病院情報システム　共通仕様書

1	サーバ、クライアント、周辺機器については、導入後7年間の修理部品がメーカから供給される機器を導入すること。
2	サーバは南棟6Fサーバルームに設置すること。
3	病院指定のウィルス対策ソフトをサーバ及びクライアントへインストールすること。ライセンスについては、病院側で調達するものとする。なお、インストールする前に病院書式の「ウィルス対策ソフト検索除外設定ヒアリングシート」を施設用度課システム担当へ提出し、許可を得ること。
4	病院指定のタイムサーバへ接続し、時刻同期を行うこと。サーバ及びクライアントの起動時に必ず時刻同期を行えるように起動ファイル等の設定すること。
5	病院指定の外部接続機器制限ソフト(PortShutter)を各クライアントへインストールし、病院から指定される設定項目で設定すること。
6	USB経由の外部機器接続は原則禁止とする。但し、業務上最低限必要なものについては、病院書式の「USB接続ヒアリングシート」を施設用度課システム担当へ提出し、許可を得ること。
7	CD/DVDドライブについて、書き込みを禁止すること。なお、設定ソフトは、病院指定の外部接続機器制限ソフト(PortShutter)を利用すること。
8	クライアントのアクセス権限については、管理者権限とユーザ権限を設定すること。一般利用者は原則ユーザ権限で業務を行うものとする。但し、一般利用者が業務上やむなく管理者権限で利用しなくてはならない場合は、施設用度課システム担当と協議し、許可を得ること。
9	サーバ機については、最新の機種を導入すること。また、購入前に機種仕様を施設用度課システム担当へ提出し、許可を得ること。
10	サーバ機のOSは、最新バージョンを導入すること。システム動作保証等の理由により、旧バージョンを導入する場合は、事前に施設用度課システム担当の許可を得ること。
11	サーバ機は、セキュリティ対策として、チーミング等による冗長化設定をすること。そのため、サーバ機のネットワークアダプタは必ず2ポート以上を搭載すること。
12	サーバ障害時のデータ復旧に対応するため、バックアップ装置を導入すること。なお、バックアップ装置に外部記録媒体(LTO等)を使用するときは、外部保管に対応するため、定期的にテープ交換する運用を構築すること。但し、外部保管に関する費用は病院の経費とする。
13	UPSの自動シャットダウンが始まるまでの待機時間については、理論値を算出し、原則、最低10分以上もしくはランタイム重視制御等を設定すること。なお、理論値及び設定値については、事前に病院書式の「UPS設定シート」を施設用度課システム担当へ提出し、承認を得ること。
14	OAソフト製品のライセンスについては、必要最低限の数量を購入対象とし、ガバメントオープンライセンスで購入すること。但し、事情により、ガバメントオープンライセンスでの購入が不可の場合には、施設用度課システム担当と協議し、最も安価の方法で購入をすること。
15	電子カルテシステムを含み、連携が必要な全ての情報システムと連携すること。連携するシステムが存在する場合には、事前に施設用度課システム担当へ説明し、承認を得ること。
16	サーバ室に設置する機器は、すべてラックマウント型とする。
17	サーバ室に設置する機器は全て施錠しない状態で設置する。
18	サーバ間のネットワーク機器及びLAN配線は受託者が準備すること。

19	基幹ネットワークからサーバラックまでのＬAN配線については病院側で準備するため、サーバ機器設置の3か月前までに、チーミング等による冗長化分を含み、必要なＬAN配線の本数を施設用度課システム担当へ連絡すること。
20	サーバ等の電源については病院側で準備するため、契約後、早急に必要容量を施設用度課システム担当へ連絡すること。
21	病院資産のリモート保守用VPN回線を使用する場合は、事前に施設用度課システム担当と協議すること。なお、導入業者で独自に回線を用意する場合には、施設用度課システム担当へセキュリティ仕様を提出し、承認を得ること。
22	サーバ及びクライアント等機器は、一意的に識別可能なIDを付与し、テプラ等で本体に貼付けを行うこと。また、サーバ機については、故障時の保守連絡先もテプラ等で本体に貼り付けを行うこと。
23	サーバ及びクライアント等機器の一覧表を作成すること。なお、一覧表は、病院指定の「システム別機器台帳」に記入し、施設用度課システム担当へ提出すること。
24	当院では、全てのサーバの運用監視を行っているため、当院に常駐するオペレータに運用監視するべき事項や緊急時の連絡先等を必ず引き継ぐこと。
25	契約してから本稼働までの作業工程表を提出すること。機器設置、データ移行等を含む。
26	サーバ保全の観点より、原則、サーバ再起動を週一回程度を自動的に実施すること。但し、実施困難な場合は、甲と協議し、承認を得ること。
27	ハードウェア・ソフトウェア・ネットワーク等の全体構成図を提出すること。
28	セキュリティ設定を十分に行うこと。（大阪府立病院機構_調査報告書_2023.3.28_P.57）
29	強固なパスワードの設定を行うこと。（大阪府立病院機構_調査報告書_2023.3.28_P.57）
30	ロックアウトの設定を行うこと。（大阪府立病院機構_調査報告書_2023.3.28_P.57）
31	管理者権限をもつものを最小限にすること。（大阪府立病院機構_調査報告書 2023.3.28 P.57）
32	サプライチェーンも含めた（外部接続）監視、監督を行うこと。（大阪府立病院機構_調査報告書_2023.3.28_P.57）
33	安全なリモート接続の設定、監査を行うこと。（大阪府立病院機構_調査報告書 2023.3.28 P.57）
34	OS、アプリケーションのバージョン管理を行うこと。（大阪府立病院機構_調査報告書 2023.3.28 P.57）
35	政府機関（省庁、NISC）、JPCERTコーディネーションセンター、IPAが注意喚起したセキュリティリスクに対応すること。（大阪府立病院機構_調査報告書_2023.3.28_P.58）
36	国内ISAC、セキュリティ関連団体が注意喚起したセキュリティリスクに対応すること。（大阪府立病院機構_調査報告書_2023.3.28_P.58）
37	OS、アプリケーションソフトのバージョンアップ情報に対応すること。（大阪府立病院機構_調査報告書_2023.3.28_P.58）
38	インシデント発生時のベンダーの協力体制を明示すること。（大阪府立病院機構_調査報告書_2023.3.28_P.58）
39	
40	