

■別紙3_非機能要件一覧

| 項番 | 大項目 | 中項目 | メトリクス (指標) | 要求目標等 | 補足説明等 |
|----------|--------|-----------------------------------|---|---|---|
| A.1.3.1 | 可用性 | 継続性 | RPO(目標復旧地点) ※(業務停止時) | 平常時、業務停止を伴う障害が発生した際には、障害発生時点(日次バックアップ+アーカイブ※からの復旧)までのデータ復旧を目標とすること。 | RPO:業務停止を伴う障害が発生した際、バックアップしたデータなどから情報システムをどの時点まで復旧するかを定める目標値。 |
| A.1.3.2 | | | RT0(目標復旧時間) ※(業務停止時) | 平常時、業務停止を伴う障害が発生した際には、1営業日以内でのシステム復旧を目標とすること。 | RT0:業務停止を伴う障害(主にハードウェア・ソフトウェア故障)が発生した際、復旧するまでに要する目標時間。 |
| A.1.3.3 | | | RLO(目標復旧レベル) ※(業務停止時) | 平常時、業務停止を伴う障害が発生した際には、一部システム機能の復旧を実施すること。 | RLO:業務停止を伴う障害が発生した際、どこまで復旧するかのレベル(特定システム機能・すべてのシステム機能)の目標値。 |
| A.1.4.1 | | | システム再開目標(大規模災害) | 大規模災害時、情報システムに基大な被害が生じた場合、情報システムは、一ヶ月以内に再開することを目標とすること。 | |
| A.1.5.1 | | | 稼働率 | 年間のシステム稼働率は、99.5%を目標とすること。 | |
| A.3.2.1 | | | 災害対策 | 保管場所分散度 | 遠隔地へのデータ保管は、ベンダーによる提案事項とすること。 |
| A.3.2.2 | 保管方法 | 大規模災害時のデータ保管方法は、ベンダーによる提案事項とすること。 | | | |
| B.1.1.1 | 性能・拡張性 | 業務処理量 | ユーザ数 | 情報システムの利用者は、不特定多数のユーザが利用できること。 | |
| B.1.1.2 | | | 同時アクセス数 | 情報システムの同時アクセス数は、不特定多数のアクセス※有りとする。(100人程度)。 | 同時アクセス数:ある時点で情報システムにアクセスしているユーザ数のこと。パッケージソフトやモデルウェアのライセンス価格に影響することがある。 |
| B.1.1.3 | | | データ量(項目・件数) | 情報システムのデータ量は、ベンダーによる提案事項とすること。 | 利用期間中に想定される申請手続の数や添付データの内容・種類等を勘案し、必要と想定されるデータ量を見込むこと。 |
| B.2.1.4 | | | 性能目標値 | 通常業務時のオンラインレスポンスタイムは、ベンダーによる提案事項とすること。 | オンラインレスポンスタイム:オンラインシステム利用時に要求されるレスポンス。システム化する対象業務の特性を踏まえ、どの程度のレスポンスが必要かについて確認する。アクセスが集中するタイミングの特性や、障害時の運用を考慮し、通常時・アクセス集中時・縮退運転時ごとにレスポンスタイムを決める。 |
| B.2.1.5 | | | アクセス集中時のオンラインレスポンスタイム | 業務繁忙等によるアクセス集中時のオンラインレスポンスタイムは、ベンダーによる提案事項とすること。 | |
| E.1.1.1 | セキュリティ | 前提条件・制約条件 | 遵守すべき規程、ルール、法令、ガイドライン等は、有りとする。(個人情報保護法、資金決済法) | | |
| E.5.2.1 | | アクセス・利用制限 | システム上の対策における操作制限 | 情報システムへの操作制限は、必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可すること。 | |
| E.6.1.1 | | データの秘匿 | 伝送データの暗号化の有無 | 伝送データについては、重要情報を暗号化すること。 | |
| E.6.1.2 | | | 蓄積データの暗号化の有無 | 蓄積データの暗号化については、ベンダーによる提案事項とすること。 | |
| E.7.1.1 | | 不正追跡・監視 | ログの取得 | ログの取得については必要なログを取得すること。 | |
| E.10.1.1 | | Web対策 | セキュアコーディング、Webサーバの設定等による対策の強化 | セキュアコーディング、Webサーバの設定等は、対策の強化をすること。 | Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。Webシステムが攻撃される事例が増加しており、Webシステムを構築する際には、セキュアコーディング、Webサーバの設定等による対策の実施を検討する必要がある。 |
| E.10.1.2 | | | WAFの導入の有無 | WAFの導入は、有りとする。 | Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。WAF※とは、Web Application Firewallのことである。 |

※本資料は、地方共同法人地方公共団体情報システム機構がホームページで公開している「非機能要求グレード活用シート(地方公共団体版)業務・情報システム分類グループ②」を用いて、必要箇所を抽出し作成。(https://www.j-lis.go.jp/rdd/chyousakenkyuu/cms_92978324-2.html)
 ※「項番」は、当該シートの内容記載しており、再附番は行っていない。