非機能要件一覧

項番	分類	要件
1	セキュリティ	サービスを利用する環境は利用者ごとに管理され、システムの誤操作や不具合等により、他利用者の情報にアクセスできないこと
2		システム利用者との通信は全て暗号化されていること
3		データベースバックアップは暗号化すること。また定期的に取得すること。
4		情報セキュリティ監査チームが組織されていること
5		システムベンダーがISO27001に基づいた情報セキュリティマネジメントシステムを構築・運用していること
6		情報セキュリティ基準に適合したセキュリティマネジメントシステムを構築していること
7		システムが利用するデータセンターは、ISO27001などの基準に基づいた外部監査を年に１回以上受けていること
8		クラウド利用の場合は、ISMAP、ISMAP-LIUの認証を取得、またはそれに相当するセキュリティ管理を行っていることを証明する資料等を提出すること
9		クラウド利用の場合は、ＳＯＣ２監査等の外部機関からの検証・評価を受けていること
10		システムが利用するデータセンターは２４時間の現場警備員の配備、侵入検知警報システム等を有すること
11		サービスの利用を終了する場合は、システム上から復元できない形でデータを完全に削除すること
12	アクセス制御	システム利用者の接続元をＩＰアドレス等で制限できること
13		システム利用者はSAML等によりシングルサインオンで認証できるこ
14		システム管理者が、指定するＩＤや時間等で運用保守を行える仕組みを有すること
15		システムへの侵入検知や侵入防止の仕組みを有し、24時間、365日の監視を行うこと
16		脆弱性テストを継続して行うこと
17		県で脆弱性テストを行う場合は、協力すること
18		セキュリティインシデントの発生に備え、システム運用におけるすべてのシステムログが保存されていること
19	信頼性	システムベンダーは製品ロードマップを公開し、ロードマップに沿った機能開発とリリースを行うこと
20		機能リリース前に品質保証テストを実施すること
21		システムの稼働率を９９％以上を目標とすること
22		稼働実績として、１万人以上の利用者、１０社以上の導入実績を有すること
23	拡張性	他システムとデータ連携できるＡＰＩやＷｅｂサービスを提供する
24	運用	システム管理者は、システムのパフォーマンス／応答時間を確認できること
25		アクセスが集中した場合も、安定してシステムを利用できること
26		システムでの動画コンテンツを視聴する場合に、安定して利用者へ配信が行えること
27		リソース監視を行い、リソース稼働率が８０％以上になった場合は、当該リソースの増強を行うこと

28		システムベンダーは事業継続性計画（ＢＣＰ）と障害復旧計画（ＤＲＰ）を策定し、随時再検証を行うこと
29		障害発生時等の迅速な復旧に対応するためのバックアップ構成とす
30	サポート	Ｗｅｂやメール、電話等でのサポートを提供すること
31		バージョンアップやセキュリティ・パッチ適用等担当者へ通知され
32		緊急時は 4 時間以内、緊急時以外では 1 日以内での初期対応をＳＬＡで保証すること
33		セキュリティ等緊急時対応として24時間、365日のサポートを行うこ
34		日本語によるサポートを行うこと