（様式５） クラウドサービス要件・適用状況一覧

区分について
　必須：クラウドサービスを提供するにあたり、必ず適合しなければならない。
　推奨：クラウドサービスを提供するにあたり、必須ではないが適合することが望ましい。
　任意：クラウドサービスを提供するにあたり、必須または推奨としないもの。

適合状況について
　クラウドサービスを提供するにあたり、各要件が適合する場合は、「○」を選択してください。
　なお、区分が必須の要件について、適合状況が「×」の場合は、失格とします。

根拠資料について
　適合状況が「○」の場合、根拠資料を提出してください。
　なお、根拠資料の欄が斜線の要件については、提出いただく必要はありません。

項番	区分	要件	区分	適合状況	根拠資料	状況説明
A セキュリティに係る国際規格等の資格・認証の取得						
A-1	セキュリティ評価制度	利用しようとするクラウドサービス（アプリケーション）が政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））に登録されていること。	推奨		適合状況が「○」の場合は根拠資料を提出してください。	
A-2	資格・認証（国際規格） ※アプリケーション提供事業者	サービス提供を行う組織（アプリケーション提供事業者）が、ISO/IEC27001認証を取得していること。	必須		適合状況が「○」の場合は根拠資料を提出してください。	
A-3		サービス提供を行う組織（アプリケーション提供事業者）が、ISO/IEC27017認証を取得していること。	推奨		適合状況が「○」の場合は根拠資料を提出してください。	
A-4		サービス提供を行う組織（アプリケーション提供事業者）が、ISO/IEC27018認証を取得していること。	任意		適合状況が「○」の場合は根拠資料を提出してください。	
A-5	プライバシーマーク ※アプリケーション提供事業者	サービス提供を行う組織（アプリケーション提供事業者）が、Pマーク（プライバシーマーク）を取得していること。	推奨		適合状況が「○」の場合は根拠資料を提出してください。	
A-6	資格・認証（国際規格） ※クラウドサービスプロバイダー	サービス提供を行う組織（クラウドサービスプロバイダー）が、ISO/IEC27001認証を取得していること。	必須		適合状況が「○」の場合は根拠資料を提出してください。	
A-7		サービス提供を行う組織（クラウドサービスプロバイダー）が、ISO/IEC27017認証を取得していること。	推奨		適合状況が「○」の場合は根拠資料を提出してください。	
A-8		サービス提供を行う組織（クラウドサービスプロバイダー）が、ISO/IEC27018認証を取得していること。	任意		適合状況が「○」の場合は根拠資料を提出してください。	
A-9	プライバシーマーク ※クラウドサービスプロバイダー	サービス提供を行う組織（クラウドサービスプロバイダー）が、Pマーク（プライバシーマーク）を取得していること。	推奨		適合状況が「○」の場合は根拠資料を提出してください。	
A-10	データセンター要件	データセンターは、日本データセンター協会が制定するデータセンターファシリティスタンダードのティア３相当の基準を満たした設備とすること。	推奨		適合状況が「○」の場合は根拠資料を提出してください。	

項番	区分	要件	区分	適合状況	根拠資料	状況説明
B 情報セキュリティ対策の実施						
B-1	情報セキュリティ対策	サービス提供業務の遂行のために提供する情報（契約等の手続に付随してクラウドサービス事業者が知りうる利用者情報等）を、サービス提供業務の遂行目的外で利用しないこと。情報の目的外利用の禁止に対する遵守（義務）の表明をすること。	必須			
B-2		サービス提供を行う組織若しくはその従業員、再委託先又はその他の者によって、本市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提示すること。	必須		適合状況が「○」の場合は根拠資料を提出してください。	
B-3		サービス提供事業の事務所、運用場所（リージョン）を情報提供すること。提供にあたっては文書にて内容を確約すること。	必須		適合状況が「○」の場合は根拠資料を提出してください。	
B-4		情報セキュリティインシデントが発生した場合に、被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について提示すること。	必須		適合状況が「○」の場合は根拠資料を提出してください。	
B-5		障害や情報セキュリティインシデントの発生、監査結果等によって、情報セキュリティ対策の履行が不十分であると認められた場合の対処（改善の実施等）方法について提示すること。	必須			
B-6		従業員に対し毎年情報セキュリティ研修を実施していること。	必須			
C サービスの中断や終了時に円滑に業務を移行するための対策						
C-1	サービス中断・終了時	次期サービスへ移行するためのデータ提供が可能なこと。	必須			
C-2		データを消去する際に、データを復元できないように電子的に完全に消去又は廃棄すること。また、データ及びアカウントを消去又は廃棄した証明書を提示すること。	必須			
D 情報セキュリティ監査の受入れ						
D-1	セキュリティ監査	第三者による情報セキュリティ監査の受入れが行われていること。	推奨		適合状況が「○」の場合は根拠資料を提出してください。	
D-2		本市による必要に応じた監査の受け入れもしくは本市の監査と同等以上とみられる認証等情報の提供が可能なこと。	推奨			
E サービスレベルの保証						
E-1	SLA（Service Level Agreement）	サービスレベルの保証が定められていること。 （例：サービス提供時間、稼働率、バックアップの取得頻度、問合せへの応答時間　など）	任意		適合状況が「○」の場合は根拠資料を提出してください。	
F 本市の情報を取り扱う場所及び契約に定める準拠法・裁判管轄						
F-1	データの所在・適用法と裁判管轄	サービス上のユーザ所有データ（バックアップデータを含む。）の所在地が日本国内に限定できること。	必須		適合状況が「○」の場合は根拠資料を提出してください。	
F-2		準拠法、裁判管轄を日本国内に指定できること。	必須			
F-3		市が登録したデータは、本市に確実に提供でき、提供後のデータの所有権・管理権は、市が保有すること。また、市が登録したデータは、本契約に明示的に定められているところを除き、本市の承諾なく、利用できないものとすること。	必須			

項番	区分	要件	区分	適合状況	根拠資料	状況説明
G クラウドサービスが提供する部分を含む情報の流通経路全般にわたるセキュリティの確保						
G-1	総合的なリスク対策	取り扱うデータの機密性・完全性・可用性及び、対象サービスの特徴・重要性を踏まえて、クラウドサービスにより発生するリスク対策が複数の手段によって講じられていること。	必須			
G-2	データ暗号化	機密性の高いデータについて、暗号化等によって蓄積・伝送データを保護できること。	必須			
G-3	ログ取得	外部サービス上におけるアクセスログ等の証跡について、本市が指定する期間の保存が可能であること。 また、その手法について提示すること。	必須		適合状況が「○」の場合は根拠資料を提出してください。	
G-4	脆弱性対策	外部サービス上の脆弱性を発見する方法があり、実施可能であること。 また、その手法について提示すること。	必須		適合状況が「○」の場合は根拠資料を提出してください。	
G-5	不正アクセス対策	通信内容を監視する等により、不正アクセスや不正侵入を検知及び通知できること。	必須			
G-6	機器停止	機器に異常があった場合、検知できること。 また、機器を死活監視し、停止した場合、検知できること。	必須			
G-7	データ取扱い時の権限管理	データの取り扱いについて、権限管理及びアクセス制御ができること。	必須			
G-8	保守端末	保守端末は、認証管理、持出管理、施錠管理、ログ管理等によりセキュリティを確保していること。	必須			
H サービス提供者がその役務内容を一部再委託する場合の、サービス提供者の 選定条件で求める内容の担保、及び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の提供						
H-1	再委託	サービス提供を行う組織が本市の情報を取り扱うに際して、その取り扱いを再委託していない、または、再委託する場合に事前に通知または公開すること。	必須			
H-2		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るよう、クラウドサービス提供者の選定条件で求める内容をクラウドサービス提供者に担保させるとともに、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。	必須			