別紙4

# クラウドサービスに関する情報セキュリティチェックシート

| | チェック事項 | はい | いいえ |
|---|---|---|---|
| **1．利用者認証** | | | |
| 1-1 | 当該クラウドサービスを提供する情報システムの運用もしくは開発に従事する者又は管理者権限を有する者について、適切な利用者確認がなされていますか？ | □ | □ |
| 1-2 | 当該クラウドサービスのログインに関わる認証機能は提供されていますか？ | □ | □ |
| **2．アクセス制御** | | | |
| 2-1 | 当該クラウドサービスに対して、アクセスする権限のない者がアクセスできないように、システム上制限する機能は提供されていますか？ | □ | □ |
| 2-2 | 当該クラウドサービスに対して、アクセス制御機能を用いて、情報資産毎に、許可されたクラウドを利用する教職員等及び児童生徒のみがアクセスできる環境を提供されていますか？ | □ | □ |
| **3．クラウドに保管するデータの暗号化** | | | |
| 3-1 | 当該クラウドサービスへのデータの保管に際し、情報漏えい等に備えて、暗号化等の保護措置を講じていますか？ | □ | □ |
| **4．マルチテナント環境におけるテナント間の安全な管理** | | | |
| 4-1 | 複数のクラウド利用者がクラウドリソースを共用する環境において、特定のクラウド利用者に対して発生したセキュリティ侵害が、他のクラウド利用者に影響を与えないように対策を講じていますか？ | □ | □ |
| **5．クラウドサービスを提供する情報システムに対する外部からの悪意のある脅威の侵入を想定した技術的セキュリティ対策** | | | |
| 5-1 | 当該クラウドサービスを提供する情報システムを監視し、セキュリティ侵害を検知する対策を講じていますか？ | □ | □ |
| 5-2 | 当該クラウドサービスを提供する情報システムのインターネット接続境界において、クラウド利用者以外による不正な通信・侵入を防ぐ措置を講じるとともに、外部脅威の侵入を検知し、防御する対策を講じていますか？ | □ | □ |
| **6．情報の通信経路のセキュリティ確保** | | | |
| 6-1 | 教育情報システムのインターネット境界から当該クラウドサービスを提供する情報システムまでの情報の通信経路において、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）を講じていますか？ | □ | □ |
| 6-2 | クラウド事業者が保守運用等を遠隔で行う場合の、保守運用拠点と管理区域間の通信回線及び通信回線装置の管理について、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）を講じていますか？ | □ | □ |
| **7．クラウドサービスを提供する情報システムの物理的セキュリティ対策** | | | |
| 7-1 | 当該クラウドサービスのサーバ等の管理について、文部科学省「教育情報セキュリティポリシーに関するガイドライン」「4 1.サーバ等の管理」に準じた対策を講じていますか？パブリッククラウド等を利用している場合、利用するサービスに同様の対策が講じられていることを確認しましたか？ | □ | □ |
| 7-2 | クラウド事業者側の管理区域（サーバ等を設置）及び保守運用拠点の管理について、文部科学省「教育情報セキュリティポリシーに関するガイドライン」「4 2.管理区域（情報システム室等）の管理（教育委員会等のサーバ室にサーバを設置している場合）」に準じた対策を講じていますか？パブリッククラウド等を利用している場合、利用するサービスに同様の対策が講じられていることを確認しましたか？ | □ | □ |
| 7-3 | クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）にあたり、セキュリティを確保した対応となっていることを確認しましたか？ | □ | □ |
| **8．クラウドサービスを提供する情報システムの運用管理** | | | |
| 8-1 | サービスの一時停止やインシデント発生時等クラウド利用者に影響が生じる場合、利用者への影響範囲（時間、サービス内容）等について、速やかにクラウド利用者側に連絡される運用手続きが確立されていますか？ | □ | □ |
| 8-2 | 当該クラウドサービスにおけるサーバの冗長化について、文部科学省「教育情報セキュリティポリシーに関するガイドライン」「4 1.サーバ等の管理（2）サーバの冗長化」に準じた対策を講じていますか？ | □ | □ |
| 8-3 | 当該クラウドサービスにおけるデータバックアップ及び復旧手順について、文部科学省「教育情報セキュリティポリシーに関するガイドライン」「6 1.コンピュータ及びネットワークの設定管理（2）バックアップの実施」に準じた対策を講じていますか？ | □ | □ |
| 8-4 | 当該クラウドサービスにおける情報セキュリティの確保や監査に必要なログの取得について、文部科学省「教育情報セキュリティポリシーに関するガイドライン」「6 1.コンピュータ及びネットワークの設定管理（3）ログの取得等」に準じた対策を講じていますか？ | □ | □ |
| **9．クラウドサービスを提供する情報システムのマルウェア対策** | | | |
| 9-1 | クラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等について、マルウェア対策を講じていますか？ | □ | □ |
| 9-2 | 内部システムに侵入した攻撃を検知して対処するために、通信をチェックする等の対策を講じていますか？ | □ | □ |
| **10．クラウド事業者従業員の人的セキュリティ対策** | | | |
| 10-1 | クラウドサービスに関わるクラウド事業者従業員に対して、クラウド事業者の情報セキュリティポリシー及び保守運用管理規程等を遵守させていますか？ | □ | □ |
| 10-2 | クラウドサービスに関わるクラウド事業者従業員に対して、業務に用いるID及びパスワードその他の個人認証に必要な情報及び媒体について、部外者及び業務に関わらない従業員に漏えいすることがないように、適切に管理していますか？ | □ | □ |
| 10-3 | クラウドサービスに関わらない従業員等がクラウド利用者のデータを知り得る状態にならないよう、業務に関わるクラウド事業者従業員に対して秘匿を義務づけていますか？ | □ | □ |
| 10-4 | クラウド利用者のデータ及びデータを格納した端末機器又は電磁的記録媒体の外部持ち出しについて、クラウド利用者の許可なく外部持ち出しできないこと及び外部持ち出しにおける安全管理手順を定めていますか？ | □ | □ |
| 10-5 | クラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等に、マルウェアを侵入させないよう対策を講じていますか？ | □ | □ |
| 10-6 | クラウド利用者のデータを目的外利用及び第三者への提供をしていませんか？ | □ | □ |
| **11．サービス終了時等のデータの廃棄及び利用者アカウント抹消について** | | | |
| 11-1 | サービス利用終了時等において、クラウド利用者のデータ及び利用者アカウント情報が不用意に残置されないよう、適切に破棄する手続きを定めていますか？ | □ | □ |
| 11-2 | サービス利用終了時等におけるデータの扱いについて、スムーズに回収、次期システムへの移行等を行えるよう、その手続きを定めていますか？ | □ | □ |
| 11-3 | クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除される手続きを定めていますか？ | □ | □ |
| **12．その他** | | | |
| 12-1 | 当該クラウドサービスは、日本の法令の範囲内で運用でき、係争時の管轄裁判所が日本国内となるものであることを確認しましたか？ | □ | □ |

提　出　日：＿＿＿＿＿＿＿＿

サービス名：＿＿＿＿＿＿＿＿

受注者名：＿＿＿＿＿＿＿＿

代表者名：＿＿＿＿＿＿＿＿

クラウドサービス事業者名：＿＿＿＿＿＿＿＿

代表者名：＿＿＿＿＿＿＿＿

岐阜市発注部署：＿＿＿＿＿＿＿＿