別紙３

外部サービスの利用におけるセキュリティ要件

No	セキュリティ対策
1	受託者は情報セキュリティに関して十分な知識があること。
2	ライセンス違反等がないよう必要な数だけアカウントを準備すること。
3	利用する端末にセキュリティ対策（ユーザ認証・ウィルス対策・デバイス管理・Web フィルタリング等）を行っていること。
4	外部サービスを利用する端末に機微なデータが保存されない対策を行っていること。
5	利用する端末を外部に持ち出す場合、Free Wi-Fi への接続禁止等の措置が講じられていること。
6	外部サービスを提供するシステム・利用する端末のリソースに不足がなく、将来の拡張性があること。
7	外部サービスで使用する時刻は、標準時刻と同期していること。
8	SLA（サービス品質保証）を締結できること
9	インシデント等の検証に必要なログを提供できること。
10	OS やアプリケーション等のバージョンアップや設定変更、パッチ適用、脆弱性診断等を行い、実施状況を報告すること。
11	サービス終了時に保存データ（事業者の複製データも含む）を消去する際は、実効性を確保でき、データが復元不可能となる処置を講じること。
12	サービス終了時は利用者アカウントや管理者アカウント等を削除できること。
13	第三者認証（ISMAP 登録や ISO27017 による認証等）や情報セキュリティ監査の結果等を有していること。
14	重要な操作（仮想化されたデバイスのインストールや変更・削除、バックアップ・リストア、サービス終了時など）に関して、手順が文書化されていること。
15	事業者または区がインシデントを検知した際、区への連絡・報告体制が取れていること。
16	サービスのサポート体制や窓口、受付時間がサービス利用において十分なものになっていること。
17	情報の盗聴、改ざん等を防止するため、VPN 接続によるサービス利用であるか、TLS による通信の暗号化がされていること。
18	政府が定めるクラウドセキュリティ評価制度「ISMAP」に登録されていること。
19	ISO 27017,18 の第三者認証または SOC 報告書によるセキュリティ管理体制を確認できること。
20	サービス提供側に外部・内部からの不正アクセスを防止措置が施されていること。
21	サービス提供側に IPS/IDS や WAF による不正通信やマルウェアの発見・遮断措置が施されていること。
22	盗難・改ざん等の防止のため、保存されたデータは暗号化されていること。

23	不必要なアクセスがされないよう、情報資産・機能に対して、各利用者に必要最低限のアクセス権のみ付与すること。
24	ID/PW による認証を行うこと。