外部サービス選定基準

資料１仕様書　別紙

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	要否のレベル （ガバメントクラウド利用の場合はすべて必須）	確認結果	不要とした場合その理由
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。	必須	□確認済 （不適切と考えられるものなし）	
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。	必須	□確認済 （不適切と考えられるものなし）	
3	外部サービス提供者の選定基準	サービス中断時の復旧要件	外部サービスの中断時の復旧要件が契約またはサービスレベル契約（SLA）に規定できること。	高	□確認済 （不適切と考えられるものなし） □不要	
4	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。	必須	□確認済 （不適切と考えられるものなし）	
5	外部サービス提供者の選定基準	利用規約、各種設定の変更に関する確認方法等	外部サービス提供者により、利用規約、各種設定が変更される可能性があるため、変更内容の確認方法や連絡方法を契約またはサービスレベル契約（SLA）に定められること。この際、変更内容の確認や事前通知の方法・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］ 利用規約、各種設定の変更について●か月前までに●の方法で事前に告知すること。	高	□確認済 （不適切と考えられるものなし） □不要	
6	外部サービス提供者の選定基準	可用性に関するサービスレベル契約等	業務の重要度に応じ、稼働率、目標復旧時間、目標復旧ポイント、バックアップの方法等の可用性に関する事項、インシデント報告義務等、必要な事項を盛り込んだ契約またはサービスレベル契約（SLA）が締結可能なこと。	高	□確認済 （不適切と考えられるものなし） □不要	
7	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。	必須	□確認済 （不適切と考えられるものなし）	

No.	大区分	小区分	確認事項	要否のレベル （ガバメントクラウド利用の場合はすべて必須）	確認結果	不要とした場合その理由
8	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。	必須	□確認済 （不適切と考えられるものなし）	
9	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	必須	□確認済 （不適切と考えられるものなし）	
10	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。	必須	□確認済 （不適切と考えられるものなし）	
11	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。	必須	□確認済 （不適切と考えられるものなし）	
12	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実施状況の確認	脅威に対する外部サービス提供者の情報セキュリティ対策（なりすまし、情報漏えい、情報の改ざん、否認防止、権限昇格攻撃への対応、サービス拒否・停止等）の実施状況等、契約の履行状況の確認方法が契約またはサービスレベル契約（SLA）に規定できること。	高	□確認済 （不適切と考えられるものなし） □不要	
13	外部サービス提供者の選定基準	他の外部サービス等を用いて外部サービスを提供する場合	他の外部サービス等を用いて外部サービスを提供する場合は、本表のセキュリティ対策を外部サービス提供者においても遵守することを契約に規定できること。	高	□確認済 （不適切と考えられるものなし） □不要	

② 外部サービスに係る事項

No.	大区分	小区分	確認事項	要否のレベル（ガバメントクラウド利用の場合はすべて必須）	確認結果	不要とした場合その理由
14	導入・構築	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ィンティティ管理（IDのプロビジョニングから廃棄まで）を実装していること。 ※ アイデンティティ管理…IDやパスワードのユーザーアカウントを一元的に管理するシステムや技術のこと。 ※ プロビショニング…設備やサービスを提供できるよう事前準備を行うこと。	高	□確認済 （不適切と考えられるものなし） □不要	
15	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。	必須	□確認済 （不適切と考えられるものなし）	
16	導入・構築	アクセス制御に関する事項	システム管理者等の特権アカウントが外部サービスに接続する際は、強化された認証技術（多様素認証等）を用いること。	中	□確認済 （不適切と考えられるものなし） □不要	
17	導入・構築	アクセス制御に関する事項	外部サービスに多大な影響を与える操作（※）を特定し、外部サービス利用者による誤操作を抑制するための対策を講じること（手順書の作成や誤操作を認識し、アラートを出す等の機能を実装する等）。 ※設定の自動化ツールなど実行が容易ではあるが、その影響がシステム全体に影響するようなものを指す。	中	□確認済 （不適切と考えられるものなし） □不要	
18	導入・構築	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（サービスを実行するのに必要なポート、プロトコル、サービスのみを有効にするなどのセキュリティ対策をすぐに行い、マルウェア対策やログ取得などのセキュリティ管理策を実施する）を行っていること。	高	□確認済 （不適切と考えられるものなし） □不要	
19	導入・構築	アクセス制御に関する事項	インターネット等の外部の通信回線から庁内通信回線を経由せずに外部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がとれること。 （外部サービスにインターネットで直接接続するケースがある場合のみ該当）	高	□確認済 （不適切と考えられるものなし） □不要	
20	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。	必須	□確認済 （不適切と考えられるものなし）	
21	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。	必須	□確認済 （不適切と考えられるものなし）	
22	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。	必須	□確認済 （不適切と考えられるものなし）	

No.	大区分	小区分	確認事項	要否のレベル（ガバメントクラウド利用の場合はすべて必須）	確認結果	不要とした場合その理由
23	導入・構築	設計・設定および開発に関する事項	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を提供していること。	高	□確認済 （不適切と考えられるものなし） □不要	
24	導入・構築	設計・設定および開発に関する事項	外部サービス上に構成された情報システムと他の外部サービス利用者のネットワークやサブネット間等の異なるネットワーク間の通信（トラフィック）を監視すること。 （SaaSの場合は対象外）	高	□確認済 （不適切と考えられるものなし） □不要	
25	導入・構築	設計・設定および開発に関する事項	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られること。	高	□確認済 （不適切と考えられるものなし） □不要	
26	導入・構築	設計・設定および開発に関する事項	外部サービスを利用する業務において必要となる可用性（冗長構成や冗長回線等の実装）を考慮した設計になっていること。	高	□確認済 （不適切と考えられるものなし） □不要	
27	運用・保守	資産管理に関する事項	外部サービス提供者の責任範囲における脆弱性について迅速に脆弱性対応が行われること。	高	□確認済 （不適切と考えられるものなし） □不要	
28	運用・保守	アクセス制御に関する事項	システム管理者等の特権を割り当てる場合のアクセス管理を適切に行うこと（必要最小限の権限のみ付与する等）。また、システム管理者特権を有する利用者の操作等に関するログを全て記録し、保存すること。	高	□確認済 （不適切と考えられるものなし） □不要	
29	運用・保守	アクセス制御に関する事項	外部サービスのリソース設定（ネットワーク、仮想マシン等）を変更するユーティリティプログラムを使用する場合は、その機能を確認し、利用者を制限できること。	低	□確認済 （不適切と考えられるものなし） □不要	
30	運用・保守	アクセス制御に関する事項	外部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外部サービスに対するアクセスログで確認する等）。	高	□確認済 （不適切と考えられるものなし） □不要	
31	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）	必須	□確認済 （不適切と考えられるものなし）	

No.	大区分	小区分	確認事項	要否のレベル （ガバメントクラウド利用の場合はすべて必須）	確認結果	不要とした場合その理由
32	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。	必須	□確認済 （不適切と考えられるものなし）	
33	運用・保守	設計・設定に関する事項	区が外部サービスの設定を変更する場合、以下を例とする設定の誤りを防止するための対策を提供できること。 ① セキュリティ設定・監視ツールの提供 ② 設定権限を与える外部サービス利用者の限定 ③ グローバルなセキュリティのガイドラインやフレームワーク、外部サービス提供者が推奨する設定情報の提供 ④ 外部サービスの機能追加に係る設定等の情報提供	高	□確認済 （不適切と考えられるものなし） □不要	
34	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。	必須	□確認済 （不適切と考えられるものなし）	
35	運用・保守	事業継続に関する事項	不測の事態に対してサービスの復旧を行うために必要なバックアップを実施（外部サービス提供者が提供する機能を利用する場合は、その実施の確認）すること。	高	□確認済 （不適切と考えられるものなし） □不要	
36	運用・保守	事業継続に関する事項	バックアップ頻度、範囲等、外部サービスが、業務に必要な可用性を満たしたものになっていること。	高	□確認済 （不適切と考えられるものなし） □不要	
37	運用・保守	事業継続に関する事項	利用する外部サービスで使用済みのデータ容量やサービスの性能について監視を行い、想定された容量・性能内で運用していることを確認できること。	中	□確認済 （不適切と考えられるものなし） □不要	
38	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。	必須	□確認済 （不適切と考えられるものなし）	
39	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。	必須	□確認済 （不適切と考えられるものなし）	