参考資料

令和６年１１月
大津市市民部戸籍住民課

ガバメントクラウドの利用に伴う 特定個人情報保護評価書（住民基本台帳および住登外に関する事務　全項目評価書）の 主な変更内容

１　ガバメントクラウドの概要

（１）ガバメントクラウド について
ガバメントクラウドは、デジタル庁が調達し、地方公共団体が標準準拠システム等を利用できるように、地方公共団体に対して提供するクラウドサービス及び関連するサービスのことです。
（２） ガバメントクラウドの利用について
令和３年９月１日に施行された「地方公共団体情報システムの標準化に関する法律（令和３年法律第 40 号)」で、各地方公共団体が独自に使用している基幹業務システムについて、国が標準仕様を示し、全国の地方公共団体で統一したシステム（標準準拠システム）を使用することが義務付けられました。 その際に、標準準拠システムを使用する場所として、ガバメントクラウドを利用することが努力義務とされています。本市でも、令和７年度末までに標準準拠システム及びガバメントクラウド への移行を行うこととしています。

２　特定個人情報保護評価書（地方税に関する事務　全項目評価書）の主な変更内容

（１）特定個人情報ファイル保管・消去について、ガバメントクラウド上での措置を追記	（該当箇所：Ⅱ　特定個人情報ファイルの概要 ６．特定個人情報の保管・消去 ①保管場所 ③消去方法）
保管場所については、クラウド事業者がセキュリティ対策を実施すること、クラウド事業者はセキュリティ管理策を適切に実施している業者であることを記載しています。特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存されることを記載しています。 消去については、地方公共団体からの操作によって行われ、国及びクラウド事業者はアクセス制限により削除できないこと、クラウド事業者が記憶装置等を交換する際は、データが復元されないように確実に消去することを記載しています。	
（２）リスク対策について、ガバメントクラウドにおける物理的・技術的な対策を追記	（該当箇所：Ⅲ リスク対策（プロセス） ７．特定個人情報の保管・消去 リスク１：特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 ⑥技術的対策）
物理的対策として、サーバーはクラウド事業者が管理する環境に構築し、適切な入退室管理を行うことを記載しています。 技術的対策として、国及びクラウド事業者はデータにアクセスしない契約となっていること、地方公共団体が委託した事業者は継続的にモニタリングを行うこと、クラウド事業者はウイルス対策ソフトを導入し、パターンファイルの更新を行うこと等を記載しています。	
（３）その他のリスク対策について、ガバメントクラウドにおける措置を追記	（該当箇所：Ⅳ リスク対策（その他） １．監査 ②監査 ３．その他のリスク対策）
クラウド事業者は定期的に政府情報システムのセキュリティ制度（ISMAP）の監査機関リストに登録された監査機関による監査を行うこととしていることを記載しています。 ガバメントクラウド上で障害が発生した場合は、ガバメントクラウドに起因する場合とガバメントクラウドに起因しない場合のそれぞれの対応を記載しています。	

3　変更内容に関係する用語の解説

用語	解説
クラウドサービス	ユーザーが利用するシステムの実態が、ユーザーのパソコンや組織拠点ではない、ネットワークでつながった外部（インターネット上等）に存在し、そこに接続してシステムを利用するサービスの総称です。システムだけでなく、ファイルの置き場所等、様々なサービスがあります。
ISMAP	政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度です。
ISO/IEC27017	ISO（International Organization for Standardization：国際標準化機構）及び IEC（International Electrotechnical Commission：国際電気標準会議）の制定による、クラウドサービスに関する情報セキュリティ管理策のガイドライン規格です。クラウドサービスに対応した情報セキュリティ管理体制を構築するための枠組みが示されています。
ISO/IEC27018	ISO 及び IEC の制定による、クラウドサービスに関する個人情報の保護を目的としたガイドライン規格です。クラウドサービスに対応した個人情報の保護体制を構築するための枠組みが示されています。
NIST 800-88	NIST（National Institute of Standards and Technology：米国国立標準技術研究所）の策定する、媒体のデータ抹消処理に関するガイドラインです。
ISO/IEC27001	ISO 及び IEC の制定による、組織における情報セキュリティマネジメントシステムに関する国際規格です。情報の機密性・完全性・可用性の 3 つをバランスよくマネジメントし、情報を有効活用するための枠組みが示されています。
ASP	Application Service Provider（アプリケーションサービス提供事業者）の略で、地方公共団体が標準準拠システム等を利用するために、業務アプリケーション等の構築、提供、運用保守等の提供を受ける一切の事業者を指します。
DDos	Distributed Denial of Service attack（ディストリビューテッド・デナイアル・オブ・サービス・アタック）の略で、複数のコンピュータから大量のデータを送りつけることで、相手のサーバーやネットワークに過大な負荷をかけ、使用不能にします。同様の攻撃方法である DoS 攻撃は 1 台のコンピュータから実行するものですが、DDoS 攻撃の場合は、例えば第三者のコンピュータをウイルスに感染させておくなどして、攻撃者の指示によって複数のコンピュータが一斉に攻撃します。