

伊那市外部サービス（クラウドサービス）利用要件

|    |                                                                               |
|----|-------------------------------------------------------------------------------|
| 1  | セキュリティに係る国際規格 ISO/IEC 2 7 0 0 1 又はそれと同等以上の認定、認証制度を保有していること                    |
| 2  | 可用性のレベル等（稼働率、目標復旧時間、バックアップの保管方法など）を保証させるための SLA や SLO 保証を契約内容に記載すること          |
| 3  | 本市の情報が取り扱われる場所（データセンター）が国内にあること                                               |
| 4  | 再委託が発生する場合、再委託先でも同様の利用要件を求めること                                                |
| 5  | 外部サービスの中断や終了に際し、円滑に業務を移行するための対策を提供すること                                        |
| 6  | 本市が取り扱う情報の目的外利用を禁止していること                                                      |
| 7  | 情報セキュリティ対策の実施内容及び管理体制を整備していること                                                |
| 8  | 本市が利用する外部サービスの開発及び運用するにおいて、「本市の意図しない変更が加えられないための管理体制」が確保されていること               |
| 9  | 外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属の情報を提供すること                             |
| 10 | 情報セキュリティインシデントへの対処方法（対処手順、責任分界、対処体制等）が整備されていること                               |
| 11 | 情報セキュリティ対策その他の契約の履行状況（利用状況、障害状況、セキュリティ対策に関する情報を含む月次保守報告書等）が確認できること            |
| 12 | 情報セキュリティ対策の履行が不十分な場合に改善できること                                                  |
| 13 | 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                                                 |
| 14 | 情報の格付及び取扱制限の明示等、運搬又は送信、消去等の情報の取扱いに関して、本市の対策基準に定める内容と同等の取扱いが行われるように合意が得られていること |
| 15 | 外部サービスに係るアクセスログ等の証跡は1年以上保存できること                                               |
| 16 | 情報の管理・保管方法について、利用前に本市と合意を得ていること                                               |
| 17 | 情報開示請求に対して、本市が指定する情報を開示できること                                                  |
| 18 | 不正なアクセスを防止するためのアクセス制御がされていること                                                 |
| 19 | 取り扱う情報の機密性保護のため、外部サービス内容及び通信経路全般における暗号化がされていること                               |
| 20 | 情報システムの構築時に外部サービスを利用する場合、外部サービスのセキュリティを保つための開発手順等が整備されていること                   |
| 21 | 情報システムの構築時に外部サービスを利用する場合、設計・設定時の誤りが防止されていること                                  |
| 22 | 取り扱う資産の管理は適切に行えること                                                            |
| 23 | 職員一般アカウント及び管理者アカウントの管理が適切に行えること                                               |
| 24 | 鍵管理機能を外部サービス提供者が提供する場合、鍵の管理手順が作成されていること                                       |
| 25 | 利用する外部サービスのネットワーク基盤が他のネットワークと分離されていること                                        |
| 26 | 外部サービスの設定を変更する場合、設定の誤りを防止するための対策がとられていること                                     |
| 27 | 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が実施できること                                       |
| 28 | 外部サービスの利用終了時に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                                        |
| 29 | 外部サービスで取り扱った本市の情報を廃棄できること                                                     |
| 30 | 外部サービスの利用終了時、作成したアカウントの削除を適切に行うこと                                             |