

クラウドサービス提供者の選定基準について

1. 本県とクラウドサービス提供者との情報の受渡し方法や利用終了時の情報の廃棄・返却方法等を含む情報の取扱手順を定め、その計画書を提出すること。
2. 経済安全保障の観点から、クラウドサービスの利用を通じて、本県が取り扱う情報のクラウドサービス提供者において本県の認める目的の外に利用しないこと。
3. クラウド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及び管理体制を示した書面等を提出すること。
4. クラウドサービス提供者においては、クラウドサービス提供者、その従業員、再委託先又はその他の者によって本県の意図しない変更が加えられないための管理体制を示した書面等を提出すること。
5. クラウドサービス提供者の資本関係・役員等の情報、クラウドサービス提供業務に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する事項が記載された書面等を提出すること。
6. クラウドサービス提供者において発生し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止めるための対処方法（対処手順、責任分界、対処体制等）を示した書面等を提出すること。
7. 情報セキュリティ対策その他の契約の履行状況が確認できる報告（クラウドサービス提供者からの定期的な報告、情報セキュリティ監査等）を作成し提出すること。
8. 情報セキュリティ対策が不十分であると分かった場合は、その対処方法（改善について本県と協議の上、実施すること。）を定めた書面等を提出すること。
9. クラウドサービスの中断又は終了時に際し、円滑に業務を移行するための次の事項を記載した計画書を作成し、提出すること。
 - (1) サービス中断時の復旧要件
 - (2) サービス終了又は変更する場合の事前告知の方法・期限及びデータ移行の方法
10. クラウドサービス提供者への立入検査又は情報セキュリティ監査の受入を認めること。又は立入検査及び監査と同等の効力を持つ書面等（SOC）を示すこと。
11. サービスレベルの保証（可用性、通信の速度及び安定性、データの保存期限及び方法、データ交換の安全性及び信頼性確保のための方法、情報セキュリティインシデントの対策方法等）を定めた書面等を提出すること。
12. 経済安全保障の観点から、バックデータを含む情報が取り扱われる場所については、日本の法令の範囲内で運用できるデータセンター等とし、契約書等において日本国内の裁判所を合意管轄裁判所と記載できること。
13. 経済安全保障の観点から、クラウドサービス提供者がその業務等を一部再委託させた場合は、再委託先にもクラウドサービス提供者と同様に当該選定基準の全てを満たす者とし、再委託先の情報セキュリティ対策の実施が確認でき、本県の承諾を得るための書類が提出できること。
14. クラウドサービスの提供を含む情報の流通経路全般にわたりセキュリティが適切に確保されるにあたり、次のセキュリティ要件を満たすことができる者であること。
 - (1) クラウドサービスに係るアクセスログ等の証拠の保存は1年以上であること。

別紙2

- (2) クラウドサービスのインターネット接続点の通信監視ができること。
- (3) クラウドサービス提供者による管理・保管の実施内容が確認できること。
- (4) クラウドサービス上の脆弱性対策の実施内容が確認できること。
- (5) クラウドサービス上の情報に係る復旧時点目標等の指標が確認できること。
- (6) クラウドサービス上の情報の確実な削除・廃棄ができること。
- (7) クラウドサービス利用者が求める情報開示請求に対する開示項目及び範囲については、本県と協議の上、契約書等に明記すること