クラウドサービスの利用における情報セキュリティ規定
（自治体機密性２以上の情報を取り扱う場合）

１　目的

本規定は、クラウドサービスの利用における情報セキュリティ対策を明確にし、組織全体の情報資産を適切に保護することを目的とする。

クラウドサービスの特性や責任分界点を踏まえ、情報システムの導入・構築、運用・保守、利用終了時におけるセキュリティ対策の基本方針を策定する。

２　適用範囲・対象者

(1) 本規定は、クラウドサービスを利用する全ての業務および情報システムに適用する。

(2) 本規定は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報システム管理者、許可権限者、クラウドサービス管理者、職員等を対象とする。

３　用語の定義

(1) クラウドサービス

庁外の組織が、情報システムの一部又は全部の機能を提供するものをいう。

＜クラウドサービスの例＞

- 仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS）
- データベースや開発フレームワーク等のミドルウェア等提供サービス（PaaS）
- Web 会議サービス
- SNS（ソーシャルメディア）
- 検索サービス、翻訳サービス、地図サービス

(2) クラウドサービス提供者

クラウドサービスを提供する事業者をいう。

(3) クラウド許可権限者

クラウドサービスの利用申請に対して、セキュリティや業務上の適合性を評価し、最終的な承認を行う責任をもつ者をいう。

(4) クラウドサービス管理者

クラウドサービスの利用における利用申請の許可権限者から利用承認時に指名された当該クラウドサービスに係る管理を行う者をいう。クラウドサービス管理者は、情報セキュリティ責任者と兼務することが可能である。

(5) 利用者

クラウドサービスを利用する自組織の職員等をいう。

4　運用規程

(1) クラウドサービス利用判断基準

クラウドサービスを利用する業務範囲を慎重に判断する。特に機密性の高い情報をクラウドサービスで利用する場合においては、以下に示す事項を実施する。

① クラウドサービスを利用する目的の明確化

② クラウドサービスを利用する業務範囲の明確化

③ クラウドサービスを利用する際における、以下のリスクに対する対策の検討

・情報の管理や処理をクラウドサービス提供者に委ねるため、その情報の適正な取扱いの確認が容易ではないこと。

・クラウドサービス提供者の運用詳細等が公開されない場合は、利用者が情報セキュリティ対策を行うことが困難となること。

・利用するクラウドサービスを自組織のセキュリティポリシーに見合うサービスかどうか評価が適切に出来ない場合は、業務継続等に対する影響が発生する可能性があること。また、クラウドサービス提供者との間の責任分界点やサービスレベルの合意が必要となること。

・クラウドサービス提供者が所有する資源の一部を利用者が共有し、その上に個々の利用者が管理する情報システムが構築されるなど、不特定多数の利用者の情報やプログラムを一つのクラウドサービス基盤で共用することとなるため、情報が漏えいするリスクが存在すること。

・クラウドサービスで提供される情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることによるカントリーリスクが存在すること。

・サーバ装置等機器の整備環境がクラウドサービス提供者の都合で急変する場合、サプライチェーン・リスクへの対策の確認が容易ではないこと。

④ クラウドサービスを利用する際のリスクの低減策についての統括情報セキュリティ責任者への届け出（クラウドサービス利用申請時確認事項）

⑤ クラウドサービスで個人情報（特定個人情報を含む）を扱う場合は、個人情報保護法で定められた安全管理措置を行う。必要に応じて、PIA（特定個人情報保護評価）を実施する。

⑥ 自治体機密性３Ａに相当する情報（「政府機関等のサイバーセキュリティ対策のための統一基準」（令和５年度版）の機密性３情報に相当）については、クラウドサービスで取り扱わない。

(2) クラウドサービス提供者選定基準

以下に示す事項については、クラウドサービス提供者から情報提供を得て確認する。また、これらの事項について基本契約又はサービスレベル契約（SLA）で定めることが出来るクラウドサービスを選定する。なお、各事項の具体的な数値やレベル等の要件については、利用する業務やクラウドサービスに応じて定める。

① 日本の裁判管轄、法令が適用される。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。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。これらの事項を基本契約に定める。

② クラウドサービスの中断時の復旧要件について基本契約又はサービスレベル契約（SLA）に定める。

③ 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等の取り決めや情報資産の移行方法について基本契約に定める。

④ 稼動率、目標復旧時間、目標復旧ポイント、バックアップの保管方法などの可用性に関する事項をサービスレベル契約（SLA）に定める。

⑤ クラウドサービス提供者が、利用者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基本契約に定める。

⑥ 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、公開資料や監査報告書（又は内部監査報告書・事業者の報告資料）の内容を確認する。

⑦ 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、公開資料や監査報告書（又は内部監査報告書・事業者の報告資料）の内容を確認する。

⑧ 情報セキュリティインシデント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、基本契約又はサービスレベル契約（SLA）に定める。

⑨ 脅威に対するクラウドサービス提供者の情報セキュリティ対策（なりまし、情報漏えい、情報の改ざん、否認防止、権限昇格への対応、サービス拒否・停止等）の実施状況やその他契約の履行状況の確認方法を基本契約又はサービスレベル契約（SLA）に定める。

⑩ 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について、基本契約又はサービスレベル契約（SLA）に定める。

⑪ クラウドサービス提供者により、利用規約、各種設定が変更される可能性があるため、変更内容の確認方法や連絡方法を基本契約又はサービスレベル契約（SLA）に定める。

(3) クラウドサービスの利用に係る調達・契約に関する事項

① 情報セキュリティ責任者は、クラウドサービスを調達する場合は、本書「(2)クラウドサービス提供者選定基準」及びその他の選定条件並びに当該クラウドサービスの利用において必要となるセキュリティ要件を調達仕様に含めること。

② 情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を基本契約に含めること。サービスレベルに関することは、サービスレベル契約（SLA）に含めること。

(4) クラウドサービスの利用承認に関する事項

① 利用申請

情報セキュリティ責任者は、利用するクラウドサービスについて、本書の基準を満たしていることを確認し、「クラウドサービス利用申請書兼許可書」及び「クラウドサービス利用申請時確認事項」を作成した上で、統括情報セキュリティ責任者（又は利用申請の許可権限者）に利用申請する。なお、利用申請においては、調達時に実施したセキュリティ要件の確認結果を提出すること。

② 許可

統括情報セキュリティ責任者（又は利用申請の許可権限者）は、情報セキュリティ責任者の申請内容を審査し、利用の可否を決定する。統括情報セキュリティ責任者（又は利用申請の許可権限者）は、承認済みクラウドサービスとして記録（承認日、クラウドサービス名、利用開始日、利用終了日又は予定日）し、クラウドサービス管理者を指名する。

③ 終了連絡

クラウドサービスの利用を終了する場合は、情報セキュリティ責任者（又はクラウドサービス管理者）は、統括情報セキュリティ責任者（又は利用申請の許可権限者）に、終了を報告する。

(5) クラウドサービスを利用した情報システムの導入・構築時のセキュリティ対策に関する事項

以下に示す事項について、別紙「クラウドサービス利用におけるチェックリスト」を用いて、クラウドサービス提供者の対応状況を確認する。

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ユーザアカウント管理（ID の提供から廃棄まで）を行う。

・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、アクセス制御ができることを確認する。また、適切なアクセス制御を実施し、情報の機密性、完全性、可用性を維持する。

・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（多要素認証）を用いる。

・クラウドサービスに影響を与える操作の特定と誤操作を抑制するために、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する。

・クラウドサービス上で構成される仮想マシンに対して、パッチ管理やウイルス対策ソフトの導入を行い、適切なセキュリティ対策を行う。

・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を判断し、必要と認める場合は適切なセキュリティ対策を実施し、リスクを管理する。（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）

② 暗号化に関する事項

・取り扱う情報の機密性を保護するため、強度の高い暗号化（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など）を実施する。

③ 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う。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する。

・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する。

・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う。

・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する。

・クラウドサービス上に他ベンダーが提供するソフトウェア等を導入する場合は、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する。

・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。

・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、必要に応じてクラウドサービス提供者に報告を求め、業務が継続できるよう考慮する。

・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を行う。

(6) クラウドサービスを利用した情報システムの運用・保守時のセキュリティ対策に関する事項

以下に示す事項について、別紙「クラウドサービス利用におけるチェックリスト」を用いて、クラウドサービス提供者の対応状況を確認する。

① 運用・保守時における利用方針に関する事項

・契約書やサービスレベル契約（SLA）において、クラウドサービス提供者と利用者の責任分界点を明確にし、リスクの受容可否を判断する。

・事前に承認を受けていないクラウドサービスの利用を禁止する。

・クラウドサービス提供者に対して、定期的にサービスの提供状態を確認する。

② 運用・保守時における教育に関する事項

・利用するクラウドサービスの手順書（操作手引書）を定め、利用者に周知する。

・利用するクラウドサービスにおける情報セキュリティリスクとリスク対応について利用者に共有する。

・利用するクラウドサービスに関する適用法令や関連する規制等がある場合は、利

用者に周知する。

③　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 資産が脆弱性による影響を受ける場合に備え、利用者側の責任範囲を明確にする。

・クラウドサービス上に情報を保存する場合は、個人情報の有無、機微性の高低等の情報に対する格付・取扱制限等が把握できるようにする。

④　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割り当てる場合のアクセス管理と操作に関するログを取得する。

・クラウドサービスの各利用者に割り当てたアクセス権限に対して、定期的な見直し（異動時、退職時等の確認）を行う。

・クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合は、その機能の確認と利用できる者を制限する。

・利用するクラウドサービスの不正な利用を監視（例：業務時間外の利用等をクラウドサービスに対するアクセスログで確認）する。

⑤　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、暗号化の仕組みや暗号化に使用する鍵の管理方法について確認をする。

・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関する内容及びリスクがないことを確認する。

⑥　運用・保守時における暗号化に関する事項

・利用するクラウドサービスのネットワーク基盤が他の利用者のネットワークや通信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する。

⑦　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、設定の誤りを防止するための対策を行う。

・利用者が行う重要な操作に関する手順書を作成する。

・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する。

⑧　運用・保守時における事業継続に関する事項

・不測の事態に対してサービスの復旧を行うために必要なバックアップを実施（クラウドサービス提供者が提供する機能を利用する場合は、その実施の確認）する。

・クラウドサービスが、業務に必要な可用性を満たしたものになっているか確認をする。また、復旧に係る手順の策定と定期的な訓練を実施する。

・クラウドサービス提供者からの設定やバージョン等の変更の確認方法と利用するクラウドサービス上のシステムに影響があった場合を想定し、復旧手順につい

て確認する。

・クラウドサービスで利用しているデータの容量、性能等を監視し、クラウドサービスまたは、クラウドサービス上のシステムへの影響について把握する。

⑨　運用・保守時におけるインシデント対応に関する事項

・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、適切な対応を行うための手順を確立する。

(7) クラウドサービスを利用した情報システムの更改・廃棄時のセキュリティ対策に関する事項

以下に示す事項について、別紙「クラウドサービス利用におけるチェックリスト」を用いて、クラウドサービス提供者の対応状況を確認する。

①　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は、移行計画書又は終了計画書を作成する。

・クラウドサービスの利用終了による業務影響が無いように、利用者に対して利用終了の予定時期を事前に知らせる。

②　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

・取り扱う情報の機密性に応じて、廃棄方法を決定する。

③　クラウドサービスの利用のために作成したアカウントの廃棄に関する事項

・作成したクラウドサービス利用者の各アカウントを削除する。

・利用したシステム管理者特権アカウントを削除する。

・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がある場合は、関連情報（資格情報等）含めて廃棄する。

(8) 利用状況の管理

クラウドサービス管理者は、利用しているクラウドサービスについて、定期的な確認を行い、統括情報セキュリティ責任者から確認があった場合に提示する。なお、内容等に変更があり、不適切と考えられるものがある場合は、情報セキュリティ責任者及び統括情報セキュリティ管理者に相談する。

5　規定の見直しと更新

本規定は、定期的に見直しを行い、必要に応じて更新する。

見直しの責任者は統括情報セキュリティ責任者とし、少なくとも年に一度見直しを行う。

6　附則

本規定は、令和７年１月２９日より施行する。