

様式4 セキュリティ要件を満たしているかの確認書

<記載方法>
全ての項番について、要件を満たす場合は「○」、満たさない場合は「×」を適用状況の列に入力してください。
適用状況が要件と一致しないが「○」に該当すると判断する項番がある場合、その項番に関する取扱いを補足事項の列に記入してください。
項番1の適用状況が「○」の場合、規程番号③⑤以外の項番はすべて適用状況の列に「○」を記載し、補足事項の列に「ISMAP登録」と記入してください。
基準日は令和7年7月1日とします。

<必須/推奨について>
必須: 満たすべき必要がある要件
推奨: 満たすべきだが、満たさないことを許容できる要件

項番	規定番号	区分	要件	必須/推奨	適用状況	補足事項
1	①	セキュリティ評価制度 ※アプリケーション	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))への登録が行われていること。	推奨		
2	②	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		
3			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		
4			サービス提供事業の事務所、運用場所(地域(リージョン))が特定できるようにすること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認すること。	必須		
5			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		
6			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		
7	③	クラウドサービス終了時	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すること。また、データを消去した証明書又は報告書を提示すること。	必須		
8	④	データの所在	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。	必須		
9	⑤	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		
10	⑥	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		
11		ログ取得	クラウドサービス上におけるアクセスログ等の証跡に係る保存期間について、一定期間の保存が可能であること。その手法について提示すること。	必須		
12		脆弱性対策	クラウド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。その手法について提示すること。	必須		
13		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		
14		機器停止	クラウドストレージサービスを提供するにあたって使用している機器(サーバ等)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		
15		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を行うこと。	必須		
16		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		