岸和田市情報セキュリティポリシー

別冊_ガバメントクラウド編

令和6年3月制定

岸　和　田　市

第１章　本規程の目的

本規程は、岸和田市情報セキュリティポリシー（平成 18 年 9 月制定）の「９．重要度 B 以上の情報を扱う外部サービスの利用」において、マイナンバー利用事務系の標準準拠システム等をガバメントクラウド上に構築する場合に、情報システム管理者等が遵守する必要があると規定されている事項について、定めるものである。

第２章　情報システム管理者の遵守事項

マイナンバー利用事務系の標準準拠システム等をガバメントクラウド上に構築する場合に、情報システム管理者等は下記の各項目について遵守しなければならない。

１　情報システム管理者は、ガバメントクラウドの環境に保存される情報資産についても本編「２．情報資産の分類及び保管」の「（１）情報の重要度による分類」の分類に基づき管理しなければならない。また、情報システム管理者は、情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）も考慮して情報資産を管理しなければならない。情報システム管理者は、ガバメントクラウドを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のガバメントクラウド事業者からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認しなければならない。

２　情報システム管理者はガバメントクラウドで利用する全ての情報資産について、ガバメントクラウドの利用終了時期を確認し、ガバメントクラウドで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

３　マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、本市の他の領域とはネットワークを分離しなければならない。

４　情報システム管理者は、マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。また、ガバメントクラウド事業者が暗号に関する対策を行う場合又はガバメントクラウド事業者が提供する情報資産を保護するための暗号機能を利用する場合、ガバメントクラウド事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

５　ガバメントクラウド事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、ガバメントクラウド事業者の方針及び手順について確認

しなければならない。なお、当該確認にあたっては、ガバメントクラウド事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

6　職員等は、ガバメントクラウドの利用にあたっても情報セキュリティポリシーを遵守し、ガバメントクラウドの利用に関する自らの役割及び責任を意識しなければならない。

7　情報システム管理者は、定期的にガバメントクラウドを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施するとともに、委託先を含む関係者については委託先等で教育、訓練が行われていることを確認しなければならない。

8　情報システム管理者は、ガバメントクラウド事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。

9　情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。なお、ガバメントクラウド事業者が収集し、保存する記録（ログ等）に関する保護(改ざんの防止等)の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

10　情報システム管理者は、監査及びデジタルフォレンジックに必要となるガバメントクラウド事業者の環境内で生成されるログ等の情報（デジタル証拠）について、ガバメントクラウド事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、ガバメントクラウド事業者に提出を要求するための手続を明確にしなければならない。

11　情報システム管理者は仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。SaaS 型を利用する場合は、これらの対応が、ガバメントクラウドを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にガバメントクラウド事業者に報告を求めなければならない。

12　情報システム管理者は、本市が定めたガバメントクラウドの利用に関するポリシー（情報セキュリティポリシー）におけるアクセス制御に関する事項が、ガバメントクラウドにおいて実現できるのか又はガバメントクラウド事業者の提供機能等により実現できるのか、利用前にガバメントクラウド事業者に確認しなければならない。

13　情報システム管理者は、ガバメントクラウドを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、ガバメントクラウドにアクセスさせなければならない。

14　情報システム管理者は、パスワードなどの認証情報の割り当てがガバメントクラウド側で実施される場合、その管理手順等が、岸和田市情報セキュリティポリシーの各規定を満たすことを確認しなければならない。

15　情報システム管理者は、ガバメントクラウド事業者に対して、利用するガバメントクラウドに影響し得る技術的脆弱性の管理内容について情報を求め、本市の業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、ガバメントクラウド事業者に確認しなければならない。

16　情報システム管理者は、利用するガバメントクラウドで使用する時刻の同期についても適切になされているのか確認しなければならない。

17　情報システム管理者は、必要となるリソースの容量・能力が確保できるガバメントクラウド事業者を選定しなければならない。また、利用するガバメントクラウドの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

18　情報システム管理者は、イベントログ取得に関するポリシーを定め、利用するガバメントクラウドがその内容を満たすことを確認し、ガバメントクラウド事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

19　情報システム管理者は、ガバメントクラウド利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。
（ア）サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除
（イ）ガバメントクラウド利用の終了手順
（ウ）バックアップ及び復旧

20　情報システム管理者は、ガバメントクラウド事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてガバメントクラウドの障害時を想定

した緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

21　情報システム管理者は、ガバメントクラウドに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

22　情報システム管理者は、以下の内容を含む情報セキュリティ対策に関する情報の提供を求め、その内容を確認し、利用するガバメントクラウドが、岸和田市情報セキュリティポリシーを満たしているか否かを評価すること。

（ア）ガバメントクラウドの利用を通じて本市が取り扱う情報のガバメントクラウド提供者における目的外利用の禁止

（イ）ガバメントクラウド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

（ウ）ガバメントクラウドの提供に当たり、ガバメントクラウド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、本市の意図しない変更が加えられないための管理体制

（エ）ガバメントクラウド提供者の資本関係・役員等の情報、ガバメントクラウド提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

（オ）情報セキュリティインシデントへの対処方法

（カ）情報セキュリティ対策その他の契約の履行状況の確認方法

（キ）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

23　情報システム管理者は、ガバメントクラウド事業者と情報セキュリティに関する役割及び責任の分担について確認すること。

24　情報システム管理者は、ガバメントクラウド事業者とガバメントクラウドの利用前に合意した事項があれば、その内容についてサービス合意書（SLA）に定めること。ガバメントクラウド事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関するガバメントクラウド事業者の定める条件を鑑み、その規約内容が本市によって受容可能か判断すること。

25　①　情報システム管理者は、ガバメントクラウドの特性や責任分界点に係る考え方等を踏まえ、以下を含むガバメントクラウドを利用して情報システムを構築する際のセキュリティ対策を確認すること。

（ア）不正なアクセスを防止するためのアクセス制御

（イ）取り扱う情報の機密性保護のための暗号化
（ウ）開発時におけるセキュリティ対策
（エ）設計・設定時の誤りの防止
（オ）ガバメントクラウドにおけるユーティリティプログラムに対するセキュリティ対策
（カ）取り扱う資産の管理
（キ）ガバメントクラウド内の通信の制御
（ク）設計・設定変更時の情報や変更履歴の管理

② 情報システム管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録すること。

③ 情報システム管理者は、前各項において定める規定に対し、情報セキュリティに配慮した構築の手順及び実践がされているか、ガバメントクラウド事業者に情報を求め、実施状況を確認及び記録すること。

26 ① 情報システム管理者は、ガバメントクラウドの特性や責任分界点に係る考え方を踏まえ、以下を含むガバメントクラウドを利用して情報システムを運用する際のセキュリティ対策を規定すること。
（ア）ガバメントクラウド利用方針の規定
（イ）ガバメントクラウド利用に必要な教育
（ウ）取り扱う資産の管理
（エ）不正アクセスを防止するためのアクセス制御
（オ）取り扱う情報の機密性保護のための暗号化
（カ）ガバメントクラウド内の通信の制御
（キ）設計・設定時の誤りの防止
（ク）ガバメントクラウドを利用した情報システムの事業継続
（ケ）設計・設定変更時の情報や変更履歴の管理

② 情報システム管理者は、ガバメントクラウドの特性や責任分界点に係る考え方を踏まえ、ガバメントクラウドで発生したインシデントを認知した際の対処手順を整備すること。

③ 情報システム管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録すること。

④ 情報システム管理者は、情報セキュリティに配慮した運用・保守の手順及び実践がされているか、ガバメントクラウド事業者に情報を求め、実施状況を定期的に確認及び記録すること。

27 ① 情報システム管理者は、ガバメントクラウドの特性や責任分界点に係る考え方を踏まえ、以下を含むガバメントクラウドの利用を終了する際のセキュリティ対策を規定すること。
（ア）ガバメントクラウドの利用終了時における対策
（イ）ガバメントクラウドで取り扱った情報の廃棄

（ウ）ガバメントクラウドの利用のために作成したアカウントの廃棄

② 情報システム管理者は、前項において定める規定に対し、ガバメントクラウドの利用終了時に実施状況を確認・記録すること。

③ 情報システム管理者は、ガバメントクラウド上で機密性の高い情報（住民情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除するなどにより、その情報資産を復元困難な状態としなければならない。

28 情報システム管理者は、ガバメントクラウドを利用している場合は、ガバメントクラウド事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に監査を行わなければならない。ガバメントクラウド事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。