セキュリティ要件一覧表

項目	要件の概要
ネットワーク	地方公共団体情報システム機構に登録されたLGWAN-ASPであること、または登録の予定があること。
サーバ及び学習利用	チャット履歴及びアップロードしたデータは、日本国内のサーバに格納され、他の契約者と共有されないこと。また、学習に利用されないこと。
情報流出対策	禁止ワードが設定可能であり、当該禁止ワードや個人情報等が送信される恐れがある場合、警告文の表示やマスキング処理等のセキュリティ対策が実施可能であること。
以下は、個人情報や機密性が高い情報をクラウドサービスにて利用する際に当市が求める要件です。 今後、個人情報等を含む業務への利用拡大の可能性を確認するため、「ネットワーク」の区分が×である場合は、以下について対応状況を確認します。	
国際規格準拠	クラウドサービスの提供又は利用に関する国際規格の認証（ISO／IEC27017）、政府情報システムのためのセキュリティ評価制度（ISMAP）への登録又はこれらと同等の認証等を取得していること。
情報の流通経路	情報の流通経路全般に対するセキュリティ対策が実施されており、適切なバックアップレベルを設定していること。
再委託	再委託が行われる場合、再委託先の情報セキュリティ対策が十分に確保されていること。
サービス中断時、終了時	サービスの中断や終了時に、変更の影響を最小限に抑えるための、システム及びデータのバックアップ計画があること。サービス終了後、発注者の指示に従い、データが削除されること。
目的外禁止	サービスの運用において、本市の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、不正が見付かったときに、追跡調査や立入検査等、本市とサービス提供者が連携して原因を調査・排除できる体制を整備していること。
インシデントへの対応	復旧を優先する場合の、サービスの利用を一時的に停止するための手順を規定していること。また、業務継続を優先する場合の、サービスの利用を継続した上でインシデントに対処する手順を規定していること。
情報管理	チャット履歴及びアクセスログが１年以上保存されること。