山形県病院事業局
統合ネットワーク環境構築
及び保守・運用支援業務委託仕様書

令和５年 10 月

山形県病院事業局

1 背景と目的

(1)はじめに

本仕様書は、山形県病院事業局における統合ネットワーク環境構築及び保守・運用支援業務(以下、「本委託業務」という。)の仕様について記載する。

(2)基本事項

山形県病院事業局統合ネットワーク環境とは、山形県立4病院及び県立病院課が共同で、インターネットへの接続口を一つに統合し、統一した管理を可能とするとともに各々の通信に対して高度なセキュリティ監視を行う環境である。

この統合ネットワーク環境は、各接続拠点が管理する医療情報及び個人情報等の重要なデータの漏えいを未然に防止することを目的とし、各接続拠点が必要とする情報セキュリティ水準を確保しつつ、各接続拠点の通信を安全で滞りのない運用を可能とするものである。

(3)現状と本委託業務の目的

現在、山形県病院事業局の医療情報におけるネットワークシステム及びセキュリティは令和4年度の「閉域網整備」及び「セキュリティ環境構築」にて、閉域網ネットワークの利用と県立病院課を除く各接続拠点にオンプレミスタイプの UTM 装置を導入し運用している(別紙1「ネットワーク概要図(現行)」)が、管理が各接続拠点個別となっていることや閉域網ネットワークであることから、集中管理や新たなクラウド型システムの利活用や外部連携、新規システムの統合利用への拡張が困難であり、統合的なネットワークシステムの設計やセキュリティ運用監視も行いにくい状態である。

このような状況において、各接続拠点の通信の利便性と安全性の更なる向上のため、以下のことを条件とした拡張性のあるクラウド型次世代ファイアウォール環境(別紙2「ネットワーク概要図(統合ネットワーク環境構築後)」)の構築を行う。

ア　アクセス集中を想定した安定した仕組みを提供する 。
イ　各接続拠点間を接続する医療情報ネットワークを不正アクセスから保護する。
ウ　各接続拠点間を接続する医療情報ネットワークにおいて、情報セキュリティインシデントが発生した場合、速やかに関係職員へ連絡する。
エ　情報セキュリティインシデントへの適切な対応のため、具体的な状況の把握と影響範囲の調査を支援する。
オ　外部環境の変化(サイバー攻撃の大規模化、手口の巧妙化)への対応· 可用性の担保等を考慮した運用サービスを提供する。
カ　機器・運用・管理・監視が一体となったセキュリティサービスを提供する。
キ　各接続拠点間通信を利用し稼働中の勤務管理システムの継続利用が可能である。

ク　導入予定の各接続拠点間通信を利用した統合 DWH システムの利用が可能である。なお、統合 DWH システムとは各拠点の医療系ネットワークに属するデータを収集・表示する BI ツールである。

ケ　医療情報システムベンダーの各接続拠点病院へのリモートアクセスの統合を行い集中管理と監視を可能にする。

コ　病院職員による院外からの医療情報システムの利活用を可能にする。ただし、現時点においては、Web 型システムに限る。また、この設定については本契約外とする。

サ　将来における医療情報システム端末からのクラウド型システムの利用や特定の医療ポータル利用などが安全に行える機能を予め有している。

シ　厚生労働省が現在計画を進めている共通基盤ネットワーク（地域医療情報・PHR・FHIR）に柔軟に対応できるようにすること。

以上のことから、これら機能を実現したクラウド型次世代ファイアウォールを構築したうえで、各接続拠点が安定的に利用できる機器と運用を提供することを本委託業務の目的とする。

なお、勤務管理システム用サーバーは、山形県立中央病院内に設置され、各接続拠点病院と連携をしており、導入予定である統合 DWH システムのサーバーも山形県立中央病院に設置の予定である。

2 事業概要

(1)委託業務名称

山形県病院事業局 統合ネットワーク環境構築及び保守・運用支援業務

(2)業務範囲

ア　業務概要【構築業務】

(ア) クラウド型次世代ファイアウォール及び周辺装置をサービス開始から最低3年間は保守・運用支援サービスと合わせて提供することを可能とし、その後、最新のサイバー攻撃などに対応した次のセキュリティプランに変更又は移行が可能であること。

(イ) 本委託業務については、事前調査を十分に行ったうえで各種設計業務を行うこと。また、業務全体に対する業務計画書を作成のうえ、進行管理を行うこと。

(ウ) 本委託業務を実施するに当たり、現地調査の一環としての各接続拠点担当者からのヒアリング及び各接続拠点における既存ネットワーク又は既存システム（医療情報システム等）の既存事業者等関係者との十分な調整を行ったうえで、業務を行うこと。

(エ) クラウド型次世代ファイアウォールとして、必要な機能をクラウドサービスにより提供を行うこと。

(オ) 各接続拠点について、現在設置されているオンプレミスタイプの UTM をクラウド型次世代ファイアウォールへ移行、又は新規追加作業を行うこと。

イ　現行セキュリティの構成概要

各接続拠点間は閉域網ネットワークで接続されている。各接続拠点内ネットワーク(L3)と閉域網ネットワークの境界にはオンプレミス型の UTM 装置が配置されている。ただし、現時点で接続端末が1台のみである県立病院課については、UTM 装置やルーター機器は配置されていない。

ウ　接続拠点

(ア) 山形県病院事業局 県立病院課

〒990-0023 山形県山形市松波二丁目 8 番 1 号

接続端末数:6台

(イ) 山形県立中央病院

〒990-2292 山形県山形市青柳 1800 番地

接続端末数:1,350 台

(ウ) 山形県立新庄病院

〒996-8585 山形県新庄市金沢 720 番地 1 号

接続端末数:600 台

(エ) 山形県立河北病院

〒999-3511 山形県西村山郡河北町谷地月山堂111

接続端末数:350 台

(オ) 山形県立こころの医療センター

〒997-8510 山形県鶴岡市北茅原町 13-1

接続数:250 台

エ　業務概要【保守・運用支援業務】

保守・運用支援業務の内容については、以下のとおりである。

(ア) ライセンスの提供

契約期間中、次世代ファイアウォールのライセンスを利用できること。

(イ) 問い合わせ業務

次世代ファイアウォール及びエージェントソフトの利用方法に関する質問に対応すること。ただし、担当職員の異動に伴い基礎的な情報から全体を網羅するような説明対応などについては、本契約においては1回を上限とし、これを超えた場合は別途有償対応を原則とする。

(ウ) 監視業務

次世代ファイアウォールの死活状況、CPU、メモリ使用率をモニタリングし、異常時に利用者に通知し、ネットワークの制限、復旧までの支援等の作業を行うこと。また、必要に応じて調査のため、技術員の手配を行うこと。

(エ) セキュリティ監視

IPS のイベントをモニタリングし、セキュリティ上の問題があるかどうか確認し、利用者へ通知すること。FW、IPS の設定で対応可能な場合は設定変更の実施を行うこと。

(オ) 障害回復支援

障害発生時において、問題の切り分けや稼働確認の支援など、電話やリモート接続などにより復旧支援を行うこと。ただし、基本的にはクラウド上での対応で終息することが想定されるため、各接続拠点での現場対応については、本契約においては1回を上限とし、これを超えた場合は別途有償対応を原則とする。

(カ) 設定変更

委託者の依頼に基づき、以下機能について設定変更を行うこと。本契約においては6件を上限とし、これを超えた場合は別途有償対応を原則とする。

・ファイアウォール
・IPS(侵入防止)
・IDS(侵入検知、ふるまい検知)
・アプリケーション制御・URL フィルタ

(キ) マルウェア検知通知

クラウドサンドボックス機能などで検知したマルウェアについて、検知リストを作成しメールで通知すること。

(ク) 月次レポート

月別の稼働状況をまとめてレポートを作成し、送付すること。
月次レポートには、以下の項目を最低限含めること。

・攻撃遮断リスト
・最近の事例の情報提供

(ケ) セキュリティ定期報告会

Web 会議又は訪問により、月次レポートの報告と、ポリシー設定についての提案を本契約においては最低でも1回は行うこと。

(コ) ファームウェアアップデート

必要に応じてリモートでファイアウォールのファームウェアのアップデートを行うこと。特に支障がない場合には基本的には最新のファームウェアアップデートを無償で適用すること。

(サ) 保守記録の保管と提出

期間中の保守記録を全て保管し、委託者の依頼に基づき提出すること。

(シ) その他

期間満了や中途解約時に、他ベンダーが現稼働状態を移行可能とする引継ぎ資料及びデータを作成し提供すること。

(3)受託要件

ア　業務詳細

(ア) 汎用性、拡張性の観点から、各接続拠点間通信を現行の閉域網に代わり、光インターネットにより各種通信プロトコルによる接続を可能とするため、従来型ファイアウォール機能に加えて、アプリケーションの制御、ユーザーの識別、アンチウイルス、不正侵入防御、アンチスパイウェア、URL フィルタリング、クラウド型サンドボックス機能等を持つクラウド型次世代型ファイアウォールを導入すること。

(イ) 導入するクラウド型次世代ファイアウォールは運用サービス付属型であること。

(ウ) クラウド型次世代ファイアウォールは、モジュール方式のクライアントで実現するファブリック VPN エージェントソフトを利用することで、個別の専用ルーター

等を使用しなくとも各接続拠点への安全なリモート接続を可能とし、医療情報システムベンダーのリモート保守でも利用可能な機能を有していること。

なお、各接続拠点へのリモート保守を想定している医療情報システムベンダー数は以下のとおりであるため、必要数のファブリック VPN エージェントソフトを提供すること。ファブリックエージェントの操作説明は各接続拠点の担当者へ個別に実施し、各接続拠点の担当者がそれぞれの医療情報システムベンダーへ配布するマニュアルも提供すること。また、ファブリックエージェントは、原則として各接続拠点の担当者から各ベンダーへ配布するため、インストーラーと設定情報についても提供すること。

・山形県病院事業局 県立病院課　0社
・山形県立中央病院　50社
・山形県立新庄病院　40社
・山形県立河北病院　35社
・山形県立こころの医療センター　25社

(エ) 機器の死活状況の監視を行い、異常時には委託者へ通知し、必要に応じて機器の交換又は修理を追加費用無しで行うこと。

(オ) リモート保守に必要な光回線（1回線）とプロバイダ契約は委託者が実施し、回線月額費用も委託者が負担する。

(カ) 各接続拠点間接続に必要な光回線（全5回線）とプロバイダ契約は委託者が実施し、回線月額費用も委託者が負担する。

3 委託期間

契約締結の日から令和6年3月31日までとする。

なお、構築完了日は、令和6年1月末日までの間で委託者と協議の上決定し、その日までにすべての接続拠点で構築を完了し、構築が完了した接続拠点から保守・運用支援業務を提供すること。

4 履行場所

本業務の履行場所は各接続拠点とするが、クラウド型次世代ファイアウォール以外で各接続拠点に必要な機器がある場合については、各接続拠点内に設置すること。

5 提供物件

(1) ハードウェア及びソフトウェア

本業務に必要となる全てのハードウェア及びソフトウェアを調達すること。 調達するハードウェア及びソフトウェアは、契約期間内において、保守可能であること。契約期間中に調達した製品のサポートが終了する場合は、受託者の責において後継製品や同等の性能を持った代替製品への移行を行い、継続してサービスが提供できるよう対応すること。なお、当該製品にかかるサポート終了についての情報を知りえた段階で、委託者に対して報告を行い、承認を受けたうえで、サービスが途切れることなく提供できるよう対応すること。ソフトウェアライセンスについては、接続拠点の利用者数又は端末数の最大数を考慮して、必要十分な数量を準備すること。また、保守・運用支援業務開始後に受託者の依頼により発生する可能性のあるライセ

ンスの追加について、あらかじめ追加方法、金額等を提示すること。
なお、委託者に設置するハードウェア及びソフトウェアについては、委託者の資産とはしないものとする。

(2)ドキュメント
受託者は本委託業務を実施するうえで、必要となるドキュメントについて、委託者に納品すること。納品方法は、電子媒体と紙面での納品を各1 部とする。なお、電子媒体のファイ ル形式については、委託者と事前に協議を行い、決定すること。ドキュメントの詳細は「8 調達全般に関する共通要件(5)ドキュメント」を参照すること。

6 費用内訳資料の提出
契約締結後、速やかに、契約額の内訳資料(税抜き金額を明記すること。)を作成し提出すること。この場合、構築費用と保守・運用支援費用について、明確に分離すること。

7 機密保持
本委託業務は、「医療情報システムの安全管理に関するガイドライン」(厚生労働省)の最新版、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」(総務省・経済産業省)の最新版、「山形県情報セキュリティポリシー」、並びに各病院の情報セキュリティポリシーを遵守するとともに、「ランサムウェアによるサイバー攻撃に関する注意喚起」(2021年4月30日付け内閣サイバーセキュリティセンター重要インフラグループ)に準じた対策を行うこと。上記に抵触する行為又は事象が発生した場合や、そのような恐れがある場合は、委託者に報告し、委託者の指示のもと速やかに対応すること。
業務遂行上知り得た個人情報、山形県及び各接続拠点に関するすべての機密事項について、本委託業務のみに利用するものとし、契約期間中又は契約終了後を問わずに第三者に漏えいしないこと。
それぞれの契約による事務を処理するための個人情報の取扱いについては、契約書別記「個人情報の取扱いに関する特記事項」を遵守すること。

8 調達全般に関する共通要件
(1)プロジェクト管理に関する要件
ア プロジェクトの体制
(ア) 受託者は、本委託業務の遂行を確実に実施できる履行体制(支援体制含む。)を確保すること。
(イ) 作業に従事する者が、委託者並びに関係者と十分な協力体制を確立できるようにすること。

イ プロジェクト管理
(ア) 受託者は契約締結後速やかに、業務計画書を作成のうえ、委託者に提出し、委託者の承認を得たうえで業務を実施すること。原則として、委託者と合意した業務計画に従って業務を実施すること。
(イ) 業務の実施に当たり、進捗管理、品質管理、変更管理を徹底すること。なお、業務計画書の内容に変更が必要となる場合は、委託者と協議し、承認を得たうえで、変更を行うこと。

(ウ) 必要に応じて適宜ミーティング等を実施し、委託者に対し報告及び作業内容の説明・協議を行うこと。

(エ) 全ての作業において、委託者が提供した、個人情報を含む業務上の情報は細心の注意をもって管理し、第三者に開示又は漏洩しないこと。また、そのために必要な措置を講ずること。

(2) 委託者からの提供資料

現行ネットワーク情報及びセキュリティに関する構成詳細、ハードウェア・ソフトウェア構成にかかる情報、監視・保守・運用支援にかかる情報については、競争入札参加資格確認申請により有資格者であることが確認され、守秘義務に関する誓約書を提出した者に対して開示することが可能である。

(3) 責任分岐点

各接続拠点にはネットワークの接続口である「L3又はL2 スイッチ」が整備されており、ネットワークに接続するだけで全ての接続拠点の本来対象とすべきではない他システムとの通信が可能となってしまう。

このことから、勤務管理システム、導入予定の統合DWHシステム以外の他システムとの接続を制限するため、本委託業務における責任分岐点を、「L3又はL2 スイッチ」における接続ポートと、ネットワーク側ルーターまでとし、これらの境界における、ゲートウェイ機器等の設置及び設定を受託者の責任で実施すること。また、医療情報システムベンダーによるリモートアクセスに関しては、各ベンダーの対象システム以外へのアクセスが出来ないよう制御できるものとするが、個々のポリシーについては各接続拠点と医療情報システムベンダー間で締結する契約の範疇とする。

(4) 他の受託事業者との調整

ア 接続拠点関連

各接続拠点の担当者の他、各接続拠点における既存ネットワーク及び既存システム(医療情報システム等)の既存事業者と協議等が必要となる場合は、委託者に報告し、承認を得た後に、受託者の責により調整を行い、実施すること。各接続拠点の既存事業者との協議等を行う場合は、各接続拠点の担当者が指定する場所での協議を基本とする。なお Web 会議等を実施の場合は、各接続拠点と調整すること。なお、既存ネットワーク事業者において当該調整に関する費用は本契約の範囲外とする。

イ 設定変更等の依頼

(ア) 既存事業者が導入した機器等について、本委託業務を実施するうえで設定変更等が必要となる場合は、委託者に報告し、承認を得た後に、それらの機器を所管する既存事業者と協議を行うこと。なお、機器等の設定変更に関する設計については、受託者が主体的に実施すること。また、これら設計については、委託者、接続拠点及び関係する既存事業者に対して説明を行い、設定変更内容についての承認を受けること。

(イ) 実際の設定変更作業は、関係する既存事業者との既存契約の範囲内の内容に限り、各接続拠点を通じて依頼することが可能だが、契約の範囲を超える内容については、委託者と協議の上実施すること。

(ウ) 既存事業者への問い合わせ等については、既存契約による対応が可能だが、本契約における作業時の立会等については、既存事業者ごとに対応が分かれるため、事前に確認すること。

(エ) 運用期間において、既存ネットワーク又は既存システムの再構築が行われる可能性があり、その際、セキュリティの設定変更や立会い等が必要になる場合がある。その場合についても、各接続拠点等との協議や、セキュリティ側の設定変更等について、各接続拠点等の依頼に基づき、対応すること。なお、これに伴うハードウェアの増設やソフトウェアにかかるライセンスの追加等が必要になる場合は、本契約の範囲外とする。

(5) ドキュメント

受託者は以下のドキュメントを指定された期日までに、委託者に納品すること。

ア 業務計画書

業務計画書の内容は以下のとおりとする。

(ア) 業務スケジュール

(イ) 業務遂行体制、業務従事者名簿

(ウ) 工程完了判定基準

イ その他設計書等

受託者は各工程の計画、成果を示すドキュメントを作成し、構築完了後1か月以内に完成図書として納めること。完成図書はデータCD1枚、及び印刷したパイプ式ファイル1ファイルに収めて1編を各拠点に納品すること。想定するドキュメントは以下のとおりとする。ただし、各工程に着手する前に、当該工程において作成するドキュメントに関し、委託者と協議を行うこと。

(ア) 保守・運用支援設計書

(イ) セ キュリティ等 監視設計書

(ウ) 各種設定一覧

a 設計概要

(a) 設計範囲

(b) 設計条件

b 構成設計

(a) 物理構成・接続構成

(b) 論理構成

c 機器一覧

機器名、型番、OS バージョン、IP、MAC 等の情報全て記載

d 収容設計

(a) ラック収容図

(b) ポート接続一覧表

e 装置名称付与

装置名称の付与規則

f IP アドレス及び VLAN 設計

(a) IP アドレス体系

(b) VLAN 及びネットワークアドレス

(c) VRF VLAN 割り当て

g ルーティング設計

h トラフィック制御設計

i リモート VPN 接続設計

j 認証設計

k システム運用設計

(a) 時刻同期方式

(b) ネットワーク監視方式

l パスワード一覧

m 各種設定一覧

config 等、設定したもの全てを提出すること

n テスト結果（全て）

ウ 保守・運用支援報告書

運用開始後、保守・運用支援に関する報告書を提出すること。

報告書は、契約書に定める業務完了報告書に併せて提出すること。

報告書の記載事項は別途協議により定める。

(6) 使用言語

本委託業務においては、会話及び文書、メール等、全てのコミュニケーションにおいて日本語を使用すること。

9 各種業務における詳細要件

(1)設計業務全体にかかる要件

ア 基本方針

以下の内容を踏まえ、セキュリティの安定した稼動、業務の継続性を第一とし、構築期間、保守・運用支援期間を通じて、安全で確実な運用が可能となるような設計とすること。

(ア) 定変更等の作業を実施する場合は、設定ミス等に起因するリスクや、作業に伴うサービス停止時間の短縮を考慮し、必ず、作業手順書を作成し、各作業に対するテストやリハーサルが可能となるようにすること。

(イ) 本業務を実施する中で、障害等の発生により作業が中断した場合を考慮し、可能な限り、切り戻し手順についても設計を行うこと。

(ウ) 委託者の担当職員が実施しなければならない作業がある場合は、作業時間を考慮し、余裕をもって伝えること。

(エ) 各接続拠点の担当職員及び関係する既存事業者等に対して、作業の依頼や立会等の依頼を行う場合は、拘束時間を短くするなど、負担が極力少なくなるよう留意すること。

(オ) 作成した設計書、手順書等については、作成の都度、委託者に対して説明を行い、承認を得ること。

(カ) 各接続拠点の担当者が監視ツールを利用できるようにすること。その権限を設定すること。その利用手順書を作成すること。

(キ) デフォルトの管理アカウント・パスワードの変更を全て必ず行うこと。不要なサ

ービスやポートの無効化を行うこと。

(ク) 設定データは変更都度バックアップとその復旧テストを実施すること。

(2) 調査にかかる要件

ア　各接続拠点における調査及びヒアリング

以下の内容を踏まえ、セキュリティを利用する各接続拠点にかかる事前調査を行うこと。

(ア) 現地確認の際は、各接続拠点の担当者の他、各接続拠点における既存ネットワークは既存システムの既存事業者等からヒアリングを行い、意見・要望等の他、障害情報、機器更新等の変更予定等の情報についても収集するとともに、必要な連絡体制についても確認すること。

(イ) 本契約において想定される、各接続拠点における既存ネットワーク及び既存システム等の設定変更時における、立ち合いの可否や、設定変更等に対する作業依頼の可否についても確認すること。

(ウ) 今回の拠点間接続ではプライベートアドレスからグローバルアドレスに変換する必要があるため、設置されるGW機器にて、NAT変換の必要性を確認し、設計に含めること。全ての機器にリモートできるように施設ローカルIP⇔拠点間IPにNATすること。その際のセグメントは理解しやすいように整理すること。IPやセグメントが増えた場合に十分対応できるように余裕を持ったセグメント設計を行うこと。

(エ) 山形県立中央病院に設置されている勤務管理システムサーバーに接続するために各接続拠点病院のL3スイッチ等にルートの記述が必要である場合は、各接続拠点の担当者などと調整を行うこと。ただし、この設定変更に係る既存ネットワークベンダーにて発生する費用は本契約の範囲外とする。

(オ) 勤務管理システムサーバーは山形県立中央病院に設置されているが、同病院も当該サーバーに折り返しの通信をすることから、山形県立中央病院内におけるUTMの機能についても考慮し、設計及び機器の設置を行うこと。なお、山形県立中央病院に設置するVPN兼UTM装置の機能は下記のとおりとする。

・ファイアウォール スループット(パケット/ 秒) : 15 M bps

・IPSec VPNスループット: 11.5 Gbps

(カ) 看護勤務管理システムほか、今後導入予定である統合DWHシステムについても、各接続拠点病院からは医療情報システム系のVLANからの接続を行う。このため、各接続拠点内外で利用のすべてのVLANの体系を詳細まで把握し、IPの競合などが発生しない仕組みを提供すること。なお、既にIPが重複し、運用に支障を来たすと判断した場合には、対象の接続拠点に報告のうえ、VLAN設定変更などの助言を行うこと。

(キ) 各接続拠点の機器設置場所、電源、LAN配線について、事前に十分に確認し提示すること。本導入において発生した各種配線については本委託に含まれるものとする。なお、電源工事や電源に関する配線の敷設等は含まれない。

イ　その他の既存事業者に対する事前調査

(ア) 委託者が別途提供する、現行ネットワーク設定及びセキュリティの詳細情報に関する資料について、内容を確認すること。

(イ) 本契約において想定される、設定変更時における、立ち合いの可否や、設

定変更等に対する業務依頼の可否についても確認すること。

(3)運用設計にかかる要件

運用設計として、本委託業務における要件について、委託者との十分な協議の上、確認を行い、具体的な運用方法を決定すること。

(4)運用開始にかかる要件

各接続拠点がセキュリティの運用を開始するために必要となる条件等を事前に洗い出し、各接続拠点の準備遅延や、感染症拡大による日程順延、運用開始後の障害発生による切り戻しの実施等の理由により、予定通りに運用切り替え作業が進まない場合も考慮し、期間内に全ての作業が完了するよう、余裕を持ったスケジュールとすること。 手戻りをなくし、かつ、障害発生をできる限り発生させないための工夫を講じること。

各接続拠点への影響を少なくするよう、各接続拠点におけるネットワークや各種サービス停止時間を最小限に抑え、かつ、安全で確実に実施可能な切り替え作業ができるよう留意すること。

運用切り替え作業実施当日において、障害発生等により作業が中断した場合、迅速にその原因を明らかにし、作業を再開できるよう又は次の機会へとつなげられるよう、あらかじめ、発生する障害等を想定し、その内容を手順書等として準備しておくこと。

作業実施時には、各接続拠点における既存ネットワーク機器や既存システム等において、設定変更等の現地作業が発生すると想定しているが、各接続拠点の担当者及び各接続拠点における既存ネットワーク又は既存システムの既存事業者等に対して、できる限り作業が生じないよう配慮すること。やむを得ず、各接続拠点の担当者及び各接続拠点における既存ネットワーク又は既存システムの既存事業者等に対して、作業を依頼する場合は、説明用の資料や手順書等を用意し、事前説明や事前のリハーサル、当日の作業立会等を行うなど、確実な移行作業が実施できるよう留意すること。

(5)保守・運用支援業務の設計にかかる要件

ア 基本方針

(ア) セキュリティにかかる保守・運用支援業務を行う上で必要となる体制が確立していること。

(イ) 各接続拠点の担当者にかかる業務負担軽減とセキュリティ・可用性の向上のそれぞれを考慮すること。

(ウ) 構築が完了した接続拠点から保守・運用支援業務の提供を開始すること。

イ 総合窓口

以下の内容を踏まえ、各接続拠点における担当職員からの問合せ、障害申告の受付及びインシデント登録、対応等を受け付けることができる総合窓口を設置すること。

(ア) 各接続拠点からの問い合わせに直接対応すること。

(イ) 窓口への連絡手段はメール及び電話など、柔軟な連絡手段を用意することとし、運用期間中に継続して利用できる連絡先として、電話番号及びメールアドレスを用意すること。連絡先は複数体制とし、担当者の交代や不在情報などは遅延なく連絡すること。

(ウ) 障害発生時や、緊急度の高いセキュリティインシデント発生時への対応として、夜間休日問わず24時間体制の受付対応ができること。
(エ) 災害など万が一の事態に備え、複数の拠点を有するなど日本国内に二重化された体制を自社で有していること。

ウ　稼動監視・障害対応

以下の内容を踏まえ、セキュリティで提供される各種サービスに対して稼動監視・障害対応を行うこと。

(ア) アラートメールや、各接続拠点からの障害等の報告を受けた場合は、障害の一次切り分け、障害発生ポイント等の特定、暫定対応等の実施、各接続拠点の担当者への報告などを速やかに行こと。その対応フローについては、事前に委託者の承認を受けること。一次報告書を1日以内、最終報告を解決後1週間以内に提出すること。問題解決が長期にわたる場合は二次報告書を1週間以内に提出すること。重大事象の最終報告書報告期限については、別途協議の上定めることとする。報告書には障害内容と範囲、時系列の事象及び対応内容、根本原因、再発防止策を記載すること。

(イ) 監視対象として、各サービスの提供状態の他、本委託業務にて調達した機器に対する疎通確認を行うこと。

(ウ) 障害等に対する一次切り分けの結果、本委託業務の範囲外の要因による障害の場合は、あらかじめ、決められた対応フローにより、各接続拠点への報告を行えるようにすること。

(エ) セキュリティで提供する各種サービスが提供できなくなるなどの重大な事案（機器障害、外部からの攻撃等によるサービス停止など）については、夜間休日問わず24時間体制の受付対応及び稼働監視を行うこととするが、ハードウェア交換を伴うような現地対応については、委託者と協議の上迅速に行うこと。

(オ) 障害対応については進捗を管理し、完了まで責任を持った対応を行うこと。

(カ) SOCを設置し、24時間365日体制でネットワークやデバイスを監視し、サイバー攻撃の検出や分析、対応策のアドバイスを行うこと。これについては、クラウド型次世代ファイアウォールの保守・運用支援実績があり、日本国内に2か所以上の自社拠点を有することで冗長化が図られていること。また、認定ホワイトハッカーが監視業務に係わり、高度なオペレーションを提供すること。

エ　調達した機器に対するリスク管理

(ア) 本委託業務にて調達した機器に対するリスク管理を行うため、脆弱性情報等の収集を行い、委託者に対しても積極的に提供すること。

(イ) 安定的な運用のために適用が必要なファームウェアバージョンアップ等については、セキュリティ上のリスクを考慮のうえ、必要に応じ実施できること。なお、緊急対応が必要な場合は、委託者と協議すること。

オ　構成情報の更新対応

運用期間中において、稼働監視・障害対応、設定変更対応、調達した機器に対するリスク管理等の業務により、セキュリティにおけるシステム構成や設定内容等に対して変更があった場合、更新履歴を残したうえで、各種設計書における必要な情報の更新をすること。

カ　セキュリティ監視等業務の設計にかかる要件

セキュリティ監視、調査、解析等の業務を行うために必要となる設計を行うこと。クラウド型次世代ファイアウォール監視等の設計に当たっては、以下の要件を満たす設計とすること。

①総合窓口の所在地は、日本国内とすること。

②総合窓口は夜間休日問わず24時間体制の有人運用とすること。

キ　性能要件

(ア) 各接続拠点が、契約期間終了時まで利用できる十分な性能とすること。(稼働率を99.9%以上とする。)

(イ) 各接続拠点にはクラウド型次世代ファイアウォール及び拠点間通信に必要なVPN装置を導入すること。なお、なお、瞬間停電に耐える程度のUPS(無停電電源装置)を3年保障付きの製品として設置すること。また、VPN装置はネットワークスイッチが格納されるラックにマウントすること。

(ウ) 拠点間通信に必要なVPN装置は統合された監視、ファームウェア更新、保守サービスが付帯されていること。

(エ) 山形県立中央病院に設置されるVPN装置はUTMの機能も有し、院内折り返し通信に必要なポート数(GbEインタフェース(RJ-45)を12)を有すること。

(オ) 各接続拠点から山形県立中央病院に設置されている勤務管理システム用サーバーに向けた通信及び勤務管理システム用サーバーから各接続拠点内に向けた通信について、ボトルネックが発生しない性能とすること。

(カ) クラウド型次世代ファイアウォールについて、本仕様書に記載された業務を滞りなく運用できる帯域及び 機能を提供するにあたり、十分な性能を有すること。

(キ) クラウド型次世代ファイアウォールについて、本仕様書に記載された業務を滞りなく運用できる帯域及び 機能を提供するにあたり、十分な性能を有すること。

(ク) 考慮すべき帯域は以下のとおりとする

・Threat Preventionスループット:約5.3Gbps

・ファイアウォールスループット:約7.8Gbps

・IPsecVPNスループット:約2.2Gbps

・セッション数:上記スループットを担保する場合は500を想定とするが、通信速度を配慮しない場合には上限は無いものとする。

(ケ) フィルタリングルールの設定によって体感速度が低下しないような性能を持つこと。

以上