【別紙4】情報セキュリティ要件一覧

| 項番 | 区分 | 要件概要 | リモート保守要件 | データセンター利用要件 | クラウドサービス利用要件 |
|---|---|---|---|---|---|
| | **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（情報セキュリティポリシー）を作成すること。 | ○ | ○ | ○ |
| 2 | | 情報セキュリティに関する基本的な方針を定めた文書は、定期的又はサービスの提供に係る重大な変更が生じた場合（組織環境、サービス提供環境、法的環境、技術的環境等）に見直しを行うこと。この見直しの結果、変更の必要性が生じた場合には、改定等を実施すること。 | ○ | ○ | ○ |
| 3 | 情報セキュリティポリシーの遵守、点検及び監査 | 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。<br>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。 | ○ | ○ | ○ |
| 4 | | 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。 | ○ | ○ | ○ |
| 5 | | サービスの提供に用いる情報システムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に点検・監査すること。 | ○ | ○ | ○ |
| 6 | 業務従事者に係る情報セキュリティ | 業務従事者に対して、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。 | ○ | ○ | ○ |
| 7 | | 業務従事者に対して、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。 | ○ | ○ | ○ |
| 8 | | 業務従事者が、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。 | ○ | ○ | ○ |
| 9 | | 業務で知り得た情報の外部への漏えいを防止すること。 | ○ | ○ | ○ |
| 10 | | 業務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。 | ○ | ○ | ○ |
| 11 | 情報セキュリティインシデント及びぜい弱性の報告 | 業務従事者に対し、サービス提供において発見あるいは疑いをもった情報システムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続きを定め、実施を要求すること。<br>報告を受けた後に、迅速に整然と効果的な対応ができるよう、責任体制及び手順を確立すること。 | ○ | ○ | ○ |
| 12 | 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）については、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。 | ○ | ○ | ○ |
| 13 | | 日本国の法律が及ぶ範囲に設置すること。 | ○ | ○ | ○ |
| | **物理的セキュリティ要件（ハウジング、クラウド）** | | | | |
| 14 | 設置環境 | 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。 | － | ○ | ○ |
| 15 | | 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。 | － | ○ | ○ |
| 16 | | 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。 | － | ○ | ○ |
| 17 | | 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。 | － | ○ | ○ |
| 18 | | 端末を設置する場所は、入退室管理を実施している管理区域であること。 | － | ○ | ○ |
| 19 | | 入退室等を管理するための手順書を作成すること。 | － | ○ | ○ |
| 20 | | サーバルームやラックの鍵管理を行うこと。 | － | ○ | ○ |
| 21 | | 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。<br>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。<br>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。 | － | ○ | ○ |
| 22 | | 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。 | － | ○ | ○ |
| 23 | | 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。 | － | ○ | ○ |
| 24 | | 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。 | － | ○ | ○ |
| 25 | | 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。 | － | ○ | ○ |
| 26 | | 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。 | － | ○ | ○ |
| 27 | | 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。 | － | ○ | ○ |
| 28 | | 通信回線の建物への引き込みは地下埋設(通信ケーブル用トンネル経由で収容)とすること。また、複数事業者の引き込みが可能であること。 | － | ○ | ○ |
| 29 | 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。 | － | ○ | ○ |
| 30 | | 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。 | － | ○ | ○ |
| 31 | | 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。 | － | ○ | ○ |
| 32 | 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。 | － | ○ | ○ |
| 33 | | 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。 | － | ○ | ○ |
| 34 | 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。 | － | ○ | ○ |
| 35 | 地震対策 | 建物は、建築基準法に規定する耐震構造であること。 | － | ○ | ○ |
| 36 | | 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** | | | | |
| 37 | 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、通信機器の稼働監視（応答確認等）を行うこと。<br>稼働停止を検知した場合は、本市に速報を通知すること。 | － | ○ | ○ |
| 38 | 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、通信機器の障害監視（サービスが正常に動作していることの確認）を行うこと。<br>障害を検知した場合は、本市に速報を通知すること。 | － | ○ | ○ |
| 39 | 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・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。 | － | ○ | ○ |
| 40 | 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、随時パッチ等による更新を行うこと。 | － | ○ | ○ |
| 41 | 追加報告 | 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・ストレージ等（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、速報をフォローアップする追加報告を本市に対して行うこと。 | － | ○ | ○ |
| 42 | 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。<br>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。 | － | ○ | ○ |

| 項番 | 区分 | 要件概要 | リモート保守要件 | データセンター利用要件 | クラウドサービス利用要件 |
|---|---|---|---|---|---|
| | **運用・管理要件** | | | | |
| 43 | 利用設計 | 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・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。 | － | ○ | ○ |
| 44 | アクセス管理 | 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。<br>また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。<br>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。 | － | ○ | ○ |
| 45 | | 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）。 | － | ○ | ○ |
| 46 | | 保守対象サーバに接続できる端末を制限すること。 | － | ○ | ○ |
| 47 | | パスワードは厳重に管理し、定期的に変更すること。 | － | ○ | ○ |
| 48 | | 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。 | － | ○ | ○ |
| 49 | ログの管理 | 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。 | － | ○ | ○ |
| 50 | | 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。 | － | ○ | ○ |
| 51 | ウイルス対策 | 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。 | － | ○ | ○ |
| 52 | | 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。 | － | ○ | ○ |
| 53 | データの保護 | 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） | － | ○ | ○ |
| 54 | | 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、本市の承認を得ること。また、報告内容に変更がある場合は、事前に報告すること。 | － | ○ | ○ |
| 55 | | 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。 | － | ○ | ○ |
| 56 | | 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。 | － | ○ | ○ |
| 57 | | 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。 | － | ○ | ○ |
| 58 | | 契約を終了した場合は、本市に関連するすべてのデータを削除し、削除の証明書を本市に提出すること。 | － | ○ | ○ |
| 59 | 媒体の保管と廃棄 | 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。<br>また、定められた区域外に持ち出さないこと。 | ○ | ○ | ○ |
| 60 | | 機器及び媒体を正式な手順に基づいて廃棄すること。また、データは復元不可能な方法で消去した上で廃棄すること。 | ○ | ○ | ○ |
| 61 | | 媒体にアクセスできる者を予め限定しておくこと。 | ○ | ○ | ○ |
| 62 | 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。 | － | ○ | ○ |
| 63 | 事業継続性 | BCP対策として、停電や災害時でもバックアップ拠点にて、業務を継続可能なこと。 | ○ | ○ | ○ |
| | **ネットワーク要件** | | | | |
| 64 | 回線設計 | 冗長化がなされていること。 | － | ○ | ○ |
| 65 | | 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。 | ○ | ○ | ○ |
| 66 | 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、広域イーサ、IP-VPN等閉域網による専用線に準ずる回線とし、宛先を特定すること。また、IP-VPN回線の場合は、通信を暗号化すること。<br>接続先は、管理セグメントに限定すること。<br>無線LANは使用しないこと。 | ○ | － | － |
| 67 | | 本市のネットワークに接続する回線は、専用線、広域イーサ、IP-VPN等閉域網による専用線に準ずる回線とし、宛先を特定すること。また、IP-VPN回線の場合は、通信を暗号化すること。<br>無線LANは使用しないこと。 | － | ○ | ○ |
| 68 | 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。 | ○ | ○ | ○ |
| 69 | 権限の割当 | 権限の割当一覧を作成して管理すること。<br>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。 | ○ | ○ | ○ |
| 70 | 障害通報 | ネットワークの障害を監視すること。障害を検知した場合は速報を本市に通知すること。 | ○ | ○ | ○ |
| | **端末におけるセキュリティ要件** | | | | |
| 71 | 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、業務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。 | ○ | － | － |
| 72 | | 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。 | ○ | － | － |
| 73 | | 端末を設置している管理区域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。 | ○ | － | － |
| 74 | | 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。 | ○ | － | － |
| 75 | プログラム管理 | 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。 | ○ | － | － |
| 76 | | 私物（パソコン、スマホ、ＵＳＢメモリ等）の機器の使用を禁止するとともに受注者の機器（パソコン、スマホ、ＵＳＢメモリ等）の使用を制限すること。 | ○ | － | － |
| 77 | | 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し、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。<br>また、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。ただし、適用することで業務に影響がある場合は、代替策を検討し実施すること。 | ○ | － | － |
| 78 | パスワード管理 | パスワードは厳重に管理し、定期的に変更すること。<br>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。<br>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。 | ○ | － | － |
| 79 | 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。 | ○ | － | － |
| 80 | 端末管理 | 端末の盗難防止対策を講じること。<br>予め定められた者以外、操作できない措置を講じること。<br>不要なデバイスが利用できない措置を講じること。<br>私物（パソコン、スマホ、ＵＳＢメモリ等）の機器の使用を禁止するとともに受注者の機器（パソコン、スマホ、ＵＳＢメモリ等）の使用を制限すること。<br>離席時に端末をログオフ又はロックすること。<br>端末にデータを保存させない措置（仮想もしくはリモートアクセスとし、端末上のハードディスクには情報を置けない措置） | ○ | － | － |
| 81 | インターネット接続の禁止 | インターネットや電子メールなどが利用できない措置を講じること。<br>インターネット及びその他のネットワークに接続しないこと。 | ○ | － | － |