部門システム等導入時の共通要求仕様

基本原則：医療情報システムの安全管理に関するガイドラインの最低限のガイドラインを準拠できるようシステムを構築すること。
運用で対応が必要な項目については、システムの利用者に説明すること。

項目	内容	備考
装置の取り付け等	ネットワークシステムの取り付けを行う場合は、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切な固定等必要な措置を施すこと	サーバ室に場所の確保ができない場合、別途ラックが必要（設置工事）
サーバ及びUPSの設置	サーバ及びUPS（無停電電源装置）はラックマウントタイプとすること	※設置に際し、情報管理係の指示に従うこと
電源	電源喪失時にサーバーが停止しないよう予備電源に切り替わるまで（5分）の電力をUPS等で確保すること。また、UPSを導入する場合にはバッテリの劣化等をアラームおよびランプで警告する機能を有すること	AC100V・単相AC200V・コンセント形状を考慮すること。電源の主幹を停止する場合システム停止が必要となる
配線	配線は傍受又は損傷を受けることがないように可能な限り措置を施すこと 主要な箇所の配線については、損傷などについて定期的な点検を行うこと ネットワーク接続口（ハブ、ルータのポート等）は他の者が容易に発見できない場所に設置すること	
端末	盗難防止措置、情報資産の漏洩を防止する処置を施すこと	
納品物	導入した機器構成リスト、部門側ネットワーク概要図を、保守連絡体制図を情報管理係に提出すること	
廃棄物	廃棄する物品の処分について、一切の責任を持って処理すること	※個人情報保護の観点から、一切のデータを消去すること
基幹システムやモダリティとのインターフェース	インターフェースの新規作成、変更を考慮すること	※上位連携に必要な一切の費用を含むこと
連絡体制	診察に関わるシステムは夜間、休日等の時間帯でも連絡がとれる体制を有すること	
ライセンス	WindowsのデバイスCALやウィルス対策のライセンスを必要に応じて準備すること	
システム監視	診察に関わるシステムはシステムの監視を実施すること	必ず操作ログがのこる仕様を構築すること
リモートメンテナンス	セキュアなリモートメンテナンス環境を必要に応じて構築すること	※申し出ていただければ、部門ベンダ共通リモート環境も提供可能
リカバリ対策（バックアップ）	障害時のリカバリ手段を用意しておくこと 障害直前の状態までリカバリできること サイバー攻撃に対応するバックアップ環境を構築すること	※導入時における「医療情報システムの安全管理に関するガイドライン」に準拠
定期再起動時間の調整	システム連携等の調整が必要な為、情報システム担当者の指示に従うこと （導入時とメンテナンス時に院内周知が必要な為）	
ブラウザ設定	電子カルテシステムが現在使用しているブラウザを利用すること（電子カルテシステム相乗り想定） 電子カルテシステムに発生する費用も含むこと	設定変更が発生します
端末設定等	電子カルテシステムを含む基幹システム更新時にはそのシステムのルールに対応すること	※原則保守の範囲で実施すること ※別途、費用が発生する場合は、施設用度係に相談すること

部門システム等導入時の共通要求仕様

基本原則：医療情報システムの安全管理に関するガイドラインの最低限のガイドラインを準拠できるようシステムを構築すること。
運用で対応が必要な項目については、システムの利用者に説明すること。

項目	内容	備考
個人情報保護	システム上のデータを利用者が、容易に匿名化できる機能を有すること	
ネットワーク①	証明書形式X509に対応すること 公開鍵暗号方式：RSA相当、DSAをサポートしていること 鍵長：RSA（2048bits、4096bits、8192bits）をサポートしていること ダイジェストアルゴリズム：SHA1、SHA256、SHA384、SHA512をサポートしていること	証明書を提供しますので導入ください
ネットワーク②	部門システム毎にVLANを設定し、IPアドレスを払い出しているので、該当のIPアドレスを管理すること	※事前に情報管理係に相談すること
ネットワーク③	ネットワークの新設、増設等がある場合はその費用を見込むこと	※事前に情報管理係に相談すること
セキュリティ対策①	ウイルス対策ソフトを導入すること ・個別ファイルをスキャンする都度スキャンが可能であること。 ・各機器へのウイルス定義ファイルの配布状況管理機能を有すること。 ・ウイルス感染・検疫・駆除の一元監視機能を有すること。 ・端末においてウイルスを検知した場合は駆除されること。駆除できない場合には削除を実施するといったウイルス検知方式が可能であること。また検知時のアクションとしてシステム管理者に対する通報とユーザーに対する通知が可能であること。 ・パターンファイルを最新に保つこと	「TRENDMICRO　ApexOne」を提供するので導入してください。 ※デフォルト設定で動作に支障がある場合にはドメインごとにセキュリティレベルを調整できますのでご相談ください ※システムの都合上、病院側で提供しているウイルス対策ソフトを導入できない場合は、部門システム側で対策ソフトを準備し、常に最新に保つこと
セキュリティ対策②	可能な限り導入時点で、最新のOSセキュリティパッチを適用すること	※導入時における「医療情報システムの安全管理に関するガイドライン」に準拠
セキュリティ対策③	病院外との接続がある場合、必ずファイヤーウォール等のセキュリティ対策を講じること ファイアウォールを利用する場合、接続先とプロトコルを限定し、接続先のセキュリティを担保すること	情報システム担当部署に必ず、申し出て承認を得ること ※導入時における「医療情報システムの安全管理に関するガイドライン」に準拠
セキュリティ対策④	原則、USB可搬媒体が利用できない仕組みを有すること	※運用上どうしてもUSB可搬媒体を使用しなければならない場合は、決められた可搬媒体しか運用できないような仕組みを構築すること
セキュリティ対策⑤	端末のローカルドライブが直接開かない仕組みを有すること	
セキュリティ対策⑥	電子カルテシステムと同様に、時刻同期をおこなうこと	NTPサーバを用意しているのでNTPサーバから時刻取得すること
セキュリティ対策⑦	サーバー、クライアントの廃棄時には情報管理係指定の場所でハードディスクを破壊し、廃棄証明を提出すること	
セキュリティ対策⑧	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」の最新版に基づき、利用者認証において二要素認証を採用すること。	※導入時における「医療情報システムの安全管理に関するガイドライン」に準拠

部門システム等導入時の共通要求仕様

基本原則：医療情報システムの安全管理に関するガイドラインの最低限のガイドラインを準拠できるようシステムを構築すること。
運用で対応が必要な項目については、システムの利用者に説明すること。

項目	内容	備考
セキュリティ対策⑨	システムを構成するソフトウェア（OS、ミドルウェア、オープンソースソフトウェア、各種ライブラリ等）のソフトウェア部品表（SBOM）を、納品時に電子データ等で提供すること。 また、将来的なシステムのバージョンアップや構成変更等により、構成部品に変更が生じた場合は、速やかに最新のSBOMを再提出すること。なお、SBOMの記述形式は、脆弱性情報の自動照合・管理が可能な標準的なフォーマット（SPDX、CycloneDXなど）またはそれに準じた可読性の高い形式とすること。	※導入時における「医療情報システムの安全管理に関するガイドライン」におけるサプライチェーンリスク管理（SBOM等の提示要求）の規定に準拠すること。
セキュリティ対策⑩	本システムに係る「製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）」（厚生労働省標準規格 HS040等に準拠したもの）を、導入時に提出すること。 また、導入後において、システムのメジャーバージョンアップ、重要な仕様変更、または契約更新等が発生した場合は、最新のシステム仕様を反映したMDS/SDSを再作成し、速やかに再提出すること。	※導入時における「医療情報システムの安全管理に関するガイドライン」に基づき、事業者のセキュリティ機能の適合性を確認・評価するために利用します。