

区分	要件概要
基本情報	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等）を作成すること。
基本情報	情報セキュリティ対策についての具体的な対策を定めた資料を作成し、本市に提供すること。
基本情報	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予め本市に報告し、同意を得ること。
基本情報	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となる容量・能力を予測し、業務が維持できるように努めること。
基本情報	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。
基本情報	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。
第三者評価	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監査を受け、その監査人が発行する監査結果をを本市に報告すること。
第三者評価	外部機関による情報セキュリティ監査の結果を報告し、本市の承認を得ること。
第三者評価	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、本市が認める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	外部サービス利用の終了に関する内容について、以下の記述を含むものをサービス利用前に文書で提出すること。 ①外部サービスの利用を終了する際に、本市が求める他の外部サービス等への情報資産の移行方法 ②複製を含む全ての情報資産の再利用が不可能な方法での削除及びその証明書の提出
情報資産	利用する情報資産（機器等）を交換または処分（廃棄）する場合の取り扱いが、本市情報資産の漏えいが発生しない方法であることを予め本市に書面で示すこと。
物理的セキュリティ	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。
物理的セキュリティ	情報資産は、日本国の法律が及ぶ範囲に設置すること。
人的セキュリティ	外部サービスに従事する者に対して、必要な教育・訓練を実施すること。
人的セキュリティ	外部サービスに従事する者が、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を備えること。
人的セキュリティ	外部サービスに従事する者が、サービスへの従事で知り得た情報を外部へ漏えいしないこと。
人的セキュリティ	外部サービスに従事する者に対して、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。
技術的セキュリティ	外部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。
技術的セキュリティ	不正アクセスを防止するために必要な対策を講じること。
技術的セキュリティ	利用する時刻の同期が確実に行われるための対策を講じること。
技術的セキュリティ	本市が求めるアクセス制御が可能であること。
技術的セキュリティ	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バッチ発行情報等）を定期的に収集し、随時バッチによる更新を行うこと。
技術的セキュリティ	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、アクセス制御となすまし対策を行うこと。
技術的セキュリティ	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。
技術的セキュリティ	情報資産へのアクセス履歴、機器への操作履歴を取得し、本市が求める期間保存すること。履歴を改ざんされないような対策を講じること。
技術的セキュリティ	本市の監査及びデジタルフォレンジックに必要となる外部サービス事業者の環境内で生成されるログ等の情報（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。
技術的セキュリティ	不正プログラムへの対策を確実に実施すること。（複数の外部サービスを組み合わせて構成する場合において、他の外部サービスが不正プログラムへの対策を実施している場合を除く。ただし、その場合は、他の外部サービスが実施する対策に協力すること。）
技術的セキュリティ	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。
技術的セキュリティ	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。
技術的セキュリティ	本市が予め認めているネットワーク以外に接続できないこと。
技術的セキュリティ	バックアップ操作は、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。
技術的セキュリティ	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。
技術的セキュリティ	重要な記録（データベース記録、監査ログ、運用手順等）は、法令又は本市と予め取り決めたルールに従って、適切に管理すること。
技術的セキュリティ	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、宛先を特定できること。
技術的セキュリティ	情報システムが正規の利用者（管理者を含む。）かどうかを判断する認証手段を、二つ以上を併用する認証（多要素認証）とすること。（閉域網で利用する場合を除く。）
運用	外部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）ができること。 稼働停止を検知した場合は、本市に速報できること。
運用	外部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）ができること。 障害を検知した場合は、本市に速報できること。
運用	外部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。
運用	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。
運用	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。