第三次医療情報通信ネットワーク構築業務
仕様書

２０１９年１月

地方独立行政法人　宮城県立こども病院

目　　次

（５）セキュリティ対策業務
イ）ライセンス管理
ロ）セキュリティ向上対応
ハ）IPA（情報処理推進機構）等の公的な情報セキュリティ機関等からの情報収集
ニ）セキュリティインシデントの影響調査及び連絡等
ホ）セキュリティ対策業務の情報管理
ヘ）パスワード・アクセス権管理
（６）障害予防業務
イ）定期点検の実施
ロ）緊急点検の実施
ハ）予防保守の実施
ニ）UPS の管理
（７）障害の対応
イ）障害対応計画
ロ）原因及び影響調査
ハ）障害発生時の動作
（８）報告等
イ）月次報告
ロ）年次報告
ハ）報告形式
（９）災害対策
イ）体制
ロ）業務継続計画(BCP)の確認
ハ）災害対策訓練の実施
（１０）その他
５　サービス水準合意（SLA）
（１）SLA の対象項目
（２）SLA の改定方法
（３）サービス水準のモニタリング
（４）SLA 評価項目と設定値
イ）問合せ窓口
ロ）監視
ハ）障害対応
ニ）セキュリティ対策
（５）モニタリング
イ）モニタリングの基本方針
ロ）モニタリング項目
ハ）サービス未達成時の対応
６　その他保守業務
（１）OA 系端末保守業務
イ）初期設定・設置業務
ロ）既存医局系端末・プリンタの接続確認
ハ）保守業務
ニ）その他
７　問い合わせ窓口業務
（１）基本事項
（２）問い合わせに対する処理
（３）エスカレーション
（４）回答
（５）障害等に対する処理
（６）ナレッジ管理

第１　調達案件名

第三次医療情報通信ネットワーク構築業務（以下，「本業務」という。）

第２　調達の概要

１　調達の背景と目的

宮城県立こども病院（以下「当院」という。）は，東北唯一の小児周産期・高度専門医療施設　として 2003 年に開院し，2016 年には小児リハビリテーション施設の中核である拓桃医療療育センター機能を引き継ぎ，在宅医療までを一貫して担う施設として展開している。また，医療情報システム等の整備について，費用対効果，県民の医療・療育需要，医療技術の進展等を総合的に勘案し，財源を含め投資計画を策定し，計画的な更新・整備を行うとともに，その効果的な活用を図ることとしている。

現在，電子カルテシステムを中心とした第二次医療情報システムが構築後５年を経過し部門システム（産科，手術，ICU，生体情報管理システム）との連携が進展している中で，ネットワークの重要性が増大しており，保守・運用の迅速性や障害発生リスクの低減が重要な課題となっている。また，高額なコストが発生しており財政運営が厳しい状況のなかより効率的・効果的な予算執行が求められておりトータルコストの削減が必要となっている。更には，院内の様々な部門システムの基盤となり，音声や映像によるコミュニケーションなど院内業務の効率化に資する新たなネットワークの構築が必要となっている。

第三次医療情報通信ネットワーク（以下「次期ネットワーク」という。）では，これら課題を解決するとともに，構築から運用まで一貫性がある効率的なネットワークを実現しなければならない。また，次期ネットワークの移行にあたっては，業務システムへの影響を可能なかぎり低減し迅速に実施するものとする。本業務の受注者は，上記の課題を踏まえて適切に調査検討及び提案を行い，単にネットワークを構築及び運用等を行うだけでなく，長期的な視点からも当院の課題の解決が図られるよう，業務を遂行しなければならない。

2013 年度に稼動開始した現行の第二次医療情報システム（以下「現行システム」という。）は，今年度で 6 年目となる。システム機器は，標準保守終了を迎えていることから，保守部品が枯渇する可能性もある。また，使用しているサーバＯＳ（Windows2008）は，2019 年度にマイクロソフト社のサポートが終了となる。

２　定義

用語の定義を下表に示す。

用語	説明
現行ネットワーク	2003 年 10 月に第一次医療情報通信システムを構築。2012 年度に第二次医療情報システムと合わせて再構築して，その後 2016 年 3 月には宮城県拓桃医療療育センターの統合に併せて，改修し現在運用している院内の基幹ネットワーク
現行システム	2013 年度に運用開始した，電子カルテシステムを中心とし一部の部門システムを含む，第二次医療情報システム
外部連携ネットワーク	遠隔カンファレンスなどの病院間等で接続する外部のネットワーク
医療系	本館及び拓桃館を接続して，電子カルテシステムなど院内の医療情報システム，及びグループウェアで利用する他，将来的にマイナンバーを利用するシステムの接続も想定しているセキュリティの高いネットワーク(インターネット接続不可)
OA 系	グループウェア，OA システムで利用する他，インターネットと接続し，電子メールの送受信及び Web 閲覧等による情報収集などで利用するネットワーク。電子メールは，既存の当院ホスティングメールサーバを活用（現行の POP メールから Web メールサービスへ契約変更を予定している）
部門系	個別部門の業務システムが利用するためのネットワーク
共有系	各系ネットワークのデータ連携のためのファイル転送システムなどを設置するための，内部 DMZ

音声系	別調達で更新するナースコールシステムなどの音声通信に利用するネットワーク
医局系	外部端末機をインターネットに接続して利用するためのネットワーク。電子メールは，既存の当院ホスティングメールサーバを活用（現行の POP メールから Web メールサービスへ契約変更を予定している）
外部持込端末機	講演会等，外部医師がピンポイントで持込する個人端末である。院内カンファレンス会場等で使用する。インターネット利用のみを想定。(macOS 端末機を含む)
外部端末機	医局に設置する医師持込端末である。インターネット利用のみを想定。(macOS 端末機を含む)

3　現行ネットワークの概要

〈別紙 1〉現行ネットワーク構成概要図を参照のこと。

4　次期ネットワークの概要

次期ネットワークは，電子カルテシステムが接続するだけでなく多くの部門システムや外部連携ネットワークが接続する基盤で，総合的なマネジメントにより，様々なシステムが円滑に利用できる環境を構築する必要があることから，今回は，電子カルテシステム構築とは別に本調達して独自に構築するものとした。

構築にあたっては，関係するセキュリティのガイドライン等を踏まえた上で，ネットワーク機器の更新の他，近く計画しているナースコールシステム更新の事前準備として無線 LAN の接続環境を拡充等，院内の業務改善を図るとともに，サイバー攻撃に対応したセキュリティ機能の高いネットワークを目指すものとする。

更に，次期ネットワーク構築で必要となる重要事項を次に掲げる。なお，下記の事項について，提案書に記載して提示すること。なお，“【必須】”と記載している事項については必須提案とする。

本調達において，当院が想定する総務省のガイドラインに則った基本要件イメージは，〈別紙 2〉第三次医療情報ネットワークの主なセキュリティ基本要件に示すとおりである。基本要件イメージ図を基に次期ネットワークの全体構成を検討し，提案すること。なお，〈別紙 2〉は，あくまで参考例であり，提案を妨げるものではないが，総務省や厚生労働省など，関係するセキュリティガイドラインに準拠した提案であること。

また以下記載の各機能に対する各セグメント(医療系，OA 系，医局系)の利用範囲については〈別紙 3〉各セグメントが利用する機能のとおりであり，〈別紙 2〉と合わせて提案の参考とすること。

【次期ネットワーク構築で必要となる重要事項】

（1）作業体制及びプロジェクトの管理【必須】

・事業者の構成(企業連合・再委託を行う場合は，その理由及び内容）および導入実績

・プロジェクトマネージャーの資質等(同等以上の実績，専任期間)

・プロジェクト管理の手法，ツール等(管理手法，管理組織の実績)

（2）ネットワーク移行の手法等【必須】

・移行方法の概要(手順，期間，作業体制，人数，実績)

・ネットワーク移行による病院業務等へ与える影響(業務への影響，既存ネットワークやサーバ機器及び職員端末等の移行・設定・確認作業)

・ネットワーク等移行障害への対応(想定される障害の範囲，テスト体制，確認及び切り戻し方策等)

・同等規模(構成や端末数 600 台以上など)以上のネットワーク移行実績と成果

（3）医療情報システムベンダー(部門ベンダーを含む)との連携【必須】

・電子カルテ・部門システム事業者等との調整体制及び実績

・電子カルテ・部門システムの接続確認・検証の方法

（4）次期ネットワークの機能【必須】

イ）ネットワークの効率的な構成

・構築から運用まで一貫性があり効率的な構築
※NTP(TIME)サーバ，DHCP，プロキシサーバ(OA 系，医局系)，AD 連携等
・ネットワーク・サーバ機器の機能活用と台数の最適化
※仮想サーバによる提案も可とする
・監視システムの機能向上(監視対象機器の強化，障害判別・対応の迅速化など)
・LAN ケーブルの老朽化に対応した再敷設
・機器障害時の即時切り替え可能な冗長化構成
・ネットワーク分離と業務効率の維持
※USB 利用によるファイル交換業務等で業務効率の低下が予測される。これに対する防止策について提案すること。
・無線 LAN の拡充による可用性と省力化の促進
※近く計画しているナースコールシステム更新の事前準備として，PoE スイッチまでの拡充と病棟を中心に AP 増設を想定している。。PoE スイッチは，将来的な AP の拡張に対応できるものとする。提案時の参考資料として，〈別紙 4〉無線 AP 配置図案を添付する。
なお，〈別紙 4〉は，全館に無線 AP を配置した場合の参考例であり，提案を妨げるものではない。

ロ）ネットワーク連携の強化(シームレスなネットワーク環境)
・外部ネットワークとの接続(MMWin，遠隔医療，カンファレンス会議など)
※Mmwin 含め 5 接続程度 。〈別紙 5〉外部接続関連概念図参照。
※〈別紙 5〉のとおり、現在はファイアウォール機器を外部接続単位で設置しているが、集約して制御する等、最適化した構成で提案すること。
・部門システムネットワークとの接続
※放射線，産科，手術 ICU，術野カメラ，生体情報，保管温度監視(薬剤・検査)など

ハ）セキュリティ対策の強化
〈別紙 2〉第三次医療情報通信ネットワークの主なセキュリティ基本要件を参照。
・ネットワーク分離論理分割
※医療系と OA 系の分離（医療系，共有系，OA 系，医局系）
・高度なセキュリティ対策
※サイバー攻撃等への対応については，以下にあげる項目について，セキュリティ，価格面で最適な提案をすること。
【必須提案】
・ウイルス対策ソフト，ファイアウォール，IPS/IDS， URL フィルタ，ログ収集サーバ，ネットワーク監視など)
※セキュリティ基盤はオンプレミスの他，クラウドサービスによる提案も可とする。
【自由提案】
・振る舞い検知装置，サンドボックス，マルウェア・スパイウェア対策機器，Web 無害化，グループウェア等の内部メール無害化，ログ分析システムなど

・端末機からの情報持ち出しの制限
・強力なアクセス制御
・医療系／OA 系／医局系の通信のリスク対策
※各系間でファイル転送時する場合の安全対策
OA 系と医療系，及び医局系(新規導入)で相互利用可能なファイルサーバの設置，及びファイル転送の承認，転送時のファイル無害化/暗号化/検知機能等
・外部持込端末機の接続環境
※外部持込端末機：講演会等，外部医師がピンポイントで持込する個人端末である。院内カ

ンファレンス会場等で使用する。インターネット利用のみを想定。

・医療系も含めた全端末機の資産管理ソフトの新規導入

※資産管理対象機器は，約 1,800 台とし，内 USB 等のデバイス制御対象は 700 台)，を想定している。想定品：skysea，AssetView 等の管理ソフトウェア)

・無線 LAN 認証暗号化の対応

ニ）外部端末とグループウェア【必須】

・外部端末機の接続環境

※外部端末機：医局に設置する医師持込端末である。インターネット利用のみを想定。

・グループウェアの更新

※医療系も含めた全端末で 600 ユーザ，想定品：サイボウズガルーン

（5）次期ネットワークの品質【必須】

・品質管理の手法

・テストの計画

・受注者の社内レビュー体制

（6）保守の体制等(障害時の迅速な体制，対応の確立)【必須】

・保守要件

・監視業務

・セキュリティ対策業務

・障害予防業務

・災害対策

・サービス水準合意（SLA)

5　調達の範囲

（1）本業務の範囲

本業務は，現在稼動中の院内ネットワークを構成する伝送機器，伝送路及び管理機器並びにそれらに付随する設備を更新し，これまで以上に高速かつ安定化した次期ネットワークとして再構築するとともに，セキュリティレベルや機能の向上を図るものである。本業務の区分は，ネットワーク等に係る設計，設定・設置，試験，導入，移行等の構築業務及び監視，保守等の業務とする。また，本業務には，各部門システム及び外部連携ネットワークとの接続調整，及び次期ネットワーク側の接続設定を含むものとする。

（2）本業務の概要

区分		作業項目
構築業務	プロジェクト管理	本調達に係るネットワーク・サーバ等の設計・構築，OA 系端末の導入，試験及び移行等のプロジェクト全体管理を行うこと。また，業務範囲に部門システム事業者及び外部連携ネットワーク運用事業者との接続調整を含む。なお，第三次医療情報システム構築業務の受注者とスケジュールを調整すること。
	設計	要件を再確認し，ネットワーク・サーバ等の基本設計，詳細設計及び設定情報等の作成を行う。作成した設定情報等をネットワーク・サーバ機器等に投入し稼働に必要な調整作業を行う。
	サーバ設定・設置	ラック本体据付作業（ネットワーク関係　設置にあたっては対荷重を考慮するとともに免震対策も行うこと)， LAN ケーブル等配線敷設， サーバ機器設定・設置，電源設備工事，現行サーバからの移行に係る諸設定及び関連工事 ユーザ関連情報の AD の構築(新規：医療系，OA 系)・連携及び各サーバ

		間連携，グループウェアの構築(更新，想定品：サイボウズ)・コンテンツ移行，資産管理(新規，想定品：skysea，AssetView 等の管理ソフトウェア)
	ネットワーク設定・設置	LAN ケーブル等配線敷設，ネットワーク機器設置，ネットワーク機器設定，電源設備工事，現行ネットワークからの移行に係る諸設定及び関連工事
	試験	設計及び構築に係る単体テスト,結合テスト,総合テスト,外部接続テスト及び運用テストの支援（電子カルテシステム運用テスト時の支援）などに係る作業を行う。
	OA 系端末の導入	OA 系端末(84 台)に係る導入計画を，設置部署と調整のうえ立案し，必要な設定を行った上で配布して接続を確認する。
	移行	現行ネットワーク・サーバのデータ調査，データ移行設計を行い,必要な場合はデータ変換ツールを活用するなど適切な移行作業を実施する。また，各部門システム及び外部連携ネットワークとの接続調整，及び次期ネットワーク側の接続設定を含むものとする。
	電源工事	導入機器等の設置の際に必要となる二次側電源配線，情報コンセントからのネットワーク配線部材及びこれらの施工作業を含むものとする。
	既設ケーブル・既設機器類の撤去	当院が不要と判断した現行ネットワーク機器及び通信ケーブル，機器は撤去の上，当院の指示に従い，指定の場所まで集積を行うこと。（次のネットワーク更新時にかかる撤去費を含めること。）
保守業務	監視・保守	次期ネットワークの監視，障害時の問い合わせ窓口，障害対応，代替機交換等及びこれらに付随する作業を行う。

（3）関係する調達の概要

本業務の受注者は，本業務に関係する下記の受注者と連携して，全体業務が円滑に行われるよう協力すること。

・（仮称）第三次医療情報システム構築・移行業務（以下「次期電子カルテ構築等業務」という。）
・（仮称）第三次医療情報システム監視・運用・保守業務（以下「次期電子カルテ運用保守等業務」という。）

（4）本業務の基本要件

本業務は，次期ネットワークの構築業務及び現行ネットワークからの移行業務，次期ネットワーク稼働開始から 2025 年 3 月 31 日までの保守・監視業務を調達対象範囲とする。 業務を遂行するにあたっては，下記の基本要件を十分考慮し業務を行うこと。

・受注者は，本仕様書の記載内容を十分理解した上で業務を行うこと。
・受注者は，単にネットワークの構築及び保守等を行うだけでなく，現行ネットワークが抱える課題が，解決できるよう検討及び提案を行うこと。
・受注者は，第三次医療情報システム構築業務の受注者と連携して業務を行うこと。

イ）作業体制及びプロジェクトの管理

受注者は，本業務においては，各部門ネットワークとの接続や院外ネットワークとの連携まで一貫性のある設計・設定等を行うことが必須であり，関係事業者と調整できる体制等を提案すること。また，プロジェクトマネージャーは，構築から運用開始までのプロジェクトを適切に進行管理するため，本委託業務を統轄できる権限と能力を有していることが望ましい。本委託業務の作業体制と合わせて，プロジェクトマネージャー，及び主担当者の経験年数，実績等を具体的に

提示すること。医療機関や同等規模(構成や端末数 600 台以上など)の構築実績があれば，中心に提示すること。プロジェクト管理を行うにあたっては，プロジェクト管理ツールを整備するものとする。また，現行システムで高額のコストが発生したことなどを踏まえて，受注者は，今後の保守経費の算定基礎となる情報を，本業務で出来高計画管理（EVM）等で把握し病院と事業者が共有するものとする。また，製造事業者へ問い合わせを行うためのパスを有さなければならない。具体的なプロジェクト管理手法や管理ツール，管理資料等について明示すること。

ロ）移行の手法等

受注者は，移行にあたって，病院の診療等業務に係る継続性を可能な限り確保し，迅速かつ安全に移行しなければならない。また，現行システムの運用保守業務については，移行に係る現行ネットワークの大規模な設定変更作業は見込んでいないため，可能な限り本委託業務の中で対応する移行方法を実施しなければならない。

受注者は，患者サービスに係る重要な業務への影響を可能なかぎり低減するとともに，既存のネットワーク及びインターネット機器の設定変更を極力抑制し，迅速な移行を実施する手法を十分な現状調査のうえ策定し，発注者の承認を得ること。各部門ネットワークの移行時には，技術的な支援を実施すること。

ハ）医療情報システムベンダー(部門ベンダーを含む)との連携

受注者は，次期ネットワークに接続して，院内の医療情報システムが効率的・効果的に運用できるよう，医療情報システムベンダーと連携して構築に努めなければならない。また，医療機器や自家検査機器の導入についての事前相談及び接続協議に対応できる体制を構築しなければならない。

電子カルテ，部門システム等の医療情報システムベンダーとの調整体制案，及び接続確認，検証方法等について過去の事例を踏まえ提示すること。

ニ）次期ネットワークの機能

受注者は，仕様に定める機能要件を踏まえ現場へのヒアリング及び無線環境及び既設 LAN ケーブルの状況を現場調査で十分に確認し，効率的・効果的な手法により院内の業務改善及び医療安全に係る提案を行い，機能の高いネットワークを構築しなければならない。

ホ）次期ネットワークの品質

受注者は，適切にテストを行い品質を確認するものとする。特に総合テストについては，十分な確認を行い円滑な稼働を確認しなければならない。

各工程(設計，構築，テスト，稼働準備)での，品質レビューの実施計画・体制(品質管理に関する社内レビュー体制も含む)，管理手法，基準，及び品質仕様について提示すること。

ヘ）保守の体制等

受注者は，ネットワーク機器を効率的及び迅速に保守しなければならない。また，手術室移転，小規模のネットワーク工事及び設定変更などを想定して，年間 3 人月相当の工数を本調達に含み対応を行うものとする。なお、保守体制案について提示すること。

ト）リモート保守の接続

IPSEC-VPN での接続環境を想定している。なお，本調達で導入するリモート保守環境は，ネットワーク保守以外に医療情報システムベンダーも含め 20 社程度利用するものとし，医療情報システムベンダーについては，医療情報システムベンダー側のルーター(1 台)までを調達に含めるものとする。保守環境の構築にあたっては，医療情報システムベンダーと協力して，情報共有，調整し構築すること。回線，当院側のルータ(VPN 装置)は本調達内とする。

6　契約方法及び業務スケジュール等

（1）契約方法

構築業務掛かる費用は，2019 年度に予算で一括請負契約とする。支払額については，契約書に定める金額により，発注者が納品された成果物について検査し合格と認められる部分について，受注者からの請求を受けて支払うものとする

稼働後以降の各年度の保守契約は，当院と協議のうえ別途契約とする。また，保守開始予定月に関しては当院へ説明し，了承を得ること。

（2）契約期間

契約締結の日から 2025 年 3 月 31 日まで

（3）業務スケジュール等

・構築業務
契約締結の日から 2020 年 3 月 31 日まで
ただし，2019 年 12 月 31 日まで構築工程を終了し使用できる状態とすること。
ハードウェア・ソフトウェア等の保守費用（5 年パック保守等を含む）は，保守等業務に入れること。
・保守等業務
2020 年 4 月 1 日から 2025 年 3 月 31 日まで

7　納入成果物
（1）納入成果物等一覧
本業務の納入成果物及び提出期限を下表に示す。

分類	納入物品		内容	提出期限
プロジェクト管理	1	業務実施計画書	本業務の範囲内における体制，スケジュール等，本業務を遂行する上で必要な事項が記載された資料。 提案書にて作成された内容をベースに，作業内容と想定するリスクに対する対応策及び問合せ連絡窓口体制・連絡先を記載したもの。 提案書にて作成された内容をベースに詳細化された作業スケジュール，作業体制と責任分担，権限を記載したもの。	契約締結後 1 週間以内
	2	WBS（Work Breakdown Structure）	業務全体のスケジュールと作業項目の関係を表示するとともに，期日の近づいた作業項目を細分化して，作業計画と進捗状況を一覧できるように整理すること。	随時
	3	進捗管理報告書	本業務の進捗状況を記載したもの。 遅延等の進捗管理上の課題が生じた場合には，その原因の分析と対応策を記述すること。	随時
	4	課題管理表	本業務において発生する課題を管理するために課題とその対応実績を管理するもの。	随時
	5	議事録	定例会等の各会議の開催日時，開催場所，出席者，決定事項，要対応事項，議事内容を記述したもの。	各会議の開催後 3 営業日以内
	6	作業完了報告書	各年度に実施した作業の完了を報告するもの。	2019 年度末
設計・構築	1	機器等の導入計画書	本業務で導入する機器について，導入スケジュール，導入作業内容，導入作業体制等について記載したもの。	機器等の導入計画策定完了時

分類	納入物品		内容	提出期限
	2	調達対象機器等	本業務において調達した機器等。	機器等の導入作業完了時
	3	ハードウェア構成定義書	本業務で導入する機器等の構成を定義したもの。	機器等の導入作業完了時
	4	ソフトウェア構成定義書	本業務で導入する OS やアプリケーションごとにパラメータ等の設定を記載したもの。	機器等の導入作業完了時
	5	機器等の導入結果報告書	機器等の導入作業が完了したことを報告するもの。	機器等の導入作業完了時
	6	機器管理台帳	機器情報（コンピュータ名，シリアル番号，MAC アドレス等，管理番号，ソフトウェアライセンス利用情報，利用者情報等）について記載したもの。	機器等の導入作業完了時
	7	要件定義書	本業務の設計を実施するために必要なネットワーク等の要件を記載したもの	要件定義完了時
	8	ネットワーク設計書	本業務で導入する機器等を利用するために必要なネットワークの設計を記載したもの。	ネットワーク設計完了時
	9	ネットワーク構築計画書	ネットワーク設計書に基づき行うネットワークの構築作業について，作業内容，スケジュール，体制等を記載したもの。	ネットワーク構築作業開始前
	10	ネットワーク構築結果報告書	ネットワークの通信確認結果等，ネットワーク構築結果を報告するもの。	ネットワーク構築完了時
	11	ネットワーク物理構成図	ネットワーク設計書に基づき構築を実施した通信機器等の物理構成を記載したもの。	ネットワーク構築完了時
	12	ネットワーク論理構成図	ネットワーク設計書に基づき構築を実施した通信機器等の論理構成を記載したもの。	ネットワーク構築完了時
	13	機器コンフィグ	ネットワーク設計書に基づき投入したコンフィグ情報を記載したもの。	ネットワーク構築完了時
	14	ラック実装図	ネットワーク設計書に基づき通信機器をラックに搭載した実装図を記載したもの。	ネットワーク構築完了時

分類	納入物品		内容	提出期限
	15	IP アドレス台帳	ネットワーク設計書に基づき割り当てた IP アドレスの一覧として記載したもの	ネットワーク構築完了時
試験	1	試験計画書	各種試験の実施スケジュール，実施体 2 制，実施内容等を記載したもの。	試験開始前
	2	試験手順書	各種試験の実施手順を記載したもの。	試験開始前
	3	試験結果報告書	各種試験の結果を報告するもの。	試験終了後
移行	1	移行計画書	移行作業の実施スケジュール，実施体制，実施内容等を記載したもの。	移行設計終了後
	2	移行手順書	移行作業の実施手順を記載したもの。	移行設計終了後
	3	移行結果報告書	移行作業の結果を報告するもの。	移行終了後
機器	1	ネットワーク機器・ファイルサーバ・サーバ類・OA 系端末等		2019 年度末
マニュアル	1	操作マニュアル	各システムの操作方法等を記載したもの。	総合テスト終了後
	2	運用マニュアル	各システムの運用方法等を記載したもの。	総合テスト終了後
保守	1	実績報告書	保守作業の実績を報告するもの。ネットワーク機器等の保守管理状況を報告するもの。	2019 年 4 月実績分から毎月

（２）納入（履行）場所

本業務の主な履行（納入）場所は，次に示す。

・発注者が指定する場所

・受注者の作業環境等で発注者が承認した場所

例：機器の検査・組立等で使用する受注者の会議室・倉庫等施設

（３）納入に関する留意事項

物品等の納入に当たり，次の要件に従うこと。

・納入予定成果物を事前に提示し，発注者の確認を受けるとともに必要に応じ見直しを行ってから最終成果物を納品すること。

・納入期限までの納入を保証すること。

・成果物を紙で印刷し製本する場合は，エコマーク及びグリーンマーク認定等の環境へ配慮した製品を使用すること。

・指定の成果物を紙及び電子媒体（DVD-R 等）により日本語で提供すること。納入する紙及び電子媒体の部数については３部を基本とすること。

・成果物に使用する紙のサイズは，日本工業規格Ａ４版を原則とする。図表については，必要に応じて，Ａ３版縦書き，横書きを使用することができる。また，バージョンアップ時等に差し替えが可能なように，バインダー方式とすること。
・電子媒体に保存する形式は，Microsoft Office 2016 で扱える形式またはテキストファイル形式を基本とする。なお，導入するアプリケーション固有のファイル形式については発注者の了承を得た上で納品すること。
・電子媒体については，事前にウイルスチェックを行い，チェックに用いたソフトウェア及び日時を記載したラベルを貼った上で提出すること。
・成果物に修正等がある場合，紙については更新履歴と修正ページ，電子媒体については修正後の全編を速やかに提出すること。
・上記納入物の検査の結果，不適合の場合は再納入すること。
・業務実施計画書作成段階で，成果物それぞれの構成について発注者と確認すること。
・機器類，パソコンの設置展開作業は，原則とし各設置場所の業務に支障がないように，騒音の抑制に留意すること。
・平日の夜間及び休祝日に作業を要する場合は，各設置場所の管理者との調整に２週間以上の期間を要するため，事前に発注者と調整し許可を受けて行うこと。詳細スケジュールは，発注者と別途協議の上決定すること。
・納入期限に間に合うよう，現地調査を踏まえて詳細な工程を検討し，発注者の承認を得て業務を実施すること。また，発注者と合意した導入作業日程を元に，受注者が各拠点の建物管理者等と直接連絡を取り，導入作業の可否等について調整を図ること。なお，発注者と合意した導入等作業日程に変更を要する場合は，早期に発注者と協議して変更日程及び作業体制の調整を行い，納入期限に間に合わせること。
・発注者が提供した情報を第三者に開示することが必要である場合は，事前に担当職員と協議の上，書面による承認を得ること。
・納入する通信機器等は未使用品とすること。
・納入する機器等の付属物（マニュアル，メディア，保証書等）は，発注者が要・不要仕分を指示し，不要なものは搬入前に受注者が引き取ること。

（４）検査に関する留意事項

受注者は，検査に係る次の条項を遵守すること。

イ）設置検査

納入物品等の納入が完了した時は，発注者の検査職員に対しその旨を報告し，検査を受けなければならない。なお，修正・改善の場合も同様とする。

契約書に規定する業務を完了したときの通知は，次に示す要件のすべてを満たす場合に，発注者に提出することができる。

調達仕様書に示すすべての業務が完了していること。

発注者の指示を受けた事項がすべて完了していること。

調達仕様書に定められた納入成果物の整備がすべて完了していること。

通知に基づく検査は，発注者から通知された検査日に受ける。

ロ）納入期限

検査の期間を考慮した納入期限に納入すること。

ハ）検査対応

作業を実施するに際し，発注者の監督職員の質問，検査及び資料の提示等の指示に応じなければならない。また，修正及び改善要求があった場合には，発注者と協議・合意をもって，これに応じなければならない。

ニ）検査結果

前各項の検査（再検査が必要な場合には再検査）に合格した時をもって，本業務の履行（部分）が完了したものとする。

第３　作業体制及びプロジェクト管理

１　作業体制

（１）資格要件

受注者は，次のいずれにも該当すること。

イ）ISO27001（ISMS 認証）の認証，又はプライバシーマーク制度の認定を受けていること。
ロ）過去２年間に種類及び規模をほぼ同じくする契約を数回以上にわたって締結し，かつ，これらをすべて誠実に履行していること。

（２）本業務の関係者

本業務の関係者と主な役割を下表に示す。受注者は，各関係者と連携し，プロジェクトを確実に推進すること。なお，当院は，当院側の立場で業務を支援する PMO を設置する場合がある。

本業務の関係者

関係者	説明	主な役割
情報システム管理室	当院における本調達業務の担当部署	本調達業務の責任者として意思決定を行う
エンドユーザ	本業務にて調達するネットワーク等を利用する当院職員等	ネットワークを利用する要件を提示し確認を行う
本業務受注者	本業務を受託した事業者	構築・保守運用作業等，本書に記載の業務を主体的に実施
次期システム業務受注者	電子カルテシステム及び関係する部門システムの事業者	本業務受注者と連携し，次期ネットワーク接続に係るシステム側の作業実施
現行システム構築事業者	現行システムを構築した事業者	現行システムから移行データを抽出して当院に提出
各部門システム保守業務	各部署が導入した部門システムを保守する事業者	本業務受注者と連携し，次期ネットワーク接続に係るシステム側の作業実施

（３）本業務のネットワーク構築に係る基本的な役割分担

本業務の導入業務における，受注者と発注者の基本的な役割分担を下図に示す。
なお，作業日程については調整を綿密に行い，効率の良い作業進行に努めること。

受注者と発注者の役割分担

作業	本業務の受注者	発注者 （業務委託職員含む）	作業事項
ネットワーク構築	・ネットワーク構築 ・サーバ構築 ・動作確認作業	・現行ネットワークに係る情報提供，調整等	受注者は，端末から利用可能なネットワークインフラ環境を設定すること
OA 系端末展開 （84 台）	・オペレーティングシステム（以下「ＯＳ」という。）等セットアップ ・現地展開 ・動作確認作業	・現行端末に係る情報提供，調整等	OS，各種アプリケーションのインストール及び Office 系ソフトウェアのインストールは受注者が行うこと

２　プロジェクト管理

受注者は，次に示す事項を踏まえたプロジェクト管理体制を提案し，発注者及び関連業者と綿密な確

認調整を行いながら業務を遂行する。

（1）プロジェクト管理上の基本事項

本業務を確実に実施するため，次の基本事項要件を満たすようプロジェクト管理を行う

・受注者は，本業務を実施するに当たり，プロジェクトのプロジェクト体制を提出すること。
・本業務の遂行に当たり，プロジェクトの全体管理を行い，本業務の遂行に問題が生じた場合には，速やかに報告及び問題解決可能な体制とすること。
・発注者から業務の改善に関する指導・助言等を受けた際には，課題解決に向けて速やかに対応すること。プロジェクトに問題が発生した時は随時会議を開催することとし，受注者は発注者と協議の上，プロジェクトの課題整理とリカバリプランを提示し，発注者の了承を得ること。また，障害発生・対応状況の報告を適時行うこと。

（2）進捗管理

各タスクの状況把握及びスケジュール管理を適切に管理するため，次に示す業務内容を実施する。各管理項目の遵守事項・留意事項は以下のとおりである。

・本業務の受注者は，各タスクの進捗が把握できる進捗管理表を提示すること。
・計画に遅れが生じた場合は，原因を調査し，改善策を提示し発注者の承認を得た上で，実施すること。
・定例報告会議について，発注者と協議を行い定期的に発注者に対して進捗状況・障害発生・対応状況の報告を行うこと。定例会議の開催場所は当院内とし，日時については発注者と調整の上決定すること。
・各業務箇所での作業にあたり，各所属の担当者と作業スケジュール等の連絡・調整を密に行い，作業の進捗に遅れが生じないよう実施すること。

（3）業務遅延リスク管理

各作業工程における目標の達成に対するリスクを最小限にすることを目的として，次に示す業務内容を実施する。

・技術的観点，財務的観点，進捗的観点，人員的観点等から，対応策（対応手順，体制等）を検討し提示すること。
・リスクが顕在化した場合は，リカバリプランを早期に提示し，発注者の了承を得るとともに速やかに実行すること。
・業務遅延に係わらないリスクについても同様に対応すること。

（4）課題管理

各種課題について，課題の認識，対応策の検討，解決及び報告のプロセスを明確にすることを目的とし，課題管理を行い，各課題のステータスについて報告する。

・課題管理に当たり，次の項目例に示す内容を一元管理することとし，その他必要と考えられる項目についても管理する仕組みとすること。（課題内容，影響，優先度，発生日，担当者，対応状況，対応策，対応結果，解決日等）
・発注者との状況共有のために，起票，検討，対応，承認といった一連のワークフローを意識した管理プロセスを確立すること。
・積極的に課題の早期発見に努め，迅速にその解決に取り組むこと。
・対応状況を定期的に監視・報告し，解決を促す仕組みを確立すること。

（5）セキュリティ管理

各作業工程において，セキュリティに関する情報流出等の事故の発生を未然に防ぐことを目的とし，次に示す業務内容を実施する。

・契約書の個人情報保護に関する規約に従い，本業務で受注者が知り得た情報を外部に漏えいすることの無いように厳格に管理すること。
・本業務について，内部のセキュリティ管理を行う管理者を設置すること。
・セキュリティ対策状況について，定期的に発注者に報告し問題が無いか確認を受けること。
・セキュリティ対策状況について，公正な立場で監査できる者によるセキュリティ監査が実施された場合には，情報セキュリティに関する調査について必要な協力を遅滞なく行い，当院が求めた場合は，速やかに情報セキュリティ監査を受け入れること
・セキュリティに関する事故及び障害等が発生した場合には，速やかに発注者に報告し，対応策について協議すること。

（6）品質管理

本業務の遂行上の成果物の品質管理を目的とし，次に示す業務内容を実施する。

・作業工程毎に評価基準を設定し，評価結果を発注者に報告し，次の作業工程へ推移する際は，発注者の承認を得ること。

・本業務の受注者の関連会社や協力会社等が参画する体制（企業連合等）を敷く場合は，関連会社等の作業範囲及び責任範囲を明確にし，関連会社等の作業及び成果物に対して十分な管理・検収を実施するとともに，関連会社等に係る一切の事項について全責任を負うこと。

（７）人的資源管理

本業務に参画する要員の選定，変更及び体制維持に関する管理を行うこと。

・要員に変更が生じた場合には，速やかに発注者に報告し承認を得ること。代替要員については，サービスレベルの低下を防ぐために能力及び経験が同等以上の者を充てること。

（８）コミュニケーション管理

・定例報告会議を原則，毎月開催し，プロジェクト遂行に係る課題やスケジュール等の報告を行うこと。

・策定した会議・情報伝達計画に基づき，各作業工程における作業関連の打合せ，成果物等のレビュー，進捗確認及び課題共有等を行うための定例会議を開催すること。

・定例報告会議以外の会議を開催するタイミング及び頻度については，各作業工程の特徴及び状況等を考慮しながら，会議に要する労力が過大とならないように適切な開催時期と回数を設定すること。

・スケジュールの遅延や重大なリスクなど，重大な事項が判明した場合，発注者から要請がある場合，又は発注者との協議が必要な事案が発生した場合には，臨時の会議を随時開催すること。

・各会議が開催される都度，全出席者に内容の確認を行った上で，原則，３営業日以内に議事録を提示し発注者の承認を得ること。

第４　次期ネットワークの設計・構築

１　次期ネットワークの概要

（１）基本事項

次期ネットワークの構築は，現行の院内業務が稼働でき，「第２調達の概要　４次期ネットワークの概要」に定める重要事項を満たしたものでなければならない。

職員が利用するネットワークは，主に以下のとおりに分類される。

各ネットワーク（医療系，OA 系，部門システム系）は，総務省の「自治体情報システム強靭性向上モデル」，厚生労働省の「医療情報システムの安全管理に関するガイドライン第５版」及び総務省発行の「一般利用者が安心して無線 LAN を利用するために」及び「企業等が安心して無線 LAN を導入・運用するために」で求められる要件に則り，現状の VLAN 情報を把握した上でセキュリティの高いネットワーク分割方式を採用し設計・構築するものである。また，ネットワーク間で必要な通信は，特定通信として，その安全性を確保するために通信経路の限定（ＭＡＣアドレス，ＩＰアドレス）に加えてアプリケーションプロトコル（ポート番号）を限定などの対策を行ったうえで許可できるようにする。

その他ネットワークについては VLAN 情報を確認の上，各ネットワークの運用・保守事業者と協議し，必要なルーティング情報等の設計を実施し，移行時の負担低減を十分考慮し，各ネットワークの運用・保守事業者と協力して構築する。

本業務においては，本仕様書に記載された各種の要件と仕様をすべて満たした上で，次期ネットワークを設計・構築するものとし，完了は本調達のすべてのシステムが動作し，全クライアント・部門システムが接続するまでとする。

（２）全体構成

想定する第三次医療情報ネットワークの主な基本要件についてのイメージ図を〈別紙 2〉に示す。

※想定案であり提案を妨げるものではない

（３）ネットワークの効率的な構成

イ）構築から運用まで一貫性があり効率的な構築

受注者は，必要な機能を有する通信機器を設置するだけでなく，その機能を踏まえた運用・監視方法を検討し提案すること。また，ユーザ ID 及びコンピュータ名などの資源の管理をどのように効率的に管理できるか提案すること。特に，年度切り替え時のアクティブディレクトリィ

(AD)の情報を他のサーバに登録するために多大な労力を要するので，配信プログラム，コマンドスクリプト等を作成して効率化を図ること。

ロ）ネットワーク機器の機能活用と台数の最適化

設置する機器は，現行の使用状況及び本仕様書で求める構築要件を満たすものを選定し，現行ベンダー機器に拘らずに適切なものを提案し当院の承認をえること。また，収容する機器数に応じて必要なポート数を提供し，今後のサーバ機器の追加の際も費用を追加することなく対応できるよう余裕を持った設計を行う。なお，コアスイッチとは，10 ギガビット以上のイーサネット方式にて接続する。サーバスイッチは筐体単位で電源を冗長化することとする。

ハ）監視システムの機能向上

監視対象機器の強化，障害判別・対応の迅速化等

ニ）LAN ケーブルの老朽化に対応した再敷設

次期ネットワークと現行ネットワークの並行期間が必要であり，継続利用する場合は並行期間の運用等について提案すること。また新規敷設する場合について，既存の配管が利用できない場合は，新たに配管を敷設するなど確実な施工を行うこと。

ホ）機器の障害時の即時切り替え可能な冗長化構成

次期ネットワークでは，機器の機能を最大限活用し，可能な限り主要ネットワーク機器は冗長化構成とすること。また，リモート保守により障害対応の迅速化に努力し，保守員による現場確認を十分に実施できる体制を構築し，停止しない信頼性の高いネットワークを構築しなければならない。

ヘ）ネットワーク分離と業務効率の維持

・次期ネットワークでは，サイバー攻撃が急速に複雑化・巧妙化している中で，将来的にマイナンバー制度の運用にも対応できる情報セキュリティを抜本的強化を図ることとし，総務省が提示する「新たな自治体情報セキュリティ対策の抜本的強化に向けて」及び厚生労働省が提示する「医療情報システムの安全管理に関するガイドライン」等を踏まえて，医療系ネットワークとインターネットに接続する OA 系ネットワークを分離しなければならない。OA 系との分離については，仮想デスクトップ，仮想ブラウザによる提案も可とする。医療系端末でのインターネットやメールの利用禁止については，次期ネットワークでも継承するものとする。なお構成等については，受託後に当院と協議，承認の上，構築すること。

・ネットワークを分離に伴い，医療系とインターネット利用可能な OA 系，及び医局系のファイルサーバも分離する必要がある。このため，データの連携などで当院内の業務に影響が発生することが考えられるため，各ネットワーク系で安全かつ円滑にデータを連携する仕組みを提案し，承認を得て構築すること。OA 系，及び医局系のファイルサーバの容量は，各々3TB 程度を想定している。なお，ディスク増設などスケールアップ時は業務に影響がないこと。バックアップは日次で差分バックアップとし，7 世代管理可能であること。医療系のファイルサーバ(参考情報　容量：6TB)やバックアップ環境については，医療情報システム側の調達とし，本調達には含まない。ただし，各系間のデータ転送やファイル無害化等の設計，構築，検証に当たっては，医療情報システムベンダーと協力して情報共有，調整して進めること。

ト）無線 LAN の拡充による可用性と省力化の促進

無線 LAN については LAN 末端における有利性（配置の自由度，施工費等）を評価し，また近く計画しているナースコールシステムの更新を念頭に，病棟をはじめとして可能な限り広範囲での採用を検討する。

その対象範囲は医療系，OA 系，音声系及び医局系に接続する端末機等とする。

ただし，有線 LAN の特長（安定性，動画や画像等大容量データ伝送時の利点）が求められる高精細モニタ接続端末，プリンタ，NAS などについてはこの限りでは無い。

・無線 LAN 接続の際は，許可されていない端末がネットワークに接続されない仕組みを導入すること。

・無線 LAN は既存無線 LAN システムや衛星電波と干渉しないよう十分調査を行い設計すること

・各執務室に設置する無線ＡＰは，異なるフロアスイッチにそれぞれ分散接続することにより，フロアスイッチ障害時にも各執務室で無線 LAN が全停止することなく，業務継続が可能なネットワーク構成となっていること。
・無線 LAN の適用に関しては，総務省発行の「一般利用者が安心して無線 LAN を利用するために」及び「企業等が安心して無線 LAN を導入・運用するために」で求められる要件を踏まえたものとすること。

（４）ネットワーク連携の強化

イ）外部ネットワークとの接続(MMwin，遠隔医療，カンファレンス会議)

遠隔医療， カンファレンス， インターネット会議などのため大学や他の病院と接続しなければならない。接続する通信の内容は，映像及び音声を含む通信が必要である。受注者は，院内の遠隔医療等が様々な会議室で実施され，時間外及び休日等々の対応を踏まえて，利用者は容易に接続できる使い勝手のよいネットワークを構築すること。また，外部ネットワークと接続する場合は，サイバー攻撃や情報漏えいに十分対応できる仕組みも構築しなければならない。

ロ）部門システムネットワークとの接続

次期ネットワークが電子カルテシステムのみならず多くの部門システム及び自家検査機器が接続する当院基盤であることを十分理解し，受注者は，既存及び新規に導入する部門システムネットワークを確実に本ネットワークに接続しなければならない。また，将来的には IoT 機器を始めとするさまざまな医療機器や部門ネットワークの導入および外部連携等が想定されることから，ネットワークの拡張性・可用性を考慮した設計・構築とすること。

（５）セキュリティ対策の強化

イ）ネットワーク分離論理分割

・「第４－１－（３）－へ）」へ示すとおりにネットワークの分離分割を行うこと。
なお，将来，医療系でマイナンバー制度に係る医療 ID を利用システムが稼働する可能性がある。医療 ID の利用にあたっては，マイナンバー利用事務と同等のセキュリティレベルが求められると考えられる。したがって，医療系の構築については，医療 ID の利用を踏まえるものとする。また，医療系のセキュリティレベルが外部連携ネットワーク接続などにより，医療 ID の利用に適さないとレベルと判断された場合は，医療系を医療 ID 系に分割することが必要となり，追加コスト及び業務の支障が生じるため，あらかじめ適切なセキュリティレベル確保し提案・構築を行うこと。
・ファイルサーバについては現状，医療系と OA 系で共有している。本調達では，セキュリティ強化の一環として，医療系とインターネット利用可能な OA 系のファイルサーバをそれぞれ分離することとする。ただし，「第４－１－（３）－へ）」記載の通り，両環境のファイルサーバ間でデータのやりとりが発生するため，分離により業務効率の低下が想定される。
このため，ファイル転送時の無害化ツールの適用など，効率的な業務が維持できる仕組みについて提案すること。なおファイルサーバについては，新たに医局系用のファイルサーバを導入するものとする。
※医療系，OA 系，医局系の各系間のファイル転送時のファイル無害化対象については，〈別紙 3〉の№8 のとおりとする。
・この他，グループウェアによる内部メール(添付ファイル含む)も無害化対象(OA 系や医局系→医療系への内部メール送信時)とする。

ロ）高度なセキュリティ対策

サイバー攻撃等への対応について，端末の保護対策はもとより，標的型攻撃などのネットワーク内の不正な通信を検出するなどの多層防御が有効と考えられる。以下にあげる項目について，セキュリティ，価格面で最適な提案をすること。

【必須提案】

・ウイルス対策ソフト，ファイアウォール，IPS/IDS， URL フィルタ，ログ収集サーバ，ネットワーク監視など)

※セキュリティ基盤はオンプレミスの他，クラウドサービスによる提案も可とする。

【自由提案】

・振る舞い検知装置，サンドボックス，マルウェア・スパイウェア対策機器，Web 無害化，

グループウェア等の内部メール無害化，ログ分析システムなど

なお「第２－４－（５)」記載の通り，サイバー攻撃対策の基盤はオンプレミスの他，クラウドセキュリティサービスによる提案も可とし，クラウドセキュリティサービスを提供しているベンダーとの連携による提案をしてもよい。ただしクラウドサービスで提案する場合は，総務省，厚労省など関係するセキュリティガイドラインに抵触しないことを確認した上で，当院との接続環境，及びセキュリティ機能等のサービス提供内容や安全性，及び当該クラウドベンダーにおける 5 件以内の導入実績(できれば医療機関)を提示すること。

ハ）端末機からの情報持ち出しの制限

USB メモリや CD，DVD 等の記録媒体やスマートフォン等を使った情報の持ち出し制限や監視ができる仕組みについて提案すること。

ニ）強力なアクセス制御

医療系においては原則として，他の領域と通信をできないようにした構成を提案すること。

ホ）医療系／OA 系／医局系の通信のリスク対策

各系間の通信時のリスクについて，以下のような対策案を提案すること。ただし，以下対策案は他の提案を妨げるものではない。

※NW 間でファイル転送時する場合の安全対策

OA 系と医療系，及び医局系(新規導入)で相互利用可能なファイルサーバの設置，及びファイル転送の認，転送時のファイル無害化/暗号化/検知機能等

ヘ）外部持込端末機の接続環境

私物 PC のような非管理端末が次期ネットワークに接続しなければならない場合がある。セキュリティ上の脅威として， 無線区間における通信傍受， 他の端末からの 不正アクセス， 利用者のなりすまし， 不正なアクセスポイントによる通信傍受等が考えられる。したがって，セキュリティを担保し接続端末の管理を的確に行い，次期システムの安全を確保できる仕組みを構築すること。

ト）医療系も含めた全端末機の資産管理ソフトの新規導入

次期ネットワークに接続するクライアントパソコン・ネットワークプリンター・NAS 等の機器類（以下「IT 資産」という）の台帳管理・情報セキュリティ対策・コスト管理の効率化を目的として，IT 資産情報管理システム（以下「資産管理システム」）を導入すること。

チ）無線 LAN 認証・暗号化の対応

認証機能の構築にあたっては，データの盗聴や不正侵入を防止対策として，許可されていない端末やユーザがネットワークに接続した際の検知，ならびにリソースにアクセスされないための認証機能と，拠点に設置する無線 AP を制御・管理する機能を実現しなければならない。

また，構築する AD サーバ上のユーザ情報を各場所に導入するスイッチや無線 AP と連携し認証を行える仕組みについて提案すること。なお，総務省発行の「一般利用者が安心して無線 LAN を利用するために」及び「企業等が安心して無線 LAN を導入・運用するために」を踏まえて設計しなければならない。

ⅰ）認証方式

- 現行の端末は WPA2 暗号化方式を使用している。同等以上の暗号化方式を使用し設計・構築すること。
- 認証方式はそれぞれ統一したセキュアな方式を採用すること。
- 複数の無線認証サーバを平行して運用する場合，マスタの無線認証サーバへの設定情報を他の無線認証サーバへ同期する機能を実装していること。
- 既存の情報系端末の設定変更作業等が発生する場合は，本業務の中で実施すること。

ⅱ）無線 LAN 制御・管理

- 無線 LAN コントローラと無線 AP を GUI ベースで管理できること。
- 無線 LAN コントローラのソフトウェア更新ができること。
- 無線 AP の物理的な設置場所が分かるように無線ネットワークを視覚化できること。また，

無線 AP 毎に電波強度等の情報を視覚確認できること。

・無線 LAN コントローラを通して，複数の無線 AP に一括でコンフィグ設定ができること。

（６）外部端末とグループウェア

イ）外部端末機の接続環境

医局などの個別の端末機は，医局系ネットワークを利用してインターネットに接続する医局系ネットワークの環境を構築すること。個人所有のパソコンの接続が見込まれるため，OA 系及び他の系のネットワークと分離し，個別のインターネット接続を行う仕組み（プロバイダや回線は現環境を継続）を構築すること。また，医療系ネットワークは，外部の連携ネットワークに接続する必要があることから，安全に接続できる環境を構築すること。

ロ）グループウェアの更新

グループウェアの更新は，既存のグループウェアからデータを移行し更なる効率性の高いシステム構築を目指すものである。また，本システムを活用して，当院の約６００人の職員間の情報の共有化を推進し，客観的・組織的な知識の共有のほか，主観的・個人的な知識の共有も進め，新たな知識創造のプロセスを構築することを目指すものである。また，システム化の範囲を以下に示す。

・メール機能
・文書管理機能(共有フォルダ機能)
・掲示板機能
・設備予約機能
・電子決裁機能(ワークフロー／承認機能)
・職員認証機能
・情報共有機能

グループウェアは，AD のユーザアカウント及びパスワードを連携して使用すること。

サーバ環境は医療系ネットワーク環境に置くものとし，医療系ユーザ以外(OA 系，医局系)のグループウェア利用ユーザが，セキュアに利用できる環境を提案すること。仮想ブラウザや仮想デスクトップによる提案も可とする。セキュリティ，価格面で最適な提案をすること。なお構成については受託後に当院と協議，承認の上，構築すること。

２　次期ネットワークの主な機能概要

（１）次期ネットワークの構成

院内 LAN 全体の通信を管理する役割をもつこと。主にコアスイッチ(〈別紙 1〉現行ネットワーク構成概要図のセンタースイッチをいう),フロアスイッチ(〈別紙 1〉のエッジ SW をいう)，エッジスイッチ(〈別紙 1〉のワークグループ SW をいう)にて構成される。配下のネットワーク機器を束ね，LAN のバックボーンとして機能する。また，ポリシーに基づいてトラフィック転送，拒否，およびルーティング処理を行う機能をもつ。

ネットワーク制御機能について，以下に示す要件を満たすように，適切に設計・構築を実施すること。

・ネットワークの追加および管理が柔軟かつ容易に行える拡張性を確保すること。
・コアスイッチ～フロアスイッチ間は，１０ギガビット以上のイーサネット方式の LAN であること。
・リンクアグリゲーション等による論理リンクを構成の上，冗長化と容量の増大を図ること。
・データ輻輳時には，QoS 制御によって各系ネットワークの上限値を設定できるよう設計・構築し，実施すること。実際のポリシーについては，設計時に決定するものとする。
・コアスイッチは筐体単位で電源を冗長化すること。
・本館，拓桃館においては 24 時間 365 日無停止による稼動を原則とする。(ただしメンテナンス時は除く)
・機器を冗長化させる場合またはシングル構成の機器にモジュールを追加させる場合は，各モジュールはホットスワップ対応が可能なものとする。冗長化しているモジュールで障害が発生した際に

も，機器を停止することなく交換作業が行えるようにする等，高可用性を確保する構成にて設計・構築を実施すること。
・停電時に配下に接続されるシステム類が正常にシャットダウンすることができるよう，５分以上電源を供給できる UPS を設置すること。

（２）外部接続の環境

院内に設置される次期ネットワークから外部連携ネットワーク・ノード（以下「外部接続の環境」という。）に接続する環境を構築すること。また，次期ネットワークと外部接続の環境との間にはファイアウォール（FW）を設置し，適切な通信制御を行うとともに，通信ログを取得しセキュリティに関する分析を行うこと。

（３）サーバ接続環境

本調達及び各部署に設置されている業務サーバ等を接続するコアスイッチの環境を構築すること。また，収容する機器数に応じて必要なポート数を提供し，今後のサーバ機器の追加の際も費用を追加することなく対応できるよう余裕を持った設計を行う。なお，コアスイッチは，現在の通信量に加えて音声・映像の通信にも適用できるよう，10 ギガビット以上のイーサネット方式にて接続するものとし，サーバスイッチは筐体単位で電源を冗長化することとする。

（４）有線 LAN 接続環境

今回の計画では無線 LAN の拡充による可用性と省力化の促進を求めるものであるが，有線 LAN の特長も踏まえ，かつ既存 LAN の活用を念頭に適材適所の合理的な設計を想定している。

特に，無線 LAN の設計・敷設については，無線 LAN の障害時における有線 LAN への暫定的な切替措置を想定し，各所属内に有線 LAN 環境にも接続可能なように情報コンセントや有線通信機器を予め配置するなど，可用性を考慮した構成とすること。

また，各部署に設置する通信機器とフロアスイッチとは，１ギガビット以上のイーサネット方式にて接続する。有線 LAN の利用の際は，構築する認証システムと連携を行い，許可されていない端末がネットワークに接続されない仕組みを導入すること。

（５）LAN 環境について

・当院は無線 LAN 環境の拡充に重点を置いており，原則として院内の有線 LAN ケーブルは，本館を中心に老朽化しているものを対象に敷設するものとする。ただし，既存 LAN ケーブルの利用については，当院が示す規格を満たし運用期間中の十分な耐久性が見込まれることとし，当院の承認を得たものについて利用を可とする。また LAN 環境については，現行ネットワークとの並行期間(3 ヶ月程度)を想定しており，考慮すること。なお，参考として現状の情報コンセント数は約 1100 である。
・新規にケーブルを敷設する際は，現地調査を実施する等事前に準備を実施し，現行ネットワークの通信ケーブルの設置状況，必要となる電源についても確認作業を実施し，LAN 環境の構築計画を策定し実施すること。
・配線ルートである既設配管に空きが無い場合は，発注者と協議し壁貫通処理及び配管新設等の対応をすること。
・LAN ケーブルは，指定のない限りは 1Gbps(cat5e 以上)以上の通信が可能な難燃性のものとすること。
・LAN ケーブルの敷設は，ネットワーク機器または情報コンセントから端末(PC，プリンタ等)までとする。
・その他事項については，別途協議の上決定するものとする。

（６）サーバ室の要件

・サーバ室に設置する機器ならびに通信経路は，24 時間 365 日無停止による稼動を原則とし，単一障害点を設けないよう冗長化し，一方の経路で障害が発生した場合には自動的に他の経路に切り替わる構成とすること。ただし，可用性に影響しないなどの合理的な説明ができる場合にはこの限りではない。
・サーバ室に設置する機器構成は可用性を高め，障害時の停止時間を短縮する工夫を行うこと。
・提供する機能と性能，可用性を確保し最適な機器構成（物理サーバ，仮想サーバ，アプライアンス）にて提案すること。
・新規でラックを準備及び設置し，既設回路の電源容量が不足する場合には，あらかじめ発注者と協議すること。また，UPS を併せて導入し，停電等には正常にサーバをシャットダウン出来るよ

う構築すること。

（７）ネットワーク個別機能

本項では当院が想定する次期ネットワークの個別機能の要件について記載している。

必須の提案については，「第２－４」に記載の通りとする。

以下に記載の個別機能について該当する機能の提案をする場合は，記載の仕様要件を考慮した提案を行うこと。なお，費用の抑制や費用対効果の観点，また実現不可などの理由等から，クラウドなど含めて代替え案を提案してもよい。

イ）ネットワーク制御機能

・ネットワーク制御機能は，次期ネットワーク全体のネットワーク制御機能と，認証機能にて構成される。想定するユーザは職員すべて(約 600 ユーザ)が対象であり，700 ユーザ程度までの拡張を見込むこと。
・認証機能を有すること。認証機能とは，データの盗聴や不正侵入を防止対策として，許可されていない端末やユーザがネットワークに接続した際の検知，ならびにリソースにアクセスされないための認証機能と無線 AP を制御・管理する機能である。
・医療系，OA 系の AD サーバ上のユーザ情報や，導入するスイッチや無線 AP と連携し，認証を行うこと。
・原則として EAP-TLS 認証方式と同等以上の認証方式を使用し，設計・構築すること。
・認証方式はそれぞれ統一したセキュアな方式を採用すること。
・複数の無線認証サーバを平行して運用する場合，マスタの無線認証サーバへの設定情報を他の無線認証サーバへ同期する機能を実装していること。
・既存の情報系端末の設定変更作業等が発生する場合は，本業務の中で実施すること。
・無線 LAN スイッチと無線 AP を GUI ベースで管理できること。
・無線 LAN スイッチのソフトウェア更新ができること。
・無線 AP の物理的な設置場所が分かるように無線ネットワークを視覚化できること。また，無線 AP 毎に電波強度等の情報を視覚確認できること。
・無線 LAN スイッチを通して，複数の無線 AP に一括でコンフィグ設定ができること。

ロ）セキュリティ機能

・インターネットからの脅威に対して対策を行うこと。
・次期情報通信ネットワークに対して，総務省策定の「サイバー攻撃（標的型攻撃）対策防御モデルの解説」に準じたセキュリティ対策を講じること。
・アンチウィルスやアンチスパイウェアに複数のエンジンを利用するなど，ネットワーク全体の安定的稼動とセキュリティの向上を実現する機能について，積極的に提案をすること。

ハ）要求性能

以下の性能指標を満たす構成とすること。なお，導入する機器および機能は，スループット，セッション数，コネクション数すべてにおいてネットワークのボトルネックとならないよう適切にサイジングを行うこと。

・近くナースコールシステムの更新を計画しており，職員約 600 人すべてが利用し耐えられる無線 LAN による音声通信を前提とする。
・OA 系ネットワークのインターネットへの接続回線は，現行のものを使用することを前提とする。
・要件・性能・可用性を満たすのであれば，複数の機能を 1 台で纏めるなど機器構成・台数は問わない。また，日々，サイバー攻撃に関する情報を収集し，セキュリティ運用に当たっては適切な措置を講じること。ポリシー等は設計時に決定するものとする。

ニ）ファイアウォール機能（L4）

ネットワークのアクセス制御を行い不正な送信元からの通信，送信先への通信を禁止することで防御を行う。

・許可された通信（送信元情報と送信先情報）以外を遮断できること
・許可された通信（プロトコルとポート番号）以外を遮断できること
・IPv4 及び IPv6 の両方のプロトコルに対応していること
・事前に作成した定義ファイルを反映できること
・管理画面や運用システムを利用し，状況がグラフ等で表示可能なこと，ログの取得が可能であること。

ホ）アプリケーションフィルタリング機能（L7）

アプリケーションやユーザを識別して通信を観察し制御し，不適切なアプリやサイトの利用を制限し，情報漏洩のリスクを低減する。ネットワークのアクセス制御を超える攻撃に対して制御を行う。

・許可されたアプリケーションによる通信を透過できること。
・管理画面や運用システムを利用し，状況がグラフ等で表示可能なこと。
・ログの取得が可能であること。

ヘ）マルウェア対策（Web）

Web アクセスの利用に対してゲートウェイ型のマルウェア対策（アンチウィルス，アンチスパイウェア）を実施し，不正な通信を遮断する。

・最新のセキュリティシグネチャの更新を，管理者の介入の必要なく自動的に行えること
・管理画面や運用システムを利用し，状況がグラフ等で表示可能なこと
・ログの取得が可能であること。

ト）進入検知・防御機能（IPS）

サーバの OS など，ソフトウェアの脆弱性を悪用してシステムに侵入しようとするネットワーク層への攻撃を検知し，防御を行う。監視対象サーバへのアクセスについて，IPS により防御すること。①不正アクセスなどの悪意のトラフィックを自動的に検出し，脅威のレベルに応じて通信の破棄および通信を行う，②不正アクセスの検出には，シグネチャとヒューリスティックベースの分析が可能であること。③インラインで接続する場合，機器の障害が発生した場合にもネットワークが切断することがないよう，パススルー（バイパス）するための回路を有すること，④最新のセキュリティシグネチャの更新を，管理者の介入の必要なく自動的に行えること，⑤管理画面や運用システムを利用し，状況がグラフ等で表示可能なこと，⑥ログの取得が可能であること。

チ）標的型攻撃対策

脅威を分析し，ウイルス対策ソフトウェアでは対応しきれない新しいタイプの攻撃に対処する。未知のマルウェア対策として，以下の機能を備える通信監視機器を設置すること。

・未知のマルウェアやサイバー攻撃（標的型攻撃）に対して，既知のマルウェアとして検出されなかったファイルやメール本文の URL へのアクセス等を保護された仮想環境で動作させ，振る舞いを可視化し詳細に分析し，標的型攻撃と疑わしい事象を検知し，検体をメーカーに提供し対応するワクチンを早期に作成するなど，セキュリティ機能全体で対策を実施するための事後対策に繋げること。
・サンドボックスにより，メール添付ファイルやインターネットからのダウンロードファイルを動的解析し，不審なファイルを検出すること
・C&C 通信や内部サーバへの侵入行為などの不正通信を検出する。
・管理画面や運用システムを利用し，状況や統計情報がグラフ等で表示可能なこと。
・ログの取得が可能であること。

リ）ＤＭＺ対策

外部と送受信するメールに対しての攻撃検知・および防御を実施する。

ヌ）プロキシサーバ

クライアントからの Web 閲覧はプロキシサーバ経由をして行い，適切なセキュリティ対策を実施および管理する。FW やコンテンツフィルタリングと連携し，クライアント PC の Web アクセスを適切に管理すること。通信ログを取得し，すべての利用者のインターネット利用状況が確認できること。複数サーバによる負荷分散環境においても，一つのルール設定を実施することで複数のサーバに同期が可能なこと。Web リクエストを遅延なく処理できること。IPv4 及び IPv6 の両方のプロトコルに対応していること。

ル）コンテンツフィルタリング

インターネットアクセスについて，以下の制御ができること。また，職員がインターネットにアクセスする際に URL に対するアクセス制限機能を導入すること。

・メーカーが保持しているデータベースに基づき，危険な Web サイトへのアクセスを自動的にブロックする。
・コンテンツフィルタを導入し，ポリシーや URL ベースでウェブサイトへのアクセス制限の設定ができること。
・Web サイトの分類や URL により，ドメインユーザー毎にアクセス禁止または許可を設定ができること。

・既設コンテンツフィルターサーバの登録データを移行もしくは同等の内容を設定すること。
・構成やソフトウェアの機能によりフィルタ処理を高速化する工夫を行うこと。
・特定の利用者のみに URL を許可する設定が可能なこと。
・海外及び国内の十分な禁止 URL データを有すること。
・多段プロキシ構成とならないよう，設計すること。
・複数サーバによる負荷分散環境においても，一つのルール設定を実施することで複数のサーバに同期が可能なこと。

ヲ）WSUS サーバ（医療系及び OA 系クライアント用）

Windows のクライアント端末及びサーバに更新プログラム（OS の修正パッチやセキュリティパッチ）を配布するサーバであり，ドメインに参加するクライアント端末及びサーバは，約 1000 台を想定している。

・修正プログラム取得は然るべき対策を行ったうえで，インターネット上から取得すること。
・資産管理機能と連携し，PC 環境を統一すること。
・資産管理機能と連携し，資産管理機能から配信ができること。
・配信時は帯域を考慮し，業務全体への影響の最小化を図る工夫を行うこと。

ワ）資産管理システム

クライアント端末等を管理するシステムを構築する。

・修正プログラム取得は然るべき対策を行ったうえで，インターネット上から取得すること。
・コンピュータ名，OS，アプリケーション等，クライアント端末の詳細情報を取得できること。
・web アクセスやソフトウェアのダウンロード等のクライアント端末の操作ログを取得できること。操作ログは 1 年間以上保持すること。
・ユーザーからの情報収集機能（アンケート機能）を有すること。
・ソフトウェアや Windows 更新プログラム等を，通信帯域を制御しつつ配布し実行する機能を有すること。
・USB デバイスの制限機能を有すること。
・リモート操作機能を有すること。

カ）マルウェア対策パターンファイル配信サーバ

院内のサーバおよびクライアント PC に対して導入するマルウェア対策ソフトウェアに対してパターンファイルの配信を行う。

・GUI で設定やログを参照できること。
・サーバ及びクライアント端末に導入するマルウェア対策ソフトの管理サーバ。設定やウィルス定義ファイルの配信等を行う。
・医療系及び OA 系ネットワークにそれぞれ構築する。
・ウィルス定義ファイルは，インターネットから取得すること。
・OA 系の端末・サーバのウイルス対策ソフトウェアの統合管理を実施すること。

ヨ）ＡＤ(Active Directory) サーバ

医療系ネットワーク及び OA 系ネットワークにそれぞれ設置し，接続し利用するユーザ毎のアクセス権の設定及び端末の管理等を行う。新規にディレクトリサービスを構築すること。なお，医療系と OA 系の AD は連携してユーザ情報の整合性を保つこと。また，医療系のユーザアカウントは共通 ID とし，自動ログオンが可能であること。

タ）ファイアウォール

医療系，OA 系，部門系，共有系の出入口に設置し，特定通信の許可を行う。

レ）DHCP サーバ

DHCP サービスを構築し，認証システムと連携し,無線 LAN ネットワークにおいて自動的に IP アドレスを付与できるようにすること。

ソ）NTP サーバ

利用者に対し，外部の信頼できる時刻情報等をもとに，正確な時刻情報を提供すること。然るべき対策を行ったうえで,インターットから正確な時刻を取得すること。うるう秒の運用を行うこと。ネットワークの部分障害時やプライマリサーバ停止時もサービスの提供を継続すること。

ツ）電子メールサーバ

電子メールサーバは，現在賃貸借している外部メールサーバを利用する。なお，現状の POP メールから Web メールサービスへの契約変更を計画している。

（８）ＡＤ連携

職員情報や人事情報に基づく ID 及びパスワードの登録，変更及び削除について，ドメインコントローラ（AD）の OU，資産管理システム，グループウェア，部門システムなどの配信先機器に連携するための，仕組みを提案すること。想定するシステムの機能を下記に示す。

・職員アカウント及びパスワードの更新データを，上記の配信先機器に反映する。
・配信は，毎日実行する。
・実行モジュールは，GUI を有さなくてもよいが，操作性，メンテナンス性を考慮すること。
・リトライ機能を有すること。
・OU の移行については，組織改編及び人事異動等に伴う所属データおよび職員データをもとに，OU 及びユーザアカウントを移動する機能を有すること。
・人事異動が発生した場合，共通基盤システムのサーバから出力されたファイル(異動情報の入った処理データ)を読み込み，AD のユーザアカウントの登録，更新，移動等を行うことができること。

（９）通信要件

イ）設計

現行ネットワーク構成（VLAN 情報（VLAN 名，VLANID 等）や IP アドレス体系）を十分に把握した上で，設計すること。

・次期ネットワーク，及び予備の VLAN 構成は当院と協議，承認の上，構築すること。
・アドレス重複による障害が起きないよう，ネットワークごとのアドレス体系を明確に区別すること。
・新規サーバについては，既設ネットワークの IP アドレス体系に注意し，新規割当てもしくは既設サーバから引き継ぐなどの対応を行うこと。なお詳細については，当院と協議の上，設計時に決定するものとする。
・既設部門サーバおよび端末に割当てている IP アドレス，サブネットマスクおよびデフォルトゲートウェイを変更することなく，新ネットワークに移行できることを原則とするが，当院と協議の上，設計時に決定するものとする。
・インタフェースに設定する，速度・IP アドレス等については，必要に応じて関係システムベンダーと調整の上，設計することとする。
・将来的な機器の増設，接続機器の増加等によるネットワーク拡張に対応可能となるよう，十分な予備アドレス空間を確保するともに，VLAN の追加や管理が柔軟かつ容易に行えるよう設計すること。

ロ）IPv6 への対応

下記の方針で Ipv6 対応を実施する。

・IPv 6 アドレス設定の範囲は DMZ までとし，内部アドレスは IPv 4 で運用を行う。
・なお，Ipv4/Ipv6 デュアルスタック方式とする。なお詳細については，当院と協議の上，設計時に決定するものとする。
・ただし，内部アドレスについては，IPv6 の利用が要求されたタイミングから IPv6 による通信を提供可能な構成とするよう IPv4/IPv6 の両方のプロトコルに対応すること。

（１０）設計・構築の際の留意点

次期ネットワークおよび構築するシステムは下記に記載する項目を考慮し設計・構築を提案すること。導入する各システムの設置場所，必要ラック数(U 数),電力数を記載すること。

・医療系ネットワーク，OA 系ネットワーク，医局系ネットワークの分離

①総務省の「自治体情報システム強靭性向上モデル」で求められる要件に則り,現状の VLAN 情報を把握した上でセキュリティの高いネットワーク分割方式を提案すること。

②各ネットワーク間の論理的独立性を確保すること。

イ）業務影響への考慮

次期ネットワークへの切り替えに際し，ネットワークの運用停止時間は最小限に抑え，移行作業に伴う障害発生のリスクを最小限に抑え，円滑な移行作業を行えるシステム構成をとること。

・システムの切り替えに際し，端末の設定変更を伴わない移行方式を基本とすること。
・本業務によるシステム切替によって，各クライアントに設定作業等が必要となる場合は，当院へ連絡，協議の上，受注者の負担において作業を実施すること。

ロ）機密性・完全性・可用性の確保

提案にあたり，本仕様書等に示すもののほか，全体の安定的稼動とセキュリティの向上を実

現する機能を盛り込むように努めること。詳細は設計時に決定するものとするが，よりよい提案があれば積極的に手法,効果を含め提案に盛り込むこと。

・機密性の確保

①情報漏えい防止，適切なアクセス権の設定,権限管理,操作ログ管理などの対策を行うこと。

②管理者以外の者がログインして，管理者権限により不正に機器の設定を変更されることがないよう，強固な認証機能を構築すること。

③機器にログインが可能なユーザー数は必要最小限に留めること。

④リモートから導入機器にログインすることが可能なユーザーを複数設定する必要がある場合には，ユーザーごとに固有の ID を設定することとし，共通の ID を用いないこと。

⑤サーバ機器に搭載されるソフトウェア等で設定可能なアクセス権限については，当院と協議の上，決定すること。

・完全性の確保

改ざん防止，検出などの対策を行うこと。

・可用性の確保

①電源の二重化,モジュール単位，ホットスワップ機器の利用,システムの二重化,通信経路の冗長化などの対策を行い可用性の高い構成すること。

②また,提案する各システムおよび通信について障害時の切り替え方式，アクセスルートについて提案書に記載すること。

③通信機器等をラックにマウントできない設置場所においては，耐震ベルト等を用いて耐震処置を施すこと。

④職員業務を中断するリスク等を最小化するため，信頼性の高い機器選定及び構成設計を行うこと。

⑤導入するハードウェア・ソフトウェアに関しては以下の点を考慮し提案すること。

・共通要件

①システムのライフサイクルを通した経済性を考慮し，導入に係る初期費用，保守費用を，可能な限り抑制した構成とすること。

②同等以上の規模の類似システムにおける採用実績が豊富なものとすること。

導入するハードウェア及びソフトウェア間の組み合わせについて，障害・不具合が発生しないよう実績のある提案とすること。

③求められる性能が発揮できない際は受注者が責任を持って対応すること。

④「国等による環境物品等の調達の推進等に関する法律（グリーン購入法)」及び，同法第６条に基づく「環境物品等の調達の推進に関する基本方針」を考慮し,低消費電力技術を採用した機器およびソフトウェアを提案すること。

⑤ハードウェア，ソフトウェアともに可能な限り特定の製品に依存しないこと。

⑥なお，本仕様書は，想定事例の掲載も含めて特定の製品を意図した仕様ではない。また，広く通信機器ベンダーの製品を検討して提案を行うこと。

・導入機器

①選定する機器は，ソフトウェア実装時に通信のボトルネックとならないよう適切にサイジングし導入すること。

②24 時間 365 日の安定稼動が実現できる，高品質の機器および機能を有する機器を提案すること。

③調達時期における最新のスペックであること。導入する機器のファームウェアやソフトウェアは,導入時に最新のバージョンであること。但し安定性や採用実績等を考慮し旧バージョンの方が望ましい場合はその限りではない。

（１１）導入ソフトウェア

・業界標準的なアーキテクチャ，技術仕様に準拠した可能な限りオープンな技術を採用すること。

・仮想化製品を利用する場合はハードウェアに依存しないソフトウェア方式とし，ハイパーバイザ型の仮想化ソフトウェアとすること。

・サーバハードウェア上で稼動する OS は，アプリケーションプログラムに対して API (Application Program Interface)を通してそのサービスと機能を提供できること。また，OS のサービスと機能及び API の仕様は，標準化され広く普及している規格に準拠したものであること。

・サーバハードウェア上で稼動するOSは，標準化されて広く普及している規格に準拠していること。
・オープンソースソフトウェアを利用する場合は，類似システムでの豊富な採用実績があること。またシステムの安定稼働やシステム稼働後のサポートに関して支障の無いよう留意すること。
・導入機器に搭載されるOS及びソフトウェアについては，稼動開始までに不要なソフトウェアを除去し，不要なサービスを停止させること。
・メーカ固有の製品（ミドルウェア等）を導入する場合には，使用条件の他に，将来に渡る拡張性・経済性を十分考慮すること。また，当該製品のメーカーがサポートを中止する場合等，システムの継続的な保守に支障が出る場合には，速やかにEOL等の情報提供を行うとともに，受注者の責任において業務運用に支障が出ないような対策を行うなどの保守サポートを継続すること。
・WindowsCALは本業務内で調達することとする。また，ソフトウェアの導入に当たり，必要となるライセンスについても本業務内で調達するものとする。
・Linuxを利用するものは，リリースされてから10年間は，セキュリティアップデートを含めた公式サポートを受けることができること。また，サブシステムの要件に合わせバージョン管理を行うものとすること。
・採用する製品により，当院と製品製造業者との間で保守契約等の締結が必要な場合は事前に申し出ること。当院が承認した場合は，当院と製品製造業者との間で保守契約等を締結するが，その契約等に係る費用は本調達の応札金額に含めること。但しこの場合でも，保守は本調達の受注者が責任を持って対応すること。

（１２）製品サポート

・設計及びソフトウェアの選定にあたっては，極力クライアント端末に特別なソフトウェアの導入を必要としないことを前提とすること。やむを得ない場合には，クライアント端末へのソフトウェアの配布，導入サポートも作業範囲とするとともに，それらについて必要な協議を行うこと。
・契約期間中にサポート切れ等による理由で機器を入れ替えることの無い機器およびソフトウェアを提案すること。また，上記理由により契約期間中に機器およびソフトウェアの交換が発生する場合は，受注者の責任において機器およびソフトウェアの入れ替えを実施すること。
・また，製造者による動作保証がなされ，かつ保守サポートが受けられるバージョンであることを確認した上で導入すること。
・調達期間内に関連するファームウェアの更新があった場合は，本調達の範囲にて発注者と調整の上ファームウェアの更新を実施すること。
・期間内にOSやソフトウェアにアップデートが必要になる場合は，当院と協議し，受注者の負担において速やかに適切な対応を実施すること。
・サーバ，ネットワーク機器などのOS及びファームウェアのアップデート等の更新について効率的な手法を提案すること。
・システムの安定稼動を脅かす脆弱性に対するセキュリティパッチなどを迅速に提供する製品であること。
・マニュアルやヘルプ，保守対応は日本語に対応していること。対応していない場合は，運用に支障がないよう対応策を提案すること。

（１３）拡張性・設定変更

・ある程度の通信量やユーザの増加に対して費用を増やすことなく対応可能な構成を提案すること。また，上限値を併せて提示すること。
・上限値を越える将来的な利用者数やトラフィックの増加に対応するため，段階的な管理データ量や処理量の増加を考慮し，主記憶装置の増設，接続機器の追加等を容易に行えること。
・今後のVLAN追加などの通信要件の追加や変更に対し,費用を追加することなく短期間で設定変更を行い,当院の運用管理業務の負担の軽減並びに運用費用を抑えることができる構成,システム，及び手法を提案すること。

（１４）業務継続性の要件

ネットワークの運用にあたっては，現行システムの設置環境及びシステム設計をもとに大規模災害の発生等によるＢＣＰを策定して目標設定を行っており，次期ネットワークにおいても継続して目標設定を行う予定である。

イ）計画

地震等の大規模自然災害発生時や機器類の大規模障害発生時の業務継続性を確保するため，ＢＣＰの目標値は「大規模災害の発生等によるＢＣＰの現行システム目標値」を参考とし,端末・サーバ等の設定を含めたデータのバックアップ管理，保守用部品の確保，作業要員の確保等の適切な復旧手段の計画を行い，当院の了解を得ること。

ロ）復旧

大規模災害等で当院が甚大な被害を受けた場合等を除く各システムの障害においては，１時間以内に影響範囲と復旧見込み，予定作業報告を行い，報告後からできる限り最短の時間でシステムを最新状態に復旧できること。但し，システムまたはデータを一から復旧する場合においては，１営業日以内にシステムを最新状態に復旧すること。

・障害発生時に，バックアップからデータのリストアが速やかに行える仕組みを構築すること。
・障害等により機器の入替やシステムの再構築が必要となった場合，ソフトウェア等のインストールやシステム環境構築に係る手順書の整備等を行い，その手順書どおりに実施できるか確認すること。

第５　クライアント端末・プリンタについて

１　共通要件

（１）既存端末・プリンタ

既存の OA 系端末は，〈別紙 6〉端末・プリンタ設置場所一覧記載のとおりであり，本調達の次期ネットワークと接続して継続利用するものとする(端末：82 台　プリンタ：49 台)。

ただし，以下の作業は調達に含めること。

・以下のソフトウェアについて，すべて正常に動作するようインストールを行うこと。
　a. ウイルス対策ソフト
　b. 資産管理ソフト
　a，b については，初期設定業務開始時点で最新の修正ファイルを適用すること。
・OA 系に接続できるように設定すること。(Active Directory ドメイン参加設定，IP アドレス設定等)
・インターネット接続ができることを確認，または設定すること。

（２）OA 系端末

OA 系で使用する端末（ソフトウェア及び付属品を含む）を新規に導入する。また， OA 系端末が使用する OS，アプリケーション等（ライセンス及びマニュアルを含む）も対象とする。調達した機器は当院と合意した設定でキッティングを行ったうえで動作試験を実施し，納入するものとする。

イ）用途

・インターネット接続および Web 閲覧
・インターネットメール送受信
・院内 OA システムの利用(グループウェア等)の利用（例：院内 OA システムを医療系ネットワーク側に配置し，仮想デスクトップや仮想ブラウザ等でセキュアな接続を行い利用）
・無害化システム等を利用し，医療系ネットワーク，医局系ネットワークとのファイル交換を行う。

ロ）調達数量

現在のインターネット系端末と置き換える形で配布するものとし， 84 台とする。

ハ）調達要件・端末仕様

・メーカー及び商品を指定しないがすべて可能な限り同一機種とすること。
・なお，ハードウェアに内蔵する機器類は，本体メーカー提供品で構成し納品すること。
・未使用品，かつ，2018 年以降に製造されたものとする。
・台数はデスクトップまたは同等モデル 44 台，ノートブックモデル 40 台で合計 84 台とする。
・Windows10Professional32/64bit，メモリ 8GB 以上，CPU:Ci3 または同等性能以上とすること。
・モニターはデスクトップについては液晶 19 インチ以上，ノートブックについては 15 インチ前後のフル HD 表示とする。
・無線 LAN での接続を行う場合は，802.1x（EAP-TLS）認証に対応し，Radius サーバ及び AD サーバと連携したネットワーク認証が行えること。
・当院が指定するラベル名，コンピュータ名，契約期間等を記載したラベル作成し，貼り付けるものとする。(詳細については，契約後，別途指示する。)

ニ）導入計画・設置作業

・発注者の指示に基づき導入・設置計画書を作成し承認を得ること。

・動作確認の上，発注者が指定する職員へ引き渡すこと。なお，引き渡しの際は，インターネット系ネットワークに接続できることなど導入・設置計画書に基づき動作確認すること。

・受注者は引き渡しの際に，作業実施報告書を作成し，当院の職員から確認（記名，押印）を受けること。引き渡し完了後，作業実施報告書をとりまとめの上，合意した期間までに発注者に提出し，検査を受けること。

・納入検査の結果，全部又は一部に不合格品を生じた場合には，直ちにその OA 系端末を引き取り，代替品を発注者に納入するものとする。

・引き渡し後，速やかに納入台帳を作成し，発注者に提出すること（紙及び電子媒体）。

ホ）その他

導入する機器及びソフトウェアに関するマニュアルや技術資料等がある場合には，すべて提供すること。なお，本調達で導入する機器及びソフトウェアに付属するマニュアルなどが１部を超える場合には，各々２部のみ提出し，残部は受注者において適切に保管すること。

第６　試験に係る要件

「第４」で提示したシステムの機能及び性能を確認し，その後の確実な運用を確保するため，十分な試験を行う。部門システム，その他ネットワークについては，運用・保守事業者と試験内容，手順，スケジュール等を協議し，適切に実施することとする。具体的な検証の方法・手順や実績について提示すること。

１　各種要件

（１）基本事項

イ）全体テスト計画

実施するテストの位置づけや目的，テスト方法，テストの開始・完了基準，テストケースの定義方法，テストツールと使用データ，テストのスケジュール，テストを実施する組織計画，計画値を含む品質評価基準等，テストにおける全体方針を定め発注者の承認を得る。

ロ）試験実施要領

受注者は試験実施計画書及び試験実施要領を作成し，発注者の承認を得た上で各種試験を実施する。

ハ）現行受託事業者との調整

現行受託事業者との調整が必要な場合は，発注者が承認した試験調整手順に従い実施する。

ニ）品質評価

テスト品質評価は客観的かつ事実に基づいた正確性を保証するため，定量分析による評価を行う。また，定量分析では検知できない品質の偏り，不良の傾向も捉える必要があるため，定性分析による評価も併せて行う。

ホ）試験後の承認

試験実施後は試験成績書を発注者に提出し，承認を受ける。試験において不良が検出された場合は，発注者に報告するとともに解決に向けた提案を行い，承認を受ける。発注者が承認できないと判断した場合は，受注者の責任により必要な措置を行う。

（２）単体テスト

導入する機器単体の初期動作を確認し，モジュール単位の品質を検証する。想定しているテスト項目については以下のとおりである。

イ）ネットワーク機器

ネットワーク機器のシステムチェック，インタフェース動作，設定内容等の初期動作をについて検証する。

ロ）サーバ機器

サーバ機器のハードウェア，ソフトウェア，ストレージ機能，OS，各ミドルウェア機能，設定内容等の初期動作をについて検証する。

ハ）通信ケーブル

通信ケーブルの伝送品質測定は，敷設，接続，コネクター取付け後に試験を行うこと。試験後にネットワーク配線試験成績書を発注者に提出し，承認を受けることとする。

（３）結合試験・システムテスト

導入する機器を全て結合しプロセス単位の品質を検証する。想定しているテスト項目については

以下のとおりである。

イ）ネットワーク機器

ネットワーク機器の物理設計及び論理設計に基づき，疎通確認試験等を行い実際の動作を検証する。なお，無線 LAN については，DFS (Dynamic Ftequency Sslection)による環境不安定の可能性について確認し，対応すること。

ロ）サーバ機器

サーバ機器のミドルウェア機能，アプリケーション機能が機能要件・運用要件に沿った動作になることを検証する。

（4）障害試験

システムの論理設計及びネットワーク論理設計に基づき，障害時の想定動作と実際の動作が同じ動作である事を確認すること。テストの際はシステム停止時間，利用者への制限・制約などを評価し発注者の承認を受けること。

（5）負荷試験

システム全体の性能・パフォーマンスが実運用に際し，応答時間を含めた，快適な利用環境を実現できることを検証する。また，帯域制御が設計どおり機能することを検証する。試験はシステム負荷ツール等を使用してテストケースの作成と管理を行い，結果を発注者に報告し承認を受けることとする。

（6）脆弱性試験

ネットワーク機器及びサーバ機器の OS，ミドルウェア，アプリケーション等に潜在的な脆弱性が無いこと，不要な機能が利用できる状態となっていないことを検証する。また，試験の項目としてペネトレーションテストを行い，結果を発注者に報告し承認を受けることとする。

（7）運用試験

障害の検知，連絡，エスカレーションが想定時間内に行えることを検証する。

第７　移行に係る要件

１　基本事項

（1）移行方針

現行ネットワーク等から本業務で構築する次期ネットワークへの移行は以下の内容を考慮し最適な移行案を提案すること。また，次期電子カルテ構築等業務，次期電子カルテ運用保守支援業務の事業者と十分連携して業務を遂行すること。

・業務影響を最小化する移行方法であること。

・移行期間の妥当性を提示すること。可能な限り短い移行期間であること。

・移行日の回数，移行作業時間の妥当性を提示すること。可能な限り少ない回数・時間であること。

（2）移行計画

移行計画書を策定し，発注者の承認を得た上で実施する。詳細は設計時に決定するものとする

（3）体制

・関係部署と調整のうえ業務影響を考慮した移行体制を組成すること。

・次期電子カルテ構築等業務，次期電子カルテ運用保守支援業務及び部門ネットワーク，その他ネットワークの運用・保守事業者との協力体制を確立すること。

（4）利用者への影響極小化

クライアント端末の設定変更など利用者に負担のかからない移行方式を提案する。

（5）関係部署との調整

・必ず事前に関係部署と協議を行い各システムの業務影響を最小化するよう努めること。システム停止などが発生する場合は事前に発注者の承認を得ること。

・極力影響の少ない時間帯に実施すること。

・上記の作業を行う場合には，当該作業を迅速かつ円滑に行えるよう作業手順書を作成するなど，事前に十分な準備を行うこと。また，障害時や緊急時にはただちに元の状態に復旧できるようにすること。

・既設関連機器に対して設定変更を行う場合は，必ず事前に発注者と協議を行うこととし，原則として発注者が指定する者にその作業を行なわせること。また，運用監視に支障が出ないように関連システムを含め必要な対応を行い，動作確認を行うこと。

（6）責任範囲
移行は，発注者と協議及び調整の上，発注者の承認を得て全て受注者の責任において実施する。
（7）作業費用
移行で発生する作業費用については，全て本調達に含めるものとする。

2　前提条件
（1）試験の完了
「第7」で記載した試験が全て完了し，発注者の承認を受けることとする。
（2）機器の設置
試験済みの機器等を設置するものとする。なお，各場所への設置作業は，病院業務影響がない時間を基本とし，場合によっては，１７時以降や土曜日または休祝日に実施するものとするが，詳細は各場所の設置場所とあわせて，別途発注者と協議の上，決定する。
（3）LAN配線の敷設
各場所に設置した機器間のＬＡＮ配線を行うこと。
配線したＬＡＮケーブルには，接続している通信機器や通信経路等が明らかになるように表示札を取り付けること。

3　移行準備
・移行に際して，現行業務システムの運用に支障を来さないよう，移行計画書を作成し，発注者の承認を得た上で移行作業を実施すること。
・システム移行に伴い障害が発生した場合，必ず切戻しが可能である移行方法を採用すること

4　移行要件
（1）移行方針
移行リハーサルを行い，移行手順，作業時間，移行体制，業務影響等を明確にする。
（2）コンテンジェンシープラン
コンテンジェンシープランを策定し，想定外の問題が発生した場合は必ず元の状態に戻すことを優先させることとする。
（3）スケジュールの考慮
スケジュールは発注者，受注者，現行受託事業者，各部署のヒアリングし，十分な余裕を持った計画を作成する。提案時においても，短期間に安全に実施可能なスケジュールを具体的かつ詳細に提案書に記載することで評価することとする。
OA 系（Ｗｅｂ及びメールなど）の移行については，業務への影響を考慮し，スケジュール調整する。
機器類の設置展開作業においては，以下の制約を考慮する。
・機器類・パソコンの設置展開作業は，病院業務影響がない時間を基本とし，場合によっては，１７時以降や土曜日または休祝日に実施する。各設置場所の業務に支障がないように，騒音の抑制に留意すること。
・平日の夜間及び休祝日に作業を要する場合は，各設置場所の管理者との調整に２週間以上の期間を要するため，事前に発注者と調整し許可を受けて行うこと。詳細スケジュールは，発注者と別途協議の上，決定すること。

（4）セキュリティ確保
設定情報が漏えいしないように，作業場所の施錠及び入退室管理等によりセキュリティ確保に特に配慮しながら作業を進める。

（5）関係者との調整
・部署担当者との日程及び施工に係る連絡調整については，発注者の指示において受注者が実施すること。
・納入期限に間に合うよう，現地調査を踏まえて詳細な工程を検討し，発注者の承認を得て業務を実施すること。また，発注者と合意した導入作業日程を元に，受注者が各場所の管理者等と直接連絡を取り，導入作業の可否等について調整を図ること。なお，発注者と合意した導入等作業日程に変更を要する場合は，早期に発注者と協議して変更日程及び作業体制の調整を行い，納入期限に間に合わせ

ること。

5　留意事項

既設ネットワークから次期ネットワークへの移行に当たり，以下の点に留意すること。

・ネットワークの切替要件または当院の要望に応じて，現行ネットワークと次期ネットワーク並行運用期間を設ける場合，ネットワークの変更運用に際し，現行ネットワークへの設定変更の必要性が生じた場合は，当院と協議，調整の上，実施すること。

・機器の移行に合わせて，監視機器にて各新規設置機器の状態監視を遅延なく実施すること。

・ネットワーク移行中の機器障害については，ネットワーク移行後の通常運用と同様の保守体制を執ることとし，遅延なく機器交換を実施すること。また，障害原因の切り分け等は，受注者の責任において当院と協議，調整の上，実施すること。

なお，作業に発生する費用は今回の受注者の負担とする。

・現行ネットワークのセキュリティレベル，各機器のパラメータ等を次期ネットワークへ移行する際，受注者の責任において実施すること。

第８　保守に係る要件

本業務は，保守，障害対応を実施するものである。安定稼働を実現するための予防保守や監視を実施し，障害が発生した場合は，関係事業者と連携し回復作業を管理し，その影響を最小限に押さえなければならない。

1　基本事項

（1）安定稼働の確保

受注者は，安定稼働を確保するためにシステム監視装置等を活用しサービスレベル，システム負荷及び障害の有無を 24 時間 365 日常時監視し最適な状態を保持しなければならない。また，障害を検知した場合は，障害のレベルに応じて直ちに障害発生場所において状況を確認し，必要があれば関係事業者に連絡し，障害対応作業の全体を管理して影響範囲を最小限に抑制しなければならない。

（2）セキュリティ対策の強化

受注者は，脆弱性に対応するためにセキュリティ更新プログラムを遅滞なく配信し，各種ログにおいて，異常があれば発注者と協議の上，直ちに必要な対応を行わなければならない。

（3）障害対応の最適化

受注者は，障害が発生した場合は，早期解決に向けて直ちに障害発生場所において状況を把握し，関係事業者と連携して障害対応にあたるとともに，対応状況を管理しなければならない。サービスレベルの維持に向けては，適正な資源配分や障害対応手段の検討をするなどして対応するものとする。

2　業務内容

対象とする保守運用業務一覧は以下のとおり。

各業務を安定運用するのに必要な構成を詳細化し提案すること。

保守運用業務一覧

業務名	概要
次期ネットワーク保守業務	院内の各部門システムの情報通信基盤として，設置したネットワーク機器，サーバ機器，端末（OA 系・部門系・医療系・共通系）等の監視，障害復旧，保守を実施するもの。
セキュリティ対策業務	各系ネットワーク及び外部ネットワークの接続箇所に設置したセキュリティ対策機器を監視・分析を行いインシデントの対応を行う。
問い合わせ窓口 (OA 系端末も含む)	院内職員からの問い合わせ，障害の申告，窓口対応を一元的に受付，電子カルテシステムや各部門システムの所管部門及び保守事業者にエスカレーションを行う。

3　保守対象機器の設置場所

本委託業務の対象となる機器の設置場所は当院本館，拓桃館とする。なお，本委託業務開始後にネットワークへの追加接続があった場合には，該当箇所を含むものとする。

4　共通要件

（1）本業務の基本方針

イ）安定稼動

保守対象システムが全て支障なく稼動するために，必要な品質を確保すること。

ロ）情報セキュリティ対策

機密性，安全性を確保するための十分な対策を実施すること。

ハ）監視の実施及びログ管理体制の整備

保守対象システムの稼動状況をリアルタイムに把握して，速やかに障害対応を行えるよう，監視システム及び担当者のシステム操作により監視を行うこと。セキュリティインシデントについては，各システムが記録する通信ログを用いて解析を行い，月次でレポートを作成し報告すること。

ニ）災害対応

大規模災害や作業停電等により稼動停止した場合でも，迅速に復旧作業を実施すること。

災害発生に伴う重大な危険が認められる場合は，直ちに必要な措置を講じるものとする。この場合は，直ちに発注者等との連絡調整を行う。

（2）保守要件

イ）当院外からのリモート保守

リモート保守を行う場合は，リモート保守申請書に使用時間帯，作業内容，作業者等を記載の上，事前に当院に申請すること。ただし，障害等緊急の場合は電話等で当院の承認を得ることとし，申請書の提出は利用日から３営業日以内に後日提出すること。

ロ）保守体制

受注者は，障害発生時の迅速な対応を可能とするため，各部門（関係者）の役割分担を明確にし，迅速な対応及び意思決定がとれる体制を構築すること。

ハ）想定される各部門(関係者)

・サポート窓口
24 時間 365 日連絡可能な拠点
・県内拠点
宮城県内に存在する受注者の拠点(センター，事業所等)
・サーバ，端末及びネットワーク機器保守業者
ハードウェア障害時に保守作業を実施する事業者
・宮城県立こども病院　医療情報部　情報システム管理室
本運用保守業務を委託するシステム所管課
・関係システム所管部署
発注者より指定する，部門システムの所管部署ならびに関係者。本調達に関連する電子カルテ，部門システム等のベンダーも含まれる。

（3）保守体制の構築

・保守体制案を提示すること。
・「6　問合せ窓口業務」で障害報告を受け付けたとき又は当院の主要な保守対象機器から発信される障害通知が送信された場合は，その時点から３０分以内に初動を開始できること。
・現地対応が必要な場合は，障害の切り分け後，概ね２時間以内に担当者又は保守作業員等を障害発生箇所に到着させる体制を整えること。
・24 時間対応できる電話窓口及び出動できる体制を整え，夜間，休日は監視システムからの通報を受けて保守対応できる体制を整えること。
・保守・連絡体制図の作成
・受注者は，上記各部門(関係者)を考慮した連絡体制図を作成し，発注者の承認を得ること。作成に当たっては，少なくとも平日における連絡体制と夜間・休日の連絡体制の 2 種類を作成すること。また，連絡体制の変更がある場合は，速やかに連絡体制図を更新し発注者へ提出し承認を得

ること。

（4）監視業務

受注者は，システムの安定稼働を維持するため，以下のとおり 24 時間 365 日監視を行うこと。ネットワークを構成する回線・機器などの監視内容，監視方法，監視体制，異常検知時の連絡方法などを詳細に定義し，発注者の承認を得ること。

イ）閾値の設定

受注者は，ネットワークを構成する機器の負荷監視項目について閾値を設定し，監視をすること。閾値の設定については，一定の調査期間を経て，ピーク時の数値等を考慮し，発注者の承認を得ること。閾値を越えた場合，発注者に報告を行い，対策を協議・検討すること。想定する負荷監視対象機器，及び負荷監視項目は以下のとおり。

①負荷監視対象機器

本仕様書により調達する全ネットワーク機器，全サーバ

②負荷監視項目

CPU の負荷

メモリの使用率

ハードディスクの空き容量　等

③その他，負荷監視対象機器及び負荷監視項目について，追加で保守上必要と認められるものについては，発注者に提案すること。また，別途発注者より追加の指示があった場合には，負荷監視対象として追加すること。

ロ）監視システムの利用

受注者は，本業務で構築した監視システムを利用するものとする。アラームの発生及び不審なログを確認した場合，速やかに発注者に報告するとともに，調査・分析・復旧を行うこと。また，必要に応じて，監視システムの設定変更等を実施し最新かつ最適な監視の状況を保つこと。

ハ）死活監視

次期ネットワークで調達する全ての機器について死活監視を行うこと。異常を検知した場合，発注者に報告を行い，対策を協議・検討すること。

ニ）トラフィック監視

以下のトラフィック情報を収集して次期ネットワークへの負荷状態を把握し，ネットワークを安定的に稼動させること。

・コアスイッチ，サーバスイッチ，フロアスイッチの VLAN ごとのトラフィック情報

・ファイアウォールのトラフック情報

また，異常なトラフィックを確認した場合は，発注者に報告のうえ内容等調査を実施すること。

ホ）監視内容の調整

受注者は，監視内容，設定，閾値等の調整を行う必要がある場合，発注者と協議し，承認を得て実施すること。また，発注者からの設定の変更要望についても検討を行い，設定の調整を行うこと。

ヘ）その他の調査

受注者は，システムの障害有無にかかわらず，発注者から指示のあったトラフィックやシステムの調査等は本業務内で実施すること。

（5）セキュリティ対策業務

イ）ライセンス管理

受注者は，委託期間中必要となる OA 系端末のウィルス対策ソフトのライセンス数は本業務にすべて含めるものとする。

ロ）セキュリティ向上対応

・保守対象機器のソフトウェアの更新作業

受注者は，保守対象機器について，ソフトウェアの更新，アップグレード，バージョンアップ，又は発注者から指示があった場合は，検証を実施し必要に応じて無償で更新作業を実施すること。

・配信する更新プログラムの選定

更新プログラム等の配信については，WSUS 及び IT 資産情報管理システムなどにより，配信するプログラムの種別に応じて最適な配信方法を発注者に提案すること。

・セキュリティのレベル設定等

受注者は，セキュリティインシデントのレベルについて，サービスに与える影響度等に応じたレベルを設定するものとする。

ハ）IPA（情報処理推進機構）等の公的な情報セキュリティ機関等からの情報収集

ニ）セキュリティインシデントの影響調査及び連絡等

受注者は，セキュリティインシデントが発生した場合，問題の事象及び影響範囲等を直ちに調査し，セキュリティ障害を特定し，レベルに応じて対応するものとする。また，受注者は，速やかに発注者に報告するとともに，セキュリティ障害が拡大することを防止する対応を発注者と協議して実施するものとする。

ホ）セキュリティ対策業務の情報管理

受注者は，セキュリティ対策等で入手した情報を業務以外の目的で使用してはならない。

ヘ）パスワード・アクセス権管理

機器にログインが可能なユーザ数は必要最小限に留めること。

リモートから導入機器にログインすることが可能なユーザを複数設定する必要がある場合には，ユーザーごとに固有の ID を設定することとし，共通の ID を用いないこと。

サーバ機器に搭載されるソフトウェア等で設定可能なアクセス権限については，当院と協議の上，決定すること。

機器にログインが可能なユーザ数は必要最小限に留めること。

（6）障害予防業務

受注者は，保守対象機器等の障害予防のため，定期点検，緊急点検，及び予防保守を実施すること。また，作業終了後に報告書を提出すること。

本業務は，目視等の簡易な方法により保守対象機器等の劣化不具合の状況を把握し，保守等の措置を適切に講ずることにより所定の機能を維持し，事故・故障等の未然の防止に資することを目的とする。

イ）定期点検の実施

調達する機器について，定期点検（12 か月毎，6 か月毎）を行うこと。

①12 か月点検の内容

装置の目視点検（ランプの点灯状況を含む）

異常音の有無

コネクタ類の緩みの有無

ラック内温度の測定

清掃

②6 か月点検の内容

装置の目視点検

イベントログ確認

ハードディスク容量確認

システムサービス状態確認

清掃

ロ）緊急点検の実施

受注者は，調達する機器について，発注者が指示した場合，協議の上緊急点検を実施すること。内容については別途指示する。

ハ）予防保守の実施

受注者は，法定点検又は工事等による宮城県立こども病院の作業停電が実施される場合に，発注者の指示に基づき,宮城県立こども病院設置の機器について事前の停止作業及び事後の起動確認等を実施すること。

ニ）UPS の管理

受注者は，調達する UPS のバッテリーについて定期的に点検し，バッテリーの消耗等により交換が必要となった場合，交換するバッテリー等の部品も本調達に含めることとする。

（7）障害の対応

受注者は，障害に対し早期発見と迅速な初期対応を可能とするため，稼働状態の常時監視を行うこと。障害が発見された際には，関係者に連絡を行うとともに，障害内容の迅速な調査，切り分け，復旧及び報告を行うこと。

イ）障害対応計画

・障害レベルの定義

受注者は，サービスの提供される範囲で障害レベルを定義し，発注者の承認を得なければならない。障害レベルは，サービス全体に及ぼす重度の障害から，利用者の影響が軽微な障害までを，概ね 3 段階以上に明確に定義し，分類しなければならない。

・復旧時間の設定

受注者は，システムを構成する保守対象機器について，機器の緊急性・重要度に応じて復旧目標時間または復旧目標ポイントを設定すること。

・障害レベルの判断

受注者は，監視システムからの通知メール，警報メッセージ，ログ及び職員の問合せから障害範囲を特定し，障害レベルを判断する。

・連絡体制

受注者は，障害が発生した場合は，直ちに発注者に報告し復旧対応を実施しなければならない。ただし，障害の切り分けの結果，個別の業務システム上の障害と判断された場合または保守対象機器以外の障害と判断された場合には，発注者が指定する関係所属及び関係事業者に連絡しなければならない。

また，受注者は，関係所属及び関係事業者へエスカレーションした障害について，その進捗を把握し，障害の回復を確認した場合は発注者へ報告すること。

関係所属及び関係事業者の情報については，毎年度当初に発注者より提示するものとする。また，人事異動による担当者の変更等があった場合は，更新の都度発注者より提示するものとする。

ロ）原因及び影響調査

受注者は，障害の復旧後に，障害発生の状況，対応の経緯，原因，影響範囲，今後の対応等を取りまとめ，発注者に報告するものとする。報告においては，各対応開始及び状況変化の時間について詳細に記録すること。

ハ）障害発生時の動作

・復旧作業の実施

発注者からの指示に基づき速やかに状況を確認するとともに，障害発生の原因究明に当たること。原因究明の結果，障害発生等がサーバ等の OS 及びソフトウェア・アプリケーション（以下，「保守対象システム」という）に起因したものであると判断された場合には，該当機能を回復させること。システムの再構築以外に回復が困難と判断された場合は，費用負担区分等について別途発注者と協議すること。

・ハード保守対応機器

保守対象機器の障害の場合は，発注者に報告のうえハード保守業者に修理を依頼すること。また，保守業者の進捗を把握し，復旧作業が完了した場合には，業務完了報告書を発注者へ提出させること。

上記ハード保守対象機器の受付時間については 24 時間 365 日である。

・関係部門等への連絡

当該業務システムの所管課や関係者に対して速やかに状況を連絡すること。連絡後，発注者からの指示があった場合は，電話又はメール等により当該業務システム所管課や関係者をサポートすること。当該業務システム所管課や関係者から障害が復旧した旨の連絡を受けた場合には，監視システム等で復旧を確認すること。

・障害対応作業報告書

受注者は，障害の申告等により復旧作業を実施する際は，発注者に対し事前に口頭等で報告し，復旧後は速やかに障害対応作業報告書を提出すること。

障害対応報告書では，障害発生時刻及び障害発生箇所到着時刻を必ず記入すること。障害対応報告書の書式は，発注者が別途指示する。

（8）報告等

イ）月次報告

受注者は，本調達のシステムに関して，毎月 1 回定期的に前月の保守管理状況及び検討事項等を「月次保守管理報告書（月報)」として提出すること。月報での報告事項を以下に示す。

・問い合わせ，障害申告

問い合わせ件数と対応状況

障害申告件数

・Web フィルタリング業務

アクセス制限状況
グループ設定，規制・解除 URL 設定状況
報告時における定義ファイル等の最新バージョン
障害等に対する対応状況
登録履歴の管理（年度単位）

・不正侵入対策
不正アクセス件数
不正アクセスの内容とその対策
障害等に対する対応状況

・標的型攻撃対策
障害等に対する対応状況

・ネットワーク負荷状況
宮城県立こども病院の LAN トラフィック状況
インターネット通信のトラフィック状況

・ネットワーク機器予備機の管理
保守対象となるネットワーク機器の予備機払い出し状況

・SLA
サービス水準の達成状況

ロ）年次報告
受注者は，各年度終了後速やかに，前年度の保守管理状況及び検討事項等を「年次保守管理報告書(年報)」として提出すること。記載項目，内容については発注者が別途指示する。

ハ）報告形式
月次及び年次の報告は，インシデントや障害等，特別な場合を除いて基本的に報告書形式にて実施するものとするが，当院から要請があった場合は，会議を実施する場合もある。

（9）災害対策

イ）体制
受注者は，地震等の災害が発生した際，当院に駆けつけ可能な体制を整えること。

・仙台市内で震度 5 弱又は 5 強の地震発生時
対象者：担当者，代替担当者，又は保守作業員
駆けつけ時間：発注者からの出動要請に基づき，概ね２時間以内

・仙台市内で震度 6 以上の地震発生時
対象者：担当者，代替担当者，又は保守作業員
駆けつけ時間：発注者からの出動要請に基づき，概ね２時間以内
※ただし，駆け付け時間は，交通機関，道路状況による。

ロ）業務継続計画(BCP)の確認
受注者は，災害による障害時の対応について当院と情報を共有すること。なお，BCP については，定期の見直し及び机上訓練により更新を行い，発注者より提示するものとする。

・BCP の見直し…毎年 5 月頃実施
発注者が，前回策定時からの運用保守の実績や組織の人事異動を踏まえ，機器の復旧目標時間，連絡体制等を更新する。

・机上訓練…毎年 10 月頃実施
想定される災害を設定し，発注者と受注者で災害発生時の流れを確認する。
災害発生に対する措置について，発注者と協議の上，次の事項をまとめた防災マニュアルを作成し，発注者の承諾を受ける。
①緊急事態への準備
②緊急事態発生後の対応
③業務の早期復旧

ハ）災害対策訓練の実施

・災害発生時の机上訓練
受注者は，発注者の指示により年に 1 回机上訓練を実施すること。その際想定する災害のレベルは発注者より指定するものとし，以下の点について確認すること。
①情報システム管理室との作業分担
②ネットワーク機器の復旧目標

③復旧作業手順

訓練により確認された問題については，その対策案を発注者に提案し，BCP の更新に協力すること。

・ネットワーク機器切り替え訓練

受注者は，発注者の指示により，年に１回ネットワーク機器の待機系への切り替え訓練を実施すること。ただし，切り替えは冗長化している範囲とする。

訓練により問題が発生した場合，問題点とその対策を発注者に報告すること。

・復旧時の対応

受注者は，災害により障害が発生した際は，発注者の策定する業務継続計画(BCP)に従い，復旧作業を実施すること。なお，災害対応の流れは概ね下表「災害時の障害対応フロー」のとおりとし，災害発生時の対応手順を作成すること。この対応手順は，定期の見直し及び訓練により，発注者の BCP 同様に更新を行うものとする。

災害時の障害対応フロー

対応	内容
参集	「体制」に従い，担当者が宮城県立こども病院へ参集する。
要員の参集状況及び安否確認	担当者の安否確認を行い，安否確認の結果を発注者へ報告する。
重要書類・データの保護	サーバ室での業務遂行が困難な場合は，端末や重要書類等を持ち出しする。
外部事業者との連絡確保	回線業者等外部事業者と連絡を取り，協力関係を確認する。
被害状況の調査，障害原因の究明	被害状況を把握し，システムに障害がある場合は，その原因を究明する。
発注者への状況報告	要員の参集状況及び被害状況等について発注者へ報告する。
予想復旧時間の見積	予想復旧時間を見積もりするほか，必要物資，要員を確認する。
復旧方針の検討	復旧に関する手順や暫定的な対応方法を検討し，発注者へ報告する。
応急措置の実施	応急措置を行い，システムの暫定復旧を行う。
システム復旧の作業計画	ネットワークやシステムの復旧状況を発注者と連携して把握し，本業務に係る機器の復旧を図るとともに，全体に係る報告を行う。
システム復旧作業	作業計画に基づき復旧作業を行う。
復旧システムの運用開始	復旧システムの運用を開始する。
通常システムへの復帰	発注者が復帰の判断を行う。

（１０）その他

・助言等

受注者は，本仕様書に関するシステムの適正かつ有効な利用を図るため，発注者からの相談及び

問い合わせに応じるほか，必要に応じて運用上の改善すべき事項について，助言又は提案をすること。

5　サービス水準合意（SLA）

保守の品質に対する発注者と受注者の運営ルールを明確にするため，保守に係る必要項目について数値で要件を設定し，目標達成型のサービス水準合意（以下「SLA」という。）を締結する。これにより利用者へより質の高いサービスの提供を目指すものとする。

（1）SLA の対象項目

SLA の対象項目は，運用する全システムで必要と思われる項目，評価基準，最低水準値，目標などを提案すること。

（2）SLA の改定方法

受注者は，当院と協議して定められたサービスレベルを毎月測定し年 1 回とりまとめ，その結果を発注者に報告して，評価をうけるものとする。

その評価の結果 SLA の改訂が必要であればサービスレベルの改善を行い，その後も改善効果及び評価を継続的に実施する。

（3）サービス水準のモニタリング

SLA の対象項目について，機器の設置環境・設備に関してはシステムの安定稼動のため，最低限必要な要件であり，サービス水準として定義せず，必須条件として実施内容を求めることとし，サービス水準とはしないものとする。

また，発注者に提供されるサービスのサービス水準への達成状況を検証するため，発注者は受注者の事業実施状況に係るモニタリングを実施する。

モニタリングの内容については，サービス水準を確認するために必要な項目を選定するものとし，モニタリングの項目を定め運用状況を確認した結果，モニタリングの内容からサービス水準が達成されていないことが確認された場合，発注者は受注者に対し，業務改善・復旧に関する改善通知を行うものとする。

（4）SLA 評価項目と設定値

以下は，当院が想定する評価項目，最低水準値及び目標値である。水準値にあたっては，公共 IT におけるアウトソーシングに関するガイドライン（総務省）（以下，公共 IT ガイドラインという。）を参考とした。

以下はあくまで参考例であり，実現可能なサービス項目，最低水準値，目標値について提案すること。なお，記載にないサービス項目があれば提案すること。

イ）問合せ窓口

サービスメニュー	サービス項目	サービス内容	評価基準	最低水準値	目標値
障害受付	問合せ窓口	当院職員からの問合せ及び障害報告を受付する。 問合せ内容を適切に判断し，関係部署へ連絡，報告する。	受付方法	電話及び電子メールでの問い合わせを受付ける。	電話，電子メールに加えて職員ポータル等にて受付できること。
	放棄率	待ちきれずに電話を放棄する割合を低水準に維持する。	待ちきれずに切った件数の割合	全コールの 20%未満	全コールの 5%未満
	再コール比率	再度同一の職員が同一の質問をしないよう回答する。	一度解決扱いになった問合せに対し，再度同一の職員から同一の問合せを受けた件数の割合	全要求件数 15%未満	全要件件数の 5%未満
	応答時間遵守率	定められた時間内に応答する。	決められた時間内に応答したコール数の割合	30 秒以内 70%以上	30 秒以内 90%以上

・再コール比率＝（解決扱いになった問合せのうち，再度問合せがあった件数）／（全問合せ件数）
・応答遵守率＝（30 秒以内に応答したコール数）／（全コール数）

ロ）監視

サービスメニュー	サービス項目	サービス内容	評価基準	最低水準値	目標値
稼働監視	ネットワーク死活監視	監視システムにより稼働状態を監視する。	Ping による応答確認の頻度	1 回／3 分	1 回／1 分
	ハードウェア監視	ハードウェアの異常の監視を行う。	異常を検知してから報告までの時間	検知後 30 分以内の報告	検知後 30 分以内の報告
性能・状態監視	トラフィック監視	トラフィックを監視し，記録する。	定期記録時間	30 分／回	5 分／回
		ログ集計レポートを提出する。	レポートの報告回数	随時	主導的に臨時報告を行うこと。

サービスメニュー	サービス項目	サービス内容	評価基準	最低水準値	目標値
	ネットワーク機器性能監視	CPU 使用率を確認する。	サーバの CPU 使用率を測定	閾値超え検知後 60 分以内の報告	リアルタイム
		メモリ使用率を確認する。	サーバのメモリ使用率を測定	閾値超え検知後 60 分以内の報告	リアルタイム
		ディスク使用率を確認する。	ディスクの使用率を測定	閾値超え検知後 60 分以内の報告	リアルタイム
		システム性能状況の報告を行う。	集計レポートの報告回数	1 回／月	1 回／月の定例報告が実施され，なおかつ手動的に臨時報告を行うこと。

ハ）障害対応

サービスメニュー	サービス項目	サービス内容	評価基準	最低水準値	目標値
障害対応	障害通知	障害発生時の通知を行う。	障害検出から通知までの時間	検知後 30 分以内の通知	リアルタイム
	復旧対応	障害復旧作業を行なう	連絡を受けてから復旧作業を開始するまでの時間	連絡を受けてから 60 分以内に作業を開始	連絡を受けてから 10 分以内に作業を開始
	駆けつけ時間	保守作業員が現地で復旧作業を行う	現地対応が必要と判明した後，保守作業員が現地へ駆けつけるまでの時間	切り分け後 180 分以内	切り分け後 60 分以内
	障害報告	障害の報告を行う。	障害の復旧後に報告書を提出するまでの時間	障害復旧後 3 日以内に報告書提出	障害復旧後 24 時間以内に報告書提出

ニ）セキュリティ対策

サービスメニュー	サービス項目	サービス内容	評価基準	最低水準値	目標値
セキュリティ管理	不正アクセス報告と対応	不正アクセスの報告を行う。	アナリストがインシデントと判断してから報告までの時間	30 分以内の報告	リアルタイム

サービスメニュー	サービス項目	サービス内容	評価基準	最低水準値	目標値
		不正アクセスへの適切な対応を行う。	対応確認の連絡をしてから対応措置を開始するまでの時間	60 分以内に対応開始	検知から 10 分以内に対応開始
	パターンファイルの更新	パターンファイルの更新を定期的に行なう。	パターンファイルの更新頻度	ベンダーリリースから３日以内	ベンダーリリースから 24 時間以内

（５）モニタリング

イ）モニタリングの基本方針

受注者から発注者に提供するサービスが，SLA を達成しているか検証するため，受注者は実施状況に係るモニタリングを実施する。

種類	主な方法(案)
定期モニタリング	・受注者は，報告事項をとりまとめ，業務月次報告書，業務年次報告書として発注者に提出する。 ・職員及び受注者が出席する会議を当院が必要と判断した場合に開催し，定期モニタリングの結果報告を行うとともに，利用者からの苦情等の発生の原因についての検討及び意見交換等を行う。

ロ）モニタリング項目

具体的なモニタリング項目，評価方法については，受注者が提出する各種計画書を基に発注者と受注者が協議のうえ発注者が定めるものとする

ハ）サービス未達成時の対応

受注者は，SLA により設定されたサービス指標を維持できるよう努め，維持できない場合には，対策を検討し発注者の承認を得たうえで実施すること。ただし，目標保証型のサービス指標を維持できず改善の見込みがないと発注者が判断した場合には，別途協議のうえ本委託業務契約金の減額ができることとする。

6　その他保守業務

次期ネットワーク保守を行ううえで「4　共通事項」に一致しない個別要件を以下に記載する。

（１）OA 系端末保守業務

イ）初期設定・設置業務

・対象端末数： 84 台
・コンピュータ名，契約名，保守事業者名，各連絡先等を記載したラベルを作成し，パソコン本体に貼り付けること。
・指定するローカルユーザーアカウント，パスワード及びコンピュータ名を設定すること。
・次のソフトウェアについて，すべて正常に動作するようインストールを行うこと。なお，導入後の運用において不具合が発生した場合は，発注者と協議の上改善に努めること。
  a. 提案する OA 系の最新 OS
  b. Microsoft Office Standard 2019 相当のアプリケーション
  c. Adobe Acrobat Reader DC
  d. ウイルス対策ソフト及び無害化／セキュリティ関連ソフト及びセットアップ
  e. 資産管理ソフト
  f. その他 OA 系に必要となる設定事項

a から f については，初期設定業務開始時点で最新の修正ファイルを適用すること。

・OA 系に接続できるように設定すること。(Active Directory ドメイン参加設定，IP アドレス設定等)

・リカバリディスク（マスターイメージ）や，リカバリ作業手順書を作成すること。
・設定が完了した端末を 2020 年 3 月 31 日までに発注者が指定する場所へ設置し，次期ネットワークに接続できることを確認した上で，発注者が指定する職員へ引き渡すこと。引き渡しが完了した際は，作業実施報告書を作成し，引き渡した職員から確認（記名，押印）を受けること。設置場所は宮城県立こども病院内とする。

ロ）既存医局系端末・プリンタの接続確認

既存持ち込み端末機がインターネットに接続できることを確認すること。接続不可の場合は，対応すること。

ハ）保守業務

納入した OA 系端末を常に良好な状態に保つように，保守業務を行うこと。

・保守対象
本仕様書により導入した端末及びプリンタの保守を行うこと。
・障害時の連絡体制
本契約の範囲において，発注者からの連絡窓口を一本化すること。
・保守体制
保守の依頼があった場合，現地に翌営業日の午前中までに出張し，障害対応を開始できる保守体制を確保すること。 ただし，電話等による遠隔診断で，翌営業日の午前中までに障害復旧が可能な場合は，この限りではない。
障害及び故障等の修理等によって，復旧に日数を要する場合は，代替機に交換すること。ただし，代替機は，一時的措置とし，障害及び故障等が復旧した端末及びプリンタは，系ネットワークに接続できることを確認した上で，速やかに元の場所に設置すること。（詳細については，契約後，別途指示する。）
・修理作業
障害で，OA 系端末のハードディスクを交換する際は，復旧媒体を用いて初期導入時点まで復旧すること。なお，データの移行作業は発注者が行う。また，復旧媒体は発注者が用意する。

ニ）その他

契約期間中に発注者から各種協力依頼があった場合には，発注者と協議の上，対応を決定すること。

7　問い合わせ窓口業務

（1）基本事項

職員等からの障害の申告を一元的に受け付け，各システム所管へのエスカレーション等対応を行うこと。

（2）問い合わせに対する処理

担当者は，職員等から問い合わせを受け付けたときは，所管部門への連絡，助言等適切に対処すること。問い合わせ受付の範囲は以下のとおり。

・ネットワーク不具合などに関する問い合わせ
・OA 系端末不具合などに関する問い合わせ
・ネットワーク利用・構成に関する相談など
・ウィルス感染に関する問い合わせ全般

（3）エスカレーション

問い合わせ内容に対しては，効率的な情報検索を行い，発注者との確認を徹底することで，受注者で回答可能な問い合わせについて，各部門システム所管部署及び納入業者及び保守業者へエスカレーションしないように努めること。

（4）回答

受注者で回答可能な問合せに対応するに当たり，以下を実施すること。

・発注者から提供される情報をもって回答可能な問い合わせについて，利用者に対して回答すること。
・職員への回答について，回答期限の超過が見込まれる場合，又は状況の変化があった場合，職員に対し回答期限の超過について具体的な時間の見込みを報告すること。なお，問い合わせ対応中，対応期限が明示された場合，それを回答期限とし，明示されなかった場合，事前に発注者と協議の上，決定した期限を回答期限とする。

（5）障害等に対する処理

担当者は，運用するシステムに関する職員等からの障害の申告を受け付けたときは，速やかに調査を実施すること。

調査の結果，運用する保守対象機器の障害であった場合は，前述「４．（７） ハ）障害発生時の動作」のとおり対応すること。

（6）ナレッジ管理

受注者は，ナレッジ管理として，以下の作業を実施すること。

・受注者は，受け付けた問い合わせ，障害の申告はその対応結果も含め記録し管理すること。また，情報システム管理室職員が，インシデント状況を随時参照できる体制を整えること。

・前任の保守業者が管理している，過去に発生，又はサービス提供開始の時点において対応中の問い合わせ等についてもナレッジとして管理すること。

8　OA 系端末の障害対応

受注者は，「７ 問い合わせ窓口業務」において，OA 系端末の障害であると判断した場合は，以下の対応を行うこと。

（1）連絡対応

職員からの問い合わせ内容を確認し，障害であると判断した場合，保守連絡先に依頼すること。

（2）障害対応結果の進捗確認

パソコン保守業者に依頼した障害対応内容について，作業が完了するまでの進捗管理を行うこと。また，障害対応が完了した場合は，業務完了報告書を確認・保管すると共に，発注者へ報告すること。

（3）その他

発注者の指示により，利用者へ操作上の注意事項等を情報提供するための資料を Web 形式及び PDF ファイル等で提供すること。

第９　特記事項・留意事項

本業務の実施に必要な資料（現行ネットワークの完成図書等）については，発注者と受注者にて協議の上，発注者が必要と認めたものに限り閲覧可能とする。なお，閲覧方法等の詳細は別途協議により決定するものとする。

1　各種要件

（1）納入機器一覧表

本業務において納入する機器については，「納入機器一覧表」を作成の上，提案書と併せて提出すること。

（2）業務の再委託

受注者は，本業務の全部又は一部を第三者に委託又は請け負わせてはならない。ただし，予め書面により発注者と協議し，承認を得た場合はこの限りではない。なお，発注者が書面により承認した場合には，承認を得た第三者（以下「再委託先」という。）も受注者と同様の義務を負うものとし，受注者は再委託先に本業務に係る情報セキュリティ保持等の義務を遵守させるために必要な措置をとらなければならない。

業務の一部について再委託の承認を求める場合は，次の事項を記載した再委託承認申請書を文書により提出すること。

・再委託先名称，代表者氏名，担当者及び連絡先等

・再委託を行う業務内容及び再委託業務履行状況管理方法・体制等

・再委託先に対するセキュリティ研修体制を含む管理方法・体制等

本業務は，受注者及び再委託先において完結できること。また，受注者は発注者に対して，承認を得た再委託先の行為について全責任を負うものとする。

（3）著作権等

・受注者は，著作権法（昭和４５年法律第４８号）第２１条（複製権），第２６条の２（譲渡権），第２６条の３（貸与権），第２７条（翻訳権，翻案権等）及び２８条（二次的著作物の利用に関する原著作者の権利）に規定する権利を発注者に無償で譲渡するものとする。

・受注者は，事前に発注者から書面による同意を得た場合を除き，著作権法第１８条（公表権），第

１９条（氏名表示権）及び第２０条（同一性保持権）に規定する権利を行使しない。

・受注者は，本契約を履行するに際し，第三者の著作権，特許権，実用新案権等その他の権利を使用する場合は，その使用に関する一切の責任を負うものとする。ただし発注者がその方法を指定した場合は，この限りでない。

・受注者は，納入物の作成のために，受注者の保有する記録媒体に存在する一切の情報について，成果物の納入後にすべて消去しなければならない。ただし，書面により発注者の承認を得たときは，この限りではない。また，発注者が承認した再委託先がある場合は，再委託先の情報の消去について受注者が全責任を負うものとする。

（４）権利義務の譲渡等の禁止

受注者は，発注者の事前の書面による承諾を得た場合を除き，この契約によって生ずる権利または義務の全部若しくは一部を第三者に譲渡，承継させてはならない。

（５）情報セキュリティに関する要件

本業務は院内業務に関する情報を扱う機器・ソフトウェア等の設置・設定を行うことから，その実施にあたっては高度な情報セキュリティ確保対策が求められる。

そのため受注者は，宮城県個人情報保護条例，当院情報セキュリティ管理規程を遵守すること。特に下記事項を遵守して機器の選定・環境構築を行うこと。

（６）情報の適正な保護・管理及び情報システムのセキュリティ確保

本業務において取り扱う情報の漏えい，改ざん，消去等が発生することを防止し，情報システムのセキュリティを確保する観点から，適正な保護・管理対策やセキュリティ対策を実施し，その状況を月１回定期的に報告すること。

また，受注者における情報の漏えい，改ざん，消去等の事象や情報システムに対する侵害等が発生した場合に実施すべき事項・手順等を明示すること。

なお，これらの実施状況について，公表された脆弱性問題等に対応するために発注者が不定期に把握・評価を行う場合があるのでこれに応じること。

（７）守秘義務の遵守

・受注者は，いかなる場合においても，本仕様書の業務を履行する上で知り得たシステムの構造，機器構成，セキュリティ設計及びソフトウェアで新たに開発された技術，知識並びに本業務において知り得た一切の情報，業務の内容及び付随する事項等については，その機密を保持するものとし，発注者の許可なく無断で公開又は第三者への提供を行ってはならないものとする。

・情報漏洩が発生しないよう必要な措置を講ずること。

・関係する情報を複製または複写しないこと。

・関係する情報を本業務の目的以外に使用しないこと。

・契約期間終了後に，関係する情報を廃棄すること。

・上記については，本契約が終了した後も有効に存続する。

（８）導入機器に対する権限設定

本業務で納入する機器に関しては，発注者の設定指示に基づき，管理者，運用者など操作者の権限に応じた操作権限の設定を適切に実施し，本業務を行うこと。

（９）入退室手続

・作業のためのサーバ室等への入退室については，発注者の指示に基づき所定の手続きを行い，あらかじめ許可を得ること。

・休祝日及び夜間作業については，作業員名簿の提出等の事務手続きを作業日の一週間前までに行うこと。

・設定・設置作業期間中における障害発生時の臨時対応については，あらかじめ定めた緊急連絡方法によって発注者と連絡調整し，入退室方法について指示を受けること。

（１０）情報の開示

発注者が提供した情報を第三者に開示することが必要である場合は，事前に発注者と協議の上，書面による承認を得ることとする。

（１１）遵守事項

受注者は，当院のネットワークの構成と接続環境を熟知した上で，この業務を実施しなければならない。また，業務の実施に当たっては，契約書及び本仕様書に定めのあるもののほか，以下の関係法令等を遵守し，安全管理に必要の措置を講じた上で業務を履行しなければならない。

・民法

・著作権法

・個人情報の保護に関する法律
・電気通信事業法
・電波法
・不正アクセス行為の禁止等に関する法律
・有線電気法
・日本工業規格
・電気設備技術基準
・電気設備工事共通仕様書
・厚生労働省「医療情報システムの安全管理に関するガイドライン第５版」
・総務省が提示する「新たな自治体情報セキュリティ対策の抜本的強化に向けて」
・総務省「一般利用者が安心して無線 LAN を利用するために」
・総務省「企業等が安心して無線 LAN を導入・運用するために」
・その他関係法令等。

（１２）業務継続計画（ＢＣＰ）に配慮した復旧手段の計画

地震等の大規模自然災害発生時や機器類の大規模障害発生時の業務継続性を確保するため，端末・サーバ等の設定を含めたデータのバックアップ管理，保守用部品の確保，作業要員の確保等の適切な復旧手段の計画を行い，発注者の了解を得ること。

（１３）業務データの情報漏えい対策

業務データの情報漏えい対策に有効なデータ暗号化・ユーザ認証管理・ネットワーク設計（ファイアウォールの組合せ等）を考慮し，高度なデータセキュリティを確保すること。

（１４）データの消去

運用期間中，ハードディスクの障害等で交換が発生した場合は，完全にデータ消去を行い，データ消去証明書を提出すること。

（１５）搬入・設置・撤去作業の留意事項

・通信機器等の設置作業は，通信機器等本体及び建築物等の損傷防止に配慮しながら行うこととし，搬入経路の確保及び必要に応じて養生を行うこと。
・次期ネットワークの稼働開始後に，当院が不要と判断した現行ネットワーク機器及び通信ケーブル，機器は撤去の上，当院の指示に従い，指定の場所まで集積を行うこと。なお，廃棄は当院で行うものとする。
・搬入・搬出作業の実施にあたっては，適切に施設設備の保護（養生）を行うこと。また，搬入・撤去作業による施設設備の破損等については，施設管理者と協議の上，受注者の負担と責任において修理等を行い原状回復すること。

（１６）設置調整経費について

本業務で調達する機器等が正常に動作するために必要となる機器の設置・設定作業及び配送料，耐震対策，発注者及び関連業者との調整及び機器導入に関する一切の経費は，本調達に含むものとする。

・設置準備作業について
機器等の設置にあたり必要となる電源の確保，ネットワーク機器の設置，サーバラックへの設置等の各作業について以下に示す。
・電源タップ・分電盤の設置作業等
電源の確保に当たっては，電源の供給元から機器まで適切な電源ケーブルを敷設し，機器の運転に十分な電源容量を確保すること。
・設置する機器に電力を供給するために必要な電源を確保するため，現場の電源状況を調査し，必要となる場合，分電盤からの電源ケーブル敷設や電源タップの設置等，現場の状況にあわせて適切に調整すること。
・業務時間中に作業を実施する場合は，作業箇所周囲の電源が落ちる等の事故が無いように，作業タイミングを調整する等，慎重に作業を進めること。
・設置作業
通信機器等をラックにマウントできない拠点においては，耐震ベルト等を用いて耐震処置を施すこと。
・機器の設置にあたり，宮城県立こども病院管理者の指示に従い作業を実施するものとする。

（１７）その他

疑義に対する協議等

・調達仕様書に定められた内容に疑義が生じた場合は発注者に質問し，指示を受けること。
・現場の納まり，取合い等の関係で，調達仕様書によることが困難若しくは不都合が生じた場合は，発注者と協議すること。
・協議を行った結果，契約図書の訂正又は変更を行う場合は，受注者及び発注者の協議によること。
・本仕様書及び発注者からの指示依頼内容に不明点がある場合は，解釈の違いによる作業対応ミスを防ぐ観点から，速やかに発注者に確認して確実に作業を行うこと。
・本仕様書に明記されていない細部の事項で，当然具備すべき作業についてはこれを行うこと。
・契約期間中に発注者から各種協力依頼があった場合には，協議の上，誠実に対応すること。
・出入り禁止箇所
業務に関係のない場所及び室への出入りは禁止する。
・服装等
業務関係者は，業務及び作業に適した服装並びに履物で業務を実施すること。また，名札又は腕章を着けて業務を行うこと。
・発注者の立合い
作業等に際して発注者の立合いを求める場合は，あらかじめ申し出ること。