

仕様書：別表第2

No	大項目	中項目	小項目	機能詳細
1	運用・保守性	保守運用	OS等パッチ適用タイミング	緊急性の高いパッチは速やかに適用し、それ以外は定期保守時に適用を行うこと。
2	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	システムのライフサイクル全体を通じて、姫路市情報セキュリティポリシー及び姫路ライフ・スマート都市推進コンソーシアム情報セキュリティポリシーを遵守すること。
3	セキュリティ	セキュリティリスク管理	ウイルス定義ファイル適用タイミング	ウイルス定義ファイルの適用は、定義ファイルリリース時に実施すること。 IaaS/PaaS等のクラウドサービスを利用する際は、上記に準じたマルウェア対策を常時実施する設定とすること。
4	セキュリティ	アクセス・利用制限	システム上の対策における操作制限	認証された利用者・管理者に対して、必要最小限の機能（プログラム・コマンド）の実行、データへのアクセスのみ許可すること。
5	セキュリティ	データの秘匿	伝送データの暗号化の有無	すべての伝送データを暗号化すること。 暗号化においては、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」の「電子政府推奨暗号リスト」記載の暗号技術を必須とする。
6	セキュリティ	データの秘匿	蓄積データの暗号化の有無	すべての蓄積データを暗号化すること。 暗号化においては、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」の「電子政府推奨暗号リスト」記載の暗号技術を必須とする。
7	セキュリティ	不正追跡・監視	ログの取得	不正アクセス等の情報セキュリティインシデントの追跡・監視のために必要なログを取得すること。
8	セキュリティ	不正追跡・監視	不正監視対象（装置）	不正アクセス等の情報セキュリティインシデントの発生又は発生の兆候を検知するために、重要度が高い資産を扱う範囲において、サーバ、ストレージ、ネットワーク機器等の監視を行うこと。
9	セキュリティ	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サーバの適切な設定等により、Webアプリケーション特有の脅威・脆弱性への対策を強化すること。
10	セキュリティ	Web対策	WAFの導入の有無	WAF（Web Application Firewall）が導入されていること。
11	セキュリティ	Web対策	Webサイト・Webアプリケーション構築等における遵守事項	WebサイトやWebアプリケーションの構築・改修にあたっては、IPA（情報処理推進機構）が公開する「安全なウェブサイトの作り方」最新版及び別冊「安全なSQLの呼び出し方」を遵守すること。
12	セキュリティ	セキュリティ診断	Webアプリケーション診断実施の有無	IPAが公開する「ウェブ健康診断仕様」に基づき、Webアプリケーション診断を実施すること。実施頻度は、運用開始前・改修時を含め、年1回以上とする。
13	可用性	継続性	RPO（目標復旧地点）（業務停止時）	平常時、障害が発生した際には、1営業日前の時点への復旧（日次バックアップからの復旧）を実施すること。
14	可用性	継続性	RTO（目標復旧時間）（業務停止時）	平常時、障害が発生した際には、12時間以内の復旧を目標とすること。
15	可用性	継続性	RLO（目標復旧レベル）（業務停止時）	平常時、障害が発生した際には、全システム機能の復旧を実施すること。
16	可用性	継続性	稼働率	稼働率は、99.5%以上とすること。
17	性能・拡張性	性能目標値	通常時オンラインレスポンスタイム	通常時の画面遷移時間は、3秒以内を目標とすること。
18	性能・拡張性	性能目標値	アクセス集中時のオンラインレスポンスタイム	アクセス集中時の画面遷移時間は、5秒以内を目標とすること。
19	運用・保守性	通常運用	運用時間	システムの運用時間は、24時間365日とする。
20	運用・保守性	通常運用	バックアップ取得間隔	すべてのデータに対して日次で差分バックアップ、週次でフルバックアップを行い、4世代まで保持すること。
21	運用・保守性	通常運用	監視情報	サービスの正常性を確認するために必要な項目（Webアプリケーションの稼働状況、各種リソースの逼迫状況等）について監視を行うこと。
22	運用・保守性	障害時運用	障害等発生時の対応	有事に際し、市・利用者へ告知するレスポンスタイム及び障害の影響度に応じた対応レベルをあらかじめ定義の上、市と合意すること。
23	運用・保守性	その他の運用管理方針	インシデント管理の実施有無	システムで発生する情報セキュリティインシデントの管理について、受託者のインシデント管理のプロセスに従い適切に実施すること。
24	運用・保守性	その他の運用管理方針	データの消去	システムの利用終了時には、業務で取り扱うすべての情報（ログ情報を含む）を、適切に消去又は廃棄すること。 また、下記の内容が確認できるデータ消去に関する証跡文書を本市に提出すること。 ・消去した情報 ・データ消去作業の実施日 ・消去作業を実施した担当者の氏名又は部署名 ・その他、消去作業を実施したことが確認できる情報