【別表１】利用判断基準別表

以下に示す①外部サービス共通の対策を講じてください。

①外部サービス共通

No.	区分	要件概要	備考
1	技術的セキュリティ	外部サービスの停止により市民サービスに多大な影響を与える場合は、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。	
2	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。	
3	技術的セキュリティ	外部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	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、アクセス制御となりすまし対策を行うこと。 認証方法…ID/PWの設定、生体認証及び多要素認証【推奨】、特定の拠点…IPアドレスの制限、クライアント証明書【推奨】	
5	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。	
6	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、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、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	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	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。）	
9	技術的セキュリティ	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	技術的セキュリティ	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	技術的セキュリティ	庁内環境から外部に持ち出したデータについて、インターネット環境にある端末等へのダウンロードを禁止すること。	
12	技術的セキュリティ	特定個人番号を含むデータについて本市と外部サービス環境を接続する際、LGWAN回線またはガバメントクラウド専用線を使用すること。	特定個人情報を扱わないため該当なし
13	技術的セキュリティ	特定個人番号を含むデータについては、インターネット環境にある端末等へのダウンロードを制限すること。	特定個人情報を扱わないため該当なし