仕様書別紙３

セキュリティ要件

※セキュリティ要件は、すべて満たすこと。

No	大区分	小区分	内容
1	セキュリティ全般に関する事項	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、住民の生命及び財産に関わる情報、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			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			サービスの中断、終了時等に円滑に業務を移行することが可能なこと。その際は、移行方法が提示され、標準化されたデータ形式やインターフェースが使用可能であること。
5			サービス提供者による情報資産の利用は、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①～⑥の情報セキュリティ対策が確実に実施され、公開資料、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サービス以外に利用できないこと ③端末にログインする際ID（第一段階）、システムに入る際にログインID＋パスワード（第二段階）で認証すること ④クラウド側の対応として脆弱性対策を行うこと ⑤クラウド側の対応としてウイルス対策を行うこと
7			サービスの開発及び運用が本市の意図しない変更が行われない一貫した品質保証体制の下でなされていること。 意図しない変更とは非公開設定が説明なく、公開設定になることや本市が保存するデータが意図せず書き換えられること等を想定しており、機能追加等はこれに含まれない。
8			情報セキュリティインシデントが発生した際に、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。
9			サービスの利用規約及び各種設定の変更について２か月前までにメール等の方法で事前に告知すること。
10			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。

11			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
12	導入・構築時の対策	アクセス制御に関する事項	不正なアクセスを防止するためのアイデンティティ管理（アカウントの発行や削除等のメンテナンス）及びアクセス制御（外部サービスに保存される情報や外部サービスの機能ごとにアクセスする権限のない職員がアクセスできないように制限）を実施すること。
13			システム管理者等の特権アカウントがサービスに接続する際は、強化された認証技術（多要素認証等）を用いること。
14			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、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。
15			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（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策、ログ取得等の実施）を行うこと。
16			庁内通信回線を経由せずにサービスを利用する場合は、多要素主体認証方式やデバイス認証による接続端末制限等の対策を行うこと。
17		暗号化に関する事項	取り扱う情報の機密性に応じた保護のための適切な暗号アルゴリズム（CRYPTRECにより安全性及び実装性能が確認された「電子政府推奨暗号リスト」）を用いた暗号化処理（情報が保存されている場合、情報が通信され転送されている場合等フローに応じた暗号化）を行うこと。
18		設計・設定及び開発に関する事項	サービスに係るアクセスログ等の証跡の保存、取得及び提供が可能であり、契約期間中はログを保存すること。
19			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。
20			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。
21			業務継続を考慮し、利用するサービス上の情報システムが利用するデータ容量及び稼働性能（移植容易性）について、報告が可能であること。
22			冗長構成、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。
23			パスワードの管理機能について次の機能を備えていること。 ・長さ10文字以上の制限 ・英大文字、英小文字、記号及び数字を含める制限 ・パスワードをハッシュ化した状態で保存する機能
24			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。
25	運用・保守時の対策	資産管理に関する事項	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。
26		アクセス制御に関する事項	管理者権限を割り当てる場合のアクセス管理と操作に関するログの取得が行われること。また、管理者権限を持つ者の操作（データ改変等の重大な帰結をもたらすような操作）等について、記録し、保存できること。
27			サービスの不正な利用を監視可能であること。 （例：業務時間外の利用等をサービスに対するアクセスログで確認）

28		暗号化に関する事項	鍵管理機能をサービス提供者が提供するものを利用する場合、鍵の生成から廃棄に至るまでのライフサイクルにおける仕組みにリスク（鍵が窃取される可能性、鍵生成アルゴリズムの危殆化の可能性等）がないこと。
29		サービス内の通信に関する事項	他の利用者が市のデータにアクセスできないよう確実な制御を行っていること。
30		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。
31	更改・廃棄時の対策	サービスで取り扱った情報の廃棄に関する事項	サービスの利用終了時に、サービスで取り扱った業務に関わる全ての情報を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。
32			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。
33			サービスの基盤の処分の確認にあたり、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。
34			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。
35			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。