

令和6年度 第1回 豊島区個人情報保護審議会

会 議 次 第

1 日 時 令和7年3月14日（金）午後2時00分から

2 場 所 豊島区役所本庁舎9階 第一委員会室

3 次 第

（1）開 会

（2）議 題

【諮 問】

- ① 特定個人情報保護評価 第三者点検
「住民基本台帳に関する事務」について …資料1
- ② 特定個人情報保護評価 第三者点検
「個人住民税賦課徴収に関する事務」について …資料2

【報告事項】

- ① 住民基本台帳ネットワークシステムの実施状況について …報告1
- ② 令和7年度以降の豊島区個人情報保護審議会の開催について …報告2
- ③ 地方自治法に基づく内部統制について …報告3
- ④ 個人情報保護委員会からの留意事項について …報告4
- ⑤ 行政情報公開及び個人情報開示の実施状況について …報告5
- ⑥ 保有個人情報の漏えい等について …報告6

特定個人情報保護評価 重要な変更に伴う評価の再実施について

1. 特定個人情報保護評価とは

特定個人情報ファイル（マイナンバーをその内容に含む個人情報ファイル）を保有しようとする又は保有する国の行政機関や地方公共団体等が、個人のプライバシー等の権利利益に与える影響を予測した上で特定個人情報の漏えいその他の事態を発生させるリスクを分析し、そのようなリスクを軽減するための適切な措置を講ずることを宣言するものである。

特定個人情報保護評価書には「基礎項目評価書」「重点項目評価書」「全項目評価書」の3種類があり、対象人数や取扱者数に応じて評価書を選択する。

地方公共団体等が全項目評価を実施する際は、パブリックコメントの実施および第三者点検を受ける必要があり、第三者点検の目的は、特定個人情報保護評価の適合性・妥当性を客観的に担保することである。

評価書の公表後、重要な変更、しきい値判断結果の変更又は一定期間経過に伴い、保護評価の再実施又は評価書の修正が必要となる。

2. 今回の評価の再実施について

このたびの特定個人情報保護評価の再実施は**重要な変更**に伴うものである。

重要な変更とは特定個人情報の漏えいその他の事態の発生の危険性及び影響が大きい変更として、特定個人情報保護評価指針の別表に定められたものの変更のことを指す。

評価実施機関は、保有する特定個人情報ファイルに重要な変更を加えようとするときは、当該変更を加える前に、特定個人情報保護評価を再実施するものとされている。

3. 重要な変更が生じた理由：基幹システムの標準化

このたびの総合窓口課および税務課の特定個人情報保護評価に重要な変更が生じた主な理由は、**基幹システム標準化**である。

基幹システム標準化、ガバメントクラウドに関しては資料[B]をご参照。

ガバメントクラウドに関しては、国が構築・運用するものであることから、デジタル庁より特定個人情報保護評価について、資料[C]のとおりその考え方と記載例が示された。

区では区独自の評価に加えて、デジタル庁の示す記載例を参考にガバメントクラウドに関する評価を追記し、再評価を実施した。

基幹システム標準化及びガバメントクラウドについて

1. 基幹システム標準化、ガバメントクラウドへの移行

「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）（以下「標準化法」と記載）、及び「標準化法」において地方公共団体情報システムの標準化の推進を図るために政府が定めることとされている「地方公共団体情報システム標準化基本方針」（令和４年１０月７日閣議決定、令和５年９月８日改定を閣議決定、令和６年１２月２４日改定を閣議決定）（以下「標準化基本方針」と記載）に基づき、地方公共団体は基幹系情報システムの標準化やガバメントクラウドへの移行に取り組んでいる。

「標準化法」にて、住民の利便性の向上、地方公共団体の行政運営の効率化や互換性の確保を目的とし統一的な基準に適合した地方公共団体情報システム（標準準拠システム）を利用することとされている。また、クラウド・コンピューティング・サービス関連技術の活用（ガバメントクラウドへの移行）も努力義務とされている。

2. ガバメントクラウドにおけるリスク対応策の概要

一般的に呼称されるクラウドサービスとはインターネットを通じて提供されるソフトウェアやアプリケーションを指し、企業や自治体がシステム導入時に実施していた機器の調達・導入が省略可能なため、経費面や迅速性・柔軟性などのメリットがうたわれている。ただし、企業や自治体の保有データが外部保管となるためセキュリティ上の適切な対処が求められる。

一方で、国が構築・運用するガバメントクラウドは、アクセスが限定される閉域のネットワーク環境上に構築されるものであり、一般的なクラウドサービスと比べてセキュリティリスクは大幅に低減される。

「標準化法」では、地方公共団体の基幹系情報システムをガバメントクラウドへ移行することが努力義務とされており、ガバメントクラウドを提供するクラウドサービス事業者の選定においては、デジタル庁の定める必要なセキュリティ対策やガバナンス機能を具備することが要件とされている。

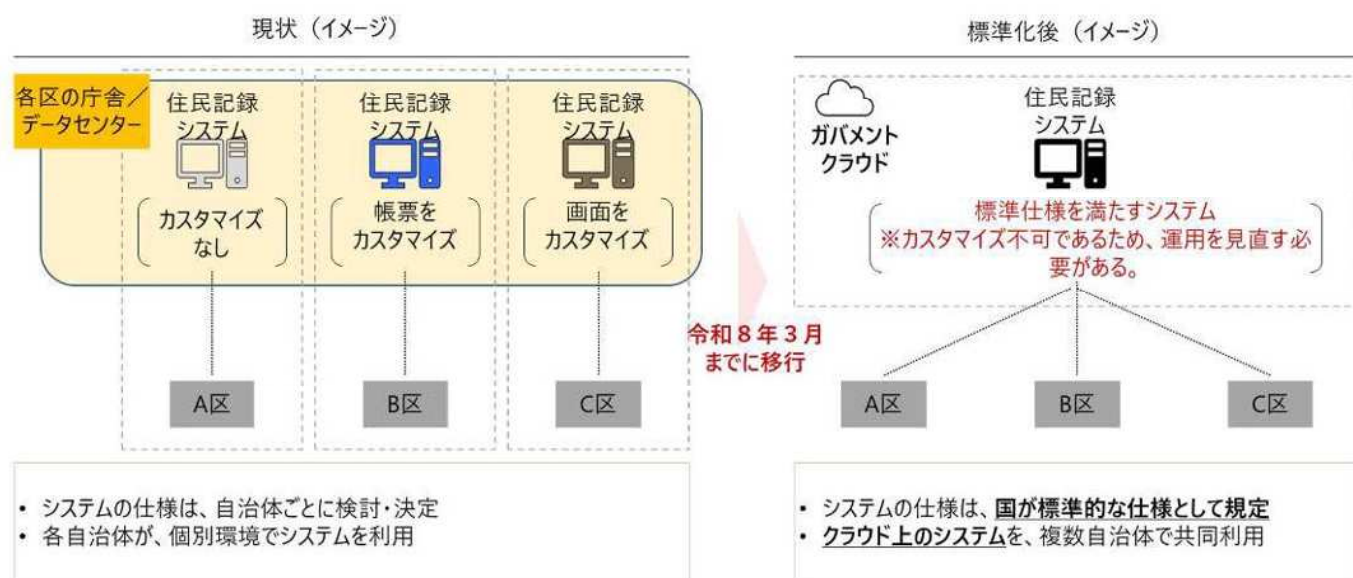
具体的なセキュリティ対策の例を２つ挙げる。

１つ目は「政府情報システムのためのセキュリティ評価制度」（以下、ISMAP と記載）である。政府機関等での導入に当たり、情報セキュリティ対策が十分に実施されていることを評価するため令和２年６月に、NISC・デジタル庁・総務省・経済産業省を所管省庁として運用を開始した。ガバメントクラウドも ISMAP に登録されていることが必要となっている。

2つ目は、デジタル庁が、クラウド利用に最適化されたベースラインのセキュリティ設定を目的に、ガバメントクラウド上のシステムへ適用を強制している「必須適用テンプレート」である。これにより不正な操作を事前に防止する「予防的統制」、管理リソースのモニタリング及び不正の検出を行う「発見的統制」などの機能が具備される。

一方、本区の庁舎からガバメントクラウドをつなぐネットワーク環境は本区の調達となっている。このセキュリティ対策を適切に実施するため、庁舎からガバメントクラウドへのネットワーク回線を閉域ネットワークとし第3者の利用を除外している。さらにガバメントクラウド上の当区住民情報システムまでの接続構成は、デジタル庁発行ドキュメント「ガバメントクラウド利用における推奨構成」に準拠し対策を講じている。

令和7年2月時点、デジタル庁のHPには「ガバメントクラウドは、セキュアでコスト効率の高いシステムとして導入するものであり（中略）「最新かつ最高レベルの情報セキュリティを確保できること」や「データ保存の安全性を確保できること」などの基準を満たすことが必須であるとして（後略）」と記載があり、今後も高い情報セキュリティが保たれると推察できる。



<情報システム標準化の移行イメージ>

ガバメントクラウドにおける特定個人情報保護評価について

令和4年10月 デジタル庁

1. 「重要な変更」について

行政機関の長等は、特定個人情報ファイルを保有しようとする場合には、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第二十七号）（以下「番号法」という。）第二十八条の規定に基づき、特定個人情報保護評価を実施する必要があります。

(1) 「重要な変更」の該当性の判断

貴市町村においては、既存のシステムについてはすでに同条に基づき特定個人情報ファイルを取り扱う事務ごとに特定個人情報保護評価を実施されているところであると認識しております。

他方、同条後段において、特定個人情報ファイルを取り扱う事務について、重要な変更が発生する場合には、重要な変更を加える前に特定個人情報保護評価を再実施することとされています。

「重要な変更」とは、特定個人情報保護評価に関する規則（平成二十六年特定個人情報保護委員会規則第一号）（以下「規則」という。）第十一条に基づき、特定個人情報保護評価指針（平成二十六年特定個人情報保護委員会告示第四号）（以下「指針」という。）第6の2（2）において、当該指針の別表に定める重点項目評価書及び全項目評価書の以下の項目が変更されることをいうものとされています。

基礎項目評価書については、「重要な変更」が規定されていないため、評価の再実施は不要です。

なお、上記に関わらず、重点項目事項評価書・全項目評価書に重要な変更に当たらない変更が生じる場合又は基礎項目評価書にしきい値判断の結果の変更該当しない変更が生じた場合には、規則第十四条及び指針第7の規定に基づいて、必要な修正を行う必要がありますので、そのような変更が生じないかについて検討・確認をお願いします。

【参考】特定個人情報保護評価指針 別表

別表（第6の2（2）関係）	
特定個人情報保護評価書の名称	重要な変更の対象である記載項目
1 重点項目評価書	1 個人番号の利用 2 情報提供ネットワークシステムによる情報連携 3 特定個人情報ファイルの種類 4 特定個人情報ファイルの対象となる本人の範囲 5 特定個人情報ファイルに記録される主な項目 6 特定個人情報の入手元 7 特定個人情報の使用目的 8 特定個人情報ファイルの取扱いの委託の有無 9 特定個人情報ファイルの取扱いの再委託の有無 10 特定個人情報の保管場所 11 リスク対策（重大事故の発生を避ける。）
2 全項目評価書	1 特定個人情報ファイルを取り扱う事務の内容 2 個人番号の利用 3 情報提供ネットワークシステムによる情報連携 4 特定個人情報ファイルの種類 5 特定個人情報ファイルの対象となる本人の範囲 6 特定個人情報ファイルに記録される主な項目 7 特定個人情報の入手元 8 特定個人情報の使用目的 9 特定個人情報の使用部署 10 特定個人情報の使用方法 11 特定個人情報の突合 12 特定個人情報の統計分析 13 特定個人情報の使用による個人の権利利益に影響を及ぼす決定 14 特定個人情報ファイルの取扱いの委託の有無 15 取扱いを委託する特定個人情報ファイルの対象となる本人の範囲 16 特定個人情報ファイルの取扱いの再委託の有無 17 特定個人情報の保管場所 18 特定個人情報ファイルの取扱いプロセスにおけるリスク対策（重大事故の発生を避ける。） 19 その他のリスク対策

(2) 特定個人情報保護評価の再実施の時期

「重要な変更」に該当する場合には、特定個人情報保護評価の再実施の時期については、ガバメントクラウド上に副本データを移行するまでに評価を実施する必要があります。

2. 記載例について

指針第3の2においては、「特定個人情報ファイルを保有しようとする者又は保有する者以外に特定個人情報ファイルに関わる者が存在する場合は、その者は、特定個人情報保護評価が適切に実施されるよう協力するものとする。」とされております。

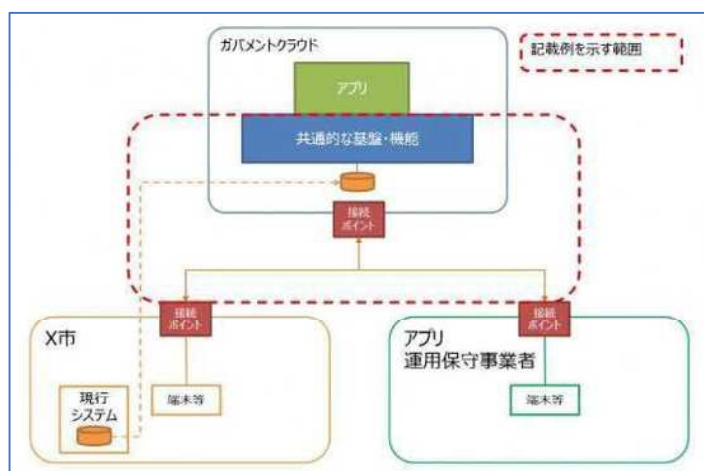
今般、ガバメントクラウドはデジタル庁が調達したことから、次の(1)及び(2)の考えに基づいて記載例を策定し、別紙のとおり提供するものです。

各市町村におかれては、番号法をはじめとする個人情報保護に関する法令の趣旨を踏まえ、記載例を含む今回の情報提供を参考に適切に評価を実施してください。

なお、内容については、令和4年8月30日時点の情報に基づき、個人情報保護委員会事務局と調整済みのものです。

(1) 記載例の射程

今回提供する記載例については、評価書に記載する内容のうち、ガバメントクラウドのクラウド事業者が提供するクラウド上の基盤及び接続に関する部分になります。



記載例を示していない箇所であっても、特定個人情報保護評価の趣旨に鑑み、上記の射程以外に関する部分について、別途記載が必要となりますので、ご留意下さい。

具体的には、委託に関する項目について、ガバメントクラウドへ移行する際のデータ抽出、移行、破棄においては委託先が特定個人情報を扱うことが想定されますので、各団体において追記する必要があります。

(2) 記載例において「重要な変更」に該当する項目

ガバメントクラウド上にシステムを構築するにあたり、上記 2 (1) の範囲において、変更が想定されるのは、次に掲げる項目です。

記載例においては、これらの項目において必要な情報を記載しています。

<重点項目評価書>

- 10 特定個人情報の保管場所
- 11 リスク対策

<全項目評価書>

- 17 特定個人情報の保管場所
- 18 特定個人情報ファイルの取扱いプロセスにおけるリスク対策
- 19 その他のリスク対策

なお、デジタル庁及びクラウドサービス事業者は特定個人情報にはアクセスしないため、クラウドサービス事業者は番号法上の「委託」先には当たらないと解されますので、委託に関する別表の以下の項目に関しては変更を想定しておりません。

<重点項目評価書>

- 8 特定個人情報ファイルの取扱いの委託の有無
- 9 特定個人情報ファイルの取扱いの再委託の有無

<全項目評価書>

- 14 特定個人情報ファイルの取扱いの委託の有無
- 15 取扱いを委託する特定個人情報保護ファイルの対象となる本人の範囲
- 16 特定個人情報ファイルの取扱いの再委託の有無

以上

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 ※		＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②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。		
②保管期間	期間	[	＜選択肢＞ 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない	]
	その妥当性			
③消去方法		＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしがたって確実にデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。		
7. 備考				

Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※(7. リスク1⑨を除く。)

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		
①NISC政府機関統一基準群	[]	<選択肢> 1) 特に力を入れて遵守している 2) 十分に遵守している 3) 十分に遵守していない 4) 政府機関ではない
②安全管理体制	[]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
③安全管理規程	[]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
④安全管理体制・規程の職員への周知	[]	<選択肢> 1) 特に力を入れて周知している 2) 十分に周知している 3) 十分に周知していない
⑤物理的対策	[]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
	具体的な対策の内容	<ガバメントクラウドにおける措置> ①ガバメントクラウドについては政府情報システムのセキュリティ制度(ISMAP)のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。
⑥技術的対策	[]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
	具体的な対策の内容	<ガバメントクラウドにおける措置> ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」(令和4年10月 デジタル庁。以下「利用基準」という。))に規定する「ASP」をいう。以下同じ。又はガバメントクラウド運用管理補助者(利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。)は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、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。 ⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。
⑦バックアップ	[]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
⑧事故発生時手順の策定・周知	[]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[]	<選択肢> 1) 発生あり 2) 発生なし
	その内容	
	再発防止策の内容	
⑩死者の個人番号	[]	<選択肢> 1) 保管している 2) 保管していない
	具体的な保管方法	

その他の措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク2: 特定個人情報が古い情報のまま保管され続けるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク3: 特定個人情報が消去されずいつまでも存在するリスク			
消去手順	[]	<選択肢> 1) 定めている	2) 定めていない
手順の内容	<ガバメントクラウドにおける措置> データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。		
その他の措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置			

IV その他のリスク対策 ※

1. 監査

①自己点検	[	＜選択肢＞ 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的なチェック方法		

②監査	[] ＜選択肢＞ 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的な内容	＜ガバメントクラウドにおける措置＞ ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP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。

2. 従業者に対する教育・啓発

従業者に対する教育・啓発	[<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的な方法	

3. その他のリスク対策

＜ガバメントクラウドにおける措置＞
ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。
ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。
具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。