外部サービス選定基準

No	大区分	小区分	内容	求めるレベル
1	外部サービス提供者の選定基準	_	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。	必須
2	外部サービス提供者の選定基準	_	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。	必須
3	外部サービス提供者の選定基準	_	利用する外部サービスのリージョンを日本国内に限定すること。	必須
5	外部サービス提供者の選定基準	_	外部サービスの終了又は変更時における事前の通知について以下を例とする取り決めが可能なこと。 当該外部サービスの終了又は変更の際に6か月前までにメール等の方法で事前に告知すること。	必須
7	外部サービス提供者の選定基準	_	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。	必須
9	外部サービス提供者の選定基準	_	外部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。	必須
10	外部サービス提供者の選定基準	_	情報セキュリティインシデントの対処について以下を例とする内容を調達仕様に含められること。 情報セキュリティインシデントが発生した際に、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外部サービス提供者が情報セキュリティインシデントを検知した際は、速やかに本市に報告を行うこと。 ②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。 ③情報セキュリティインシデント発生後、即時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。 ④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。 ⑤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。 ⑥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。	必須
13	外部サービス提供者の選定基準	_	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。	必須
14	外部サービス提供者の選定基準	_	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	必須
16	導入・構築時の対策	アクセス制御に関する事項	業務の特性及び取り扱う情報に応じて以下を例とする接続制御が可能なこと。 ・インターネット接続可（接続可能な端末の限定）	必須
19	導入・構築時の対策	アクセス制御に関する事項	外部サービスに影響を与える操作（サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除・外部サービス利用の終了手順・バックアップ及び復旧等）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。	必須
20	導入・構築時の対策	アクセス制御に関する事項	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（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。 SaaSを利用する場合は、これらの対応が、外部サービス提供事業者側でされていること。	必須
22	導入・構築時の対策	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。	必須

No	大区分	小区分	内容	求めるレベル
25	導入・構築時の対策	設計・設定及び開発に関する事項	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。	必須
33	運用・保守時の対策	アクセス制御に関する事項	パスワードなどの認証情報の割り当てが外部サービス提供者側で実施される場合、以下を例とする管理手順が実施されること。 ・パスワードは、他者に知られないように管理しなければならない。 ・パスワードを秘密にし、パスワードの照会等には一切応じてはならない。 ・パスワードは十分な長さとし、文字列は想像しにくいもの（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）にしなければならない。 ・パスワードが流出したおそれがある場合には、速やかに報告し、パスワードを変更しなければならない。 ・サーバ、ネットワーク機器、パソコン及びモバイル端末等にパスワードを記憶させてはならない。	必須
34	運用・保守時の対策	資産管理に関する事項	当該外部サービスに関連する脆弱性情報の提供を行うこと。また、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。	必須
38	運用・保守時の対策	暗号化に関する事項	鍵管理機能を外部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や鍵生成アルゴリズムの危殆化の可能性等）がないこと。	必須
39	運用・保守時の対策	外部サービス内の通信に関する事項	利用する外部サービスのネットワーク基盤が他の利用者のネットワークや通信と分離されていること及び利用する外部サービスの仮想マシンのネットワークが他の利用者のネットワークと分離されていること。 SaaSの場合は、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。	必須
43	更改・廃棄時の対策	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が、外部サービス基盤上から確実に削除可能であること。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。 削除にあたっては、情報資産を暗号化した鍵（暗号鍵）を削除するなどにより、復元困難な状態としなければならない。	必須
44	更改・廃棄時の対策	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。	必須
46	更改・廃棄時の対策	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、情報の廃棄の実施報告書を提出すること。	必須
47	更改・廃棄時の対策	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。	必須