I．システム全般に関する包括的な要件

I. システム全般に関する包括的な要件

I. システム全般に関する包括的な要件

1 那覇市保健医療福祉ネットワークシステムに関する基本要件

1-1 目的と役割への合致

1-1-1 那覇市および近郊医療施設の連携促進

1-1-1-1 地域医療機関連携の促進により, 那覇市としての医療費増大の抑制に資すること.

1-1-1-2 地域医療機関連携の促進により, 那覇市としての医療品質の維持向上に資すること.

1-1-1-3 地域医療機関連携の促進により, 那覇市および近郊医療施設における診療業務の迅速性向上に資すること.

1-1-1-4 地域医療機関連携の促進により, 那覇市および近郊医療施設における診療業務の生産性向上に資すること.

1-1-2 市民サービスの向上

1-1-2-1 那覇市民の疾病予防や早期発見に資すること.

1-1-2-2 那覇市民のライフステージやライフサイクルに即した保健医療情報の提供に資すること.

1-1-2-3 那覇市民個々人に見合った体系的健康指導や継続的な健康支援の実施に資すること.

1-1-3 個人情報の保護

1-1-3-1 前二項とその目の全ては, 個人情報の秘匿を保全したうえで実現されること.

1-1-3-2 前二項とその目の全ては, 個人情報の自己制御権を実現する機構を具備または事後に機能拡張できるよう設計されること.

1-2 堅牢性・信頼性・保全性

1-2-1 堅牢性

1-2-1-1 1日 24 時間, 年 365 日の連続無人自動運転が可能な堅牢なシステムであること.

1-2-1-2 電源供給の途絶や空調設備の停止の際に auto-shutdown を実現する方策を施すこと.

1-2-2 信頼性

1-2-2-1 データベースならびにミドルウエアは充分な roll back 機能を有していること.

1-2-2-2 診療記録の電子保存に堪えるべく, 真正性･見読性･保存性に対する適合度を明示し, その証拠書類を提出すること.

1-2-3 保全性

1-2-3-1 利用者認証とサーバ認証に加え, 通信データの機密保護機構を備えること.

1-2-3-2 改竄や消去等の破壊, ならびに詐称や盗聴に対する充分な対策が, 個々の機器の configuration 段階, すなわち disk partition, volume mount, file permission の段階から, 堅実に設計設定されること.

1-2-4 アクセス管理

1-2-4-1 役割に応じたアクセス制御ができること.

1-2-4-2 職員マスタの各アカウントの属性履歴について, 多様な役割の履歴を保持しつつ, 所属施設や課･係･科･部や氏名の変更に影響されることなく, 完全な遡及性を確保すること.

1-2-4-3 全てのアクセスについて記録された詳細なログは, 相当期間保存すること.

ログ・ファイルはタイム・サーバによる時間認証を受け・かつ・埋め込まれた時刻情報が暗号化されていることが望ましい.

1-2-4-4 アクセスに関して, システム監査機構の付加が可能であること.

1-3 標準への対応

1-3-1 共通要件

1-3-1-1 全てのコードマスタは版管理され, かつコード値を格納するデータベースにはコード値と併せてコード体系の同定情報ならびに版情報が格納されること.

1-3-1-2 コードマスタは, サブシステムや外部接続システム等システム間で, 適宜交換できること.

1-3-1-3 通信では, 文字コードは ANSII safe 7 bit, 8 bit SJIS, または UTF-8 を使用すること.

1-3-1-4 ISO, CEN, IEC, W3C, HL7, NEMA/JIRA 等にて決議された normative document ほか formal document として出版されている国際標準や国際的な de facto standard, もしくは国内標準等に準拠したコード, エンコード方式, フォーマットあるいはプロトコルを用いること.

1-3-1-5 新たな定義が必要な場合には, 定義書式は ASN.1(ISO/IEC 8824) に則ること. ただし eXtensible Markup Language(XML) については Document Type Definistion (DTD) で可とする.

1-3-2 コード

1-3-2-1 以下の事項についてコード化が必要な場合, 以下に挙げたコードまたはエンコード方式を用いること. なお文字コードについてはいずれかを選択することとなる.

１）JIS X 0301:1992（ISO 8601:1988）
ただし年は４桁完全表記とする.
また当該フィールドを, 元号による年と併用しないこと.

２）JIS X 0304:1997（ISO 3166:1997）

３）ITU-T E.164.1 and ITU-T B.19

４）JIS X 0401:1973

５）JIS X 0402:1994
なお沖縄県中央保健所の管理する地域コードとの対応表も用意すること.

６）JIS X 0403:1997

７）JIS X 0404:1987

８）JIS X 0201:1997, JIS X 0208:1997

９）JIS X 0202:1998（ISO 2022）
同附属書１（通称 SJIS エンコード；JIS X 201 での１バイトカタカナ禁止）
同附属書２（通称 ISO-2022-JP；RFC1468 符号化表現）

１０）Unicode または ISO/IEC 10646

1-3-3 医用コード

1-3-3-1 以下の事項についてコード化が必要な場合, 以下に挙げたコードを用いること.

１）MEDIS-DC 病名マスタ第二版（ICD10 対応版）

２）厚生労働省 電算処理基本マスタ ７種：
傷病名マスタ, 修飾語マスタ, 診療行為マスタ, 特定保険医療材料マスタ, 医薬品マスタ, 調剤行為マスタ, コメントマスタ.

３）HOT

４）JLAC10（ただし LOINC への変換ユーティリティを提供すること）

1-3-4 通信プロトコル

1-3-4-1 以下のプロトコルを用いること.

1）ARP, RARP
2）ESP, GRE
3）IP（TCP, UDP, ICMP）

1-3-5 医用通信プロトコルほか

1-3-5-1 以下のプロトコル／フォーマットに対応できるシステム設計であること.

1）HL7
2）DICOM3
3）MERIT9
4）SGML および XML（XML Schema, RELAX を含む）
5）CORBA（もしくは相当の objext borker）

1-3-6 公開鍵基盤関係の規格ほか

1-3-6-1 以下の規格に準拠適合するシステムであること. ただし hcRole は割愛してよい.

1）ISO/TS 17090-1:2002（Health Informatics - Public key Infrastructure- Part 1: Framework and Overview）
2）ISO/TS 17090-2:2002（Health Informatics - Public key Infrastructure- Part 2: Certificate profile）
3）ISO/TS 17090-3:2002（Health Informatics - Public key Infrastructure- Part 3: Policy management of certification authority）

1-3-6-2 以下の規格等を満たすこと.

1）IETF RFC 2510:1999 "PKIX: Certificate Management Protocols" または同等の安全な方法によって, 証明書所有者に当該私有鍵を引き渡すこと.
2）IETF RFC 2511:1999 "PKIX: Certificate Request Message Format" または PKCS #10 v1.7:2000 “Certification Request Syntax Standard” のうちいずれか.
3）IETF RFC 2527:1999 "PKIX: Certificate Policy and Certification Practices Framework" に準拠した認証ポリシで運用できること.
4）IETF RFC 2528:1999 "PKIX: KEA in PKC" または IETF RFC 3279:2002 "PKIX: Algorithms and Identifiers for the PKC and CRL" のうちいずれか.
5）IETF RFC 2559:1999 "PKIX: Operational Protocols - LDAP v2"
6）IETF RFC 2560:1999 "PKIX: Online Certificate Status Protocol - OCSP" に対応することが望ましい.
7）IETF RFC 2585:1999 "PKIX: Operational Protocols - FTP, HTTP"
8）IETF RFC 2587:1999 "PKIX: LDAP v2 schema"
9）IETF RFC 2649:1999 "LDAP Control and Schema for Holding Operation Signatures"
10）IETF RFC 2807:2000 "XML Signature Requirements"
11）IETF RFC 3029:2001 "PKIX: Data Validation and Certification Server Protocols"
12）IETF RFC 3039:2001 "PKIX: Qualified Certificates Profile"
13）IETF RFC 3161:2001 "PKIX: Time-Stamp Protocol (TSP)"
14）IETF RFC 3279:2002 "PKIX: Algorithms and Identifiers for the PKC and CRL"
15）IETF RFC 3280:2002 "PKIX: Certificate and Certificate Revocation List (CRL) Profile" または IETF RFC 2459:1999 "PKIX: Certificate and

Certificate Revocation List (CRL) Profile" のうちいずれか.
16) IETF RFC 3281:2002 "PKIX: An Internet Attribute Certificate Profile for Authorization"
17) IETF RFC 3275:2002 "XML-Signature Syntax and Processing"

1-3-6-3 以下の規格を採用すること.
1) IETF RFC 3174:2001 (US Secure Hash Algorithm 1 (SHA1))
2) IETF RFC 1321:1992 (The MD5 Message-Digest Algorithm)
3) PKCS #1:1993 RSA Encryption Version 1.5 (IETF RFC 2313:1998)
PKCS #1:1998 RSA Encryption Version 2.0 (IETF RFC 2437:1998)
PKCS #1:2002 RSA Encryption Version 2.1 のうちいずれか
4) IEEE P1363:2000 (Public-Key Cryptography)
5) NIST FIPS 46-2, 44-2:1993 (Data Encryption Standard (DES))

1-3-6-4 以下の法律または指針に準拠したシステムであること.
1) 電子署名及び認証業務に関する法律
2) 電子署名及び認証業務に関する法律施行令
3) 電子署名及び認証業務に関する法律施行規則
4) 電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針

1-3-6-5 以下の規格を採用すること.
1) IETF RFC 2251:1997 (Lightweight Directory Access Protocol (v3))
2) IETF RFC 2252:1997 (Attribute Syntax Definitions
3) IETF RFC 2253:1997 (UTF-8 String Representation of Distinguished Names)
4) IETF RFC 2254:1997 (The String Representation of LDAP Search Filters)
5) IETF RFC 2255:1997 (The LDAP URL Format)
6) IETF RFC 2256:1997 (A Summary of the X.500(96) User Schema for use with LDAPv3)
7) IETF RFC 2589:1999 (Extensions for Dynamic Directory Services) に対応することが望ましい.
8) IETF RFC 2596:1999 (Use of Language Codes in LDAP)
9) IETF RFC 2829:2000 (Authentication Methods for LDAP)
10) IETF RFC 2830:2000 (Extension for Transport Layer Security)
11) IETF RFC 2849:2000 (The LDAP Data Interchange Format (LDIF) - Technical Specification)
12) IETF RFC 2891:2000 (LDAP Control Extension for Server Side Sorting of Search Results)
13) IETF RFC 3062:2001 (LDAP Password Modify Extended Operation)

1-3-7 ＩＣカード

1-3-7-1 以下の規格のうちいずれかまたは両方に対応すること.
1) ISO/IEC 14443
2) ISO/IEC 7816

1-3-7-2 NIST FIPS 140-1:1994 (Security Requirements for Cryptographic Modules) に対応し, level 2 以上であること.

1-3-8 バーコード

1-3-8-1 以下のコードならびにバーコード形式に拡張対応できるシステム設計であること.
1) UCC/EAN-128

２）Code39 および Code128
３）NW-7

1-3-9 診療情報におけるアクセス制御

1-3-9-1 ENV 13606-3:1999 に準じたアクセス制御機構に準拠した，もしくは拡張可能なシステム設計であること．

2 システム・アーキテクチュア

2-1 概念構成

2-1-1 機能概要

2-1-1-1 本調達システムは，PKI（Public Key Infrastructure）に即した認証機構ならびに属性認証機構，公開鍵認証（PKC）と属性認証（AC）に基づく権限管理機構，時間認証機構，諸属性の検索抽出配信機構，諸属性の広域収集機構，諸属性の登録機構，ログ保管検索抽出閲覧機構，端末アプリケーション，およびこれらの稼動に必要なデータベース（DB），データウエアハウス（DWH）またはディレクトリサービスから構成されること．

2-1-1-2 本調達システムは，さらに，将来の診療情報交換等の機能拡張に備えて，地域における診療情報交換のフロー制御，フローログの保管検索抽出閲覧機構，ならびに必要となるミドルウエアにも対応できる設計であること．なおここでいうフロー制御とは，権限管理 DB による reflector 的な機能を逸脱しない範囲であることを条件とする．

2-1-2 外部連携

2-1-2-1 PKI による認証および属性認証機構，ならびに PKC と AC に基づく権限管理機構については，個々の医療施設における病院情報管理システム等との効率的な連携を図るべく，必要なインターフェイス仕様を定め，これを提出すること．

2-1-2-2 本調達システムは前目に則った仕様による通信にて本調達システムに求められる機能の実現を完遂すること．

2-1-2-3 諸属性の広域収集機構については，必要な XML の書式定義すなわち DTD もしくは XML Schema ならびに eXtensible Hypertext Markup Language（XHTML）の運用指針を，本調達システムへの接続仕様として定め，これを提出すること．

2-1-2-4 本調達システムは前目に則った仕様による通信にて本調達システムに求められる機能の実現を完遂すること．

2-2 前提条件

2-2-1 前提とする機器環境

2-2-1-1 本調達システムを稼動させるサーバやネットワーク機器は別途調達する．ただし，それら機器類の設定や本調達システムのインストール等の役務は，本調達に含める．

2-2-1-2 なお本年度においては前目の物品には Virtual Private Network（VPN）機器を含まない予定であることに留意すること．

2-2-2 前提とするネットワーク環境

2-2-2-1 Internet において Secure Sockets Layer（SSL）/Transport Layer Security（TLS：RFC-2246）もしくは IPsec（IP Security Protocol：RFC-2401，RFC-2411 ほか）を応用して session を暗号化して本調達システムと医療施設およびエンドユーザとの通信を確立する

こと. ただし前項の留意事情の通り.

2-2-2-2 独自のネットワークサイトを有するエンドユーザの運用指針の提出も, 本調達に含めるものとする. なおエンドユーザの端末(PC)は専用端末を想定しているが, エンドユーザのネットワーク環境は本調達システムのみならず多目的に利用されうることに留意すること.

2-2-2-3 独自のネットワークサイトを有する医療施設の運用指針の提出も本調達に含めるものとする.

2-2-3 前提とするユーザ

2-2-3-1 当面の間, 本調達システムが想定する業務ユーザは以下の通りとする:

1）本調達システムの管理者 （但し本調達システムに関わる業務を行う者のみ）
2）各施設のサイト管理者 （但し本調達システムに関わる業務を行う者のみ）
3）医療施設の医師・歯科医師（但し本調達システムに関わる業務を行う者のみ）
4）那覇市医師会 （但し本調達システムに関わる業務を行う者のみ）
5）南部歯科医師会 （但し本調達システムに関わる業務を行う者のみ）
6）那覇市消防本部 （但し本調達システムに関わる業務を行う者のみ）
7）那覇市の担当課 （但し本調達システムに関わる業務を行う者のみ）
8）県中央保健所 （但し本調達システムに関わる業務を行う者のみ）

したがって上記組織に所属していても, 本調達システムに関わる業務を行わない者には, 業務アカウントを与えない.

2-2-3-2 本調達システムが想定する一般利用者は, 全那覇市民および那覇市内に勤労する者とする.

2-2-4 前提とするエンドユーザ用業務端末

2-2-4-1 エンドユーザ用の業務端末は以下の通りとする:

1）Network port（100Mbps）を1ポート以上.
2）入力デバイスにはキーボード, マウス, 近接型 IC カードリーダを備えること.
3）Client server model の client に適し, GUI をサポートし, かつログオン・ポリシーや file permission が設定できる PC 用 OS（Windows2000 など）.
4）日本語フロントエンド・プロセッサを備えること.
5）業務アプリケーションと関連するツールやユーティリティ, ならびにこれらが頻用するマスターファイルを内蔵ハードディスクに搭載すること.
6）業務アプリケーションは自動タイムアウト時間の設定ができること.
7）アンチ・ウィルス・ソフトウエアが提供されること.
8）POP3（Post Office Protocol ver.3：RFC-1939）対応電子メールクライアント, および HTTP （Hypertext Transfer Protocol：RFC-2616）ブラウザを備えること. なお HTTP ブラウザは, https にも対応していること.

2-2-5 前提とする医療施設側サイト

2-2-5-1 医療施設側サイトは以下のうちいずれかを想定する:

D型（dependent type）
- サーバを有さず, エンドユーザ用業務端末のみ.
- 常時接続またはダイヤルアップ接続.
- パケットフィルタリング等は期待できない環境.

W型（web type）
- サーバを有して, 自施設 WWW を公開している.
- WWW 公開情報は病院情報システムと連携していない.
- 属性登録はエンドユーザ用業務端末または WWW で行う.

・パケットフィルタリング等は高機能を期待できない環境.

Ｉ型（Independent type）

・サーバを有して，自施設 WWW を公開している.

・WWW 公開情報は病院情報システムと連携している.

・属性登録は WWW または LDAP で行う.
但し他院の医療リソースを取得する場合はエンドユーザ用業務端末とする.

・他施設からの医療リソース取得要求は，自施設システムの属性情報管理機能による自動運用を行う.

・パケットフィルタリング等を期待できる環境.

2-2-5-2 本調達システムは，上記の医療施設側サイトの型のいずれにも対応できること.

2-2-6 前提とする開発環境

2-2-6-1 プラットフォームは Linux とすること.

2-2-6-2 トランスポートレイヤーでセキュアにする場合は SSL を用いること.

2-2-6-3 ディレクトリサービスには LDAP を用いること.

2-2-6-4 DBMS は SQL 対応であること.

2-2-6-5 開発言語は Java, C, C++ とすること.

2-2-6-6 WWW コンテンツの提供は Apache, PHP にて行うこと.

3 機器設定等に関する基本要件

3-1 機器と通信の保全

3-1-1 端末ならびにクライアント側

3-1-1-1 BIOS は，管理番号を振れるならば管理番号を振り，個別のパスワードを設定すること.
BIOS の版番号や MAC address ほか管理に必要な番号を記録保管すること.

3-1-1-2 OS の特性に従って，適切なパーティションを設定すること.

3-1-1-3 不要なコンポーネントやアプリケーションは，あらかじめ全て削除･もしくは･エンドユーザには使用不能とすること.

3-1-1-4 不必要な通信ポートは，原則として全て，丁寧に閉じること.

3-1-2 クライアント側とサーバ側と通信

3-1-2-1 必要の無いポートは，ネットワーク機器において，全て閉じること.

3-1-2-2 全端末は DNS（Domain Name System：RFC-1034）の順引きならびに逆引きによって認証された後にのみ，個々のサーバのサービスを享受できること.

3-1-2-3 DNS サーバには充分な DNS spoofing 対策を施し，維持においてはログのみならず finger print の照合を行うなど丁寧な維持対策を実施すること.

3-1-2-4 IP spoofing を応用した，SYN flooding，UDP flooding，ICMP flooding に対する耐性があること.

3-1-2-5 ARP spoofing に対してはルータ等における ARP time out 等の簡易な方法による spoofing 対策で可とする.

3-1-3 サーバ側

3-1-3-1 必要の無いポートは，各サーバにおいても，全て閉じること.

3-1-3-2 クライアント側のエンドユーザには，各サーバの shell を与えないこと.

3-1-3-3 サーバ側の shell account 発行は，契約業者のシステムエンジニアまたは本調達システムの関係者を問わず，システム構築段階から，本調達システム責任者の許諾に拠ること．

3-1-3-4 Root（Administrator）または同権限を有するアカウントは，remote ログインできないこと．なおログイン後の su の実行による Root 権限の取得は可とする．本目要件は，契約業者のシステムエンジニアならびにシステム管理者にも適用される．

3-1-3-5 サーバ側では，server サイトにおいても rsh，yp，NFS，X-Windows を用いず SSH（Secure Shell）を用い，NIS が必要な場合には SSH を介すること．
コンソールにおける操作のみにおいては X-Windows の使用は許可するものとする．

3-1-3-6 必要の無いサービスは，rpm または source code さえ，サーバに置かないこと．

3-1-3-7 必要の無い開発アプリケーションやライブラリは，rpm もしくは source code さえ，サーバに置かないこと．

3-2 時刻管理

3-2-1 時刻の統一

3-2-1-1 全システムは，時刻が統一されていること．
本システム内のサーバおよび端末の時刻ズレ許容範囲は 600msec 未満とする．
本システム内のタイム・サーバが認識する UTC（Coordinated Universal Time）と実際のそれとのズレ許容範囲は 400msec 未満とする．

3-2-1-2 システム時計の自動修正を実施または試行する回数は，1時間あたり 1 回を限度とする．なお特別な事由の無い限り NTP（Network Time Protocol：RFC-1305）にて時刻校正を行うこと．

4 データの扱い

4-1 オンライン参照期間

4-1-1 各種データ

4-1-1-1 各種データは少なくとも5年間は稼動ハードディスク上に保管しオンラインで即時に検索できること．

4-1-2 各種マスタ

4-1-2-1 各種マスターファイルは少なくとも7年間分の経過を稼動ハードディスクに保管し必要に応じて即時にオンライン検索できること．

4-2 バックアップ

4-2-1 バックアップおよびファイル転送の基本要件

4-2-1-1 バックアップは，通常営業日の通常営業時間内に開始して，同日の通常営業時間内に完了できること．

4-2-1-2 バックアップのためのシステム停止時間は存在しないこと．

4-2-1-3 バックアップは，本調達システム内の全トランザクションの整合が保たれるよう実施できる構成であること．

4-2-1-4 バックアップの転送保存先となる記憶媒体は，テープもしくは特定サーバの内蔵ハードディスクとすること．

4-2-1-5 バックアップサーバとは必ずしもそれ専用のサーバ・アプリケーションおよびクライアント・アプリケーション間の通信および制御によるバックアップを意味するものではないので，異なるサーバからのオンライン・バックアップではサーバ間ファイル転送は sftp または scp（自動起動ほかの script 制御を含む）による実現手法も可とする．ただし稼動中のデータベースの整合性については，これを保持すること．

4-2-1-6 ファイル形式は XML とし，S-JIS テキストファイル群であること．

4-2-2 テープバックアップの要件

4-2-2-1 診療情報サーバ，経営分析サーバおよび医事会計サーバのバックアップ対象データは，自動テープチェンジャによる自動バックアップ（追記型）が，現実的な時間内で実施完了できるバックアップ・アプリケーション構成であること．

4-2-2-2 自動スケジューリングにより，オンラインで自動一括バックアップできること．

4-2-2-3 自動テープチェンジャによる自動バックアップ（追記型）ではない場合にも，月次の一括バックアップの際にも，処理途中で手動での磁気テープ交換が発生しないハードウエア構成ならびにバックアップ・アプリケーション構成であること．

4-3 システム更新への準備

4-3-1 継続性と連続性

4-3-1-1 継続性と連続性とを確保して，社会に対する道義的な責務を全うすること．

4-3-2 必要資料の提出

4-3-2-1 本調達システムから次の更新システムへと移行する際，各種データやマスターファイルを円滑かつ完全に移行できるよう準備するために，マニュアルと共に必要な移行ファイルのリストとそれらのファイルのフォーマット等を提出すること．

4-3-2-2 上記以外に必要な情報または資料がある場，それらも併せて提供すること．これらにより，本調達システムの管理者が支障なく更新作業をできるようにすること．

4-3-2-3 更新作業に関して協力要請した場合には，誠意をもってこれに応じること．

5 諸作業等

5-1 製造体制

5-1-1-1 本調達システムで提供される業務アプリケーションの製造体制ならびに人員陣容などの組織体制を明らかにすること．

5-1-1-2 以下の体制が整っていることが望ましい：

1）プロジェクトを実施する組織は，要件管理，プロジェクト計画進捗管理，品質保証の成熟度が CMM（Capability Matured Model）のレベル２に達している．

2）プロジェクトを実施する組織は，CMM レベル２を実現するための具体的な計画が既に実施されている．

なおいずれの場合にも，これを証明する書類等も併せて提出すること．

5-1-1-3 開発体制が ISO 15408 に準拠して管理されていることが望ましい．

5-2 協議体制

5-2-1-1 営業責任者を明確にすること．

5-2-1-2 本院側への技術責任者を明確にすること．

5-2-1-3 各作業の日程は事前に提示し，担当者と協議のうえ，その指示に拠ること．

5-2-1-4 作業のために各室への立ち入る際には各部署責任者の許可を得て通常業務に支障を来たさぬよう配慮すること．
また前述した本院の技術窓口に事前報告すること．

5-2-1-5 協議内容，設置場所または作業場所，作業内容または動作確認結果，運用経過，保守内容，障害内容，障害対策内容は，それぞれ完了後5営業日以内に，(1)電子メールに添付ファイル，および(2)書面によって報告し，承認を得ること．

5-3 導入作業全般

5-3-1-1 導入作業は全て，落札者が行うこと．また全ての導入システムを既設ネットワークに接続し，全体として技術要件を満たした状態で引き渡すこと．

5-3-1-2 本調達システムの導入にかかる人員体制，作業日程，稼働スケジュールを提案し，予定担当要員一覧等の組織体制を明示すること．

5-3-1-3 導入に際しては業務に支障のないよう計画的に行うこと．加えて，施設設備等に損傷を与えないよう十分な注意をするとともに，受注者が必ず立ち会うこと．

5-3-1-4 納入される機器に必要な一次側設備については用意するので設置条件に関する資料を提出すること．それ以外に必要となる二次側設備に関する部材ならびに施工作業は，本調達に含まれるものとする．

5-3-1-5 本調達物品の搬入，据付，配線，調整，ネットワーク設定ならびに接続機器への接続，調整，ソフトウエアのインストール，動作確認は，本調達に含むものとする．
なおLAN担当者と綿密な打ち合わせを行ったうえで，これを実施すること．

5-3-1-6 ネットワークの配線等の施工作業に際しては，コンセントから端末機器までの配線をタグ付けすること．また通行に支障がないように配線すること．

5-4 ソフトウエア導入調整

5-4-1-1 サーバ毎および端末毎の基本ソフトウエア(OS および基本ユーティリティ)ならびに業務アプリケーションをインストールし，動作確認を行うこと．

5-4-1-2 端末については，セキュリティ保持に必要なBIOS設定，デバイス設定を行うこと．

5-4-1-3 設定および登録データの詳細内容を，書面および電子媒体で提出すること．

5-5 ネットワーク接続調整

5-5-1-1 既設ネットワークとの接続調整作業ならびに通信障害の切り分け確認作業も，本調達に含まれること．

5-5-1-2 既設ネットワークの設定変更に必要な技術情報の提供および作業への協力を行うこと．

5-5-1-3 集線装置と接続機器装置との間は，UTP(カテゴリー5)を用いて接続すること．
なお指示に拠って色分けしたケーブルを用い，配線にはタグ付けすること．また通行に支障がないように配線すること．

5-5-1-4 本システムと接続を行った既存各装置との通信テストを含む動作確認を行うこと．

5-6 ユーザ教育

5-6-1-1 利用者への各システムの講習を行うこと．

5-6-1-2 十二分なエンドユーザ用操作説明書と資料とを提供すること．

5-6-1-3 エンドユーザ用の操作説明書はオンライン参照できること．
なおHTML形式またはPDF形式ファイルは，いずれの場合においても，hyper link機能やアウトライン機能（栞やカスケーディングを含む）を活用すること．

5-7 障害対応

5-7-1 復旧体制

5-7-1-1 障害発生時には，遠隔操作にて復旧できる場合には，これを実施すること．
この際，下記の事項も併せて遂行すること．
１）本調達システム担当者への通知は，必ず事前に行うこと．
２）本調達システム担当者との協議が可能な場合には協議のうえ承認を得ること．
３）全てのオペレーションログを記録し，事後に報告資料として提出すること．

5-7-2 事後処理

5-7-2-1 障害発生時には，取得保管するログを過去に遡って解析し，明確に切り分けを行うこと．

5-7-2-2 既存システムと本調達システムとの障害切り分けが困難な事象については，原因究明に協力すること．

5-7-2-3 頻度の多い障害事象については，その予防および改善方法に関する協議に応じること．

5-7-2-4 復旧後5営業日以内に障害対応報告書を本院に提出し，その承認を得ること．

6 法令対応

6-1 日本国における使用

6-1-1-1 本調達システムは日本国における使用を前提としている．よって，日本国における医療制度ならびに医療制度等を規定する各種法令条例に則した機能を有すること．

6-2 那覇市における使用

6-2-1-1 本調達システムは沖縄県那覇市における使用を前提としている．よって沖縄県那覇市における特例もしくは特令制度，沖縄県もしくは那覇市の条例に則した機能を有すること．

7 提出ドキュメント

7-1-1 一般事項

7-1-1-1 納入期限までに，本節に示すドキュメントを提出すること．

7-1-1-2 提出されるドキュメントは，日本語で提供すること．ただし英語版しかない場合には，英語版のみでも可とする．

7-1-1-3 提出されるドキュメントには，リリース日付も付する（記載または入力）こと．

7-1-1-4 提出されるドキュメントは XML document ファイルと当該ファイルの DTD，および必要な場合には XSL を，各々２部提出すること．
なお表は .XLS，.CSV，図は .PDF，.PPT または .VSD 形式，通常文書は .DOC 形式でも可とする．
ただし応札者以外の者が製造販売する製品を導入する際には，この限りではない．

7-1-1-5 前項を基にしたオンライン操作マニュアルを提供すること．

7-1-2 構成図表

7-1-2-1 ハードウエアの構成図および構成表を提出すること．

なおラックマウント構成やクラスタ構成についてはその状況が理解できる図とし，さらに配線状況も併せて示すこと．

7-1-2-2 ネットワークの構成図および構成表を提出すること．
なお配線状況図に加え，これを基にしたサービスポートのトンネリング状況図も添付すること．

7-1-2-3 ソフトウエアの構成図および構成表を提出すること．
ソフトウエア構成図の作成視点は以下の２種類とし，それぞれ別図表とすること．
１）サーバ，端末等の機器ごとのサブシステムやモジュール等の構成
２）サブシステムごとのモジュール構成および関連するデータベース
なお通信される data entity も提供すること．

7-1-2-4 データベースの構成概要図および構成表を提出すること．
また database schema も提供すること．

7-1-3 基本ソフト等

7-1-3-1 サーバサイトならびに部門サイトにおける業務アプリケーションの各マニュアルを，各2部づつ提出すること．
１）業務運用マニュアル （操作，設定，監視等）
２）バックアップマニュアル
３）障害切り分けマニュアル
各マニュアルには，本調達システム業務担当者が操作して業務を行うべき諸手順，および頻用するコマンドに関する若干の解説，確認すべき値とその項目名が記載されていること．

7-1-3-2 業務アプリケーションの各マニュアルを，各2部づつ提出すること．
１）簡易マニュアル （A4 判 2 枚程度）
２）業務運用マニュアル （操作，設定等）
３）障害切り分けマニュアル
各マニュアルには，本調達システム業務担当者が操作して業務を行うべき諸手順，および頻用するコマンドに関する若干の解説，確認すべき値とその項目名が記載されていること．

7-1-3-3 全てのソースコードが提供されることが望ましい．