クラウドサービス選定基準

①　クラウドサービス提供者に係る事項

No	大区分	小区分	確認事項（対策）	補足説明
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の運用	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に指定できること。	
2	クラウドサービス提供者の選定基準	国内リージョンおよびデータの保存	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）を国内に指定できること。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の選定基準	サービス終了または変更時の事前通知	クラウドサービスの終了または変更時における事前の通知等の取り決めや情報資産の移行方法を契約に規定できること。 特に事前の通知については、事前通知の方法・期限について、以下を例とする条項を盛り込んだ契約が締結可能なこと。 ［例］当該サービスの終了または変更の際に、●か月前までに●の方法で事前に告知すること。	契約に規定できない場合、当該サービスの利用規約等において、同等の内容が規定されていれば適合しているものとする。
4	クラウドサービス提供者の選定基準	情報セキュリティ対策の履行が不十分な場合の対処方法	情報セキュリティ対策の履行が不十分な場合の対処方法（改善、追完、損害賠償等）について、契約またはサービスレベル契約（SLA）に規定できること。	契約またはSLAに規定できない場合、当該サービスの利用規約等において、同等の内容が規定されていれば適合しているものとする。
5	クラウドサービス提供者の選定基準	目的外利用の禁止	クラウドサービス提供者が、区の情報資産へ目的外のアクセスや利用を行わないように契約に定められること。	契約に規定できない場合、当該サービスの利用規約等において、同等の内容が規定されていれば適合しているものとする。 また、ISO27017およびISO27018を取得している場合も適合しているものとする。
6	クラウドサービス提供者の選定基準	クラウドサービス提供者における情報セキュリティ対策の実施内容および管理体制	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および管理体制について、公開資料や監査報告書（または内部監査報告書・事業者の報告資料）、各種の認定・認証制度の適用状況から、クラウドサービス提供者の信頼性が十分であることを総合的・客観的に評価し、判断可能なこと。 ① ISO/IEC 27017 ② ISMAPクラウドサービスリスト ③ ISMAP-LIUクラウドサービスリスト ④ SOC報告書 ※ガバメントクラウドを利用する場合は、上記①～④の国際規格またはそれ以上の認定、認証が必須 上記を満たさない場合、組織内全ての情報資産を管理するISMSを構築・運用するセキュリティ対策を成していることを示す、ISO27001、ISMS認証を取得済であることを必要要件とし、クラウドサービス特有の事項について、ISO27017または ISMAP管理基準と同等の適切な対策が講じられていることを事業者の報告資料等において確認できること。	・区が利用しようとしているサービスの基盤部分（AWS等）が認証を受けていればOKという項目ではない。当該サービスがSaaSとして認証を受けている必要がある。 ・ISMS認証（ISO27001）のみを取得している場合は、②クラウドサービス特有確認事項を満たすことで、左記確認事項におけるISO27017等と同等の対策の確認をしているものとする。
7	クラウドサービス提供者の選定基準	区の意図しない変更が加えられないための管理体制	クラウドサービス提供者もしくはその従業員、再委託先またはその他の者によって、区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、公開資料や監査報告書（または内部監査報告書・事業者の報告資料）の内容を確認できること。	【区の意図しない変更とは】 設定ミスによりセキュリティが脆弱になることや、設計変更によりサービスの性能や可用性に影響が出ること、データの不適切な取扱いが行われること等 　例）非公開に設定した情報が、仕様変更や新しく追加された機能等により、勝手に公開するように変更されてしまうケース　等 公開資料や監査報告書で確認できない場合、ISO27017を取得していれば適合しているものとする。
8	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への対処方法	情報セキュリティインシデント（情報セキュリティ事故およびその兆候）への対処方法について、クラウドサービス提供者との責任分担や連絡方法を取り決め、契約またはサービスレベル契約（SLA）に規定できること。	契約またはSLAに規定できない場合、当該サービスの利用規約等において、同等の内容が規定されていれば適合しているものとする。また、専用ホームページでの情報提供等、明確な対処方法が取り決められている場合も適合しているものとする。

No	大区分	小区分	確認事項（対策）	補足説明
9	導入・構築	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ンティティ管理（アカウントの発行から利用停止・削除等までの一連の管理・メンテナンス）とアクセス制御（クラウドサービスに保存される情報やクラウドサービスの機能ごとにアクセスする権限のない職員がアクセスできないように制限する等）を実施すること。	
10	導入・構築	アクセス制御に関する事項	クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御（クラウドサービスに保存される情報やクラウドサービスの機能ごとにアクセス権限のない者がアクセスできないように制限すること）ができること。	
11	導入・構築	暗号化に関する事項	クラウドサービス内および通信経路全般において暗号化処理が行われていること。この際、利用される暗号化方式は、「電子政府推奨暗号リスト」に記載された方式であること。	・サービス内で取り扱われるデータについて暗号化（※）されていること。 ※　通知経路の暗号化、サーバ内データの暗号化
12	導入・構築	設計・設定および開発に関する事項	必要となる各種ログの取得機能を実装していること。区はクラウドサービスで取得可能なログの種類、範囲を確認すること。	不正アクセス、不正操作、インシデント対応等のためのログの取得およびログの監視が行われていること。
13	導入・構築	設計・設定および開発に関する事項	取得するログの時刻、タイムゾーンが統一されること。区は時刻同期方法について確認すること。	ログの時刻同期の必要性：各デバイスが正確な時刻を共有し、ログの時刻が一致する タイムゾーン統一の必要性：ログの時刻が一貫して表示され、解析が容易になる
14	運用・保守	暗号化に関する事項	【SaaSの場合は対象外】 暗号化に関し、クラウドサービス提供者が提供する鍵管理機能を利用する場合、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関する内容等が確認できること。区は、その内容にリスク（鍵が窃取される可能性や鍵生成アルゴリズムが危険にさらされる可能性等）がないことを確認すること。	
15	運用・保守	クラウドサービス内の通信に関する事項	利用するクラウドサービスのネットワーク基盤内における区が利用するネットワークが他の利用者のネットワークや通信と分離され、論理的に独立していること。 SaaSの場合は、他の利用者が区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。	
16	運用・保守	設計・設定に関する事項	利用するクラウドサービスの仮想マシンのネットワークが他の利用者のネットワークと分離されていることを、クラウドサービス提供者の開示している情報等で確認できること。SaaSの場合は、他の利用者が区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。	
17	更改・廃棄	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、外部クラウドサービスで取り扱った区の全ての情報がクラウドサービス基盤上から漏えいを来さない方法で確実に削除されること。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も含むこと。 これらについてクラウドサービスの利用終了時に、区に情報の廃棄の実施報告書を提出すること、または確実に削除されることが文書で確認できること。	契約終了時に区のデータがサービス上から復元困難な形で確実に削除されること。および削除されたことを証明できること。 当該サービスの利用規約等で利用終了後の確実なデータ削除が規定されている場合、文書の提出等ができなくても、適合しているものとする。
18	更改・廃棄	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。	

②クラウドサービス特有確認事項（①クラウドサービス提供者に係る事項No.6において、ISO27017等の認証を保有していない場合の追加確認事項）

No	大区分	確認事項（対策）	補足説明
1	CLD.6.3.1クラウド環境における役割・責任の共有	クラウドサービスの利用においてクラウド顧客とプロバイダ双方にまたがる情報セキュリティ責任を明確化し、各者の担当者に割り当てて文書化・周知すること。	クラウドサービス利用に関する貴社と顧客それぞれのセキュリティ責任を明文化し、お互いに認識・合意していますか？
2	データ所在地の通知	クラウドサービス提供者は、自社の所在地およびクラウド顧客データを保存する可能性のある国・法域を契約書や利用規約、Webサイト等で顧客に通知すること。	クラウドサービス契約において、サービス提供者の所在地および顧客データの保管場所（国や法域）を明示していますか？ ※データは国内リージョン、管轄裁判所は国内とすること
3	クラウドサービスに関する教育	クラウドサービス提供者の従業員に対し、クラウド顧客データ及び派生データを適切に取り扱うための意識向上・教育・訓練を提供し、必要に応じて契約先にも同様の取り組みを求めること。	クラウドサービス固有のセキュリティ（クラウド顧客データの適切な取扱いなど）について、従業員への教育訓練を行い、必要に応じて外部委託先にも要求していますか？
4	クラウド顧客データの識別	情報資産台帳に、クラウドサービスカスタマのデータ（契約情報等）およびクラウドサービスに関連して発生する派生データ（ログや設定情報等）を明確に特定・識別すること。	情報資産の一覧に、クラウド顧客から預かったデータや、それに関連するログ・設定情報などの資産が漏れなく含まれ明示されていますか？
5	CLD.12.1.5実務管理者の運用のセキュリティ	クラウド環境における管理運用上の重要な操作手順を定義・文書化し、適切に監視すること。	クラウドサービスの提供に伴う重要な管理作業（仮想サーバの作成・削除、サービス終了手順、バックアップ/リストア等）について、手順書を整備し実施時に記録・監視していますか？
6	CLD.12.4.5クラウドサービスの監視	クラウドサービス顧客が、自身の利用しているクラウドサービスの特定の状況を確認できるような仕組みを提供すること。	クラウドサービスの稼働状況（障害・メンテ・影響範囲・復旧状況）、異常な状態などの監視情報等について、顧客が確認できる手段（ホームページでの公開等）を提供していますか？
7	CLD.9.5.1仮想環境における分離	クラウド上で稼働する各クラウド顧客の仮想環境は、他の顧客や不正なアクセスから隔離・保護されるように論理的分離を実施する。マルチテナント環境では、異なるテナントが使用する資源が相互に干渉しないようネットワーク、ストレージ、仮想サーバなどを適切に分離し、クラウド提供者内部の管理ネットワークとも分離すること。	クラウド上で稼働する各クラウド顧客の仮想環境は、他の顧客や不正なアクセスから隔離・保護されるように論理的分離を実施していますか？ マルチテナント環境では、異なるテナントが使用する資源が相互に干渉しないようネットワーク、ストレージ、仮想サーバなどを適切に分離し、クラウド提供者内部の管理ネットワークとも分離していますか？
8	CLD.9.5.2仮想マシンの要塞化	クラウド環境の仮想マシンについて、必要なポート・プロトコル・サービスのみ有効化するなど適切にセキュア設定（要塞化）し、各VM上でマルウェア対策やログ取得などの技術的対策を実装すること。	クラウド環境の仮想マシンについて、必要なポート・プロトコル・サービスのみ有効化するなど適切にセキュア設定（要塞化）し、各VM上でマルウェア対策やログ取得などの技術的対策を実装してますか？
9	CLD.8.1.5クラウド顧客資産の除去	クラウドサービス利用契約の終了時に、クラウドサービスカスタマの全ての資産（データ等）を確実に返却または消去する取り決めを事前に定め、契約書に明記しておく。終了に際してその取り決め通りに資産の返却・削除を実施し、削除対象の資産を特定しておくこと。	クラウドサービス契約終了時に、顧客データやバックアップ等すべての顧客資産を確実に返却または消去する手順を定めていますか？また、その手順に従って速やかに実行されていますか？
10	顧客とのインシデント対応合意	クラウドサービスカスタマとの間で、セキュリティインシデント発生時の責任分担および対応手順をサービス契約の一部として事前に取り決めていること。	クラウド顧客とのサービス契約上（利用規約等の規定を含む）で、インシデント対応における相互の責任範囲と連絡・対処手順を定めていますか？
11	クラウド顧客からの報告	クラウドサービス利用者（顧客）から提供者へのセキュリティ事象報告の仕組みを確立すること。	クラウド顧客がサービス障害やセキュリティ事象を報告できる窓口・プロセスを用意していますか？（例：問い合わせ窓口の明示、緊急連絡手段）
12	法的措置に備えた証拠保全	クラウドサービスにおけるインシデントの結果、法的措置が取られる可能性がある場合には、関連記録や証拠を保全する手順を整備すること。	重大なクラウドセキュリティインシデント発生時、捜査や訴訟に耐えうるようログや証跡を速やかに取得・保全する手順がありますか？
13	クラウドサービスの法域通知	クラウドサービス提供者は、クラウドサービスに適用される管轄法（法域）を契約書や利用規約に明示し、関連する法令・契約上の要求事項についてクラウド顧客に情報提供すること。	必要となる各種ログの取得機能を実装していること。区はクラウドサービスで取得可能なログの種類、範囲を確認すること。