

別紙3 セキュリティ要件

項目		要件概要
ネットワーク		インターネット環境下で利用可能なものとし、インターネット上の通信経路においては暗号化を行うこと。 Microsoft Edge109.0.1518.78 (公式ビルド) (64 ビット)及び GoogleChrome124.0.6367.61 (Official Build)(64 ビット)で利用できるもの。
データセンター		データセンターは Tier 3 4相当であり、建築基準法（昭和 25 年法律第 201 号）の新耐震基準に適合していること。 データセンタの物理的所在地を日本国内とし、情報資産について、合意を得ない限り日本国外への持ち出しを行わないこと。
		データセンター側のネットワーク（インターネット回線）の冗長化をすること。
		監視ソフト等により、システムログ、CPU使用率、メモリ使用率等のサーバやネットワーク機器の稼働状況、個人情報保管されたサーバへのアクセス状況監視、アクセスログ保管を監視すること。また、一日複数回、目視によりサーバやネットワーク機器の稼働状況を監視すること。
		データセンター内の入退室者を識別・記録できるセキュリティ設備（生体認証）により、許可された者のみ入退室が可能なこと。
		サーバラックの不正アクセスや不正操作防止のため鍵付きラックを使用すること。
		システム（サービス）の稼働環境及び開発・テスト環境においては、コンピュータウィルス等不正プログラムの侵入や外部からの不正アクセスが起きないように対策を講じるとともに、それら対策で用いるソフトウェアは常に最新の状態に保つこと。
		システム（サービス）の稼働環境及び開発・テスト環境で用いるOSやソフトウェアは、不正プログラム対策に係るパッチやバージョンアップなど適宜実施できる環境を準備すること。
以下は、個人情報をクラウドサービスで利用する際に当市が求める要件です。		
	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。
	システム中断時	システムの中断に、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。
	契約終了時	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。

別紙3 セキュリティ要件

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、不正が見つかったときに、追跡調査等、本市とシステム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、システム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、システム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	アクセスログが1年以上保存されていること。