セキュリティ要件

導入		
No	**区分**	**セキュリティ要件**
1	認証・認可	IDの発行から廃止までのライフサイクル管理および適切なアクセス制御が実装されていること。
2	認証・認可	サービス提供者等の管理者等の特権アカウントは多要素認証等の強化された認証方式を採用していること。
3	操作統制	重要操作に対する誤操作防止または検知の仕組みが備えられていること（手順書の作成や誤操作を認識可能なアラート等）。
4	基盤保護	仮想マシン等の基盤に適切なセキュリティ対策が講じられていること。
5	クラウド要件	インターネット回線から庁内通信回線を経由せずクラウドサービス上で提供する構成について、情報セキュリティ上のリスク評価を実施し、その妥当性を説明できること。
6	暗号化	情報の機密性に応じ、適切な暗号化が実装されていること。
7	暗号化	安全性が確認された暗号技術を採用していること。暗号アルゴリズムは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」に掲載された方式を採用していること。
8	リスク分析	設計段階から脅威分析を実施し必要な対策を設計に反映していること。
9	ログ設計	取得すべきログの種類・範囲が定義されていること。
10	時刻管理	ログの時刻同期およびタイムゾーン統一が行われていること。
11	設計管理	設計レビューや標準フレームワークとの比較検証を実施していること。
12	開発管理	安全な開発手順またはフレームワークを活用していること。
13	ライセンス管理	クラウドサービス上に他ベンダが提供するソフトウェア等を導入する場合、ライセンス規定を確認・遵守していること。
14	通信監視	異なるネットワーク間の通信（トラフィック）を監視すること。
15	データ容量	利用者数及びデータ量の増加に応じて、通常の保育業務に支障が生じない性能を確保できること。クラウドサービスの利用状況（ストレージ使用量等）について、本市から求めがあった場合、合理的な範囲で情報提供できること。
16	業務継続性	クラウドサービスの障害等が発生した場合においても、業務への影響を最小限とする体制を有すること。バックアップ取得及び復旧手順を有していること。
17	可用性設計	必要な可用性（冗長構成等）を考慮した設計であること。
18	データ所在	国内リージョンで運用し海外保存を行わないこと。データセンターは、JDCC（日本データセンター協会）のデータセンターファシリティスタンダードTier3相当の要件を満たすこと
19	目的外利用防止	クラウド提供者が目的外アクセスを行わない規定があること。
20	不履行対応	セキュリティ対策不十分時の対処方法が規定されていること。
21	侵入・攻撃対策	不正アクセスやサイバー攻撃等を想定した監視および対策が講じられていること。
22	侵入検知	クラウド基盤で不正侵入検知・防止のための技術的対策が講じられていること。
23	法令遵守	日本法および日本裁判管轄が適用されること。
24	認証取得	ISO27001等の認証を取得していること。

セキュリティ要件

25	確認資料	セキュリティ対策を資料で確認可能であること。
26	テナント分離	園単位でデータが論理的に分離されていること。
27	閲覧権限	保護者が利用する機能は、各幼稚園が発行するユーザ以外は利用不可とし、ユーザであっても、所属する幼稚園で取り扱っている情報及び自身の子供の情報以外の閲覧、利用ができないこと。
運用・保守		
No	**区分**	**セキュリティ要件**
28	責任分界	クラウド基盤との責任分界点が明確であること。
29	SLA管理	サービスレベルを定期確認できること。
30	インシデント対応	インシデント発生時の責任分担と連絡体制を明確にすること。
31	利用者対応	利用者（在園児の保護者等）にシステムサービス（保護者アプリ）を周知できるマニュアルを提供できること。
32	利用者対応	利用者（在園児の保護者等）に情報セキュリティリスク、リスク対応について利用規約等において提供すること。
33	利用者対応	クラウドサービスを在園児の保護者等が利用するにあたって、周知すべき法令や規制に関する情報を、利用者（市）に提供できること。
34	脆弱性対応	クラウドサービス上で利用するIT資産が脆弱性やセキュリティインシデントによって影響を受ける場合に備え、クラウドサービス提供者と利用者（市）の責任範囲を明確に定めていること。
35	情報分類・取扱管理	クラウドサービス上に保存される情報について、個人情報の有無や機微性の高低などに応じて分類（格付け）し、取り扱い制限や管理方法を定めていること。
36	アクセス管理・操作ログ	システム管理者権限（特権アカウント）について、付与・変更・削除の管理ルールを定め、操作に関するログを取得・保管していること。
37	アクセス権限の定期レビュー	利用者（市の個別職員アカウント）ごとに割り当てたアクセス権限について、異動・退職などの状況を踏まえ、定期的に見直しを行い適切に管理できる構造であること。
38	変更管理	設定変更ユーティリティの利用制限が行われていること。
39	アクセス監視	アクセスログ、操作ログ等が取得・管理され、不正または異常な利用が確認された場合には、速やかに対応するとともに、本市へ報告する体制であること。
40	ログ情報	サービス提供者が保有するログ情報を、必要性に応じて遅滞なく提供（または報告）できること。
41	暗号化確認	保存データの暗号化方式および鍵管理方法を確認できること。 から変更。AWSの鍵方式を細かく業者が説明できないから、変更も妥当性があると判断。
42	鍵管理	鍵管理機能利用時のリスク確認が行われており、クラウド提供者の仕様に基づき適切に鍵のライフサイクル管理が実施されていることを、サービス仕様書等で確認できること。
43	ネットワーク分離	他利用者との論理的分離が確保されていること。
44	設定誤り防止	クラウド提供者側における基盤設定変更時の承認フローの確立や、利用者側の重要設定変更時の警告表示等、設定誤りを防止・検知する対策が講じられていること。
45	基盤の論理分離	仮想ネットワークが他利用者と論理的に分離されていること。
46	規約変更管理	利用規約変更時の確認方法が定められていること。
47	バックアップ	全体的なバックアップを適切に実施すること。
48	復旧手順	業務に支障が出ない稼働率を確保しており、障害発生時にはサービス提供者が速やかに通知を行う体制が整備されていること。また、障害発生時の復旧手順が策定され、定期的な訓練が実施されていること。

セキュリティ要件

49	復旧手順	クラウド基盤の設定やバージョンの変更が業務に影響する可能性を想定し、必要に応じて復旧手順の確認が行われていること
50	容量監視	データ容量や性能影響について、本市から求めがあった場合、または容量の閾値を超過する恐れがある場合は、速やかに利用状況に関する報告を行うこと。
51	インシデント対応	システム利用者（市）が利用者（園児の保護者等）からシステムインシデント報告を受けた場合の、クラウドサービス提供者への報告経路や対応について定めていること。
52	マルウェア対策	サーバ環境でマルウェア対策が実施されていること。
53	パッチ管理	OS等に対するパッチ適用体制を有すること。
54	脆弱性管理	脆弱性情報収集および診断を実施し、対策を行う体制であること。
55	ログ保全	ログの改ざん防止および一定期間保管が行われていること。
56	監視体制	クラウド基盤を含む監視体制が整備されていること。
57	変更管理	仕様変更時の影響確認およびロールバック手順があること。
58	利用ドメイン提供	利用に必要なドメイン一覧を提供できること（本システムを利用する端末においてMDMホワイトリスト管理で運用予定のため）。なお、クラウド側の仕様変更によりドメインが追加・変更される場合は、速やかに市へ通知を行うこと。
更改・廃棄		
No	**区分**	**セキュリティ要件**
59	終了通知	利用終了時に利用者へ事前通知できること。
60	データ廃棄	情報の機密性に応じた廃棄方法が定められていること。
61	アカウント削除	各利用者アカウントを削除できること。
62	特権削除	特権アカウントを削除または返却できること。
63	特殊アカウント廃棄	各アカウント以外に特殊なアカウントがある場合、そのアカウント情報を廃棄できること。