

食品表示ウォッチャーシステム G C P 移行業務仕様書

この仕様書は、契約書に定めるものを除くほか、委託業務に関し必要な事項を定める。

1 業務名

食品表示ウォッチャーシステム GCP 移行業務

2 委託業務期間

令和 8 年 1 1 月 1 日から令和 9 年 2 月 2 8 日まで

3 実施場所

徳島県庁万代庁舎（徳島県徳島市万代町 1 丁目 1 番地）内及び受託者社内

4 システム概要及びシステム情報

(1) 概要

本県では、食品表示の適正化を推進するため、消費者目線で食品表示のモニタリング調査を行う「食品表示ウォッチャー」（以下、「ウォッチャー」という。）を設置し、ウォッチャーから報告された調査結果に基づき、県職員が事業者への指導等を行うことで、食品表示の監視体制を構築している。

ウォッチャーからの報告については、調査結果等をスマートフォン等から報告できる「食品表示ウォッチャーシステム」を運用しており、県職員はシステムから、調査結果の確認や集計及び「食品表示 G メンシステム」との連携データの出力等を行うことができる。

(2) システム情報

ア サーバ

ネットワーク構成図（別紙 1）を参照。

イ 開発言語及びデータベース

開発言語は PHP、データベースは MySQL を使用。

ウ ブラウザ

ブラウザは Google Chrome、Microsoft Edge に対応。

5 業務目的

本業務は、県が保有する食品表示ウォッチャーシステムについて、現在稼働している徳島県自治体情報セキュリティクラウド（以下「現クラウド」という。）上の環境から、Google Cloud Platform（以下「GCP」という。）上の環境へ移行し、継続して安定運用できる環境を整備することを目的とする。

なお、本業務はシステム機能そのものの刷新を目的とするものではなく、現行システムの機能、利用形態及び運用を原則維持したうえで、必要な環境移行、データ移行、試験、切替及び関連資料の整備を行うものである。

6 業務内容

(1) GCP 環境設計

- ア 本システムを稼働させるための徳島県 GCP 環境の設定を把握の上、GCP 設計書としてとりまとめること。なお、詳細な設定内容は県と協議の上で決定すること。
- イ バックアップを取得できるように設計すること。取得頻度や保管世代数は県と協議の上で決定すること。

(2) GCP への移行

- ア システムのサーバを、現クラウドから GCP に移行すること。なお、移行対象は、本番サーバ1台である。
- イ 現クラウドに保存しているすべてのデータを抽出し、不足なく新クラウドへ移行すること。
- ウ 現行の機能は原則そのまま移行すること。
- エ ネットワーク設定及びドメイン等の設定等は、県と協議の上で設定すること。

(3) 結合テスト

- ア 稼働状態としたシステムについて、総合試験を実施し、システムに瑕疵がないことを確認すること。
- イ 稼働状態としたシステムについて、次のセキュリティ要件を満たすことを確認すること。
 - (ア) 利用者に応じて、システムへのアクセス方法や、システムにおいて利用できる情報及び機能を制御できる仕組みが整備されていること。
 - (イ) パスワードに係る要件を満たさない値が設定できない仕組みとなっていること。

7 業務体制等

(1) 業務環境

- ア 業務の実施に当たっては、「情報セキュリティに関する特記事項」を遵守し、適切な作業場所を確保するものとする。
- イ 受託者はリモート保守環境を利用することで、受託者社内から業務の一部を実施することができるものとする。ただし、二要素での認証を行うなど、受託者以外の者が、本システムに不正にアクセスできない仕組みとすること。また、アクセス履歴について常に監視・確認できること。

(2) 業務体制

- ア 県担当者に適切に進捗を報告し、協議しながら実施すること。
- イ 業務の実施に当たって、システムの運用保守業務受託者との協議及び調整が必要な場合は、受託者が主体となって十分な調整を行うことのできる体制をとり、運用保守業務及びそれに伴い発生する改修等に関して支障とならないようにすること。

(3) セキュリティ要件

- 業務の実施に当たって、次のセキュリティ要件を満たすこと。
- ア 県が取り扱う情報の受託者における目的外利用を行わないこと。
- イ 業務に従事する者に対しては、利用者ごとに必要最小限の権限のアカウントを割り当て、不要となったアカウントは速やかに削除又は無効化すること。また、管理者権限を持つアカウントについて、操作記録を残すこと。

- ウ プライバシーマーク及び情報セキュリティマネジメントシステム（ISMS）に準拠した体制を確保すること。また、県の求めに応じて証明書の写しを提出すること。
- エ 情報の管理、保管及び廃棄に関する取扱い手順及び情報セキュリティ対策の実施方法を定めること。
- オ システムを運用する上で必要十分なリソースを用意するとともに、関係法令を遵守すること。また、利用するサービス等に応じたセキュリティ対策及び脆弱性対策を講ずること。
- カ 情報は、日本の法令の範囲内で運用できる場所にて取り扱うこと。
- キ 定期的にログファイルを確認しシステム稼働状況を確認するとともに、各種ログは適切に管理・保管すること。併せて、時刻同期が行われているか確認すること。
- ク システム内のデータ及び通信経路は暗号化し、暗号化に用いる SSL サーバ証明書等は適切に管理・保管すること。
- ケ システムがクラウドサービス内の他のネットワークと分離されていることを確認するとともに、セキュリティ要件の異なるネットワーク間の通信を監視・制御すること。
- コ バックアップデータの適切な保管及び復旧手順を整備し、障害発生時に速やかな復旧が可能な運用体制を確保すること。また、サーバ障害発生時には、速やかに原因を特定し、復旧手順に従いシステムを復旧できること。
- サ 受託者において発生した情報セキュリティインシデントによる被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）を定めること。
- シ 障害の未然防止のため、設定の誤りや設定漏れを防止するための対策を講ずること。
- ス 厳格な変更管理プロセスに基づき、システムの完全性を維持すること。
- セ 設定変更、バージョンアップ、メンテナンス等、システムに関して変更が生じる場合には、事前に県に通知をすること。また、当該変更によって事業継続性に影響がないかどうかを確認すること。
- ソ 新たなサービスを利用する場合は、あらかじめ県の承認を受けること。また、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は、機能及び利用者を管理・制限すること。
- タ 情報セキュリティ対策の履行が不十分な場合、改善について協議を行い、合意した改善策を実施すること。
- チ 受託者がその役務内容を一部再委託する場合は、県が受託者に求めるセキュリティ要件が再委託先においても十分に確保されることを受託者の選定基準にて担保するとともに、選定した再委託先の情報セキュリティ管理体制について、県の求めに応じて資料を提出し、県の承認を受けること。なお、再委託に当たっては、クラウドサービス利用基準及び受託者の選定基準に従って承認の可否を判断する。

(4) 県への報告

- 業務開始に当たって、次の内容について県に報告すること。
- ア 業務に従事する者の情報セキュリティに係る資格及び教育・訓練の状況または計画
- イ 情報の管理・保管方法
- ウ 情報セキュリティ対策の実施内容及び管理体制

8 費用負担

業務の実施に必要な機材等（リモート保守環境で必要となる費用を含む）は、受託者の負担とする。

ただし、現クラウド及び GCP 利用料は県が負担する。

9 運用開始時期

令和 9 年 3 月 1 日から（ただし令和 9 年 2 月 1 日からテスト運用期間とする）

10 成果物

業務の履行を確認するため、次のデータを書面または電磁的記録によって県に提出すること。

- (1) サーバ構築手順書
- (2) GCP 設計書
- (3) 環境設定シート
- (4) 結合テスト結果報告書

11 その他

- (1) 業務の実施に当たっては、事前に県と協議し承認を得ること。
- (2) 業務委託期間中及び運用開始後 6 か月以内に、システムに障害が発生した場合は、受託者において切り分け作業や状況報告等、復旧作業の責任を負うこと。
- (3) この仕様書に定めのない事項については、必要の都度、県と受託者が協議して定めるものとする。