別紙２　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	都区市町村情報セキュリティクラウドへの接続及び LGWAN を利用する場合は、それらの帯域を圧迫しないこと。 推奨通信速度　２Mbps 程度
9	システムのレスポンス（応答時間）は概ね５秒以内であること。
10	ユーザが特別な知識を必要とせず、直感的に利用できるシンプルなデザインの画面や操作性となっていること。
11	サービスの稼働率は概ね９５％であること。
12	SLA（サービス品質保証）を締結できること
13	データのバックアップ及びリストアができること。 バックアップのタイミング：日次 保存世代：１０世代
14	障害発生時にシステム及びデータの復旧方法や復旧時間等の目標を定めていること。
15	システムまたはネットワークが冗長化されていること。
16	インシデント等の検証に必要なログを提供できること。
17	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。
18	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。
19	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。
20	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。
21	システムを事業者が構築する場合、事業者内において適切なセキュリティ管理体制（職員の資格取得や研修等）がとられていること。
22	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。

23	システムを事業者が構築する場合、管理者等のアカウントは適切に管理（パスワード管理や多要素認証、アクセス権限、終了時の削除など）されていること。
24	再委託や第三者の外部サービス利用がある場合、上記№21 と同様に再委託先等の情報セキュリティ対策を実施していること。
25	データはすべて国内に保存されること。 （データが保存されているサーバは国内に設置されていること）
26	データセンターの防災対策や入退室管理・監視体制が整っており、サービス利用において安全な設備になっていること。
27	事業者または区がインシデントを検知した際、区 CSIRT への連絡・報告体制が取れていること。
28	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。
29	情報の盗聴、改ざん等を防止するため、TLS による通信の暗号化がされていること。
30	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。
31	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。
32	サービス提供側にファイアウォールによる外部・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。
33	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。 対策内容：【IPS ・ IDS ・ WAF ・マルウェア検知】
34	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。
35	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。
36	ID/PW による認証を行うこと。