別紙3　情報セキュリティ要件一覧

No	区分	要件概要
	セキュリティ基本要件	
1	基本方針 （情報セキュリティポリシー）	情報セキュリティについての基本的な方針を定めた文書等（情報セキュリティポリシー）を策定していること。
2	情報セキュリティ対策	情報セキュリティについての具体的な対策を計画書等に記載するなど、予め本市に示すこと。
3	変更時の報告	業務実施方法、サービスの提供に関する重大な変更が生じる場合は、あらかじめ本市に報告し、同意を得ること。
4	リソースの確保	利用者が快適に利用するために必要なリソースの容量・能力を確保すること。利用において必要な監視機能を確認するとともに、監視により業務継続の上で必要なる容量・能力を予測し、業務が維持できるように努めること。
5	堺市情報セキュリティポリシー	本市の情報セキュリティポリシーに従った利用が可能であること。
6	SLA	サービス品質保証（SLA：Service Level Agreement）を定め、本市の合意を得ること。
7	情報セキュリティポリシーの遵守、点検	取り扱う各情報について、管理責任者を定めると共に、取扱いの慎重さの度合いや重要性の観点から各情報を分類すること。 分類した情報に対する閲覧可能者、閲覧目的、閲覧方法等を明確にし文書化すること。
8		各情報における管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、定期的にレビュー及び見直しを行うこと。
	第三者評価	
9	監査、評価等	情報セキュリティに関するルールの遵守について、定期的に内部監査を実施する等、情報セキュリティに関する内部統制を行っていること。また、当該内部統制の概要について本市に報告すること。
10		外部機関による情報セキュリティ監査を定期的に受けている、又は外部機関による定期的な審査を伴う情報セキュリティ評価制度の認証を取得している。また、当該事実を確認できる資料を本市へ提示すること。
11		ISMAP等クラウドサービスリストに掲載されていること、または、ISO27001等、本市が認める情報セキュリティ評価制度の認証を取得していること。
	情報資産要件	
12	情報資産のバックアップ等	データ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること（申請情報、ユーザ情報、申請書（帳票）データなど）。なお、バックアップデータはネットワークから隔離し保存する、WORM方式で保存するなど、ランサムウェア等のマルウェア対策を講じること。
13		バックアップの頻度、バックアップデータの保存期間、バックアップデータからのリカバリー方法などを報告し、本市の承諾をえること。また、報告内容に変更がある場合は、事前に報告すること。
14		バックアップデータはサービスの提供に支障のないよう自動的に取得すること。
15		バックアップデータを格納した媒体は、厳重に管理すること。
16		バックアップにNetwork Attached Storage等のネットワークに直接接続して使用するファイルサーバを利用する場合、予め決められた者以外、操作できない措置を講じ、不正アクセス防止の措置をとること。
17	提出データの暗号化	本市へデータの提出を行う際は、パスワードの設定等データの暗号化を講じること。

別紙3　情報セキュリティ要件一覧

No	区分	要件概要
18	機器･媒体等の管理と廃棄	利用する情報資産（機器等）の交換または処分（廃棄）する場合の取扱いが、本市情報資産の漏えいが発生しない方法であることを計画書等に記載するなど、予め本市に示すこと。
19		紙、磁気テープ、光メディア等の媒体の運用手順書を作成し保管管理を適切に行うこと。 また、定められた区域外に持ち出さないこと。
20		機器及び媒体を正式な手順に基づいて廃棄すること。
人的セキュリティ要件		
21	業務従事者に係る情報セキュリティ	本契約の従事者に対して、情報セキュリティポリシーに関する意識向上のための適切な教育･訓練を実施すること。
22		本契約の従事者が、情報セキュリティポリシーもしくはサービス提供上の契約に違反した場合の対応手続を備えること。
23		本契約の従事者が、本契約への従事で知り得た情報を外部へ漏えいしないこと。
24		本契約の従事者に対して、機密性･完全性･可用性に係る情報セキュリティ上の要求及び責任の分界点を提示･説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。
25		本契約の従事者でなくなった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること。
物理的セキュリティ要件（データセンター）		
26	設置環境等	データセンターは、日本国の法律が及ぶ範囲に設置すること。
27		建物及び部屋は、火災、水、落雷、電界、磁界及び空気汚染の被害を受ける恐れのない場所に設けられていること。
28		外部及び共用部分に面する窓は、防災、防犯の措置及び外光による影響を受けない措置が講じられていること。
29		データセンタへの入室可能な者を明確に定め、それ以外の者がアクセスできない措置を講じていること。
30		出入り口は、不特定多数の人が利用する場所を避けるとともに入退室を許可された外部組織等に対する入退室記録･管理を行うこと。
31		入退室等を管理するための手順書を作成すること。
32		サーバルームやラックの鍵管理を行うこと。
33		本市が実施するデータセンタへの立ち入り検査を認めること。 なお、その際にサービスの提供設備、その他運用状況の確認が行えること。 もしくは、外部機関による監査の検査内容及びその結果を報告し、本市の承認を得ること。
34		建物及び部屋は、建築基準法に規定する耐火性能を有すること。
35		建物及び部屋は、水の被害を防止する措置が講じられていること。
36		建物及び部屋の内装、什器･備品は、不燃、防災性能を有する材料を用いるとともに静電気による影響を防止する措置が講じられていること。

別紙3　情報セキュリティ要件一覧

No	区分	要件概要
37		建物及び部屋は、避雷設備、火災報知設備、消化設備、非常照明設備、避難器具、小動物被害防止等の建築設備が設置されていること。
38		提供システムの設置に必要十分な空間が確保されていること。左右いずれかの側面または別のルートから、背面作業スペースへの進入経路が確保されていること。
39	情報漏えい、盗難対策	情報漏えい、記録媒体の盗難防止措置が講じられていること。
40	電気設備	受電容量は建物全体として十分な容量が確保されていること。また建物における電気点検は、機器設備（サーバ、ネットワーク等）を停止せずに実施すること。
41		非常用発動発電機を備え、非常時に機器設備の受電容量をまかなえること。
42		UPSを備え、非常時に非常用発動発電機が起動するまでの間、機器設備に電源を提供できること。
43	空気調和設備	システム周囲環境温度は摂氏0度から40度、湿度30%から80%の範囲で常に安定的に保持するとともに、結露が発生しない動作環境であること。特に夏季においては室内の換気が十分に確保されていること。
44		空気調和設備は、防災、防犯及び水漏れ防止の措置を講じていること。
45	監視設備等	建物及び部屋の人の出入り、防災設備及び防犯設備の作動、電源設備及び空気調和設備の稼働状況について適切な監視が可能であること。
46	地震対策	建物は、建築基準法に規定する耐震構造、免震構造又は制震構造であること。
47		開口部、内装、設備、什器・備品は、落下、転倒及び振動等地震による被害を防止する措置を講じていること。
	技術的セキュリティ要件	
48	冗長化	サービスを安定して利用するために必要な冗長化対策を講じること。
49	ネットワーク構成	ネットワーク構成図を作成すること。ネットワーク構成に変更があった場合は、本市へ報告すること。またアクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。
50	回線の要件	本市のネットワークに接続する回線は、専用線または広域イーサ等閉域網による専用線に準ずる回線とする等、宛先を特定すること。 無線LANは使用しないこと。
51	接続先ネットワークの制限	本市が予め認めているネットワーク以外へ、システムからの能動的な接続ができないこと。
52	不正プログラムへの対策	不正プログラムへの対策を確実に実施すること。
53	その他の不正アクセス防止	外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。
54	権限の割当	権限の割当一覧を作成して管理すること。 また、管理者の権限の割当及び使用を必要最小限に制限すること。

別紙3　情報セキュリティ要件一覧

No	区分	要件概要
55	アクセス管理	市職員及び管理者（情報システム管理者、ネットワーク管理者等）のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。
56		パスワードを認証要素とする場合は、パスワードの桁数、文字種等、複雑性をシステム側で制御できること。
57		認証手段が漏えいする等、不正アクセスの危険が生じた場合、アカウントの利用停止が容易にできること。
58	ログの管理	システム利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得すること。
59		情報資産へのアクセス履歴、システム・各種機器等の操作履歴（ログ）を取得すること。
60		取得した各種ログは90日以上保存すること。また、ログを改ざんされないような対策を講じること。
61		本市の監査及びデジタルフォレンジックに必要となるログ等の情報（デジタル証拠）を本市の求めに応じて速やかに提供すること。
62	時刻同期	サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器等の時刻同期が確実に行われるための対策を講じること。
63	技術的ぜい弱性対策	サービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。
64	法令と規則の遵守	サービスの提供及び継続上重要な記録（データベース記録、監査ログ、運用手順等）は、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。
	運用・管理要件	
65	不正侵入監視	不正侵入検知ネットワーク上のトラフィックを監視し、不正侵入検知を行うこと。不正侵入の兆候を検知した時は、直ちに侵入及び実行を防止するための対策を講じること。
66	不正改ざん検知	サーバ上にあるファイルの改ざん通知を行うこと。改ざんを検知した時は、修復もしくは代替ファイルへの移行を行うこと。
67	稼動監視	サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器等の稼働監視（応答確認等）を行うこと。 稼働停止を検知した場合は、本市に速報するとともに、直ちに対処すること。
68	障害監視	サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器等について、ログ監視を含む障害監視（サービスが正常に動作していることの確認。）を行うこと。 障害を検知した場合は、本市に速報するとともに、直ちに対処すること。
69	ログ監視	不正侵入、稼働停止、システム障害等の検知に当たり、ログ監視を実施すること。また不正ログ検知時には本市に速報するとともに、直ちに対処すること。
70	監視結果報告	サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器等に係る稼働停止、障害、パフォーマンス低下等について、本市に詳細を報告すること。
71	監視手順書等	情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。 また、サービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークの運用・管理に関する手順書を作成すること。
72	インシデント対応	情報セキュリティインシデントを検知した場合、検知した内容、被害状況、対応予定等、本市が必要とする情報を、本市に速報すること。
73	インシデント調査	検知した情報セキュリティインシデントを速やかに調査し、調査結果の詳細を本市に報告すること。

別紙3　情報セキュリティ要件一覧

No	区分	要件概要
74	ウィルス対策	サービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。万が一、ウイルスの感染を検知した場合は、直ちに必要な対策を講じること。
75		ウイルス対策ソフトを導入し、ウイルス定義ファイルを定期的に最新化すること。また、全てのファイルのウイルスチェックを定期的に行うこと。
76	リカバリ	障害発生時には、迅速にシステムが復旧できるようしておくこと。
77	事業継続性	BCP対策として、停電や災害時でも業務を継続可能なこと。
	運用・端末におけるセキュリティ要件	
78	端末の設置場所	重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、本契約の従事者及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。
79		重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像を予め定められた期間保存すること。
80		重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること。
81	プログラム管理	運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。 従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを定期的に行うこと。 技術的脆弱性に関する情報（OS、ソフトウェアのパッチ情報等）を定期的に収集し、随時更新を行うこと。
82	アクセス管理	リモートでアクセスできるサーバを限定すること（業務範囲に限る）
83		保守対象サーバに接続できる端末を制限すること。
84		パスワードは厳重に管理し、定期的に変更すること。 パスワードが漏えいした場合に備えて、必要な対策を講じること。 パスワードの桁数は8桁以上とし複雑性（英小文字、英大文字、数字、記号）を強制すること。
85	ログの管理	端末操作履歴（ログ）を取得し、予め定められた期間保存すること。
86	特権ID管理	特権IDの付与は必要最小限とし、特権ID情報の漏えい対策を講じるとともに、操作ログの監視など、不正利用を検知・防止する措置を講じ、適切にIDの管理を行うこと。
87	端末管理	端末の盗難防止対策を講じること。 予め定められた者以外、操作できない措置を講じること。 不要なデバイスが利用できない措置を講じること。
88	通信の暗号化	外部端末と機器設備のサーバ間通信において、電気通信事業者の通信改正を使用する場合は、IPsec-VPN等を用いる等の対策を講じ、情報漏えい・不正アクセス等を防止すること。