船橋市生涯学習施設予約システム更新業務仕様書　別紙3「その他のセキュリティ要件」

No	大区分	小区分	内容
1	クラウドサービス提供者の選定基準	－	日本の法令の範囲内で運用できるサービスであること。また、日本国内の裁判所を合意管轄裁判所とすること。
2	クラウドサービス提供者の選定基準	－	個人情報や住民の生命・財産に関わる情報、その他、非公開情報のデータが保存されるデータセンターは日本国内にあること。
3	クラウドサービス提供者の選定基準	－	利用するクラウドサービスのリージョンを日本国内に限定すること。
4	クラウドサービス提供者の選定基準	－	クラウドサービスの終了又は変更時における事前の通知について以下を例とする取り決めが可能なこと。 当該クラウドサービスの終了又は変更の際には、速やかに電話・メール等で事前に告知すること。
5	クラウドサービス提供者の選定基準	－	クラウドサービス提供者による本市の情報資産の利用は、クラウドサービスの提供に必要な範囲で認めるものであり、それ以外の目的で本市の情報資産の利用は認めない。
6	クラウドサービス提供者の選定基準	－	クラウドサービスの開発及び運用が本市の意図しない変更が行われない一貫した品質保証体制の下でなされていること。 意図しない変更とは非公開設定が説明なく、公開設定になることや本市が保存するデータが意図せず書き換えられること等を想定しており、機能追加等はこれに含まれない。
7	クラウドサービス提供者の選定基準	－	情報セキュリティインシデントの対処について以下を例とする内容を調達仕様に含められること。 情報セキュリティインシデントが発生した際に、クラウドサービス提供者と連絡がつかない、営業時間外の対応が不可能等の状況にならないこと。また、情報セキュリティインシデントによる被害を最小限に食い止めるために情報セキュリティインシデント発生時に以下の対応を行うこと。 ①クラウドサービス提供者が情報セキュリティインシデントを検知した際は、速やかに本市に報告を行うこと。 ②情報セキュリティインシデントが発生した際に、運用状況・影響範囲調査等、事案解決のために積極的に調査を行うこと。 ③情報セキュリティインシデント発生後、遅くとも1時間以内に調査に着手すること。 なお、情報セキュリティインシデントの疑いに対する連絡を受けた場合も同様に調査に着手すること。 ④当該事案の原因特定のため、各種システムログを取得すること。また、取得したログの分析に必要な情報を提供すること。 ⑤調査の結果、サービス停止等の措置が必要な場合は、市担当者に報告した上で速やかにその対応を行い、インシデント収束後、速やかに復旧を行うこと。 ⑥調査の結果、ファームウェア・ソフトウェア等のバージョンアップ等が必要となった場合は、速やかに対応すること。
8	クラウドサービス提供者の選定基準	－	再委託が発生する場合、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されていること。
9	クラウドサービス提供者の選定基準	－	再委託が発生する場合、再委託先の情報セキュリティ対策の実施状況を確認するために次をはじめとした情報を本市に提供可能であること。 ・再委託先事業者情報 ・再委託内容 ・再委託先の情報セキュリティ責任者 ・再委託先の個人情報管理者 ・再委託先の従事者の情報　　等
10	導入・構築時の対策	アクセス制御に関する事項	システム事業者等の特権アカウントがクラウドサービスに接続する際は、強化された認証技術（多要素認証等）を用いること。 （例）生体認証または証明書等の入った端末からの接続＋ID/パスワード認証
11	導入・構築時の対策	アクセス制御に関する事項	クラウドサービスに影響を与える操作（サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除・クラウドサービス利用の終了手順・バックアップ及び復旧等）について、誤操作を抑制するための手順書の作成や誤操作を認識可能なアラート等を実装する等の対策を行うこと。
12	導入・構築時の対策	アクセス制御に関する事項	クラウドサービスが利用する仮想マシンに対して適切なセキュリティ対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策、ログ取得等の実施）を行うこと。 ※事業者が提供するクラウドサービスがSaaSの場合は、上記の対応がクラウドサービス基盤側で提供されていること。
13	導入・構築時の対策	暗号化に関する事項	取り扱う情報の機密性に応じた保護のための適切な暗号アルゴリズム（CRYPTRECにより安全性及び実装性能が確認された「電子政府推奨暗号リスト」）を用いた暗号化処理（情報が保存されている場合、情報が通信され転送されている場合等フローに応じた暗号化）を行うこと。
14	導入・構築時の対策	設計・設定及び開発に関する事項	クラウドサービス内において確実に時刻同期を行い、取得するログの時刻、タイムゾーンを統一すること。
15	運用・保守時の対策	資産管理に関する事項	当該クラウドサービスに関連する脆弱性が見つかった場合は情報の提供を行うこと。また、クラウドサービス提供者の責任範囲で発生した脆弱性対応が迅速に行われること。
16	運用・保守時の対策	暗号化に関する事項	鍵管理機能をクラウドサービス提供者が提供するものを利用する場合、鍵の生成から廃棄に至るまでのライフサイクルにおける仕組みにリスク（鍵が窃取される可能性や鍵生成アルゴリズムの危殆化の可能性等）がないこと。
17	運用・保守時の対策	クラウドサービス内の通信に関する事項	他の利用者が市のデータにアクセスできないよう確実な制御を行っていること。
18	更改・廃棄時の対策	クラウドサービスで取り扱った情報の廃棄に関する事項	クラウドサービスの利用終了時に、クラウドサービスで取り扱った業務に関わる全ての情報が、クラウドサービス基盤上から確実に削除可能であること。なお、削除する対象はバックアップ等により複製されたものにも及ぶ点に注意すること。 削除にあたっては、情報資産を暗号化した鍵（暗号鍵）を削除するなどにより、復元困難な状態としなければならない。
19	更改・廃棄時の対策	クラウドサービスで取り扱った情報の廃棄に関する事項	クラウドサービスの基盤となる装置等の処分についてセキュリティを確保した対応が行われること。 ※事業者が提供するクラウドサービスがSaaSの場合は、上記の対応がクラウドサービス基盤側で提供されていること。
20	更改・廃棄時の対策	クラウドサービスで取り扱った情報の廃棄に関する事項	クラウドサービスの利用終了時に、情報の廃棄の実施報告書を提出すること。
21	更改・廃棄時の対策	クラウドサービスで取り扱った情報の廃棄に関する事項	クラウドサービス利用者の各アカウント以外に特殊なアカウント（ストレージアカウントなど）がある場合は、関連情報（資格情報等）含めて廃棄可能であること。