

「住民基本台帳に関する事務に係る特定個人情報保護評価書(全項目評価書)(案)」に関する  
意見募集(パブリックコメント)の結果について

1. 意見募集の概要

募集期間	令和 8 年 6 月 3 日(水)から令和 8 年 7 月 3 日(金)
閲覧場所	区政推進課、情報公開室、各区市民保険年金課・支所・地域センター
意見の提出方法	直接持参、郵送、ファックス、電子メール
意見の提出先	区政推進課

2. 意見募集の結果

提出意見 意見数 1 件(1 人)

意見要旨
<p>私は岡山市民ではありませんが、自治体 DX、住民基本台帳、マイナンバー、特定個人情報保護、行政サービスの安全管理に関心を持つ個人として、意見を提出します。</p> <p>本件は、岡山駅地下マイナンバーカード臨時交付センターを拡充し「マイナンバーカードセンター」として、土日・夜間を含めた受付体制を整えるとともに、交付前設定処理等のマイナンバーカード関係事務・管理を集約して実施することに伴う、住民基本台帳に関する事務の特定個人情報保護評価であると理解しています。</p> <p>住民基本台帳に関する情報は、氏名、住所、生年月日、性別、世帯、転入・転出、マイナンバー等と結びつく極めて重要な情報であり、行政サービスの基盤となるものです。万一漏えいした場合、なりすまし、詐欺、二次被害、長期的なプライバシー侵害につながる可能性があるため、極めて慎重な安全管理措置が必要だと考えます。</p> <p>私自身も、過去にクレジットカード情報の漏えい被害や、写真販売サイトにおける個人情報漏えいの当事者となった経験があります。こうした経験から、個人情報漏えいは単なる一時的な事故ではなく、対象者に不安や確認作業、二次被害への懸念を長く残す問題だと感じています。</p> <p>また、近時の公表事例として、2026 年 6 月には、九州電力送配電株式会社において、お客さま情報を保存した外部記憶媒体が所在不明となる事案が発生しています。同社の公表によれば、需要者名、供給場所住所、使用電力量データ、電話番号等の情報が最大 1,090 万口分保存されていたとされ、現時点で流出の事実は確認されていないものの、社外に漏えいのおそれがあるとされています。</p> <p>この事案は、重要情報が外部記憶媒体やバックアップ環境に保存されている場合、保管場所、施錠、持ち出し管理、棚卸し、委託先・関係者の取扱いなど、人が介在する運用のわずかな不備によって、大規模な漏えいリスクが生じ得ることを示す具体例だと考えます。</p>

今回のように、マイナンバーカード関係事務・管理を集約し、受付体制や処理体制を拡充する場合、住民の利便性は高まる一方で、重要な特定個人情報が集約されることによるリスクも高まります。そのため、従来の「侵入を防ぐ」「アクセス権限を管理する」「ログを取得する」「暗号化する」といった対策に加えて、万一データが外部に流出した場合でも、流出したデータ単体では意味を持たず、復元・悪用されにくい状態にしておく設計が重要だと考えます。暗号化は重要な基礎対策ですが、どの情報を暗号化対象とするかの判断、鍵の管理、権限設定、運用ルールの徹底などに人が関与します。そのため、設定ミス、鍵管理の不備、誤送信、端末紛失、外部記憶媒体の紛失、委託先での取扱いミスなど、人が介在することによる漏えいリスクを完全に防ぐことは難しいと考えます。

さらに、量子コンピューターの発展により、現在広く使われている暗号方式が将来的に危殆化する可能性について、NIST等の専門機関も警鐘を鳴らしています。耐量子暗号への移行は重要ですが、方式によっては公開鍵、署名、暗号文等のサイズが大きくなり、通信・記憶・処理・運用負荷が増える可能性があります。そのため、暗号方式の強化だけに依存するのではなく、データそのものを分散・無意味化し、一部が流出しても単体では復元・悪用されにくい状態にする多層的な対策が必要だと考えます。

一方で、秘密分散、データ無意味化、分散保管といった考え方は、通常の業務で保存・利用されるデータについて、利用者が個別に暗号化対象を判断しなくても、システム側で自動的に保護し、データの一部が流出しても単体では意味を持ちにくい状態にする方向性の対策です。

つきましては、評価書案における安全管理措置、委託先管理、マイナンバーカードセンターにおける事務処理・管理、システム運用、バックアップ環境等において、以下の観点を明確に位置付けることを要望します。

1. 住民基本台帳に関する特定個人情報ファイルについて、流出したデータ単体では意味を持たず、復元・悪用されにくい状態にする「データ無意味化」「秘密分散」「分散保管」等の技術的対策を検討対象に含めること。
2. マイナンバーカードセンターへの事務・管理の集約に伴い、職員端末、委託先、再委託先、クラウド環境、バックアップ環境、外部記憶媒体等からの流出を想定し、漏えい時の被害を最小化する設計を安全管理措置に含めること。
3. 暗号化、アクセス制御、認証、ログ監視等の従来対策に加えて、「データそのものを、外部に出ても単体では悪用されにくい状態にする」という観点を評価項目に加えること。
4. 住民基本台帳やマイナンバーカード関係事務は、行政サービス全体の基盤であるため、利便性や処理効率の向上だけでなく、住民の信頼を確保するため、情報漏えい時の被害最小化を調達仕様や運用設計の中で重視すること。
5. 将来的な量子コンピューター時代の暗号危殆化や耐量子暗号への移行負荷も踏まえ、暗号方式だけに依存しない多層的なデータ保護を検討すること。

特定の企業や製品の採用を求めるものではありません。秘密分散、データ無意味化、分散保

管といった技術カテゴリを、住民基本台帳及びマイナンバーカード関係事務における特定個人情報を守るための選択肢として、明確に検討していただきたいという趣旨です。

今後の自治体 DX では、「情報を漏らさない」対策に加え、「万一漏えいしても、漏えいしたデータだけでは悪用されにくい」対策がますます重要になると考えます。住民基本台帳に関する事務の特定個人情報保護評価においても、この観点をより明確に反映していただくことを要望します。

#### 意見に対する市の考え方

ご意見いただきましたとおり、様々な通信技術の向上や多様な変化を見込み、今後も継続的に個人情報保護評価の見直しを行っていきたいと考えております。