【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
	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。	○
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。 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。	○
	運用・管理要件		
14	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。 また、定められた区域外に持ち出さないこと。	○
15		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。	○
16		媒体にアクセスできる者を予め限定しておくこと。	○
17	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		
18	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。	○
19	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。 接続先は、管理セグメントに限定すること。 無線LANは使用しないこと。	○
20	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。	○
21	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。	○
22	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		
23	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。	○
24		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。	○
25		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。	○
26		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。	○
27	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。	○
28		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。	○
29		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。 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。	○
30	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。 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。	○
31	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(本賃貸借(リース)期間）保存すること。	○
32	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。 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。 離席時に端末をログオフ又はロックすること。 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）	○
33	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。 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。	○