利活用を行うため、BIツール導入作業計画を作成し、監督職員の承認を得ること。 監督職員の承認を受けたBIツール導入作業計画に基づき、BIツールの導入に向けた設計、基盤改修、プログラム改修、プログラムテスト、受入テストを実施すること。 テストの実施に当たってはテスト計画書を作成し、計画書に基づき、テストを実施すること。			
１．設計	BIツールの導入に必要となるサーバやネットワーク設定等の基盤設計、及び、アプリケーションの画面設計やデータベース設計を実施し、BIツール導入設計書を作成する。 なお、BIツールは、ストックDBが稼働するAWS内に新規サーバを構築し、構築したサーバ上に導入すること。また、AWSサービスの設計にあたっては、MAFFクラウド命名規約に基づき実施すること。	実施回数1回	
２．基盤改修	BIツール導入設計書に基づき、BIツールを導入し、アプリケーションからのアクセスやBIツールからストックDBデータベースへの疎通確認を実施する。 なお、BIツールは、「受入テスト」が完了するまでの期間、発注者拠点及び受注者拠点以外からのアクセスを制限するものとする。	実施回数1回	
３．プログラム修正	BIツール導入設計書に基づき、ストックDBからBIツールへの遷移及び各画面の構築・集計設定を実施する。なお、BIツールの画面や集計設定については、監督職員と協議のうえ実施するものとする。	実施回数1回	
４．プログラムテスト	構築したBIツールの動作確認を実施する。 テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載したテスト計画書を作成し、監督職員の承認を受けること。 また、テスト計画書に基づき、テストを実施し、テストの実施状況を監督職員に報告すること。	実施回数1回	
５．受入テスト	監督職員によるBIツールの動作確認を実施する。 なお、受注者は、監督職員の作業実施にあたって必要な支援を行うこと。 動作確認の結果、成果物等に不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点について監督職員に説明を行った上で、再度指定する期日までに納品すること。 また、本工程完了後に指定した利用者に公開するため、ネットワークのアクセス制限設定を解除すること。	実施回数1回	
【Ｉ-2 通信設定変更、セキュリティ対策に伴う基盤改修】 CloudFrontを利用する通信設定への変更及びAWS WAFマネージドルールを活用したストックDBのセキュリティ対策を行うため、通信基盤改修作業計画を作成し、監督職員の承認を得ること。 監督職員の承認を受けた通信基盤改修作業計画に基づき、CloudFrontとAWS WAFマネージドルールの導入に向けた設計、基盤設計、実装を実施すること。			
６．設計	ストックＤＢの通信設定変更及びＡＷＳ ＷＡＦマネージドルールに必要となる設定事項等を検討する。 なお、設定事項及び手順については、貸与資料「NWHBE-001_クラウド基盤設定書及び構築手順書」に追記すること。また、AWSサービスの設計にあたっては、MAFFクラウド命名規約に基づき実施すること。	実施回数1回	
７．基盤改修	貸与資料「NWHBE-001_クラウド基盤設定書及び構築手順書」に追記した設定事項に従い、CloudFrontとAWS WAFへのマネージドルールの導入を実施する。 なお、導入後にストックDB利用者がアクセス可能となるようにドメイン申請を実施する。	実施回数1回	
【Ⅱ システム運用及び保守】 ストックDBにおける運用計画及び保守作業計画を作成し、監督職員の承認を得ること。 監督職員の承認を受けた運用計画及び保守作業計画に従い、下記に示す運用、保守作業を実施すること。 運用作業については、クラウドサービス環境のサービス内容等を踏まえ、下記の要件を満たす範囲で、可能な限りクラウドサービス環境のサービスを用いて実施することとし、難しい場合は代替案の提案を許容するものとする。 なお、死活監視、性能監視、稼働状況監視、ログ管理、バックアップ管理、構成管理についてはクラウドサービス環境のサービスを利用して運用作業を実施することを想定しているが、その他の運用作業項目についても、クラウドサービス環境のサービスを用いて運用作業を実施できる場合は提案すること。			
8.クラウドサービスの引継ぎ及び提供	IaaS型のクラウドサービスを利用し、ストックDBが稼働する基盤を提供すること。詳細は、別紙2のとおりである。 ・採用するクラウドサービスは、現行の基盤を引継ぐことを前提とするが、受注者は、前年度の運用・保守業務の事業者からパブリッククラウド上に構築された情報システムの引継ぎを受け、アカウントの契約の移管を行い、環境を維持すること。なお、AWS以外を提案し基盤を再構築する場合は、そのメリットを明確に示すこと。	実施回数1回	
９．システム模擬環境構築	受注者拠点内にストックＤＢが稼働するシステム運用及び保守作業に利用する模擬環境を構築する。ストックＤＢシステム及びデータは発注者が貸与する。 本作業で構築する環境は【MAFFクラウド参入に伴う基盤改修作業】で実施する環境とは別に構築すること。 ＯＳ、ミドルウェア、ソフトウェア及び機器等は受注者の負担によるものとする。なお、模擬環境のストックＤＢシステム、ＯＳ、ミドルウェア、ソフトウェア等のバージョンは本番環境と同一となるよう期間中も更新を行うこと。模擬環境には、内部ネットワークにより接続する関連システムは含めないこととする。 また、本番環境の更新に伴い、ＯＳ、ミドルウェア、ソフトウェア、ハードウェア等の種類を変更する場合は、監督職員と協議するものとする。 業務完了後は模擬環境のシステム及びデータの消去を行い、監督職員に報告するものとする。	構築回数1回	業務開始後14日以内
１０．サービスデスク	監督職員からの質問及び作業依頼への対応を行う。 （1）質問の受付 質問（動作検証、データ調査等）を受付け、回答を行う。内容が障害の場合は障害管理として対応する。 （2）データ調査 依頼により、データ調査、データ抽出、データ整理を行う。	質問、依頼毎に対応する。 (1)(2)の対応件数は30件まで。	様式１ Q&Aシート

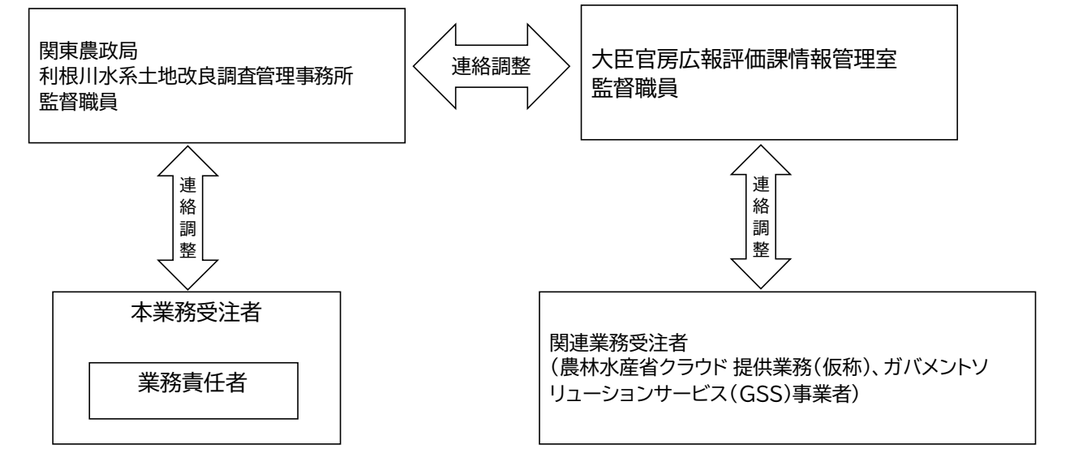
表については、以下省略

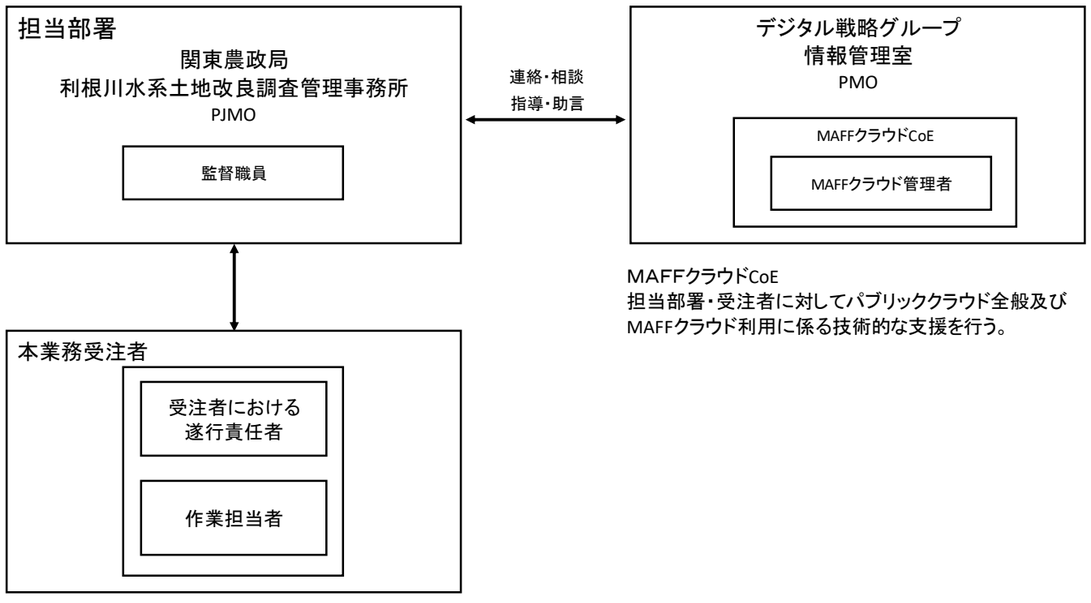
令和５年度　基幹水利施設保全管理対策　農業水利ストック情報データベースシステム運用保守・改修及びクラウドサービス提供業務　仕様書（令和４年９月 20 日付け公告）新旧対照表

修　正　後

別紙7

システム構成図における専用ネットワーク接続（PMO調達）に関する作業体制図



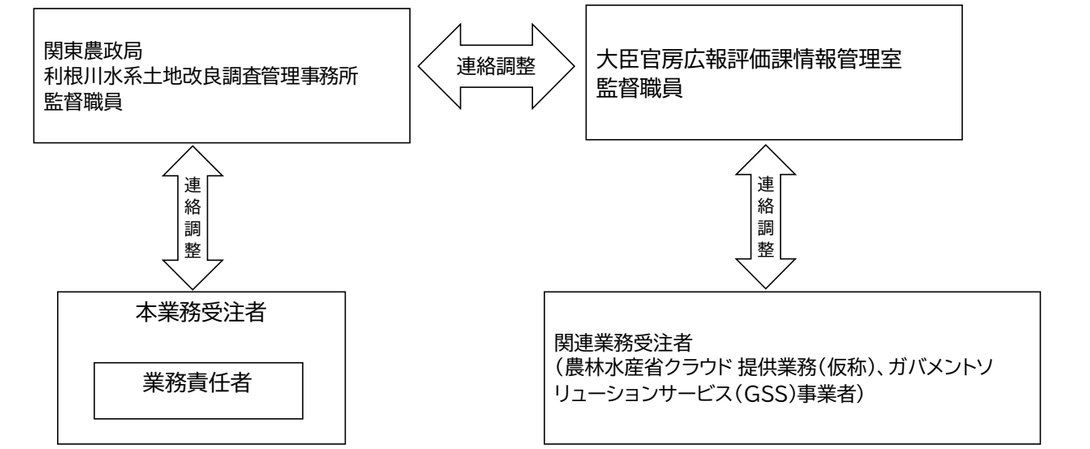


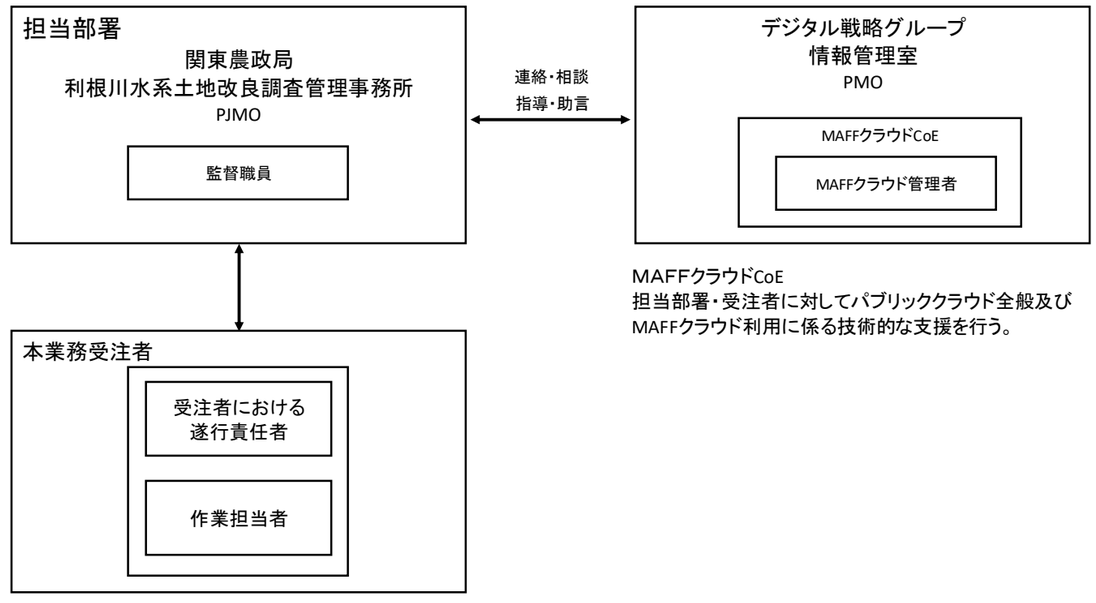
MAFFクラウドCoE
担当部署・受注者に対してパブリッククラウド全般及び
MAFFクラウド利用に係る技術的な支援を行う。

現　行

別紙5

システム構成図における専用ネットワーク接続（PMO調達）に関する作業体制図





MAFFクラウドCoE
担当部署・受注者に対してパブリッククラウド全般及び
MAFFクラウド利用に係る技術的な支援を行う。

修　正　後

別紙8

ソフトウェア構成

WEBサーバ、APDBサーバに導入するOS、ソフトウェア等の詳細なバージョンについては、発注者と協議の上、決定する。

ソフトウェア構成			WEBサーバ	APDBサーバ	BIツールサーバ	バックアップストレージ
No	カテゴリ	名称	仮想	仮想	仮想	仮想
1	OS	Red Hat Enterprise Linux 8(64bit)	●	●	-	-
2		Windows Server	-	-	●	-
3	Web機能	Apache http Server 2.4	●	-	-	-
4		OpenSSL 1.1.1	●	-	-	-
5	AP機能	Apache Tomcat 9	-	●	-	-
6		Open JDK(Red Hat) 11	-	●	-	-
7		Tableau Server	-	-	●	-
8		Tableau Desktop	-	-	●	-
9	DB機能	PostgreSQL 11	-	●	-	-
10	ウィルス対策機能	ESET Server Security for Linux	●	●	-	-
11		ESET Server Security for Windows	-	-	●	-
12	システム監視機能	クラウド側提供サービス	●	-	-	-
13	バックアップ機能	クラウド側提供サービス	●	●	-	●

なお、ソフトウェアについては、一般的に普及されたソフトであり、サポート期限についても十分な期間があるものを選定すること。
また、脆弱性による問題が発生しないように適切に管理すること。

別紙9

過年度ディスク増加量

過年度ストックDBサーバディスク使用量、増加量

サーバ	分類	パーティション	パーティション別 全体量(GB)	パーティション別 使用量(GB)	パーティション別 年間増加量(GB)	分類別 全体量(GB)	分類別 使用量(GB)	分類別 年間増加量(GB)	分類別 月最大増加量(GB)	分類別 日最大増加量(GB)
WEB	EBS提供	/	100.0000	47.0000	38.0000	100.0000	47.0000	38.0000	22.0000	0.7333
	EC2標準提供	/dev	3.8000	0.0000	0.0000	15.2000	0.3780	0.2660	0.0475	0.0016
		/dev/shm	3.8000	0.0000	0.0000					
		/run	3.8000	0.3780	0.2660					
		/sys/fs/cgr	3.8000	0.0000	0.0000					
APDB	EBS提供	/	100.0000	27.0000	1.0000	985.0000	362.0000	36.4000	29.8500	0.9950
		/data2	885.0000	335.0000	35.4000					
	EC2標準提供	/dev	16.0000	0.0000	0.0000	64.0000	0.0588	0.4800	0.8000	0.0267
		/dev/shm	16.0000	0.0008	0.0000					
		/run	16.0000	0.0580	0.4800					
		/sys/fs/cgr	16.0000	0.0000	0.0000					

※期間：2021/04/01 ～ 2022/04/01
※「日最大増加量(GB)」は、「月最大増加量(GB)」÷30で計算。

現　行

別紙6

ソフトウェア構成

WEBサーバ、APDBサーバに導入するOS、ソフトウェア等の詳細なバージョンについては、発注者と協議の上、決定する。

ソフトウェア構成			WEBサーバ	APDBサーバ	BIツールサーバ	バックアップストレージ
No	カテゴリ	名称	仮想	仮想	仮想	仮想
1	OS	Red Hat Enterprise Linux 8(64bit)	●	●	-	-
2		Windows Server	-	-	●	-
3	Web機能	Apache http Server 2.4	●	-	-	-
4		OpenSSL 1.1.1	●	-	-	-
5	AP機能	Apache Tomcat 9	-	●	-	-
6		Open JDK(Red Hat) 11	-	●	-	-
7		Tableau Server	-	-	●	-
8		Tableau Desktop	-	-	●	-
9	DB機能	PostgreSQL 11	-	●	-	-
10	ウィルス対策機能	ESET Server Security for Linux	●	●	-	-
11		ESET Server Security for Windows	-	-	●	-
12	システム監視機能	クラウド側提供サービス	●	-	-	-
13	バックアップ機能	クラウド側提供サービス	●	●	-	●

なお、ソフトウェアについては、一般的に普及されたソフトであり、サポート期限についても十分な期間があるものを選定すること。
また、脆弱性による問題が発生しないように適切に管理すること。

別紙7

過年度ディスク増加量

過年度ストックDBサーバディスク使用量、増加量

サーバ	分類	パーティション	パーティション別 全体量(GB)	パーティション別 使用量(GB)	パーティション別 年間増加量(GB)	分類別 全体量(GB)	分類別 使用量(GB)	分類別 年間増加量(GB)	分類別 月最大増加量(GB)	分類別 日最大増加量(GB)
WEB	EBS提供	/	100.0000	47.0000	38.0000	100.0000	47.0000	38.0000	22.0000	0.7333
	EC2標準提供	/dev	3.8000	0.0000	0.0000	15.2000	0.3780	0.2660	0.0475	0.0016
		/dev/shm	3.8000	0.0000	0.0000					
		/run	3.8000	0.3780	0.2660					
		/sys/fs/cgr	3.8000	0.0000	0.0000					
APDB	EBS提供	/	100.0000	27.0000	1.0000	985.0000	362.0000	36.4000	29.8500	0.9950
		/data2	885.0000	335.0000	35.4000					
	EC2標準提供	/dev	16.0000	0.0000	0.0000	64.0000	0.0588	0.4800	0.8000	0.0267
		/dev/shm	16.0000	0.0008	0.0000					
		/run	16.0000	0.0580	0.4800					
		/sys/fs/cgr	16.0000	0.0000	0.0000					

※期間：2021/04/01 ～ 2022/04/01
※「日最大増加量(GB)」は、「月最大増加量(GB)」÷30で計算。