別表3　セキュリティ要件

1　情報セキュリティを確保するための体制	
1-1	本業務の作業実施体制・連絡体制を提示すること。なお、セキュリティ対策の責任者にはセキュリティ対策を十分に管理できる者を配置すること。
1-2	本業務の一部を合理的な理由及び必要性により再委託する場合には、セキュリティ対策が確認できる資料を提出し、委託者の承認を受けること。また、受託者は、再委託先の行為について一切の責任を負うこと。
1-3	情報セキュリティインシデントが発生した場合は連絡体制表に基づき速やかに委託者に報告すること。なお、不正アクセス、サービス不能攻撃、不正プログラムの感染等、短時間で被害が拡大する情報セキュリティインシデントについては緊急時対策を受託者が行うこと。
2　ウイルス対策	
2-1	サーバのウイルス感染を防ぐため、ウイルス対策ソフトを導入すること。
2-2	最新のウイルスパターンファイルを取得し、サーバ等にインストールすること。
2-3	システムへの影響を考慮し、必要に応じて OS 等の修正 プログラムを適用すること。
3　情報の改ざん防止	
3-1	不正アクセス等を防止するため、ファイアウォールを設置すること。
3-2	IDが不要となった場合は、速やかに削除が可能であること。
3-3	ホームページ 等 の管理に必要な通信は、保守を担当する委託業者の固定 IP アドレスからの接続のみを許可し、通信は暗号化すること。
3-4	知識情報、所持情報、生体情報を利用する認証手段のうち２つ以上を併用する多要素認証を備えること。もしくは、パスワードは英数字と記号を含めたのものが設定可能であり、かつ、認証に何回か失敗したらロックする機能を有していること。
3-5	「いつ」「誰が」「何を」したかを特定できるように情報システムへのアクセス状況を適切に記録し、管理すること。
3-6	Ｗｅｂアプリケーション診断及びネットワーク診断を少なくとも年１回以上実施して、ぜい弱性を把握し、早期に対策を行うこと。
3-7	以下のセキュリティ対策を実装する 。 ・不要なポートの閉鎖 ・ウェブページのデータの不正な書換えの検出 ・重要なシステムの設定を行ったファイルに対する定期的な改ざん有無の検査
4　情報漏えい対策	
4-1	本業務の遂行に当たり知りえた全ての情報は、履行期間及び履行後において第三者に漏らしてはならない。データの取扱についても同様とする。また、秘密保持及びデータの取扱について、従業員その他関係者への徹底を行うこと。
4-2	Ｗｅｂブラウザを利用するシステムにＴＬＳ を使用し、Ｗｅｂサーバ及び端末間の通信を暗号化すること。

5　運用ルールの確立	
5-1	情報システムの運用に関し、クラウドサービス等のサービス変更、終了時の事前告知及び問い合わせ先、サービス提供時間、サービス稼働状況の監視、ID及びパスワードの盗難によるなりすましへの対策等の必要な事項を定めた運用基準を策定しなければならない。
6　物理的技術対策	
6-1	サーバを設置する部屋は、ＩＣカード等による電子錠の開閉及び入退室記録が収集可能な入退室管理システムを導入し、入退室日時及び入退室者の記録を管理すること。
6-2	入退室管理と組み合わせ、職員や警備員を配置することによる有人監視又は監視カメラによる監視を行い、管理区域への入退室者の 本人性確認又は映像の記録及び監視を行うこと。
6-3	入退室記録は１年間、映像記録は３ヶ月間保存し管理を行うこと。
6-4	サーバは、CVCF（Constant Voltage Constant Frequency）や非常用発電機等から安定した電力を継続的に供給可能な場合を除き、無停電電源装置を設置すること。
6-5	サーバは、震度６弱でも耐えうるような対策を行うこと。
6-6	設置する機器への影響を考慮し、サーバを設置する部屋は、目安として 18～ 27 ℃以内を保持するよう管理する。また、結露による影響を受ける場所を避け、湿度は、目安として20％～60％以内で管理すること。
7　システム開発・構築における技術対策	
7-1	管理者権限と一般利用者権限を分けることが可能であること。
7-2	複数のハードウェアで業務処理を実行し、一部のハードウェアが故障しても業務処理に影響なく運用できるようシステム構成を冗長化する。
7-3	ハードウェア 故障時に早急な復旧を行うため、システム構成の全て又は一部の代替設備を用意する。
7-4	通信回線二重化 （バックアップルート）を行い 、 回線障害時に切替えること。
7-5	電源ユニットを複数台設けることにより、電源ユニットの故障時にも、停止することなく運用することができること。
8　システム運用における技術対策	
8-1	バックアップ運用を定期的に実施すること。なお、世代管理は２世代以上で運用すること。
9　その他	
9-1	サーバの設置国は日本国内とする。
9-2	情報システムを設置する管理区域の管理、情報システムの運用及び情報セキュリティ対策は委託先、情報システムの利用は札幌市で行う。
9-3	受託者の責に起因する情報セキュリティインシデントが発生するなどの万一の事故があった場合は直ちに報告する義務や、損害に対する賠償等の責任を負うこと。