

目次

1.	非機能要件.....	4
1.1.	システム規模要件	4
1.1.1.	業務処理件数等.....	4
1.1.2.	保持する想定データ件数	4
1.1.3.	システム利用者数	5
1.2.	可用性要件	5
1.2.1.	システム利用時間	5
1.2.2.	稼働率	5
1.2.3.	目標復旧水準	5
1.3.	性能・拡張性要件	5
1.3.1.	性能要件.....	6
1.3.2.	拡張性要件	6
1.4.	保守性要件	6
1.4.1.	バックアップ	6
1.4.2.	リストア	7
1.4.3.	システム保守	7
1.4.4.	文字集合・文字コード.....	7
1.5.	セキュリティ要件	7
1.5.1.	個人情報保護	8
1.5.2.	アクセス権限	8
1.5.3.	不正侵入防止	8
1.5.4.	ウィルス対策	8
1.5.5.	脆弱性対策	9
1.5.6.	改ざん防止	9
1.5.7.	データの暗号化.....	9
1.5.8.	監査証跡（アクセスログ）	9

2.	全体システム構成.....	9
2.1.	全体システム構成イメージ.....	9
2.1.1.	通信帯域.....	10
2.1.2.	インターネット接続	10
2.1.3.	時刻同期.....	10
2.1.4.	SMTP サーバの利用	10
2.2.	ハードウェア要件	10
2.3.	ソフトウェア要件	11
2.4.	本県が提供する「統合サーバ」を使用する場合の、統合サーバ責任者の責任範囲	11
3.	運用保守業務委託要件	12
3.1.	運用保守計画・体制.....	12
3.1.1.	運用保守計画	12
3.1.2.	運用保守体制	12
3.2.	運用要件	13
3.2.1.	問い合わせ対応.....	13
3.2.2.	リモート作業	13
3.2.3.	運用管理.....	13
3.2.4.	バックアップ	15
3.2.5.	報告	15
3.2.6.	正常時システム運用	15
3.2.7.	障害時の運用	15
3.2.8.	システム利用時間帯	16
3.2.9.	運用管理システムの利用	16
3.3.	保守要件	16
3.3.1.	ソフトウェア保守	16
3.3.2.	ソフトウェア保守対象.....	17
3.3.3.	ソフトウェア改修・予防措置.....	17

3.3.4.	ソフトウェア構成管理	17
3.3.5.	新健康管理システムにおける保守の提供	18
3.3.6.	新健康管理システムのアップデート対応（法改正含む）	18
3.4.	サービスレベル合意（SLA）	18
4.	移行要件	20
4.1.	データ移行要件	20
4.1.1.	移行範囲	20
4.1.2.	移行設計	20
4.1.3.	作業分担	20
4.1.4.	現行健康管理システムの設計書提供	21
4.1.5.	移行データ確認	21
4.1.6.	移行データ変換	21
4.1.7.	移行リハーサル・移行実施	21
4.1.8.	移行対象データの参考	21
4.2.	システム移行要件	21
4.2.1.	新健康管理システムの本稼働	21
4.3.	システム移行における留意事項	22
5.	マニュアル・操作研修	22
5.1.	マニュアル	22
5.2.	操作研修	23
6.	その他の留意事項	23
6.1.	業務の引継ぎに関する事項	23

1. 非機能要件

新健康管理システムで取扱うデータは身体等の個人情報が含まれるため、損失、漏洩等に配慮が必要である。ここでは、新健康管理システムに求められる非機能要件について示す。

提案にあたってはライフサイクル管理（基本設計、詳細設計、開発・単体テスト、テスト、移行、運用、保守、システム改修、システム更新、撤去等）における各段階での主要作業と期間および関係者の役割を定める

1.1. システム規模要件

以下の規模要件を満たすこと。

1.1.1. 業務処理件数等

下表に現行健康管理システムの処理件数を示す。

（提案にあたっては、将来的な増加を考慮すること。）

◆管理対象者数 10,000 人

正規職員

会計年度任用職員

その他（再任用職員、特定任期付職員、臨時的任用職員、特別職等）

◆管理対象組織

知事部局（企業局、各種委員会等含む）

教育委員会（事務局、出先機関、県立学校含む）

※小中学校や警察本部は対象外

表 1 現行健康管理システムの処理件数

処理	件数	備考
職員データ取込み	10,000	4 月
名簿作成	10,000	4 月
健診結果データ取込み	10,000	5 月以降随時

1.1.2. 保持する想定データ件数

表 2 表 1 の処理件数より算出

マスタ名	データ件数
健診マスタ DB	10,000 件

1.1.3. システム利用者数

現時点でのシステム利用者数を示す。新健康管理システムでも同程度の利用を想定する。(提案にあたっては、将来的な増加を考慮すること。)

ユーザ数

業務担当者 15 人 (給与厚生課、教育政策課)

健診受診者 10,000 人

端末台数 約 10,000 台

利用者数 約 10,000 人

1.2. 可用性要件

新健康管理システムは次に示す可用性要件を満たせること。

ただし、可用性要件は本県の統合サーバ上に構築することを想定している。

おって、別途ハードウェアが必要となる場合は、本県と協議の上、要件を策定すること。

1.2.1. システム利用時間

新健康管理システムは、原則 24 時間 365 日の稼働とする。

ただし、バックアップ、保守メンテナンスによるシステム停止を除く。

1.2.2. 稼働率

年間のシステム稼働率の目標値を定めること。本県で想定する目標値は「3.4. サービスレベル合意 (SLA)」を参照のこと。

1.2.3. 目標復旧水準

(1) 目標復旧地点 (RPO)

業務停止を伴う障害が発生した場合、最新のバックアップ取得時点までのデータ復旧を目標とすること。本県で想定する目標値は「3.4. サービスレベル合意 (SLA)」を参照。

(2) 目標復旧時間 (RTO)

業務停止を伴う障害が発生した場合のシステム復旧に係る時間の目標。本県で想定する目標値は「3.4. サービスレベル合意 (SLA)」を参照。

(3) 目標復旧レベル (RLO)

業務停止を伴う障害が発生した場合、システム全機能の復旧を実施すること。本県で想定する目標値は「3.4. サービスレベル合意 (SLA)」を参照。

1.3. 性能・拡張性要件

新健康管理システムは、次に示す性能・拡張性要件を満たすこと。

1.3.1. 性能要件

(1) レスポンス

レスポンスタイム等、著しい性能劣化を判定できる指標を設定すること。

なお、本県で想定する目標値は「3.4. サービスレベル合意（SLA）」を参照のこと。

また、データの増大によりシステム稼働後徐々にレスポンスが悪化していくことが懸念されるため、安定したレスポンスが得られるように工夫すること。

(2) ユーザーインターフェース

G UI を利用した簡易な操作での作業を可能とすること。

(3) アクセシビリティ

視覚障害を有する職員、その他の配慮を要するユーザへの情報アクセシビリティへの対応を検討すること。

1.3.2. 拡張性要件

(1) サイジング

本稼働時のサイジングは、毎年 10,000 名分、稼働後 10 年間を想定すること。

なお、将来の利用者数増加やアクセス数に増加に対応可能なシステムの性能を保持していること。

(2) システム改修への柔軟な対応

業務内容の変更に柔軟に対応できるようにするため、構造化、部品化されているシステムであること。

なお、コード・テーブル等定期的に発生する軽微な変更についても容易に行うことができるようにすること。

また、対応のためのコストを最小限に抑えられる方式を採用することが望ましい。

(3) 他システムとの連携対応

他システムとの新たな連携が生じた場合、極力改修作業が発生しない仕組みや方式を確保すること。

なお、本県が提供しているサービス連携基盤の利用を前提に考えること。

1.4. 保守性要件

新健康管理システムは次に示す保守性要件を満たせること。

なお、障害発生時には、業務データの損失を防止し、かつ業務データの整合性を保持できること。

1.4.1. バックアップ

(1) バックアップ計画の設計

信頼性や業務継続性を維持するため、障害発生時の決められた目標復旧時点へデータ回復ができるようにバックアップ計画を立てること。

(2) バックアップ取得間隔

バックアップ取得間隔は、障害発生時に決められた目標復旧時点へ戻せる状態にできる頻度

とすること。

なお、自動スケジュールより日次で実施されるおよび、業務運用状態に応じて手動でのバックアップが実施できること。

(3) バックアップ範囲

本県が提供する統合サーバを使用してシステム運用する場合は、統合サーバのサービスとしてバックアップ機能が利用できる。その他の方法でバックアップが必要な場合は、受託者にて行うこと。

(4) バックアップ実施時間帯

バックアップ処理が本来性能に影響を及ぼさないように実施時間帯を設計すること。

(5) バックアップ保存期間

日次で保存したデータベースのデータは7世代保存すること。

(6) バックアップ保存場所

取得したデータベースのバックアップは、仮想サーバ上に保存すること。

なお、本県が提供する統合サーバを使用する場合、仮想サーバのミラーリングおよび遠隔地バックアップが統合サーバで実施される。

1.4.2. リストア

障害が発生した場合、統合サーバ管理者（本県、DG課）および統合サーバ運用保守業者（以下、統合サーバ管理者と統合サーバ運用保守業者を合わせて統合サーバ責任者という）と協力し、新健康管理システムを速やかに復旧できること。

復旧を行う際は、最新の定期バックアップ時点とすること。

1.4.3. システム保守

システムの不具合が発生した場合、原因の追及やシステムの変更・修正が容易であること。

なお、不具合の伴うサービスの停止があった場合は、SLAに基づいて迅速に再開すること。本県で想定する目標値は「3.4. サービスレベル合意（SLA）」を参照のこと。

1.4.4. 文字集合・文字コード

(1) 文字集合

システム使用可能な文字集合は「JIS X 0213」とする。

(2) 文字コード

文字コードは「UTF-8」を検討している。

他システムとの連携においては、適切な文字コードの変換を行うこと。

なお、新健康管理システムでは外字を扱わないが、他システムからの連携データに外字が含まれる場合は、変換して取り込むこと。

また、変換文字については本県と協議し、詳細を決定すること。

1.5. セキュリティ要件

山口県情報セキュリティポリシー（情報セキュリティ対策基準）に基づき、システム開発・運用保

守並びにセキュリティ対策を実施すること。

なお、新健康管理システムで取扱う情報資産は個人情報を含むものであることを十分に考慮した開発、運用および保守を行うこと。

また、以降の各項目について、必要なレベルや実装する機能を本県と協議し、詳細を決定すること。

1.5.1. 個人情報保護

(1) 本業務受託に関する要件

「山口県情報セキュリティポリシー」

(<https://www.pref.yamaguchi.lg.jp/soshiki/33/147965.html>) のとおりとする。

なお、同ポリシーは改定される場合があるので、都度最新版の内容に従うこと。

(2) 新健康管理システムに関する要件

(ア) 個人情報データの転送は、使用プロトコルにかかわらず、県庁 LAN 等機密が確保されたネットワークのみを経由して行うこと。

(イ) 個人情報データについては、必要最小限の者のみ利用できることとし、当該利用者には、利用者ごとのアカウントとパスワードを設定すること。

1.5.2. アクセス権限

(1) アクセス権限設定

個人情報データごとに規定する手段より、アクセス権限を設定できること。

(2) 個人情報データの持ち出し

サーバに保管されている個人情報データについては、正当な権限を持った者が新健康管理システムを用いて行う以外の方法により、記録媒体やネットワークを通じて複写または転送等出来ないよう措置すること。

1.5.3. 不正侵入防止

(1) 利用者の限定

新健康管理システムへの不正侵入を防ぐため、新健康管理システムを利用できる者を限定すること。

(2) 利用者権限設定

アカウント毎に、アクセスできる機能（利用者権限）を設定できること。

(3) 不正アクセスを防ぐ仕組み

利用者等が権限外の機能に不正にアクセスしないような仕組みを構築すること。

(4) 不正ログイン試行検知

システムにアクセス許可のないユーザが一定期間内に複数回のログインを試みようとした場合は検知可能であること。

1.5.4. ウィルス対策

ウィルスやマルウェア等に対する対策を講じること。ウィルス対策は受託者の責任において行うこと。

なお、仮想サーバについて、統合サーバの標準としてウィルス対策ソフトウェアのライセンスを提供することが可能で、提供可能なウィルス対策ソフトは、WindowsServer であれば「APEXONE」、Linux サーバであれば「ServerProtect」である。

これら以外のウィルス対策ソフトを利用する場合は受託者の責任・負担で準備・導入・設定を行うこととし、その旨、企画提案書にその旨明記し、導入にあたっては統合サーバ責任者と事前に協議を行うこと。

1.5.5. 脆弱性対策

脆弱性対策のため使用するソフトウェアの定期的なアップデートを受託者の責任において実施すること。

1.5.6. 改ざん防止

原本性保証は不要だが、第三者により情報が改ざん、破壊されることのないよう対策すること。

1.5.7. データの暗号化

特に重要な情報については、サーバと職員用端末間での通信時およびダウンロードした電子ファイルについて、暗号化やパスワードによる保護を行うこと。

原則、HTTPS 通信には、SSL (SecureSocket Layer) の暗号化を施すこと。

1.5.8. 監査証跡（アクセスログ）

各サーバの証跡（ログ）として、イベントログ、エラーログおよびアクセスログ等を記録し、保持する設定とすること。

なお、ログの保持期間については、本県と協議の上、決定すること。

また、新健康管理システム内のログについては、情報セキュリティポリシーの観点から、変更、削除ができないように設定すること。

2. 全体システム構成

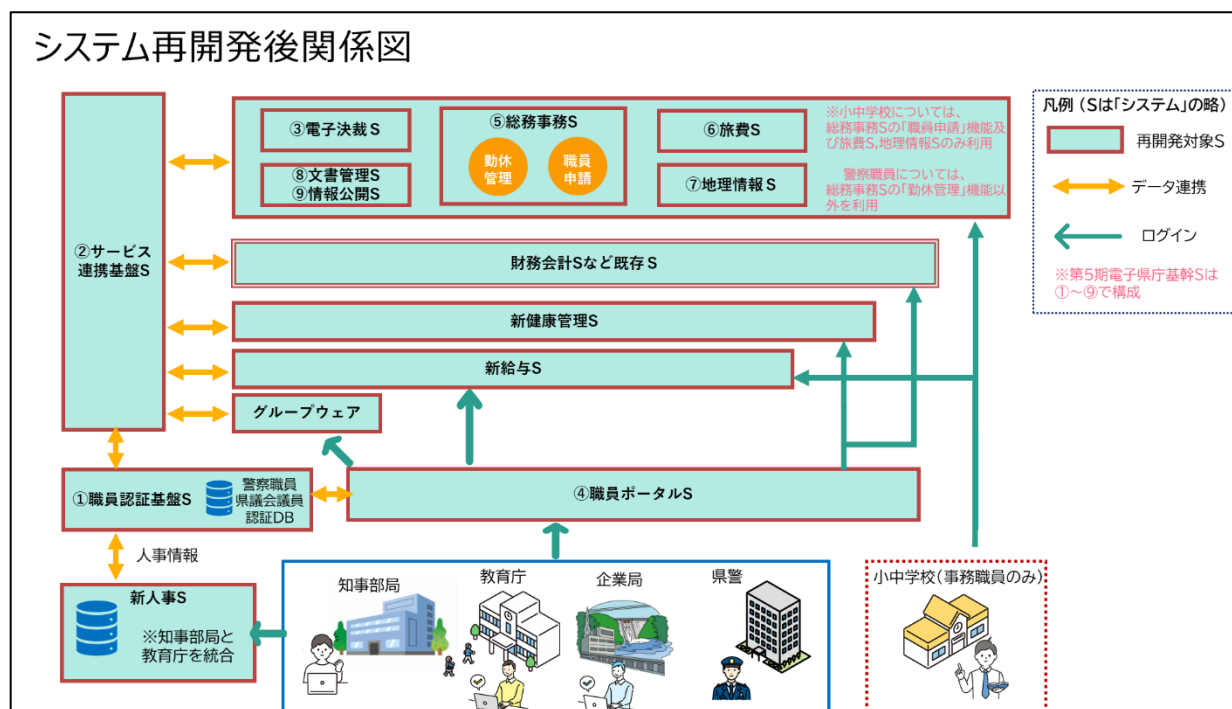
ハードウェアや基本ソフトウェアは、本県が提供する「統合サーバ」を使用することが可能である。

よって、新健康管理システムの全体構成は、本県が用意する統合サーバの使用を原則とする。

ただし、リモート保守等を提案する場合、ネットワーク機器等に係る当該費用（回線費用等含む）は予算に含めること。

2.1. 全体システム構成イメージ

新健康管理システムの構成イメージを図 1 に示す。



2.1.1. 通信帯域

県庁 LAN の帯域は、最大で次のとおりである。他のシステムも帯域を共用しているため、過大なトラフィックが流れないように配慮すること。

庁内 LAN 1Gbps（一部 100Mbps）

出先事務所 10Mbps～1Gbps

2.1.2. インターネット接続

各サーバは、インターネットへの接続を不可とし、県庁 LAN の利用を前提とする。

2.1.3. 時刻同期

時刻同期に関しては、本県の指定する時刻同期環境を使用すること。

2.1.4. SMTP サーバの利用

メール送信に関しては、本県の指定する SMTP サーバを使用すること。

2.2. ハードウェア要件

(1) クライアント端末

クライアント端末は原則として既設の庁内 LAN 接続端末（一人 1 台パソコン）を利用する。

よって、他システムへの影響およびインストール作業や脆弱性対応等に係る作業負担等を考慮し、原則としてクライアント端末に対するソフトウェアやプラグイン等のインストール作業は不要とすること。また、システムを利用するブラウザは「Microsoft Edge」を前提とする。

(2) サーバ、ストレージ

新健康管理システムが稼働するためのサーバ、ストレージ等のハードウェアについては、本県の統合サーバを提供できる。

この場合、本業務で必要となるリソースを提示すること。また、OS ライセンスとして「Windows Server 2019」、「Windows Server 2022」、「Windows Server 2025」、「Red Hat EnterpriseLinux 9」等の提供が可能である（Windows Server 2025 は今後調達予定である）。

(3) ロードバランサ（負荷分散装置）

統合サーバにロードバランサは装備していないため、必要であれば準備すること。

2.3. ソフトウェア要件

(1) 新健康管理システム

新健康管理システムにおいては、原則として Web アプリケーションとすること。

(2) 個別ソフトウェア

新健康管理システムで使用する個別のソフトウェアは、不具合に対して迅速な対応が可能なサポート提供があること。

また、基幹システムに多くの導入実績を持ち、オープンな標準的技術を使用しているものを提供すること。

提供ソフトウェアはバージョンアップも考慮し安定稼働可能なバージョンを導入することとし、最新版を適用するものは本県と協議の上決定すること。

(3) オープンソースソフトウェア

オープンソースソフトウェアを採用する場合、脆弱性に対するセキュリティ更新プログラムが提供されるものとし、不具合については受託者にて対応すること。

(4) データベースソフトウェア

データベースソフトウェアは、受託者にて必要なライセンスを準備すること。また、Oracle 社のデータベースは使用しないこと。

(5) ソフトウェアの重複防止

統合サーバで提供予定のソフトウェアとの整合を図り、ソフトウェアの重複が発生しないよう努めること。

(6) 開発用ソフトウェア

開発用のソフトウェアは受託者にて準備すること。

2.4. 本県が提供する「統合サーバ」を使用する場合の、統合サーバ責任者の責任範囲

統合サーバはプライベートクラウドとして提供している。

よって、統合サーバ責任者の責任範囲はハードウェア、仮想化ネットワーク基盤のインフラとなり、本業務受託者の責任範囲は OS 以上とする。

なお、システム動作確認、試験については、その際必要に応じて統合サーバ責任者と協議を行い作業すること。

また、障害発生、仕様変更等により、設定変更の必要が発生した場合も同様とする。

3. 運用保守業務委託要件

新健康管理システムの運用管理作業は、受託者と本県が共同で実施し、今回開発対象となる業務アプリケーションと業務データベースの範囲で運用を行う。

業務のデータベースバックアップ管理等、業務システムに関する知識を要する部分の運用は、受託者が本県職員を支援すること。

3.1. 運用保守計画・体制

3.1.1. 運用保守計画

運用計画を作成し、本県の承認を得ること。また、計画作成後に随時の事案が生じた場合、本県と協議の上で実施事項を見直し、必要に応じ計画を変更すること。

3.1.2. 運用保守体制

運用保守業務において、受託者は本県の運用の支援および新健康管理システムを確実に維持管理するため次の点を踏まえ体制を整えること。

- (1) 健康管理業務について十分に理解し、必要な事項を適切に反映できる体制とすること。
- (2) 作業の円滑な実施と品質の確保を実現するために必要な体制を整備すること。
- (3) 導入パッケージおよび本県構築内容を十分に把握し、適切に保守できる体制とすること。
- (4) 運用管理体制や連絡体制を文書で作成し、本県の承認を得ること。
- (5) 体制等に変更が発する場合は、速やかに文書を再提出し承認を得ること。
- (6) 運用設計書（運用保守業務計画書）に運用・保守手順を定め新健康管理システムの運用保守を行うこと。

本県が想定する「運用保守従事者の役職・役割（案）」を基に、運用設計工程において運用保守従事者の役職・役割の取り決めること。

表 3 運用保守従事者の役職・役割（案）

役職	役割
責任者	・ 運用保守における変更や対応への承認
管理者	・ 本県担当者と運用保守における変更や対応への調整
担当者	・ 新健康管理システムの監視 ・ 新健康管理システムの仕様変更、障害・不具合等の対応 ・ 本県職員から問い合わせ対応 ・ 運用状況報告書（運用保守業務実績報告書）の作成 等
品質責任者	・ 納品物の検査 ・ 保守手順書の検査

3.2. 運用要件

3.2.1. 問い合わせ対応

運用保守業務は、原則営業日(年末年始・祝日を除く)の 8:30～17:15 で行うこと。

ただし、翌日のシステム利用に影響を与えると思われる場合は、本県と協議の上、対応を決定する。

なお、状況に応じて時間延長および休日対応を要することがあるため、留意し対応すること。

(1) 受付

表 4 に示す通り、日々のシステム運用を円滑に進めるため、電話や電子メール等による受付窓口を有すること。

表 4 受付窓口

受付窓口	要件
電話	原則 営業日 8:30～17:15
電子メール等	24 時間 365 日

(2) 記録/報告

問い合わせ・要求・依頼内容(日時、内容、連絡者、回答内容)等を記録し、運用状況報告書(運用保守業務実績報告書)にて、本県に定例的に報告すること。

3.2.2. リモート作業

運用保守業務においてリモート接続による作業は原則認めていない。

ただし、セキュリティポリシーに準拠し、かつ費用面でメリットがある場合はその限りではない。

その場合、新健康管理システム以外の環境に接続できないようなネットワーク設定にする等のセキュリティ上必要な措置を前提とする。

なお、必要となるリモート回線(インターネットを経由しない閉域網や専用線に限る。)、ネットワーク機器、端末等は受託者が準備すること。

リモート保守を導入・実施するにあたっては、別途提示する「リモート保守チェックリスト」に記載する内容を満たすことを条件とし、それに要する費用等は全て受託者の負担とする。

なお、「リモート保守チェックリスト」については「入札説明書」に記載する「入札参加資格確認通知」により入札への参加を認められた者でかつ配布を希望する者にのみ個別に配布するものとする。

3.2.3. 運用管理

(1) 構成管理

(ア) 個人情報データの転送は、使用プロトコルにかかわらず、県庁 LAN 等機密が確保されたネットワークのみを経由して行うこと。

(イ) 定期的な修正パッチの適用やバージョンアップは、システムへの影響や作業内容を事前に

協議し、適用可否を判断するものとする。必要と判断した場合は、迅速に適用を行うこと。

(ウ)新健康管理システムにおいて、最新の構成情報（ミドルウェア、パッケージの適用バージョン・リビジョン 等）を管理すること。

(エ)ドキュメント（設計書、作業手順書、マニュアル 等）のバージョン、所在等を管理すること。

また、変更が生じるものについては適宜反映し維持・管理すること。

(2) システム稼働管理

(ア)システムの稼働統計（CPU 使用率、MEM 使用率、ディスク使用率等）を取得し、利用状況等を調査、確認すること。

(イ)なお、本県が提供する統合サーバの稼働監視や稼働管理は統合サーバ運用保守業者が行う。

(3) セキュリティ管理

(ア)セキュリティインシデント発生時の対応指針、対応体制、対応手順について、事前に定めておくこと。

(イ)セキュリティインシデントのリスクを低減させる予防策について、実施すること。

(ウ)システムに対するセキュリティチェックを定期的の実施すること。

(エ)業務システムへのアクセスログを必要に応じて調査、報告できること。

(オ)セキュリティパッチの適用等、業務システムの運用管理として必要なセキュリティ対策について設計し整備すること。

(カ)ウィルスが検知された際には、本県へ通知・連絡を行い、速やかにウィルス感染駆除等の対応を実施すること。

(キ)新健康管理システム（OS、ミドルウェア、パッケージ等）に対する脆弱性対策等については「3.3. 保守要件」に従い実施すること。

(4) データ管理

データベース使用率等データベースの状態監視を行い、必要時にはデータベースの再編成、拡張を行うこと。

なお、拡張についてハードウェアのスケールアップが必要な場合は、統合サーバ管理者との協議が必要であるため、留意すること。

(5) 課題管理

運用業務において発生する仕様変更や障害・不具合等の課題について、プロジェクト管理ツール等を活用して、その内容や対応期限等の管理を行うこと。

なお、インターネット接続が必要な場合は本県と協議の上、最大限のセキュリティを考慮したうえ使用すること。

(6) 利用者管理

(ア)利用者管理（アカウントの登録、削除、権限設定）について、画面での更新や CSV 等による一括更新など、新健康管理システムから実施できる処理については本県が実施する。ただし、プログラミングやデータベースを直接操作する必要がある場合は受託者において実施すること。

(イ)本県が実施する場合において、年度末などの大量更新の際にも対応できる簡易な仕組みを提案すること。

(7) ジョブ管理

- (ア)即時実行するジョブについて、実行スケジュールを設計し、複数のジョブ（プログラム、パッチ処理、バックアップ等）の起動・終了が制御できること。
- (イ)メンテナンス等による不定期・臨時に実行するジョブについて、ジョブを実行し、実行結果について確認できること。
- (ウ)ジョブの異常を検知できること。

3.2.4. バックアップ

「1.4. 保守性要件」の「1.4.1. バックアップ」に則り、バックアップ取得時点までの復旧を受託者にて行うこと。

また、セキュリティパッチの適用やバージョンアップを実施する等、システム構成に大きな変更を伴う際には、システム構成の変更前後でシステムバックアップを取得すること。

3.2.5. 報告

本県に対して、運用および保守に関する定期報告会を開催すること。定期報告会は適宜開催し、対面または Web 会議での開催を想定する。随時計画される計画停止（定期バックアップ等の定例運用は除く）は、原則 1 ヶ月前までに本県へ連絡し、実施時期の調整を本県と行い、本県の承認を得た上で実施とすること。

3.2.6. 正常時システム運用

正常時のシステム運用を次に示す。

(1) システムの運用

システムの稼働時間は、24 時間 365 日（システムメンテナンス時間を除く）である。システムメンテナンス時は、サービスの起動や停止は自動又は手動で対応できること。

(2) 随時運用

業務繁忙期や、年次の特例処理等に対しては、臨時のバックアップ処理の実行等、柔軟に対応できること。

(3) システム運用状況の把握

日々の稼働状況を把握できること。

3.2.7. 障害時の運用

障害発生時には、本県の運用担当者および統合サーバ運用管理者と協力して早期の障害復旧に努めるものとする。また、緊急時対応計画を本県と協議して作成し、それを遵守すること。

(1) 障害発生前

(ア)障害発生前、早期復旧のための作業

障害発生時の障害時対応マニュアルを策定すること。

(イ)バックアップ

バックアップデータが、障害復旧に必要な十分なデータであることを定期的に確認すること。

(2) 障害発生時

障害発生時には、本県運用担当者に対して状況を随時報告し、復旧計画について協議すること。なお、障害の原因が特定できない場合、また障害が複合的な要因により発生する場合等、責任の所在が不明確であり、統合サーバ運用保守業者と本業務受託者の間にトラブルが発生した場合、または発生することが予測される場合には、本県が受託者間の調整等を実施し、トラブルの解決にあたるものとする。

(3) 障害対策後

障害復旧後、障害に関する原因、復旧作業の内容および今後の対策について、その詳細を本県に対して報告する。

3.2.8. システム利用時間帯

基本的なシステム利用要件を次に示す。

- (1) システム利用時間については「1.2. 可用性要件」の「1.2.1. システム利用時間」のとおり。
- (2) システム利用時間中は、データの参照・更新・削除が可能であること。

3.2.9. 運用管理システムの利用

統合サーバの稼動に関わる運用管理システムは、統合サーバ管理者が準備する。

統合サーバの運用管理システムの監視項目を次に示す。その他に新健康管理システムとして運用管理システムが必要な場合は、受託者にて開発すること。

表 5 運用システムの利用

#	監視項目
1	Ping 監視
2	リソース監視
3	プロセス監視
4	syslog 監視
5	アプリケーションログ監視
6	Web サーバ監視
7	応答監視（レスポンス監視）
8	ジョブ運用

3.3. 保守要件

新健康管理システムに関する運用保守業務は、今回開発対象となる業務アプリケーションと業務データベースの範囲で保守を行うこと。

3.3.1. ソフトウェア保守

ソフトウェア（新健康管理システム構築のために使用したパッケージ等のアプリケーション）に関する、障害（問題）発生時の迅速な対応、予防対策を行うための保守を実施すること。保守にあたっては、次の点に留意すること。

(1) ソフトウェア不具合対応、修正パッチ対応

納入した全てのソフトウェア製品に関する不具合対応およびセキュリティ対応等の情報収集・調査を行い、新健康管理システムに対する影響の調査および適用の検討を行うこと。その結果、重大な脆弱性や不具合が見込まれる場合等、新健康管理システムの安定稼働に向けてセキュリティパッチ適用の必要がある場合は、その必要性を本県に説明すること。その際、事前に影響調査を実施し、セキュリティパッチの適用に係る安全性を確認した上で、実施に向けた実行計画案を運用設計書（運用保守業務計画書）に反映し、本県の承認を得ること。

(2) ソフトウェアライフサイクル情報の収集およびバージョンアップ対応

新健康管理システムの稼働の前提となる OS やソフトウェア、WEB ブラウザ等全ての製品に関するライフサイクル情報（公式サポート期間、延長サポート期間等の情報）を収集すること。また、収集した情報（サポート切れ等）の新健康管理システムへの影響分析を行うこと。影響分析の結果、バージョンアップや代替策の実施等、何らかの対応が必要な場合には、バージョンアップや代替策の実施に向けた実行計画案を運用設計書（運用保守業務計画書）に反映し、本県の承認を得ること。なお、バージョンアップに伴う新健康管理システムのアドオン開発・カスタマイズ開発部分の設計・改修作業等は受託者側で行うこと。また、設計・改修作業等に係る費用は本県と協議すること。

3.3.2. ソフトウェア保守対象

毎年発生するライセンスの保守費用など、導入したソフトウェアの維持に必要な費用は追加費用なく運用保守業務委託に含めること。

3.3.3. ソフトウェア改修・予防措置**(1) 定期実施**

機能改善や不具合対応等の是非を判断し、保守計画に沿って定期的に改修を実施すること。

(2) 随時実施

ソフトウェアに不具合がある場合は、改修等の是非を判断し、必要に応じて改修を実施すること。

3.3.4. ソフトウェア構成管理**(1) 資源管理**

各種ソフトウェアに関する改修履歴を管理し、本番環境、テスト環境にそれぞれ適用されているバージョンを明確にすること。

(2) 保守手順書管理

各種ソフトウェアに関する保守（開発、試験及びリリース等）手順が定められた保守手順書の管理を実施すること。

(3) ソフトウェア構成

各種ソフトウェアに関する構成情報を管理すること。

(ア) ソフトウェア一覧

導入済みソフトウェアの一覧を管理すること。

(イ)ソフトウェア環境設定書

自身が納入、変更したソフトウェアの設定情報等を管理すること。

3.3.5. 新健康管理システムにおける保守の提供

新健康管理システムの利用時間が担保されるように実施すること。

(1) 保守体制

運用設計書（運用保守業務計画書）に定めた運用保守手順に従って新健康管理システムの保守を行うこと。

(2) 保守時間帯

本県の運用担当者と協議・調整を行いスケジュールを作成し、スケジュールに合わせた新健康管理システムの運用保守を行うこと。

画面を利用した照会・更新・削除系機能については、新健康管理システムのバックアップやプログラム更新等の時間帯を除き、原則「1.2. 可用性要件」の「1.2.1. システム利用時間」に示すシステム利用時間での利用を可能とする。

(3) 法改正対応

全国的な法改正等については、本県と受託者が協同で調査した結果をもとに、受託者が改修仕様を提示して、本県と協議すること。また、本県に係る改正については、本県の情報提供をもとに、受託者が改修仕様を提示して、本県と協議すること。

なお、国の制度改正については受託者から要請があれば、本県から国の関係省庁に問い合わせを行う場合もある

3.3.6. 新健康管理システムのアップデート対応（法改正含む）

新健康管理システムに関する運用保守期間中での全国的な法改正に基づくパッケージ改修やプログラム改修における費用や対応方法等の考え方を提案すること。

3.4. サービスレベル合意（SLA）

運用保守業務におけるサービスの内容と範囲、品質に関する要求水準と、それが達成できなかった場合のルールを含め、本県および受託者間にて合意することとする。

サービスレベル合意（SLA）内容は、「運用設計書（運用保守業務計画書）」に明記するとともに定例報告会にて報告すること。

サービスレベル合意内容（SLA）の要求水準が達成できなかった場合、または達成できない恐れがある場合は、原因を調査・分析し速やかに本県へ報告すること。

なお、表 6 に示す本県が想定する「サービスレベル項目（案）」を基に、運用設計工程において項目および目標値の取り決めを行うこと。

表 6 サービスレベル項目（案）

項目	定義	目標値
システム稼働率	$(\text{システム稼働時間} - \text{システム停止時間}) \div \text{システム稼働時間}$	99%
レスポンス時間（通常時）	システム利用時（通常時）に要求されるレスポンス時間の目標値	5 秒以内
レスポンス時間（アクセス集中時）	システム利用時（アクセス集中時）に要求されるレスポンス時間の目標値	10 秒以内
目標復旧地点（RPO）	業務停止を伴う障害が発生した場合の健康管理システム復旧時点	最新のデータバックアップ取得時点までのデータ復旧を目標とする。
目標復旧時間（RTO） （業務停止時）	時間業務停止を伴う障害（主にハードウェア・ソフトウェア故障）が発生した際の、統合サーバが利用可能な状態になってから健康管理システム復旧までの時間	48 時間以内（大規模災害時等除く）
目標復旧時間（RTO） （大規模災害時）	大規模災害が発生した際、どれ位で復旧させるかの目標	統合サーバが利用可能な状態になってから 1 週間以内
目標復旧レベル（RLO）	業務停止を伴う障害が発生した場合の、健康管理システム復旧レベル。	健康管理システム全機能を復旧する
障害復旧に着手する時間	害検知一次窓口または監視システムが故障を検知（ウイルス検知含む）し通知および対応に着手するまでの時間	営業日 8:30～17:15：1 時間以内 その他：翌営業日の 9:30 まで
問い合わせ応答時間	本県職員から受託者の運用担当者に問い合わせを行った場合の、対応に着手するまでの時間	営業日 8:30～17:15：1 時間以内 その他：翌営業日の 9:30 まで
問い合わせ回答率 （回答件数/問い合わせ件数）	本県職員から受託者の運用担当者に問い合わせを行う場合の回答指標	100%

4. 移行要件

移行作業にあたっては、データの対象範囲、本県と受託者における役割分担、作業内容およびスケジュール等について設計段階で明確にする必要があり、「移行計画書」や「移行設計書」を作成し本県の承認を受けることを基本とする。

なお、他システムからのデータ連携により登録が必要となるデータや、新規に作成が必要なデータについても同様である。

また、新健康管理システムへの移行においては、本県の健康管理業務や現行健康管理システムの運用に支障がないよう十分配慮し、本県の作業が極力簡易になるよう努めること。

4.1. データ移行要件

本業務の受託者が主体となり、本県および現行業者と移行に必要な要件の確認を行い、確実に健康管理業務ができるようにデータ移行を実施すること。

4.1.1. 移行範囲

原則、現行健康管理システムに蓄積されているデータ項目のうち、新健康管理システム稼働時（令和 10 年 4 月）の健診対象者の過去 5 年分の健診結果データを全て移行対象とする。ただし、外字は移行対象外とし、新健康管理システムでは外字を取り扱わない点に留意すること。

なお、移行元データは本県が現行健康管理システム（Oracle）から抽出または作成し、CSV で提供するものとする（本県が現行健康管理システムの開発・運用保守業者（以下、「現行業者」）と別途契約予定の移行支援業務にて作成）。

また、新健康管理システムが必要とし現行健康管理システムで管理しない項目等は本県と協議の上、情報の追加登録を実施すること。

4.1.2. 移行設計

データ移行の設計では、本県と協議の上、移行方法、移行対象データ項目、移行対象期間等を設計すること。

4.1.3. 作業分担

データ移行作業における、受託者と現行業者との作業分担は以下のとおりである。なお、現行業者の作業経費については本県が別途負担する。

(1) 現行業者の作業

- (ア) 受託者との打ち合わせ（現行データ不明点への対応等）
- (イ) 現行健康管理システムから移行対象データの抽出

(2) 新健康管理システム受託者の作業

- (ア) 移行計画の策定
- (イ) 移行データの分析・設計作業および設計書の作成
- (ウ) 現行業者との打ち合わせ（現行データ不明点の問い合わせ等）
- (エ) 移行や移行結果の確認等に必要とする各種移行プログラムの設計、開発、テスト
- (オ) 新健康管理システムへのデータ移行作業

4.1.4. 現行健康管理システムの設計書提供

現行健康管理システムの設計書（データレイアウトや項目定義書等）は本県より提供するので移行作業にて活用すること。本県および現行業者と協議が必要な場合は、受託者より、本県に対して依頼すること。

4.1.5. 移行データ確認

稼働前データの移行、臨時入力および移行前後の確認作業について効率的かつ確実な手法について提案すること。移行すべき対象データ（データベース、テーブル、ファイルおよびバックアップデータ）の調査を十分に行い、本県と協議の上、移行の範囲を決定すること。なお、各業務データは表 7 に示す期間として新健康管理システムの移行対象とすること。

表 7 データ移行範囲

項目	移行対象
健診結果データ	新健康管理システム稼働時（令和 9 年 4 月）の健診対象者の過去 5 年分の健診結果データ

4.1.6. 移行データ変換

移行作業を実施するにあたり、システムデータのデータ変換（コード変換、文字同定等の文字コード変換作業、不足項目追加等含む）、変換データの確認、変換によるエラーデータの除去を実施すること。

4.1.7. 移行リハーサル・移行実施

テスト時の移行、本番業務向けの移行等、開発期間中においては複数の移行作業が発生するため、必要とする移行回数等を本県と事前に協議して実施すること。また、業務やその業務が行われるタイミングおよび対象データの特性から段階的な移行が必要な場合も想定されるため、対象データやタイミング等十分に協議し漏れなく移行すること。移行方法や移行後のデータ管理方法等について最適な方法で実施すること。

移行実施にあたっては移行手順書を作成し、本番移行を想定した移行リハーサルを少なくとも 1 回は実施すること。移行リハーサルによって得られた知見を活かして移行手順書の改訂を行い、本県の承認を得ること。必要に応じて改定後の移行手順書を用いた移行リハーサルを実施すること。

4.1.8. 移行対象データの参考

移行対象データの参考として、現行健康管理システムで保持しているデータは、別紙（非機能）1「健康管理_テーブル一覧」にて提示したとおり。

4.2. システム移行要件

新健康管理システムの本稼働は令和 10 年 3 月とする。

4.2.1. 新健康管理システムの本稼働

総合テスト、受入テスト、移行リハーサルの結果から、システム移行計画書に規定する本番切替え

の判定基準を満たすことを示し本県の承認を得ること。本番切替えの承認をもって現行健康管理システムを停止する予定である。

4.3. システム移行における留意事項

システム移行にあたっては、次の点に留意すること

(1) データ移行の調査およびデータ移行作業環境

移行設計までに現行健康管理システムのシステムデータおよび設計関連ドキュメントを本県から受託者へ提供するため、それを基に受託者は各業務の設計に向けたデータ調査・移行設計を行うなど、導入するパッケージに必要な作業を行うこと。なお、必要に応じてマスキングを行った上で移行作業を行うこと。

(2) 移行設計・開発の手順

現行健康管理システムからの移行元データに対して、新健康管理システムへのデータ移行方法、各テーブルの変換仕様等を設計し、本県がレビューを行った上で移行プログラムを開発すること。開発したプログラムにて移行元データを変換し、テスト環境等にセットアップを行い、変換結果の検証を行うこと。

(3) 本番切替え計画の策定

データ移行および本番切替えの実施に向けた本番切替え計画には、データ移行の失敗や受入れテストでの不具合発生など、不測の事態に備えた復旧計画についても検討し、要素として含めること。

(4) システム移行にあたっての制約等の事前整理・承認

本番切替え前および本番稼働開始後に新健康管理システムでデータ補正・入力対応を行う場合等、移行に係る制約事項、留意事項、残作業等があれば、事前に整理し、本県の承認を得ること。

5. マニュアル・操作研修

5.1. マニュアル

職員が操作を行うものについて、マニュアルを作成すること。また、作成したマニュアルは、新健康管理システムから容易に参照できるようにすること。

なお、想定するマニュアルの役割分担は以下のとおり。（業務マニュアルについては本件で作成をおこなう想定）

表 8 マニュアル一覧

対象	役割		備考
	県	受託者	
業務マニュアル	○		業務ごとの手引き等を記載。
閲覧職員用マニュアル	-	○	健診結果を閲覧する職員用のマニュアルとして、システムの基本操作、事象別の操作手順を記載。
業務管理者用マニュアル	△	○	業務管理者（本県の業務担当職員）向けとして、新健康管理システムに関して業務担当者が行うべき作業の操作方法や障害時の緊急対応方法について記載。
Q&A	-	○	システムを利用する際に想定される Q&A を記載

【凡例】 ○：作成主体 △：補助作業、協力等

5.2. 操作研修

受入テストで代替すること。

6. その他の留意事項

6.1. 業務の引継ぎに関する事項

本業務の契約履行期間の満了、全部若しくは一部の解除、又はその他契約の終了事由の如何を問わず、本業務が終了となる場合には、受託者は本県の指示のもと、新健康管理システムの利用終了日までに本県が継続して健康管理業務を遂行できるよう必要な措置を講じ、後継システムに移行する作業の支援を行うこと。また、業務引き継ぎに伴いデータ移行等が発生する場合、以下の対応事項について、本県または後継システム構築事業者に対して誠意を持って協力すること。なお、業務の引継ぎに係る費用は、本調達の費用には含めない。

- ・ 構築・運用を行っている全てのシステムについて、移行のために必要となるデータを汎用的なデータ形式（CSV 等）に加工し提供すること。
- ・ ファイル・データレイアウト等の資料を提供すること。
- ・ 機器上に保存された一切のデータについては、これを消去すること。データ消去が完了した場合には、報告書を提出すること。