

非機能要件一覧表

| | |
|--|------|
| | 必須項目 |
| | 推奨項目 |

| | 大項目 | 中項目 | 小項目 | 要件 | 区分 |
|-------------------------------------|--------------------|-----------------|-----------------|---|----|
| 非機能要件 | (1) 規模要件 | - | - | 基本仕様書に記載の端末数に必要なシステムリソースを確保すること。 | 必須 |
| | (2) 性能要件 | レスポンス時間 (画面) | - | 通常時要件：3秒 ※通信環境による遅延を考慮しない前提で利用者が一般的な入力・検索・参照画面などの閲覧等の操作を行った場合 ※検索条件及びデータ量によってはこの限りではない | 必須 |
| | | - | - | 貸出・返却時のバーコード読み取り時のデータ応答：1秒以内 | 必須 |
| | (3) 拡張性 | - | - | 学校図書管理システムなど将来的に他のシステムとの連携について提案すること。 ※本項に係る提案はオプション扱いとする。 | 必須 |
| | (4) OSバージョンアップ対応 | - | - | 端末のOSのサポート期限に合わせて、パッケージ標準としてバージョンアップすること。特にWindowsのサポート期限に注意し、サポート期限の2か月前までにバージョンアップ対応されること。 ただし、Windows O Sの大規模更新など、変更が大きい場合は、別途協議するものとする。 | 必須 |
| | (5) 信頼性要件 | ①可用性 | ア) 稼働時間 (通常) | システムの稼働時間は、開館時間内とし、土・日・祝日の運用も可能とすること。利用可能時間の延長が可能な場合は、その内容を明記すること。 | 必須 |
| | | | イ) 稼働率 | システムの稼働率は、99%以上とする。なおシステムメンテナンス等の計画停止は除く。 | 必須 |
| | | ②保守性 | ア) バックアップ | 5日間以上のデータのバックアップを行うことができること。 | 必須 |
| | | | | | |
| 情報セキュリティ対策・データセンター要件・ネットワークセキュリティ要件 | (1) 情報セキュリティ対策 | ①脆弱性対策 | ア) セキュリティの維持管理 | 適切な権限設定、不要なサービスの停止、最新のセキュリティパッチの適用等の脆弱性を排除し、セキュリティの維持管理が行えること。 | 必須 |
| | | | イ) 脆弱性への対処 | システム及びOS等の脆弱性が発覚した場合は、速やかに報告し、バージョンアップ等の必要な作業を実施すること。 | 必須 |
| | | ②個人情報・機密情報保護 | - | システムで作成する文書の中には個人情報や機密情報も含まれるため、本番運用時や保守作業時、開発・テスト作業時等のあらゆる場面において、個人情報・機密情報保護の観点からセキュリティ対策を講じること。 作業時の人的ミスを防ぐことから、個人情報保護に関して社員に対する独自の研修等を実施していること。 | 必須 |
| | | | - | 職員が使用する業務端末に接続される外部デバイス（USBメモリ、外付けハードディスク等）の利用を制限できること。 | 必須 |
| | | | - | 管理者権限にて業務用端末にログインした場合にのみデバイス制限を解除できること。 | 必須 |
| | | ③マルウェア対策 | - | 各端末において専用ソフト等を用いて必要なセキュリティ対策を講じること。また、パターンファイルの更新を随時実施すること。 | 必須 |
| | | ④ユーザ等管理 | - | システム利用時のユーザ IDは本システムにて管理すること。 | 必須 |
| | | | - | IDとパスワードによる利用認証を行うこと（利用権限の付与）。OSレベル（業務端末ログイン時）とシステムレベル（新システム起動時）の二重パスワード認証を必要とすること。 | 必須 |
| | | | - | 職員のデバイス制限（USBメモリ、外付けハードディスク等データを外部持ち出し可能な装置の使用制限等）をすることで、外部媒体による個人情報の持ち出しを制限すること。なお、管理者パスワードでログインした場合にのみデバイス制限を解除すること。 | 必須 |
| | | | - | 各機器が盗難にあっても、部外者が業務システムのデータを閲覧したり抽出することができないこと。 | 必須 |
| | | | - | 使用するソフトウェアについて修正パッチ（プログラムの一部分を更新してバグの修正や機能変更を行うためのデータ）等がリリースされた場合、セキュリティ面、業務システム面において問題がある場合は、遺漏なく速やかにパッチをあて、セキュリティホールを放置しないこと。 | 必須 |
| | | | - | 個人情報の暗号化やネットワーク上のセキュリティなど、個人情報の不正引き出しへの対策がなされていること。 | 必須 |
| | (2) ネットワークセキュリティ要件 | | - | インターネット接続に関してWebフィルタリング等を導入して接続先等の制限を行うこと。 | 必須 |