別紙3

No.	要件
1	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。
2	時刻の同期が確実に行われるための対策を講じること。
3	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脆弱性に関する情報（OS、その他ミドルウェア等を含めた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。
4	アクセスを管理するための適切な認証方法、特定のスマートフォン（以下、専用端末）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。
5	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。
6	情報資産へのアクセス履歴、機器への操作履歴、サービスの利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）などを取得し、最低１年以上保存すること。履歴を改ざんされないような対策を講じること。
7	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）をインシデントが起こった際などに本市の求めに応じて速やかに提供すること。
8	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。）
9	外部ネットワーク及び内部ネットワークからの不正アクセスを防止する措置を講じること。 例）ファイアウォール又はリバースプロキシの導入
10	本市の指定する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を実施すること。バックアップの頻度や保存期間について本市の指定する範囲と異なる変更を行う場合はあらかじめ本市の承諾を得ること。
11	クラウドPBXに接続する専用端末は、電子メール機能などクラウドPBX以外に外部に情報を送付する機能を原則禁止すること。外部記録媒体を使用したデータ持ち出しは厳格に制限すること。
12	許可された専用端末のみ外部サービスに接続できる。
13	不要なアプリのインストールを禁止すること。
14	専用端末に業務と無関係もしくは不要なデータのダウンロードを禁止する。（人的セキュリティ対策を含む）
15	専用端末を廃棄する時は物理的に破壊するなど内部データを再度読み込みができない状態で廃棄すること。