外部サービス選定基準

【別紙３】

① 外部サービス提供者に係る事項

No.	大区分	小区分	確認事項
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の運用	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に指定できること。
2	外部サービス提供者の選定基準	国内リージョンおよびデータの保存	海外への機密情報の流出リスクを考慮し、外部サービスを提供するリージョン（国・地域）を国内に指定できること。国内の外部サービスにおいて、利用者のデータが、海外に保存されないこと。
3	外部サービス提供者の選定基準	サービス終了または変更時の事前通知	外部サービスの終了または変更時における事前の通知等の取り決めや情報資産の移行方法を契約に規定できること。 特に事前の通知については、事前通知の方法・期限について、以下を例とする条項を盛り込んだ契約が締結可能なこと。 ［例］ 当該サービスの終了または変更の際に、●か月前までに●の方法で事前に告知すること。
4	外部サービス提供者の選定基準	情報セキュリティ対策の履行が不十分な場合の対処方法	情報セキュリティ対策の履行が不十分な場合の対処方法（改善、追完、損害賠償等）について、契約またはサービスレベル契約（SLA）に規定できること。
5	外部サービス提供者の選定基準	目的外利用の禁止	外部サービス提供者が、区の情報資産へ目的外のアクセスや利用を行わないように契約に定められること。
6	外部サービス提供者の選定基準	外部サービス提供者における情報セキュリティ対策の実施内容および管理体制	外部サービス提供者における情報セキュリティ対策の実施内容および管理体制について、公開資料や監査報告書（または内部監査報告書・事業者の報告資料）、各種の認定・認証制度の適用状況から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し、判断可能なこと。 認定・認証制度の例は以下のとおり。 ① ISO/IEC 27017 ② ISMAPクラウドサービスリスト ⑤ ISMAP-LIUクラウドサービスリスト ④ SOC報告書 ⑤ ISMAP管理基準を満たすこと ※ ガバメントクラウドを利用する場合は、上記①～④の国際規格またはそれ以上の認定、認証が必須
7	外部サービス提供者の選定基準	区が意図しない変更が加えられないための管理体制	外部サービス提供者もしくはその従業員、再委託先またはその他の者によって、区の意図しない変更が加えられないための管理体制について、公開資料や監査報告書（または内部監査報告書・事業者の報告資料）の内容を確認できること。
8	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への対処方法	情報セキュリティインシデント（情報セキュリティ事故およびその兆候）への対処方法について、外部サービス提供者との責任分担や連絡方法を取り決め、契約またはサービスレベル契約（SLA）に規定できること。

② 外部サービスに係る事項

No.	大区分	小区分	確認事項
9	導入・構築	アクセス制御に関する事項	外部サービス上に保存する情報や外部サービスの機能に対してアクセス制御（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者がアクセスできないように制限すること）ができること。
10	導入・構築	暗号化に関する事項	外部サービス内および通信経路全般において暗号化処理が行われていること。この際、利用される暗号化方式は、「電子政府推奨暗号リスト」に記載された方式であること。
11	導入・構築	設計・設定および開発に関する事項	必要となる各種ログの取得機能を実装していること。区は外部サービスで取得可能なログの種類、範囲を確認すること。
12	導入・構築	設計・設定および開発に関する事項	取得するログの時刻、タイムゾーンが統一されること。区は時刻同期方法について確認すること。
13	運用・保守	暗号化に関する事項	暗号化に関し、外部サービス提供者が提供する鍵管理機能を利用する場合、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関する内容等が確認できること。区は、その内容にリスク（鍵が窃取される可能性や鍵生成アルゴリズムが危険にさらされる可能性等）がないことを確認すること。（SaaSの場合は対象外）
14	運用・保守	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内において区が利用するネットワークが、他の利用者のネットワークや通信と分離され、論理的に独立していること。 SaaSの場合は、他の利用者が区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。
15	運用・保守	設計・設定に関する事項	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を、外部サービス提供者の開示している情報等で確認できること。SaaSの場合は、他の利用者が区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。
16	更改・廃棄	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区の全ての情報が外部サービス基盤上から漏えいを来さない方法で確実に削除されること。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も含むこと。 これらについて外部サービスの利用終了時に、区に情報の廃棄の実施報告書を提出すること。
17	更改・廃棄	外部サービスの利用終了時における対策に関する事項	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）を含めて廃棄可能であること。