クラウドサービスの特記事項

〇クラウドサービス確認事項

Ｎｏ.	確認事項
1	**★自治体機密性３Ｂ又は３Ｃの情報をパブリッククラウドサービスで取り扱う場合** 利用するサービスが、次の条件を満たしていること。 ・クラウドサービス提供者が国際規格ＩＳＯ／ＩＥＣ２７００１の認証（情報セキュリティマネジメントシステム［ISMS］適合性評価制度等）の取得又は同等程度の水準を備えているクラウドサービスを選定すること。
2	日本の裁判管轄、法令が適用されること。海外への機密情報の流出リスクを考慮し、クラウドサービスを提供するリージョン（国・地域）を国内に指定すること。国内のクラウドサービスにおいて、利用者のデータが、海外に保存されないこと。
3	クラウドサービス提供者における情報セキュリティ対策の実施内容及び管理体制について、公開資料、監査報告、内部監査報告若しくは事業者の報告資料の内容で確認できること。
4	クラウドサービス提供者若しくはその従業員、再委託先又はその他の者によって、利用者の意図しない変更が加えられないための管理体制について、公開資料、監査報告、内部監査報告若しくは事業者の報告資料の内容で確認できること。

〇クラウドサービスの導入・構築時に遵守するべき事項

Ｎｏ.	確認事項	
1	アクセス制御に関する事項	不正なアクセスを防止するためのアイディンティティ管理（IDのプロビジョニングから廃棄まで）とアクセス制御を実装していること。
2	アクセス制御に関する事項	システム管理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（多様素認証等）を用いていること。
3	アクセス制御に関する事項	クラウドサービス利用者によるクラウドサービスに影響を与える操作の特定と誤操作の抑制するために、手順書の作成や誤操作を認識可能なアラート等の実装を考慮していること。
4	アクセス制御に関する事項	クラウドサービス上で構成される仮想マシンに対して、適切なセキュリティ対策を行っていること。 ※確認に当たっては、IPAの安全なウエブサイトの作り方（E列にリンク挿入）及びセキュリティ実装チェックリスト（E列にリンク挿入）を参照ください。
5	アクセス制御に関する事項	インターネット等の外部の通信回線から庁内通信回線を経由せずクラウドサービス上に構築した情報システムにログインすることの要否の判断を行っていること。（リモートからクラウドサービスにインターネットで直接接続するようなケースが有る場合のみ該当）

6	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に、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が行われていること。
7	設計・設定及び開発に関する事項	クラウドサービスの利用の企画、要件の確認の段階から想定される脅威やリスクに対するセキュリティ対策を検討し、その検討結果を踏まえ、設計・開発におけるセキュリティ対策を行っていること。また、クラウドサービスで取得可能なログの種類、範囲等を確認し、必要となるログの取得機能を実装していること。
8	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ける時刻同期の方法について確認し、取得するログの時刻、タイムゾーンを統一していること。
9	設計・設定及び開発に関する事項	設計・設定時の誤りの防止の対応として、設計書や設定のレビューやクラウドサービスのフレームワークとの比較などを行っていること。
10	設計・設定及び開発に関する事項	セキュリティを保つための開発手順やフレームワーク等の情報を活用していること。
11	設計・設定及び開発に関する事項	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のそのソフトウェアのクラウドサービス上におけるライセンス規定を確認していること。
12	設計・設定及び開発に関する事項	クラウドサービス上に構成された情報システムと他のクラウドサービス利用者のネットワークやサブネット間等の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。
13	設計・設定及び開発に関する事項	利用するクラウドサービス上の情報システムが利用するデータ容量や稼働性能（移植容易性）について、必要に応じて報告すること。
14	設計・設定及び開発に関する事項	クラウドサービスを利用する業務において必要となる可用性（冗長構成や冗長回線等の実装）を考慮した設計になっているか確認していること。

〇クラウドサービスの運用・保守時に遵守するべき事項

Ｎｏ.	確認事項	
1	運用・保守時における利用方針に関する事項	クラウドサービス利用者とクラウドサービス提供者との責任分界点と当該分界点に基づくリスクについて確認できること。
2	運用・保守時における利用方針に関する事項	クラウドサービス提供者が定めるサービスレベルについて、定期的に確認できること。
3	運用・保守時における利用方針に関する事項	クラウドサービスに関して情報セキュリティインシデントが発生した場合の連絡体制が明確であり、サービス利用開始時に確認できること。
4	運用・保守時における教育に関する事項	クラウドサービスに関する手順書（操作手引書）を整備し、利用者への周知が可能であること。
5	運用・保守時における教育に関する事項	クラウドサービスにおける情報セキュリティリスク及びその対応方針について、確認できること。
6	運用・保守時における教育に関する事項	クラウドサービスに関連する適用法令又は規制等がある場合、当該内容を確認できること。
7	運用・保守時における資産管理に関する事項	クラウドサービス上で利用する IT 資産が脆弱性の影響を受ける場合に備え、利用者側の責任範囲を明確にしていること。
8	運用・保守時におけるアクセス制御に関する事項	システム管理者特権を付与する場合、アクセス管理を実施し、かつ、管理者操作に関するログを取得し、1年以上保管すること。
9	運用・保守時における暗号化に関する事項	クラウドサービスに情報資産（データ）を保存する場合、暗号化の方式及び暗号化に使用する鍵の管理方法について確認できること。
10	運用・保守時における暗号化に関する事項	鍵管理機能を提供する場合、その利用に伴うリスクの有無を確認できること。
11	運用・保守時における暗号化に関する事項	鍵管理機能を提供する場合、鍵の生成から廃棄までのライフサイクル管理の仕組みと当該仕組みに伴うリスクの有無を確認できること。
12	運用・保守時における設計・設定に関する事項	クラウドサービスの設定を変更する場合、設定ミスを防止するため、グローバルなセキュリティガイドライン又はフレームワークとの差異を確認する等の対策を実施できること。
13	運用・保守時における設計・設定に関する事項	利用者が実施する重要な操作について、当該操作に関する手順書を作成していること。

14	運用・保守時における事業継続に関する事項	障害や災害等の不測の事態に備え、サービス復旧に必要なバックアップを取得できること。なお、バックアップ機能を提供する場合は、その取得状況を確認できること。
15	運用・保守時における事業継続に関する事項	クラウドサービスが業務に求められる可用性水準を満たしていることを確認できること。
16	運用・保守時における事業継続に関する事項	設定変更又はバージョン変更に関する情報及び当該変更がクラウドサービス上のシステムに及ぼす影響を確認できること。
17	運用・保守時における事業継続に関する事項	クラウドサービスで利用しているデータ容量や性能等を監視し、クラウドサービス又はクラウドサービス上のシステムに及ぼす影響を利用者に通知すること。
18	クラウドサービスの利用終了時における対策に関する事項	クラウドサービスの利用を終了する場合、データ移行計画書又はサービス終了計画書を策定に係る必要な情報を確認できること。
19	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	取り扱った情報の暗号化に使用した暗号鍵を削除する等により、暗号化されたデータを復元困難な状態にできること。また、暗号鍵のバックアップが存在する場合は、当該バックアップについても削除できること。