（別添3）セキュリティ要件一覧票

No.	カテゴリ	機能要件
1	情報セキュリティ	一定時間操作がない場合に、自動的にログアウトされること。
2	情報セキュリティ	ネットワーク通信が暗号化されていること。
3	情報セキュリティ	ハードウェア（サーバ、ストレージ、ネットワーク等）が冗長化されていること。
4	情報セキュリティ	ログインやログアウトの利用状況等、外部からの非定期的なアクセス等のセキュリティ事象・ログデータを記録し、本市の求めに応じて提供できること。なお、タイムゾーンは日本標準時で統一すること。
5	情報セキュリティ	ユーザーのアクセスログや操作ログについて、最低１年間は記録し、本市の求めに応じて提供すること。
6	情報セキュリティ	バックアップデータは日次取得することとし、7世代以上のデータを保管すること。また、人事異動等の年次処理時など本市の求めに応じて、バックアップデータを提供すること。
7	情報セキュリティ	バックアップデータは遠隔地保管とすること。
8	情報セキュリティ	サーバに格納するデータは暗号化されていること。
9	情報セキュリティ	機密性の高い情報資産をインターネットに接続しているサーバ等の公開領域に保管しないこと。また、データベースサーバー等は、ファイアウォール等によりインターネットと分離されたセグメントに設置し、不要なアクセスは遮断すること。
10	情報セキュリティ	事業者は定期的（年1回以上）に第三者による脆弱性診断を行い、指摘項目の改修等を行うこと。なお、改修等の費用は事業者にて負担すること。
11	情報セキュリティ	本市が使用している人材マネジメントシステムと自動データ連携（API連携）を行う際の認証方式について、単なるID・パスワードのみの認証ではなく、2つ以上のAPI認証キーを設定し、連携できること。
12	データセンター	使用データセンターは、事業者にて用意すること。また、データセンターは日本国内に立地し、物理的なデータの保管場所が日本国内であること。立地条件は地盤、周辺環境の観点で安全であること。（ISMAPリストに登録されたデータセンターであれば可。以下No.20まで同じ。）

No.	カテゴリ	機能要件
13	データセンター	データセンターには非常用電源設備が設置されていること。
14	データセンター	データセンターは震度6以上の耐震もしくは免震設計であること。
15	データセンター	データセンターはDDos攻撃対策、OS・ミドルウェアのパッチ管理等が適切になされていること。
16	データセンター	データセンター内は常駐要員もしくは監視カメラによる監視が行われていること。
17	データセンター	従業員に対して、事故発生時の教育・訓練が定期的に実施されていること。
18	データセンター	1年365日、1日24時間運用可能である（保守作業による停止は1～2回／年とし、計画的に行っている）こと。
19	データセンター	データセンターへの入退室管理が適切であること。
20	データセンター	システムを運用するオペレーションが日本国内で実施されていること。
21	その他クラウドサービスのセキュリティ	クラウドサービスにおけるセキュリティ対策が公開されていること。
22	その他クラウドサービスのセキュリティ	事故予防策が策定され、適切に運用されていること。
23	その他クラウドサービスのセキュリティ	事故発生時・発生後の対策が策定され、訓練の結果が反映されていること。