医療費助成オンライン報告システム基盤構築業務委託仕様書

1. 業務名

医療費助成オンライン報告システム基盤構築業務（以下「本業務」という。）

2. 委託期間

(１)医療費助成オンライン報告システム基盤構築業務

契約締結日から令和７年２月２８日（金）まで

(２)運用保守業務

令和７年３月１日（土）から令和８年３月３１日（木）まで

※運用保守業務については、別途委託予定。ただし、次年度以降の運用保守業務を行うことが可能であり、かつ今回見積もり金額を提示することを契約締結の条件とする。

3. 運用開始時期

(１)本格運用

令和７年３月１日（予定）

4. 背景と目的

保険医療機関がオンラインで医療費助成事業における報告・請求を行うシステムとして、平成 26 年度より「オンライン報告システム」（以下「本システム」という）が稼働している。しかし、現在利用しているネットワークおよびサーバ機器の保守延長が困難となっており、継続的な運用にリスクが生じている。 本業務の目的は、オンプレミス環境の維持管理に伴うコスト削減を図り、システムの柔軟性、拡張性、運用効率の向上を実現するため、AWS 上に基盤を構築し、その上で本システムを稼働させることで安定した運用と将来的な拡張性を確保することにある。

5. 仕様書の目的

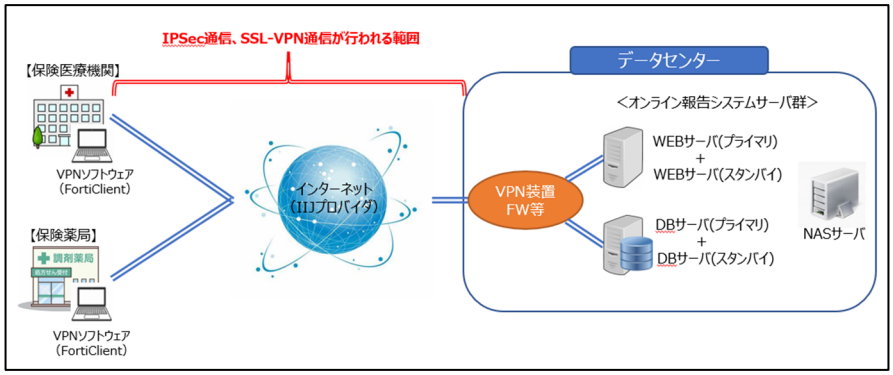
この仕様書は、沖縄県国民健康保険団体連合会（以下「本会」という。）が実施する本業務に係る指名競争入札に参加する者が提案すべき内容について、基本的な事項を示すものである。

なお、本仕様書に定めのない事項であっても、システムを正常に稼働させる上で必須の事項については、必ず提案に含めること。

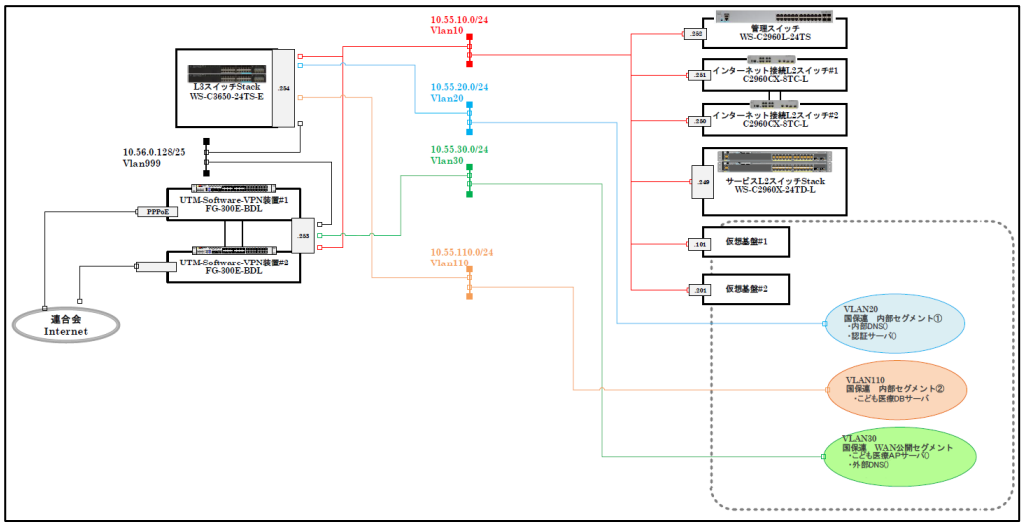
また、仕様の詳細については、本業務の受託候補者として特定された者と本会との協議の上、確定するものとし、本仕様書に全ての提案すべき内容が盛り込まれているとは限らないことに留意すること。

6. 現行システムの概要

(１)システム構成図



(２)ネットワーク構成図



(３)サーバおよびソフトウェア構成

①　オンライン報告システムのサーバ機器（オンプレ環境）

【Webサーバ】

項目	現在の容量/サイズ
プライマリサーバー	
物理コア数：	8コア XeonB 3106 1.7GHz 1P8C CPU
メモリ数：	8GB 8GB 1Rx8 PC4-2666V-R Smartメモリキットx2
OS：	RedHat Enterprise Linux 7.4
ストレージサイズ：	2.00TB ※RAID 1+0 1TB 7.2krpm SC 2.5型 6G SATA HDDx4
プロセッサタイプ：	Intel
バックアップ：	なし
スタンバイサーバー	
物理コア数：	8コア XeonB 3106 1.7GHz 1P8C CPU
メモリ数：	8GB 8GB 1Rx8 PC4-2666V-R Smartメモリキットx2
OS：	RedHat Enterprise Linux 7.4
ストレージサイズ：	2.00TB ※RAID 1+0 1TB 7.2krpm SC 2.5型 6G SATA HDDx4
プロセッサタイプ：	Intel
バックアップ：	なし

【DBサーバ】

項目	現在の容量/サイズ
プライマリサーバー	
物理コア数：	12コア XeonS 4116 2.1GHz 1P12C CPU
メモリ数：	32GiB 16GB 2Rx8 PC4-2666V-R Smartメモリキットx2
OS：	RedHat Enterprise Linux 7.4
ストレージサイズ：	1.20TB ※RAID 1+0 600GB 10krpm SC 2.5型 12G SAS DS HDDx4
プロセッサタイプ：	Intel
バックアップ：	Acronis Backupにより、夜2:00にDBのダンプがバックアップされます。 一週間（月～日）ごとに差分バックアップし、最大一か月分を保持します。 バックアップ対象はプライマリーサーバのみです（スタンバイサーバはプライマリーサーバのレプリカのため）。
スタンバイサーバー	
物理コア数：	12コア XeonS 4116 2.1GHz 1P12C CPU
メモリ数：	32GiB 16GB 2Rx8 PC4-2666V-R Smartメモリキットx2
OS：	RedHat Enterprise Linux 7.4
ストレージサイズ：	1.20TB ※RAID 1+0 600GB 10krpm SC 2.5型 12G SAS DS HDDx4
プロセッサタイプ：	Intel
バックアップ：	なし

② その他機器

ア NetAttest 認証サーバ

・形態：アプライアンス機器

・モデル：NetAttest EPS Virtual Applicance

・バージョン：Ver 4.10.15

イ FortiGate ファイアウォール

モデル：FortiGate-300E

(４)接続関係と依存関係

① システム接続関係図

ア 接続関係図

・(２)ネットワーク構成図を参照。

イ 接続関係の詳細

・ユーザは FortiClient VPN を使用して、インターネット経由で FortiGate に接続。

・VPN 接続時に、NetAttest 認証サーバでユーザ認証が行われます。認証に成功したユーザのみが VPN 接続を確立。

・VPN 接続が確立されると、ユーザの通信は FortiGate を通過。

・FortiGate はセキュリティポリシーに基づき、許可されたトラフィックのみを通過。

・ネットワーク内では、ユーザは Web サーバにアクセス。

・Web サーバは、必要に応じて MySQL（データベース）と通信。

② オンライン報告システムにおけるアプリケーション間の通信

ア 各サーバやサービス間の通信経路

・Web サーバが DB サーバと TCP or UDP ポート 3306 で通信。

イ データフロー

・ユーザからの入力が Web サーバを経由して DB サーバに渡り、データベースにデータが保存。

(５)接続方式とプロトコル

① 医療機関端末から VPN 装置まで

・プロトコル：SSL-VPN または IPsec

・認証方式：NetAttest によるユーザ認証（ID/パスワード）

② FortiGate ファイアウォール

・アクセス制御：セキュリティポリシーに基づくトラフィックの許可/拒否

・ポート設定：必要なポートのみ開放（例：TCP 80、443、3306 など）

③ ネットワーク内の通信

・Web サーバと DB サーバ間の通信：セキュリティグループで許可されたトラフィックのみ許可

・プロトコル：HTTP/HTTPS、TCP/IP など

（６）現行システムの課題と制約

現行システムには以下の課題と制約があります。

① ハードウェアの老朽化

・現行システムのサーバやネットワーク機器は導入から 5 年以上が経過しており、保守サポートの期限も近づいている。

② スケーラビリティの限界

・現行のオンプレミス環境ではリソースの拡張が困難であり、将来的な負荷増加に対応できていない。

③ IPv6 に対応していない

・現行システムは IPv6 プロトコルに非対応であり、IPv6 ネットワークからのアクセスができない。

・将来的なインターネット環境の変化に伴い、IPv6 対応が求められている。

④ HTTPS に対応していない

・現行システムはHTTPによる平文通信のみを行っており、HTTPS（SSL/TLS暗号化通信）に非対応。

・ユーザの個人情報や機密データを扱うため、通信の暗号化が必要。

7. 対象範囲

（１）既存オンプレミスシステムの AWS 東日本リージョンへの移行（クラウドリフト）

① 現行システムの構成を変更せず、AWS 東京リージョンに移行すること。

② AWS Application Migration Service（AWS MGN）を利用してオンプレミス環境のサーバを AWS へ移行すること。

③ オンプレミス環境および移行後のオンライン報告システムサーバに対する作業は本会にて実施する。

（２）VPN 環境（基盤）の構築

① AWS 上で VPN 接続環境（基盤）を構築し、FortiClient VPN、NetAttest、FortiGate との互換性を確保すること。

② 必要に応じて、仮想アプライアンスの導入を検討すること。

③ 以下のクライアント OS から VPN 接続できること。

・Windows 10

・Windows 11

（３）AWS 上でのシステム設計、構築、設定、およびテスト

① クラウドリフトに必要な最小限の設定変更を行うこと。

（４）データ移行およびシステム統合

① データの完全性と整合性を維持したまま移行すること。

② 必要に応じて、接続先や設定の調整を行うこと。

（５）セキュリティ対策の実装

① クラウド環境に適したセキュリティ設定を適用すること。

(６)運用・保守に関するドキュメントの作成

① 移行後の運用手順書やマニュアルを作成すること。

8. 業務用件

(１)機能要件

① 本システムの全ての機能が AWS 上でも同等に動作すること。

② ユーザが安全にシステムを利用できるよう、通信の暗号化やセキュリティ対策を強化すること。

(２)ネットワーク要件

① IPv4 および IPv6 の両方に対応すること。

9. 技術要件

(１)クラウドプラットフォームの指定

「Amazon Web Services（AWS）」をクラウドプラットフォームとして採用することとする。

(２)AWS サービスの利用

別紙１のとおり。

(３)AWS 上のシステム構成

① 本システムの Amazon EC2 インスタンス構成

サービス	用途	台数	インスタンスタイプ	OS	その他設定
Amazon EC2	Web サーバ	1 台	c5.xlarge	RedHat Enterprise Linux 7.4	ストレージ：EBS（gp3）、50 GiB
Amazon EC2	DB サーバ（マスタ）	1 台	c5.xlarge	RedHat Enterprise Linux 7.4	エンジン：MySQL 5.7、ストレージ：EBS（gp3）、100 GiB
Amazon EC2	DB サーバ（スレーブ）	1 台	c5.xlarge	RedHat Enterprise Linux 7.4	エンジン：MySQL 5.7、ストレージ：EBS（gp3）、100 GiB

② AWS 上のネットワークにおける方針

AWS VPC 内のネットワーク構成における方針を以下に示す。

ア インターネット接続

・パブリックサブネットは、インターネットゲートウェイを構築し、ファイアウォールと接続する。

・パブリックサブネットは、インターネット経由で VPN 接続を可能とする。

・プライベートサブネットは、インターネットゲートウェイと接続せず、パブリック IP も所持しない。

・プライベートサブネットは、国保連合会と VPN による接続を行い、メンテナンス可能な状態にする。

イ ルーティング構成

・パブリックサブネットのデフォルトルートは、インターネットゲートウェイとする。

・パブリックサブネットとプライベートサブネットは、相互に接続可能とする。

・プライベートサブネットは、連合会のローカルエリアネットワークと接続可能とする。

ウ　FW ポリシー

・各医療機関からの接続は、HTTP、HTTPS による WEB サーバへの接続を許可する。

・IPsecVPN、SSL-VPN 接続に必要なポリシー設定を行う。

エ　セキュリティグループ

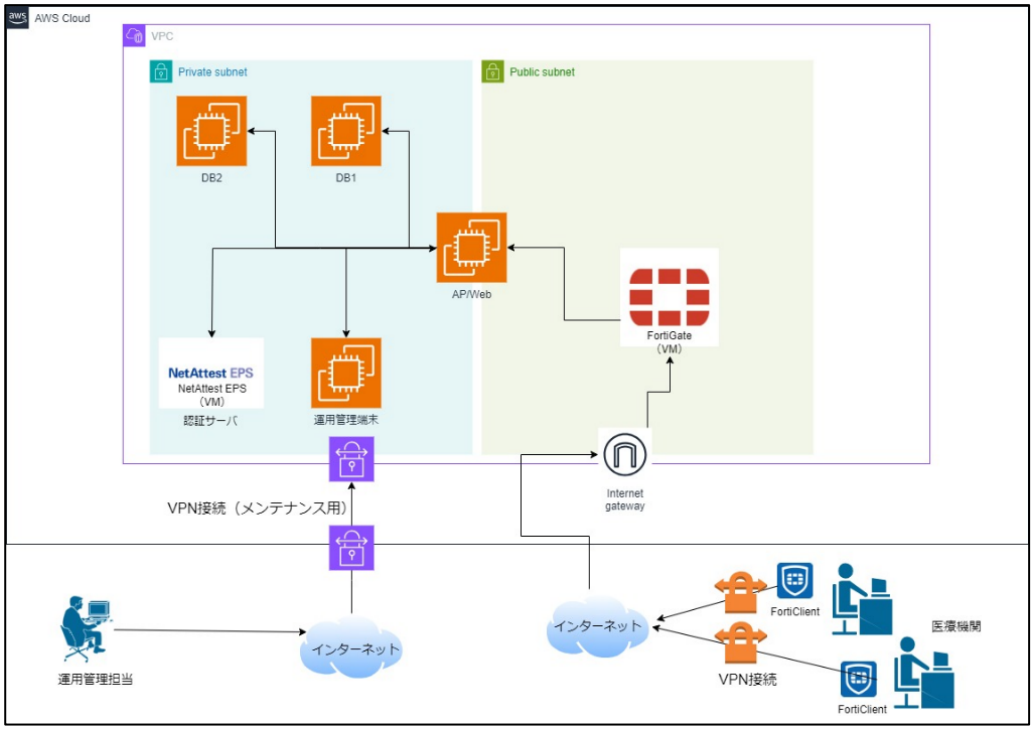
・WEB サーバは、HTTP,HTTPS のみ接続可能とし、運用管理端末からは、TELNET,SSH による接続を許可し、DB サーバとの接続は、プロトコルによる制限はしない。

・DB サーバは、WEB サーバとの通信に制限をせず、運用管理端末からは、TELNET,SSH による接続を許可する。

・運用管理端末は、連合会のローカルエリアネットワークからの接続を許可し、プロトコルによる制限はしない。

・認証サーバは、運用管理端末からの接続を許可し、プロトコルによる制限はしない。

③　AWS 上のネットワーク構成図（参考）



④　設計・構築要件

・AWS のベストプラクティスに従い、セキュリティ、可用性、スケーラビリティを考慮した設計を行うこと。

・現行システムとの互換性を保ち、移行をスムーズに実施するための設計を行うこと。

⑤　将来の拡張性を考慮した設計

現時点では、AWS 上で稼働するシステムはオンライン報告システムのみを想定しているが、将来的に新たなシステムが稼働する可能性があるため、設計時には以下を考慮すること。

ア　プライベートサブネットの追加に対応可能な設計

・将来的にプライベートサブネットが追加される可能性を考慮し、既存の VPN 接続の仕組みを利用してこれらのサブネットにアクセスできるように設計すること。

・ネットワークアドレス設計（CIDR ブロックの割り当て）やルーティング設定、セキュリティグループ、ネットワーク ACL などを、拡張性を持たせた構成とすること。

イ　ネットワーク構成の柔軟性

・VPC およびサブネットの構成を、将来的な拡張や変更に対応できるように設計すること。

・IP アドレス空間の確保や、アドレス重複の回避を考慮すること。

ウ　VPN 接続環境のスケーラビリティ

・新たなシステムやサブネットが追加された場合でも、VPN 接続環境が問題なく機能し、ユーザがアクセス可能であることを保証すること。

・FortiGate や NetAttest の設定が、新規サブネットやシステムへのアクセスを容易に追加・管理できるようにすること。

（４）VPN 接続の詳細設定

① VPN ソフトウェア

・FortiClient VPN（Ver6.0 及び Ver7.0）を利用できること。

・クライアント証明書は、既に配布されている証明書を継続して利用できること。

② VPN 認証

・「NetAttest EPS Virtual Appliance DX モデル(EPS-DX05A-V 又は EPS-DX05A-W)」を利用すること。

・1,000 ユーザ分のクライアント証明書（ユーザ単位）が発行できること。

・認証方式や設定については、別添 1 のセキュリティ要件を満たすこと。

③ ファイアウォール（FW）

・「Fortinet FortiGate Next-Generation Firewall」を利用すること。

・ネットワークのセキュリティ強化のため、現行と同等の適切なルール設定と運用を行うこと。

・VPN 接続および通信データは適切な暗号化方式（例：AES 256bit）を用いて保護すること。

（５）セキュリティ要件

① ネットワークセキュリティ

セキュリティグループとネットワーク ACL を用いたアクセス制御を行うこと。

② 無操作時の通信遮断設定

・ユーザが VPN 接続を行った後、30 分間無操作状態が続いた場合には、自動的に通信を遮断し、VPN 接続を切断すること。

・再接続が必要な場合は、ユーザが再度認証を行い、VPN 接続を確立できるようにすること。

③ データ暗号化

ユーザ端末と Web サーバ間の全ての通信は HTTPS（SSL/TLS 暗号化通信）を使用すること。

④ 認証と認可

AWS IAM を活用し、最小権限の原則に基づいたロールおよびポリシーを設定すること。重要な操作には二要素認証を導入し、全てのアクションのログを CloudTrail で記録・監査可能とすること。

⑤ ログ管理

CloudWatch Logs にてログ管理を行うこと。

⑥ 第三者機関によるセキュリティ評価の実施

ア セキュリティ評価

・基盤構築完了後、第三者機関によるセキュリティ評価（セキュリティ監査、脆弱性診断など）を実施し、その結果を報告すること。

・セキュリティ評価の範囲には、AWS 上の基盤環境、ネットワーク設定、サードパーティ製品（FortiGate、NetAttest）などを含むものとする。

・セキュリティ評価の結果、指摘事項があった場合は、適切な是正措置を講じ、再評価を行うこと。

イ 報告書の提出

・第三者機関から提供されたセキュリティ評価報告書を納品すること。

・報告書には、評価の範囲、手法、結果、指摘事項、推奨事項などを含めること。

（６）可用性と冗長性

・現行システムと同等の可用性を維持すること。

（７）ドメイン名および DNS 設定

① ドメイン名の継続利用

・現行システムで使用している FQDN（完全修飾ドメイン名）を、AWS 上でも引き続き利用すること。

② Amazon Route 53 の利用

・DNS 管理には、AWS のマネージド DNS サービスである Amazon Route 53 を利用すること。

・Route 53 上に対象ドメインのホストゾーンを作成し、必要な DNS レコード（A レコード、CNAME レコードなど）を設定すること。

③ ネームサーバーの設定

・ドメインレジストラで、ドメインのネームサーバー（NS レコード）を Amazon Route 53 で提供されるネームサーバーに変更すること。

・ネームサーバーの変更に伴う DNS 伝播時間を考慮し、切り替え計画を策定すること。

・DNS 設定の移行手順とタイミングを明確にし、サービスへの影響を最小限に抑えること。

（８）データ移行

① オンライン報告システムサーバのデータ移行

・データの完全性を確保した移行手順の策定と実施を行うこと。
・ダウンタイムを最小限に抑える計画を作成すること。
・AWS Application Migration Service（AWS MGN）を利用して、AWS 上にオンプレミス環境と AWS 環境間でセキュアな通信(VPN 接続)を行った上でデータ移行を行うこと。

② NetAttest（アプライアンス機器）のデータ移行
・現行システムで利用している NetAttest から、AWS 上の「NetAttest EPS Virtual Appliance DX モデル（EPS-DX05A-V 又は EPS-DX05A-W）」へのデータ移行を行うこと。
・移行対象データには、ユーザ情報、認証ポリシー、設定ファイルなどを含むものとする。
・データ移行に伴うリスクを評価し、適切な対策を講じること。

（９）AWS アカウント管理とクラウド利用料

① AWS アカウント
・AWS アカウントは委託者が用意し、受託者に対して環境構築に必要なアクセス権限（IAM ユーザまたは IAM ロール）を付与する。
・受託者は提供された IAM ユーザまたは IAM ロールの範囲内で、システムの構築および設定を行うこと。

② クラウド利用料
・クラウド利用料（AWS リソースの利用料金）は、委託者が負担するものとする。

③ クラウド利用料の制御と責任
・受託者は、事前に環境構築及び本番運用時のクラウド利用料に関する詳細な見積もりを提出すること。見積もりに基づき、予算を大幅に超える追加費用が発生しないよう管理する責任を負うものとする。
・クラウド利用料が予定を大幅に超過する場合、その原因が受託者のミスや設定不備に起因する場合は、追加のクラウド利用料は受託者が負担するものとする。
・委託者は AWS Budgets および Cost Explorer を利用して、クラウド利用料の上限とアラートを設定し、定期的にコストを監視する。
・委託者は、クラウド利用料の上限に達した場合、事前に受託者と協議の上でリソースの見直しや利用制限を行うことができる。

10. 非機能要件

（１）インフラパフォーマンス要件
・同時接続数 100 ユーザに対応可能なインフラ構成を設計し、処理遅延が発生しないことを保証すること。
・トラフィックが通常時の 2 倍になっても、インフラのパフォーマンスに影響がないように構成すること。

（２）可用性
・サービス全体で現行システムと同等の稼働率を維持すること。
・VPN 接続環境（基盤）およびファイアウォールも高可用性を確保すること。

（３）スケーラビリティ

・必要に応じてリソースを拡張できること。

・ＶPN 接続ユーザ数の増加にも対応可能な設計とすること。

（４）運用監視

・VPN 接続環境およびファイアウォールの状態を常時監視し、異常時には迅速に対応できる体制を整えること。

・AWS CloudWatch などの監視ツールを使用し、システム全体の稼働状況をモニタリングすること。

・接続ログや認証ログ、ファイアウォールのログを適切に収集・保管し、必要に応じて分析できるようにすること。

（５）アラート設定

・システムに異常が発生した場合、または閾値を超えた場合には、事前に設定した条件に基づき、システム管理者に対してアラートを送信すること。

・アラートは、メール、SMS、または他のリアルタイム通知手段で送信されるよう設定すること。

・主要な監視項目としては、各サービスの死活監視、サーバの応答速度、CPU 使用率が 80%を超えた場合、メモリ使用率が 90%を超えた場合、ディスク使用率が 90%に達した場合などが含まれる。

11. 運用保守業務

（１）サーバ要件

① 設置場所及び費用

ア サーバは、日本国内のデータセンターに設置されたサーバを利用すること。

イ サーバは、クラウドサービスを前提としたサーバの構築を行うこと。

ウ クラウドサービスの利用契約に関して生じる一切の紛争は、日本の地方裁判所を専属的合意管轄裁判所とするものであること。

② セキュリティ

クラウド事業者は、情報セキュリティマネジメントシステム（ISO/IEC27001）適合性評価制度またはこれに準ずる認定を取得していること。また、認定を証明できること。

③ データ容量

サーバは、利用状況を考慮した運用に耐えうるデータ容量を保持できること。

④ サーバ OS

本システムのサーバ OS は限定されるが、それ以外のサーバ OS は問わない。

⑤ 拡張性

利用状況に応じて、スケールイン及びスケールアウトが行えること。

（２）運用・保守要件

① システム運用時間

ア システムの運用時間は、以下のとおりとする。運用時間外には、停止可能なサービスを停止させるものとする。

期間	運用時間	備考
１日～４日	9:00～17:00	休日 (土、日、祝日)除く
５日～７日	8:00～21:00	休日 (土、日、祝日)含む
８日～１５日	8:00～24:00	休日 (土、日、祝日)含む
１６日～月末	9:00～17:00	休日 (土、日、祝日)除く

※年末年始（12/29～1/3)は運用を停止する。

イ　全システムに関連するハード・ソフトウェアのメンテナンス作業時は除くものとする。メンテナンスを目的とした計画的な停止を行う場合は、本会に連絡し承認を得ること。

ウ　障害の早期発見・復旧のため、常時システムの監視（アクセスログ、システムログ）を行い、障害を予見した際には速やかに本会へ報告すること。

② システム自動運転

システムの起動、停止、日次処理、月次処理、バックアップ等については、自動運転が可能なシステム構成であること。その際、処理時間はシステム利用者に支障をきたさない範囲であること。

(３)セキュリティ対策要件

① サーバのセキュリティ対策

ア　ウイルス対策等

・ウイルス対策ソフトとして、「Sophos Central Intercept X Advanced for Server」を利用すること。※ウイルス対策ソフトは本会にて調達する。

・セキュリティ対策ソフトのウイルス定義ファイル及びサーバ OS の更新プログラムを適切なタイミングで更新すること。インターネットに接続する必要がある場合は、アクセス制限を行った上で「NAT Gateway」を利用すること。また、ドメイン単位でのアクセス制限が行えること。

イ　データの保護、改ざん防止等

利用者情報保護及び改ざん防止、不正利用などセキュリティ対策を講じ、情報へのアクセスログの取得、厳重なアクセス権限の管理、データの漏洩、データ改ざん防止するような対策を講じること。

ウ　脆弱性

本基盤の稼働までに発見された脆弱性及び今後発生される脆弱性の情報を定期的に収集し、適切な対応を行うこと。

エ　暗号化

保険医療機関等の端末とサーバ間の通信は暗号化（SSL）すること。

オ　管理者の操作ログ

管理者のログイン時には、管理者ID 及びパスワードによる認証を行うこと。管理者ID 毎に、操作ログを取得できること。

(４)データ保全要件

① バックアップ

・構成要素である全てのインフラサーバに対して、バックアップを行う仕組みを提供すること。受託者はインフラに関わるサーバのバックアップ設定を行うものとする。
・バックアップ先の確保は受託者の責任で行い、適切なクラウドストレージとしてバックアップ先を提供すること。
・オンライン報告システムにおける業務データおよびアプリケーションのバックアップは委託者側で実施するものとする。
・OS、ミドルウェアについては、初期設定時やシステム変更時に静的なバックアップを実施できるようにすること。
・セキュリティパッチ等についても管理できること。

② バックアップデータ格納
・バックアップを実施する際、システム停止なしでのバックアップが可能であることを保証すること。
・バックアップ取得時点のシステム復旧が可能であることを確認すること。

③ バックアップ方式
・日次、月次バックアップデータの世代管理が可能であり、委託者が利用できるバックアップ運用環境を提供すること（2 世代程度を想定）。
・インフラサーバに対して自動化された日次・月次のバックアップ運用を行うこと。

④ バックアップ管理機能
システムやデータのバックアップ、リストア、スケジューリング、ログ確認、エラー通知、サーバのバックアップ運用に関して、一元的かつ効率的に管理できる仕組みがあること。業務データのバックアップは委託者側が行う。

⑤ 障害発生時のリカバリ方式
バックアップやリカバリについて設計し整備すること。手順書を作成し、本会へ提供すること。
何かしらの障害が発生した場合、バックアップからの復旧手順が明確化されていること。

12. 知的財産権および機密保持

(１)知的財産権の帰属
・本業務の遂行により新たに作成された全ての成果物（プログラム、設定ファイル、スクリプト、テンプレート、ドキュメント、デザイン等）の著作権およびその他の知的財産権は、全て委託者に帰属するものとします。
・受託者が予め保有する技術やノウハウを利用した場合、その部分については受託者が権利を有しますが、委託者は当該成果物を業務上自由に利用・改変・複製できるものとします。

(２)第三者の知的財産権の利用
・受託者は、第三者の知的財産権を利用する場合、適切なライセンス契約を締結し、その証明を委託者に提示するものとします。
・ライセンス料や使用許諾に関する費用は、見積書に明示してください。

(３)機密保持義務
・受託者は、本業務を通じて知り得た委託者の機密情報を、委託者の事前の書面による承諾なし

に第三者に開示・漏洩してはなりません。

・この機密保持義務は、契約終了後も 5 年間継続するものとします。

(４)競業避止義務

・受託者は、委託者の事前の書面による承諾なしに、本業務で得た情報やノウハウを利用して、同様のサービスを第三者に提供してはなりません。

13. 運用支援体制

(１)実施計画の策定

契約締結後、1 週間以内に、本業務に係る業務実施計画書を提出すること。業務実施計画書には、以下の内容その他必要事項を記載し、本会の承認を得ること。

・作業スケジュール、作業項目（WBS）と役割分担

・業務実施体制図（連絡先）

・業務運営方法

(２)会議の開催・議事録作成

受託者は、本会と調整の上、原則として以下のとおり会議を開催すること。

ア　進捗報告会議の開催

システム構築期間中、進捗報告会議を開催し、本業務全体の進行手順の確認、進捗状況の確認、進行上の課題への対応策の協議を行うこと。

イ　会議資料及び議事録の作成

会議に用いる資料の作成は、受託者がすべて実施すること。議事録は、受託者が原則として会議開催後 5 営業日以内に作成し、本会の承認を得ること。いずれも、電子データを本会へ提出するものとする。

14. 成果物の作成と提出

受託者は、本業務の趣旨に基づき、別紙 2 のとおり成果物を作成し、本会へ提出すること。

(１)納品時期

・設計フェーズ終了時：システム設計書、システム構成図、移行計画書。

・構築フェーズ終了時：設定手順書、設定ファイル、スクリプト類。

・テストフェーズ終了時：テスト計画書、テスト結果報告書。

・移行フェーズ終了時：移行手順書、移行結果報告書。

・基盤構築完了後、是正措置後：セキュリティ評価報告書。

・運用開始前：運用手順書、ユーザーマニュアル、管理者マニュアル。

(２)納品形式

ア　電子データ

ドキュメント類はPDF形式および編集可能な形式（Word、Excel、Visioなど）で納品すること。

イ　媒体

電子メール、クラウドストレージサービス、または指定のファイル転送サービスを利用すること。

（３）更新履歴の管理

全ての成果物には、作成日、バージョン、作成者、変更履歴を明記すること。

（４）言語

全ての成果物は日本語で作成すること。

（５）品質要件

成果物は正確かつ分かりやすい内容であり、品質基準を満たすこと。

15. その他

（１）本書に明示されていない事項であっても、委託者と協議のうえ、その履行上必要な事項について、すべて受託者が責任を持って対応すること。

（２）保守業務にかかる契約後、本書に記載されていない事項で疑義が生じた場合や、委託者が委託作業内容等の変更の必要が生じた場合、受託者は協議に応じなければならない。