別紙2「セキュリティ要件等一覧」

No	区分	内容
1	セキュリティ全般に関する事項	日本の法令の範囲内で運用できるサービスであること。また、日本国内の裁判所を合意管轄裁判所とすること。
2		個人情報や住民の生命・財産に関わる情報、その他、非公開情報のデータが保存されるデータセンターは日本国内にあること。
3		当該外部サービスの終了の際は6か月前までに、変更の際は2週間前までに文書、電子メール等の方法で事前に告知すること。※基本機能に影響のない軽微な仕様・デザイン等の変更は除く
4		外部サービスの中断や終了時等に円滑に業務を移行することが可能なこと。
5		外部サービス提供者による情報資産の利用は、外部サービスの提供に必要な範囲で認めるものであり、それ以外の目的で本市の情報資産の利用は認めない。
6		以下の①～⑦の情報セキュリティ対策が確実に実施され、公開資料や監査報告書(又は内部監査報告書・事業者の報告資料)等からセキュリティ対策の実施内容・管理体制を市が確認することが可能なこと。また、設計・設定時や変更時の設定誤りの防止対策を講じること。 ①外部サービス自体はインターネットにアクセスできないこと ②SIMはフィルタリングにより外部サービス以外に利用できないこと ③MDMにより登録されたアプリ以外追加することができないこと ④端末にログインする際に生体認証、システムに入る際にログインID＋パスワードで認証すること ⑤クラウド側の対応として脆弱性対策を行うこと ⑥クラウド側の対応としてウイルス対策を行うこと ⑦クラウド側の対応としてサーバーの監視を行うこと
7		情報セキュリティインシデント(システムに起因する重大なセキュリティインシデント及び緊急を要する児童相談対応にシステムを利用することができない等)が発生した際に、外部サービス提供者と連絡がつかない、営業時間外の対応が不可能等の状況にならないこと。また、情報セキュリティインシデントによる被害を最小限に食い止めるために情報セキュリティインシデント発生時に以下の対応を行うこと。 ①情報セキュリティインシデントが発生した際に、運用状況・影響範囲調査等、事案解決のために積極的に調査を行うこと。 ②情報セキュリティインシデント発生の連絡を受けた後、発生確認後速やかに調査に着手すること。なお、情報セキュリティインシデントの疑いに対する連絡を受けた場合も同様に調査に着手すること。 ③当該事案の原因特定のため、各種システムログを取得すること。また、取得したログの分析に必要な情報を提供すること。 ④調査の結果、サービス停止等の措置が必要な場合は、市担当者に報告した上で速やかにその対応を行い、インシデント収束後、速やかに復旧を行うこと。 ⑤調査の結果、ファームウェア・ソフトウェア等のバージョンアップ等が必要となった場合は、速やかに対応すること。 ⑥また、市はサービス停止及びその理由について公表することがある。
8		当該サービスの利用規約の変更について2か月前までにメール等の方法で事前に告知すること。
9		再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されていることとし、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けること。
10		再委託先の情報セキュリティ対策の実施状況を確認するために次をはじめとした情報を本市に提供可能であること。 ・再委託先事業者情報 ・再委託内容 ・再委託先の情報セキュリティ責任者 ・再委託先の個人情報管理者 ・再委託先の従事者の情報　　等
11	アクセス制御に関する事項	サーバー等への不正アクセスを防ぐ仕組みを有していること。
12		外部サービスに影響を与える操作について、誤操作を抑制するための手順書の作成や誤操作を認識可能なアラート等を実装する等の対策を行うこと。
13		外部サービス上で構成される仮想マシンに対して適切なセキュリティ対策を行うこと。
14	設計・設定及び開発に関する事項	システムのアクセスログ、操作履歴、閲覧履歴、障害記録等、システムの利用状況及び処理状況を把握するために必要なログを取得すること。
15		外部サービス内において確実に時刻同期を行い、取得するログの時刻、タイムゾーンを統一すること。
16		セキュリティを保つための開発手順やフレームワーク等の情報が活用されていること。
17		業務継続を考慮し、利用する外部サービス上の情報システムが利用するデータ容量や稼働性能(移植容易性)について、必要に応じて外部サービス提供者に報告を求めることが可能であること。
18		冗長構成や冗長回線等の実装により可用性を十分に考慮した設計となっていること。
19		パスワードの管理機能について、英大文字、英小文字、記号及び数字を含める制限機能を備えている。
20		一定回数続けてログインに失敗した場合に、ログイン不能にするアカウントロック機能を有していること。
21	資産管理に関する事項	外部サービス提供者の責任範囲で発生した脆弱性対応が迅速に行われること。
22	事業継続に関する事項	バックアップからの復旧に係る手順の策定と定期的な訓練を実施すること。
23	外部サービスで取り扱った情報の廃棄に関する事項	外部サービスの利用終了時に、外部サービスで取り扱った業務に関わる全ての情報を、外部サービス基盤上から確実に削除すること。なお、削除する対象はバックアップ等により複製されたものにも及ぶ点に注意すること。
24		外部サービスの基盤となる装置等の処分についてセキュリティを確保した対応が行われること。
25		外部サービスの基盤の処分の確認にあたり、外部サービス提供者が利用者に提供可能な第三者による監査報告書や認証等を取得していること。
26		外部サービスの利用終了時に、情報の廃棄の実施報告書を提出すること。
27		外部サービス利用者の各アカウント以外に特殊なアカウント(ストレージアカウントなど)がある場合は、関連情報(資格情報等)含めて廃棄可能であること。