

デジタル庁に対す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及び個人情報の保護に関する法律に基づく行政上の対応について

令和 5 年 9 月 ● 日
個人情報保護委員会

第 1 事案の概要等

1 事案の概要

公金受取口座は、公金受取口座登録制度に基づきデジタル庁が管理する「口座情報登録・連携システム」において登録・管理されているところ、本件は、同登録手続を支援するマイナポイント支援窓口（市区町村に設置。以下「支援窓口」という。）において、共用端末を用いたマイナポータル経由の登録支援を行っていた際、本人又は手続を支援する者による操作ミス（ログアウトの失念）等により、別人のマイナナンバーと銀行口座情報を紐付けた、公金受取口座の誤登録事案である。

2 当委員会の調査経緯

個人情報保護委員会（以下「当委員会」という。）は、本件に関し、デジタル庁に対して、令和 5 年 6 月 15 日、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 25 年法律第 27 号。以下「番号法」という。）第 35 条第 1 項に基づく報告徴収を実施し、同月 16 日、デジタル庁から個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）第 68 条第 1 項に基づく漏えい等報告を受領、同月 30 日、前記報告徴収に対する報告書を受領した。その後、更なる事案解明に向けた調査を行うため、同年 7 月 19 日、当委員会は、番号法第 35 条第 1 項に基づくデジタル庁への立入検査を開始した。

3 公金受取口座の登録について

公金受取口座の登録は、マイナポータル経由での登録又は所得税の確定申告（還付申告）での登録の方法があるところ、本件はマイナポータル経由での登録において発生した。

マイナポータル経由での公金受取口座の登録では、本人がパーソナルコンピュータ（以下「PC」という。）又はスマートフォン・タブレット（以下「スマートフォン等」という。）を用いて以下の登録フローを操作することで、デジタル庁に公金受取口座の申請・登録が行われる。

- (1) 本人がマイナナンバーカードを読み取り機にかざし（利用者証明用電子証明書の情報を送信）、4桁の暗証番号（電子証明番号）を入力することにより、マイナポータルにログインする。
- (2) マイナポータルのトップメニューより公金受取口座の登録・変更に移行し、本人

情報登録画面①にて、本人が、マイナンバーカードを読み取り機にかざし（券面事項入力補助アプリケーションの情報を送信）、4桁の暗証番号（電子証明番号）を入力することにより、マイナンバー、漢字氏名、生年月日及び住所を入力（自動入力のため修正は不可）する。

- (3) 本人情報登録画面②にて、本人が、氏名カタカナ、電話番号及びメールアドレスを入力（手動入力）する。この際、前記(2)の漢字氏名と本操作で本人が入力した口座名義人欄の氏名カタカナの同一性に関するシステムチェックは行っていない。
- (4) 口座情報入力画面にて、本人が、金融機関名、支店名、口座種別及び口座番号を入力（手動入力）する。この際、口座名義人欄の氏名は、本人情報登録画面②で入力した氏名カタカナが自動反映される。
- (5) 口座情報入力画面で入力された口座情報については、統合ATMスイッチングサービス¹を用いて口座実在性の確認を行っており、入力された口座が実在した場合のみ登録が可能となる。
- (6) 確認画面にて、本人が、本人情報及び口座情報に誤りがないか確認をし、利用規約に同意した後、登録が行われる²。

4 マイナポイント支援窓口

マイナポイント支援窓口は、自身の端末（PC又はスマートフォン等）を持たずマイナポイント申込手続を行うのが難しい国民の利用手段として提供され、総務省の施策であるマイナポイント事業により、市区町村に任意設置された。

同支援窓口では、市区町村の職員又は市区町村との間で委託契約を締結した支援事業者所属の支援員（以下、総じて「支援員」という。）が手続支援を行っていた。同手続支援の実施にあたり、総務省から、「マイナポイント申込支援マニュアル」が配布されるとともに、同支援の際、①支援員は本人の登録補助のみを行うこと、②支援窓口では同一の端末を多くの住民で連続・共用して使用するため、履歴等が残らないようにログアウト確認及び端末シャットダウン等の措置を行うことを徹底すること等の指示が行われていた。

¹ ATM・インターネットバンキングにおける他金融機関との取引を中継するサービスで、本件では金融機関名・支店名・口座番号等から口座が金融機関に実在しているかを確認することができる。

² 本件誤登録事案の発覚を受けて、デジタル庁は、令和5年6月23日、同登録操作完了時に、再度のマイナンバーカード読み取りを行い、前記(1)で使用したマイナンバーカードとの同一性を確認（ログアウト忘れ防止機能）するシステム仕様変更を行った。

第2 事実関係

1 公金受取口座登録開始までの経緯

- (1) 令和3年3月4日、内閣府番号制度担当室（当時）は、当委員会に対し、公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律（令和3年法律第38号。以下「口座登録法」という。）案に関する事務の特定個人情報保護評価につき相談を開始した。
- (2) 同年10月20日、当委員会は、デジタル庁（同年9月1日発足）の作成した公的給付支給等口座登録簿への登録等に関する事務の特定個人情報保護評価に係る全項目評価書を審査し、承認した。
- (3) 同年11月19日、「マイナポイント第二弾」としてマイナポイントを付与する追加政策（公金受取口座登録を含む。）が決定³された。
- (4) 令和4年3月28日、デジタル庁は、口座情報登録・連携システムをリリースし、マイナポータルを經由した公金受取口座登録サービスを開始した。
- (5) 同年6月24日、デジタル庁は、市区町村に対して「公金受取口座登録に対する手続支援及び端末の設定について」と題する事務連絡を発出し、来庁者の利用の都度、ログアウト等の履歴等を残さないための措置を実施するように注意喚起する内容が含まれる事務手順を周知した。
- (6) 同月30日、「マイナポイント第二弾」として公金受取口座登録に伴うマイナポイント付与政策の開始に伴い、市区町村の支援窓口における手続支援が開始された。同政策開始後の公金受取口座登録数は、飛躍的に増加した（同年4月から6月における月間登録件数は約30万～約90万件、同年7月は月間約670万件。）。

2 漏えい事案発生に対するデジタル庁の対応

- (1) 令和4年7月19日、豊島区内の支援窓口において、公金受取口座の誤登録（デジタル庁の保有個人情報である公金受取口座情報の漏えい。以下「誤登録」と記載した事案につき同旨。）事案が発生し、同月20日、同区からデジタル庁公金受取口座事務担当職員A（以下「A職員」という。）に対し、同誤登録について報告があった。A職員は、同日、デジタル庁公金受取口座事務担当管理職B（以下「B管理職」という。）に対し、同事案の発生報告をした。B管理職は、デジタル庁内において、それ以上の報告を実施しなかった。その後、同区とデジタル庁にて、誤登録状況の

³ コロナ克服・新時代開拓のための経済対策。マイナンバーカードの普及を促進するとともに、消費喚起や生活の質の向上につなげるため、①マイナンバーカードを活用して幅広いサービスや商品の購入などに利用できるマイナポイント（1人当たり最大2万円相当）を付与すること、②公金受取口座の登録を行った者に7500円相当のポイントを付与すること等が明記された（閣議決定）。

解消と本人説明の内容等を協議し、対応を終了した。B管理職は、同対応終了にあたり、A職員を含む公金受取口座事務担当職員らに対し、同種誤登録事案が発生したことをデジタル庁として把握するための具体的指示（管理職に全ての事案を報告させる指示や、職員間で発生件数を共有し、記録させる指示等。）を行うことはなかった。

- (2) 同年8月30日、盛岡市内の支援窓口において、公金受取口座の誤登録が発生し、同年9月2日、同市からデジタル庁の公金受取口座事務担当職員C（以下「C職員」という。）に対し、同誤登録について報告があった。C職員は、同事案について、B管理職に対し報告せず、誤登録事案が再発したことはデジタル庁内で共有されなかった。C職員は、他の公金受取口座事務担当職員に相談するなどした上で、前記(1)事案（豊島区）と同様の誤登録の解消と本人説明に関する内容を同市に確認するなどした後、対応を終了した。
- (3) 以降、同年11月頃から令和5年4月10日までの間、デジタル庁公金受取口座事務担当職員らは、4市区町村から、支援窓口における公金受取口座の誤登録に関する報告を受けたが、いずれもB管理職には報告せず、前記(2)と同様の対応を行い、誤登録の解消を確認した後、その対応を終了した。

なお、令和4年11月頃、同種誤登録事案の連続発生を受け、C職員は、他の公金受取口座事務担当職員に相談するなどした上で、地方公共団体向けコールセンターに対して同種誤登録事案が報告された際の対応手順書を提供し、事務対応の効率化を行った。この際、デジタル庁が、市区町村に対して、同種誤登録事案が相次いで発生している旨を周知することはなかった。

- (4) 令和5年4月10日、福島市内の支援窓口において、ログアウト漏れを原因とする公金受取口座の誤登録が発生し、同月11日、同市からデジタル庁公金受取口座事務担当職員D（以下「D職員」という。）に対し、同誤登録について報告があった。同市は、同報告の際、「他にも同様の誤登録が発生している懸念があるため、同市から住民に対して、各自の口座情報が正しく登録されているかをマイナポータル上で確認するように呼びかけたい。そこで、デジタル庁において、福島市住民に関し同様の誤登録が他に発生していないか調査して欲しい。」旨依頼を行った。同依頼を受けたD職員は、同市の事案は複数のアカウントに同一の口座が登録されている事象に伴って発生していることを突き止めた上で、同日、同市の前記依頼に関するデジタル庁としての対応を協議すべく、B管理職へ報告を行った。D職員及びB管理職は、同市の前記依頼事項に対応するために、口座情報登録・連携システムから複数のアカウントに同一の口座が登録されているデータを抽出する調査方針を決定した。B管理職は、この方針に基づき口座情報という機微情報を同市に提供するにあたっては、組織としての判断が必要と考え、同日、デジタル庁公金受取口座事務担当統括官E（以下「E統括官」という。）に対し、同誤登録事案（福島市に限る。）

及び同市の前記依頼事項について、口頭報告を行った。E 統括官は、同市に対する情報提供が必要と判断した上で、B 管理職に対し、同誤登録事案については詳細を確認した上で、追加の報告を上げるよう指示した。

同月 19 日、D 職員及び B 管理職は、福島市居住の公金受取口座登録者を対象として調査（口座情報登録・連携システムから複数のアカウントに同一の口座が登録されているデータを抽出。）した結果、誤登録の可能性がある事案が、同市が当初報告した 1 件の他に 3 件発生していることを認知した。同日、D 職員及び B 管理職は、E 統括官に対し、同市において計 4 件の誤登録が発生している旨と、誤登録が発生しているアカウントの本人情報及び誤登録の可能性がある口座情報に関する同市への情報提供の可否を改めて相談し、E 統括官はこれを許可した。同月 20 日、D 職員は、同市に対し、前記 4 件の誤登録事案に関する本人情報及び口座情報を提供し、本人対応結果等の共有を依頼した。

同年 4 月 28 日から同年 5 月 10 日にかけて、福島市は、誤登録のあった対象者のうち 3 名への説明及び経緯の聞き取りを実施し、誤登録は同市内の支援窓口におけるログアウト漏れが原因であると確認した（同年 5 月 10 日、同市は、同確認結果をデジタル庁に報告した。）。

同月 18 日、福島市は、誤登録のあった対象者全員への説明を完了した。

同月 19 日、B 管理職及び E 統括官は、福島市との本人対応結果共有の過程において、同市が同事案の経緯を近日中に对外公表する旨の情報を得たことから、同市における同誤登録事案の発生につき、デジタル大臣室へ報告を行った。

- (5) 同月 20 日、B 管理職及び E 統括官は、河野デジタル大臣に対し、前記(4)の福島市における誤登録事案 4 件を報告すると共に、過去に他の市区町村でも同様の誤登録事案が発生しており、デジタル庁公金受取口座事務担当職員らがその発生報告を受けていた旨説明した。
- (6) 同月 23 日、福島市及びデジタル庁は、前記(4)の誤登録事案の発生を公表した。同日、デジタル庁は、公金受取口座の総点検を実施する旨公表した。

3 発生事象の詳細

(1) 福島市の誤登録について

- ア 福島市内の支援窓口において、来庁者 X がマイナポイント登録のためマイナポータルアカウントにログインした（前記第 1 の 3(1)）。X は、公金受取口座登録の手続を行おうとしたものの、口座番号がわからないなどの理由により同手続を中止したが、ログアウトをせずに支援窓口を離れた。X の離席後、X に対応していた支援員は、ログアウト確認及び端末シャットダウン等の措置を行わなかった。
- イ 次に、来庁者 Y が、X のマイナポータルアカウントにログインしている状態の端末を操作し、公金受取口座登録の手続を開始した。その結果、Y は、X のマイ

ナポータルアカウントにログイン中の画面において、公金受取口座登録の操作（前記第1の3(4)）を開始し、Yの口座情報を入力したため、Xのアカウント（マイナンバーを含む）に紐づくXの公金受取口座登録情報欄に、Yの銀行口座情報が登録された。

ウ その後、Yが、登録情報を確認しようなどと考え、Yのマイナポータルにログインしたところ、自己の公金受取口座情報の登録が未了状態であることを認識した。Yは、Yのマイナポータルアカウントにログイン中の画面で、再度公金受取口座登録の手続きを行い、Y自身の口座情報を入力して登録した。

その結果として、XのアカウントとYのアカウントの双方に、来庁者Yの口座情報が紐付くこととなった。

エ その後、Xが、公金受取口座登録の手続きを改めて行おうと考え、再度、福島市内の支援窓口に来庁し、Xのマイナポータルアカウントにログインしたところ、Yの口座情報が既に登録されていることを認識した。Xは、Xのマイナポータルアカウントにログイン中の画面で、公金受取口座の変更手続きを行い、X自身の口座情報を入力（Yの口座情報を上書き）して登録した。

(2) 公金受取口座の総点検で判明した誤登録について

ア デジタル庁は、前記福島市事案の発生を機に、令和5年5月下旬頃、全国の市区町村に対して、ログアウト漏れを原因とする公金受取口座の誤登録の発生調査を依頼し、前記2(1)乃至(4)を含む計16市区町村（22件）にて誤登録が発生していることを確認した。

イ デジタル庁は、福島市の事案と同様に複数のアカウントに同一口座が登録されている事象の発生有無を調査し、そのうち、誤登録のおそれがある事例を940件確認した（同年6月22日時点）。

ウ デジタル庁は、前記イの調査の過程において、複数のアカウントに同一の口座が登録されている事象のうち、アカウントの本人情報（住基4情報から登録されたもの）の住所と姓が一致（住所又は姓の一方が一致する場合を含む。）する登録事例（同日時点で約14万件の存在を確認。）については、親族関係又は内縁関係にある者の口座（以下、総じて「家族口座等」という。）を本人が意図的に登録した事例として、誤登録とは別に分類している。

第3 問題の所在

1 前提となる法律上の整理

(1) 「口座情報登録・連携システム」は、デジタル庁の特定個人情報ファイル（番号法第2条第9項）かつ個人情報ファイル（個人情報保護法第60条第2項）である「口座情報登録・連携ファイル」を取り扱うシステムであり、同システム内で管理されている「公金受取口座情報」はマイナンバーに紐付けられた本人情報（氏名、

住所等)及び口座情報の総称であるから、デジタル庁が保有する特定個人情報(番号法第2条第8項)かつ保有個人情報(個人情報保護法第60条第1項)に該当する。

- (2) デジタル庁は、公金受取口座情報の取扱いに関し、番号法上の個人番号利用事務実施者(番号法第2条第12項)の義務を負うとともに、マイナンバーを含まない保有個人情報の取扱いについては個人情報保護法上の行政機関等(個人情報保護法第2条第11項)の義務を負う。

具体的には、デジタル庁において、口座情報登録・連携システムを開発し運用する上で誤登録を防ぐためのマイナンバー取得時の本人確認の措置(番号法第16条)や、漏えい防止等の安全管理措置(番号法第12条、個人情報保護法第66条第1項)等を講ずる義務を負う。

- (3) なお、マイナポータル経由での公金受取口座登録の事務において、デジタル庁は、その提供する口座情報登録・連携システムを本人に直接利用させていた(市区町村に設置された支援窓口においても、支援員は本人の登録補助を行う旨定められていた。)。すなわち、誤登録の直接原因となった端末操作の実施場所が市区町村であったとしても、公金受取口座情報が漏えいした場合は、デジタル庁の保有個人情報の漏えい(個人情報保護法第68条第1項)に該当する。

2 誤登録に関する問題点

(1) 直接的原因

公金受取口座の誤登録の直接的な原因は、支援窓口において、先にマイナポータルアカウント上で手続を開始したXが、ログアウト確認不徹底などによりログアウトを失念した結果、後に手続を開始したYが、Xのマイナポータルアカウントに紐付けて、Yの口座情報を登録したことである。

(2) 問題点の分析

公金受取口座の目的は、緊急時の特別給付金のほか、年金、児童手当、所得税の還付金等、幅広い公的給付等の支給事務に利用されるものであり、マイナンバーを保有する全ての者が登録できる状態を維持することが求められる。そのためには、登録者が自身の端末を用いた円滑な登録を可能ならしめる高品質なユーザビリティも重要であり、独力では手続を行うことが困難である者に対して、支援窓口等の代替手段が提供されることも重要である。

このような老若男女様々な登録者が想定される事務において、全ての者の安全性を確保して公金受取口座を登録するためには、「誤操作の発生を前提として、予め

対策を講ずる考え方（フルプルーフ⁴）」が何より必要である。この観点から、デジタル庁が実施したシステム開発及び制度運用において適切に安全性が確保されていたか、支援窓口等の環境下でも誤った操作が発生することを想定し対処できていたかを検討することが、重要な論点となる。

3 家族口座等登録に関する問題点

(1) 直接的原因

公金受取口座に家族口座等が登録されることの直接的な原因は、現行システム上、公金受取口座の本人情報（前記第1の3(2)でマイナンバーカードから読み取った漢字氏名）と、口座情報（前記第1の3(3)で本人が氏名カタカナとして入力し、同(4)で自動入力された口座名義人の氏名カタカナ）の一致確認が行えず、口座が金融機関に実在するか否かはシステムの的に確認できるものの、本人が意図的に本人名義でない口座情報を入力した場合は、システムの的に確認できないことにある。

(2) 問題点の分析

ア 口座登録法において、公金受取口座は、本人名義の預貯金口座（同法第2条第6項）、かつ、一人一口座と定められている（同法第3条第1項）ため、本人が公金受取口座に家族口座等を登録する行為は想定されていなかった。

イ もっとも、本人が家族口座等を自己の公金受取口座として意図的に登録（本人の個人情報として家族口座等情報をデジタル庁に提供）した場合、本人のマイナンバーに別人の口座情報が紐付く状態は不適切であるものの、本人が意図した通りの状況が生じている以上、原則として、デジタル庁による個人情報の漏えい（個人情報保護法第68条又は番号法29条の4で報告対象等となる事態）には該当しないと考えられる。

ウ しかしながら、デジタル庁は、後述の特定個人情報保護評価に係る評価書において「本人が入力した口座情報については、統合ATMスイッチングサービスを用いた口座情報の実在性確認を行い、正確性を担保する」などと記述していることや、前記口座登録法の規律を前提とした公金受取口座登録の目的からすると、家族口座等が登録されている状態は、解消されることが望ましい。

この点、デジタル庁は、家族口座等の問題を中長期的に解消すべき課題として認識していたところ、本件の発覚を受け、①マイナポータルにおいて家族口座等の登録変更又は削除を求める通知を実施すると共に、今後、②登録口座重複チェック機能の追加実装、③漢字氏名・カタカナ口座名義の検知モデルの開発及び検知精度の検証を踏まえた実装の検討、④戸籍法改正（令和5年法律第48号附則第

⁴ ソフトウェア開発等における信頼性確保のための設計手法の一つで安全工学上の考え方。

1 条第 3 号の施行) 後の漢字氏名・カタカナ口座名義の自動照合機能の実装等、具体的な再発防止策を実施していくことを予定している。

当委員会は、家族口座等の問題は解消されるべきとの観点から、これらの対策の実施状況を注視することとしたい。

第 4 法律上の問題点の検討

1 本人確認の措置 (番号法第 16 条)

- (1) 口座情報登録・連携システムは、本人が申請するマイナンバー及び公金受取口座情報等を登録する情報システムであることから、個人番号利用事務実施者であるデジタル庁は、口座情報登録・連携システムを通じて本人からマイナンバーの提供を受ける際に、マイナンバーカードの提示を受けることその他「その者が本人であることを確認するための措置」として政令で定める措置をとらなければならない⁵。
- (2) この点、デジタル庁は、公金受取口座の登録・変更に移した後の本人情報登録画面①で本人のマイナンバーカードを機械的に読み取ること (券面事項入力補助アプリケーションを用いたマイナンバーカード情報の取得⁶) 及び本人に 4 桁の暗証番号 (本人にしか知り得ない電子証明番号) を入力させることにより (前記第 1 の 3 (2))、マイナンバーを含む本人情報の提供を受けるとともに、政令で定められた本人確認措置を行っていたものである。
- (3) もっとも、「本人確認」には、身元確認⁷と本人認証⁸の側面があり、手続開始時にマイナンバーカードの所持確認 (身元確認) 及び暗証番号の確認 (本人認証) を行っていたとしても、手続全体を通じた申請者 (実行主体) の同一性確認 (手続全体を通じた本人認証) を十分に行っていないと、事務全体において必要な本人確認の目的を達成できない場合があることに、注意が必要である。

ア 公金受取口座登録手続は、マイナポータルアカウント情報、マイナンバー及

⁵ 番号法第 16 条、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施行令第 12 条、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施行規則 (以下「番号法施行規則」という。) 第 3 条。

⁶ 番号法施行規則第 3 条第 1 項第 2 号ニで示される本人確認のための措置。

⁷ 手続の利用者の氏名等を確認するプロセスのこと。この確認プロセスは、一般的には、氏名、住所、生年月日、性別等について、当該情報を証明する書類の提示を求めるなどにより実施される (2019 年 2 月 25 日 各府省情報化統括責任者連絡会議決定「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」3 頁等)。

⁸ ある行為の「実行主体」と、当該主体が主張する「身元識別情報」との同一性を検証することによって、「実行主体」が身元識別情報にあらかじめ関連付けられた人物であることの信用を確立するプロセスのこと。(同ガイドライン 3 頁等)。

び公金受取口座情報を、全て同一人の情報として適切に紐づけることで完了する一連の事務手続である。

それにも拘らず、本件では、支援窓口を介した場合において、この手続全体を通じた本人認証が十分に行われなかった結果、前記第2の3（福島市事案）のように、操作者Xのマイナンバーカード及び本人確認情報を機械的に読み取るフロー（前記第1の3(2)）の後、Xがログアウト等を実施しないまま登録作業を中断した際、別の操作者Yがその後の手続（前記第1の3(3)乃至(6)のフロー）を行うことにより、結局、本人確認をしたXのマイナンバーに、別人であるYの口座情報が紐づけられるという誤登録事案が発生していたものである。

- イ 確かに、デジタル庁は、前記のとおり政令で定められた方法での本人確認措置を実施していたものではあるが、法が本人確認を要求した趣旨は、本人認証にもあることからすると、事務全体の仕組みを考慮し、当該事務の完遂に必要な本人確認ができていないか否かについても検討する観点が必要であった。
 - ウ 法定された本人確認措置に加えて、本人認証の目的を達成するために講ずる具体的措置の内容（本件誤登録発覚後に追加された、前記第1の3(6)段階におけるログアウト忘れ防止機能等のシステムチェック機能による方法や、手続中断時のログアウトを徹底するなど運用で回避する方法等。）は、当該事務手続の実施者の裁量に委ねられるべきである。しかしながら、ログアウト管理を徹底した運用という人為的ミスが介在しうる方法を採用したのであれば、フルプールの観点から、その手段の妥当性と目的の達成状況を継続的に検討することは必須である。

この点、デジタル庁は、マイナンバーの提供を受ける際、本人に4桁の暗証番号（本人にしか知り得ない電子証明番号）を入力させる手法で本人認証性の確認を行っていたものであるが、この手法では、前記の通り、支援窓口を介した場合において手続全体を通じた本人認証を十分に担保できず、結果として、ログアウト漏れが原因と思料される事態が実際に発生したものである。それにもかかわらず、デジタル庁は、当該事態の発生を適切に組織内で共有せず、令和5年4月に福島市における誤登録事案（前記第2の2(4)）が発覚して同年6月にログアウト忘れ防止機能等を搭載するまでの間、実効的な対応をしなかったのであるから、本件では、デジタル庁が自ら選んだ本人認証の目的を達成するための具体的措置に関する継続的な検討が、不十分であったと言わざるを得ない。
- (4) 以上のことから、デジタル庁は、本人確認の措置を求める番号法16条の趣旨に鑑み、特にオンラインでマイナンバーに紐づく特定個人情報を取得する場合には、法定された本人確認措置に加え、複数の操作によって取得した特定個人情報の全項目につき同一人の情報であることを確認するため、公金受取口座登録手続全体を通じた実効的な本人確認の手法について、検討することが望ましい。

2 安全管理措置等（個人情報保護法第 66 条第 1 項・第 68 条第 1 項、番号法第 12 条）

(1) 保有個人情報の漏えい等発生時における報告体制

ア 行政機関等は、保有する保有個人情報の漏えいが発生した場合は、個人情報の保護のために定められた管理規程及び管理体制に従い、適切に組織内で報告等を行い、原因の分析及び再発防止のために必要な措置を講ずるための検討を行わなければならない⁹。

イ 前記規定を受け、デジタル庁が定めた「デジタル庁の保有する個人情報管理規程」では、個人情報保護法事務対応ガイド 4-8-11 に沿って、「保有個人情報の漏えい等安全管理の上で問題となる事案又は問題となる事案の発生のおそれを認識した場合に、その事案等を認識した職員は、直ちに当該保有個人情報を管理する個人情報管理者に報告しなければならず、個人情報管理者は、事案の発生した経緯、被害状況等を調査し、総括個人情報管理者に報告しなければならない」と規定されている。

ウ しかしながら、豊島区における誤登録事案（前記第 2 の 2(1)）が発生した際、デジタル庁公金受取口座事務担当職員は、担当管理職まで報告をしたものの、同職員及び担当管理職に、デジタル庁の保有する特定個人情報及び保有個人情報の漏えいであるとの意識が欠如していたことから、同(4)の福島市における事案が発生し事態が大事に至るまで、個人情報管理者及び統括個人情報管理者に報告しなかった。また、前記第 2 の 2(2)及び(3)の誤登録事案が発生した際は、同職員から担当管理職に対しても報告しなかった¹⁰。

エ 以上のことから、デジタル庁は、保有個人情報の漏えい等事案が発生した場合の対応に関する各規程の内容を全職員に正しく理解させた上で、報告対象事案が生じた際には、適時適切に組織体制上の上位者へ報告させ、事実関係を組織内で共有して安全管理上の対応を策定するための体制を整備するなど、組織的安全管理措置に改善が必要である。

(2) 取扱手順の見直し

ア 行政機関等は、特定個人情報等の取扱いを検討するに当たって、特定個人情報

⁹ 個人情報保護法第 66 条第 1 項。個人情報の保護に関する法律についての事務対応ガイド（以下「個人情報保護法事務対応ガイド」という。）4-8-11(1)～(5)。

¹⁰ その他、デジタル庁「情報セキュリティインシデント対応手順書」に、本件のような要機密情報の漏えい案件については、統括官等のデジタル庁幹部やデジタル庁 CSIRT に報告を行わなければならないと規定されており、前記第 2 の 2(1)乃至(3)の事案は同規定の報告対象でもあったが、同規定も担当者の理解不足等により遵守されず、統括官及びデジタル庁 CSIRT に報告されることはなかった。

等の範囲及びその取り扱う職員を明確にした上¹¹、明確化した事務の取扱手順を策定し、必要に応じて見直さなければならない¹²。

イ デジタル庁は、本人が自身の端末を用いて公金受取口座を登録する方法又は本人が支援窓口を設置された共用端末を用いて公金受取口座を登録する方法によりマイナンバーの提供を受ける事務手続に関し、令和4年3月、「口座情報登録・連携システム利用に関する利用規約」を公表し、その事務手順を明確化した。

また、同年6月、公金受取口座に係る「マイナポイント第二弾」開始に向けて、市区町村に対して事務連絡（公金受取口座登録に対する手続支援及び端末の設定について）を発出し、ログアウト漏れを発生させないために、利用の都度、共用端末のシャットダウンを行う等の運用方法を含めた手順を策定し、これを周知した。

ウ しかしながら、デジタル庁は、策定した前記手順の重要性や、その改訂に関わりうる問題が生じた際の情報共有体制を、組織として適切に策定しなかった結果、同年7月、デジタル庁公金受取口座事務担当職員及び同管理職が豊島区の支援窓口を設置された共用端末で誤登録が発生したことを認知し、その後も、デジタル庁職員が同種事案の連続発生を把握していたにもかかわらず、令和5年5月に福島市の支援窓口での誤登録事案が発生したことを受けて注意喚起を行うまでその情報共有が適切に行われず、組織的に、前記手順の見直し及び周知を行うことはなかった。

エ 以上のことから、デジタル庁は、特定個人情報等の取扱手順の見直しを行い、市区町村と情報共有を図るなど、組織的安全管理措置を講ずる必要がある。

(3) 当委員会に対する漏えい等の報告

ア 行政機関等は、保有個人情報の漏えい等が生じたときは、当該事態が生じた旨を当委員会に報告しなければならない（速報の目安は、当該事態を知った時点から概ね3～5日以内。）¹³。

イ デジタル庁は、令和5年5月下旬頃に把握した16市区町村（22件）の誤登録の判明時点において当委員会に連絡・相談を行い、本人数100人未満の案件であ

¹¹ 番号法第12条。特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）（以下「番号法ガイドライン」という。）別添1 特定個人情報に関する安全管理措置（行政機関等編）（以下「番号法ガイドライン別添1」という。）の $\boxed{1}$ A。

¹² 番号法第12条。番号法ガイドライン別添1の $\boxed{2}$ B。

¹³ 個人情報保護法第68条第1項。個人情報保護法事務対応ガイド4-4-1、4-8-11(6)。

保有個人情報の数が100人を超える漏えい等が発生し、又は発生したおそれがある事態は、報告の対象に該当する（個人情報の保護に関する法律施行規則第43条第4号）。

ったため、報告義務がないと判断していたものである。しかしながら、同年6月7日に、総点検の結果として、口座情報登録・連携システムに登録されている口座情報の中に第三者の口座が誤登録されている可能性が高く漏えいのおそれがある事態が748件発生していることを把握したにもかかわらず、「利用者側の操作手順漏れ（ログアウト漏れ）に起因するものでありシステム側の設定ミスや不具合が原因ではなく、インターネットに公開されている状態ではないため、個人情報保護法に基づく漏えい等の報告対象にはあたらない」との誤認から、漏えい等報告を当委員会に提出せず、当委員会から誤認であるとの指摘を経て、同月16日に至るまで漏えい等報告を提出しなかった。

ウ 以上のことから、デジタル庁は、個人情報保護法に基づく漏えい等の報告対象の事態を把握した場合は、速やかに当委員会に漏えい等報告を提出できるよう、報告義務について職員の理解を醸成する教育を実施するなど、人的安全管理措置を講ずる必要がある。

3 特定個人情報保護評価（番号法第27条・第28条）

(1) 公的給付支給等口座登録簿への登録等に関する事務の評価書について

ア 行政機関の長等は、特定個人情報ファイルを保有する前に、番号法第28条第1項各号に掲げる事項を評価した結果を記載した書面（以下「評価書」¹⁴という。）を作成し、当該特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を与え得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、このようなリスクを軽減するための措置について記載しなければならず¹⁵、評価書に記載した全ての措置を講ずる必要がある¹⁶。

なお、特定個人情報ファイル新規保有時以外にも、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場合等には、再度、特定個人情報保護評価を行わなければならない¹⁷。

イ これらの規律に基づき、デジタル庁は、公的給付支給等口座登録簿への登録等に関する事務について評価書を作成し、その記載項目である「入手した特定個人情報情報が不正確であるリスク」については、入手の際の本人確認措置の内容としてマイナポータルにおいて、マイナンバーカードおよびパスワード入力により当該預貯金者の本人確認を行う旨記載して、当該リスクへの対策は十分であるとして

¹⁴ 特定個人情報保護評価指針 第5-2(8)。特定個人情報ファイルを取り扱う事務につきその対象人数が30万人以上の場合。

¹⁵ 特定個人情報保護評価指針 第1-3。

¹⁶ 特定個人情報保護評価指針 第11。番号法ガイドライン第4-2(2)。

¹⁷ 番号法第28条第1項。特定個人情報保護評価指針 第6-2(2)。

いる。この時点でデジタル庁は、市区町村の支援窓口の共用端末を用いて多数の者が公金受取口座登録手続を連続して行う事態は想定していなかった。

- ウ 当委員会は、令和3年10月20日、デジタル庁が実施した特定個人情報保護評価に対する審査を実施し、審査の観点¹⁸に照らして当該評価書に記載された特定個人情報ファイルの取扱いについて、「全項目評価書に記載されたリスク対策を確実に実行することに加え、組織的・人的安全管理措置について実務に即して適切に運用・見直しを行うこと、情報漏えい等に対するリスク対策全般について、不断の見直し・検討を行うことが重要である。」等を指摘した上で、これを承認した。

(2) リスク変動時の組織的対応

- ア 特定個人情報保護評価とは、前記指針の示すとおり、特定個人情報ファイルの適正な取扱いを確保することにより、特定個人情報の漏えいその他の事態の発生を未然に防ぐため、事前に特定個人情報ファイルの取扱いに伴う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、このようなリスクを軽減するための措置を講ずるとともに、評価実施機関が特定個人情報ファイルの取扱いにおいて個人のプライバシー等の権利利益の保護に取り組んでいることを自ら宣言し、どのような措置を講じているかを具体的に説明することにより、国民・住民の信頼を確保することを目的とするものである¹⁹。

この趣旨からすると、情報漏えい等を発生させるリスクを変動させ得る事実関係の変更が生じた際、適時に対応することが重要である。当委員会は、前記評価書の承認時、この観点から、リスク対策全般について、既に記載されたリスク対策を確実に実行することに加え、不断の見直し・検討を行うことが重要である旨指摘した（前記(1)ウ）。

- イ デジタル庁は、公金受取口座登録に関する「マイナポイント第二弾」政策の実施決定を受け、令和4年6月24日、地方公共団体に対してログアウトの徹底を依頼する内容の手順書を送付する対策を行っており、これは、デジタル庁が、同政策の実施に伴い、共用端末を用いた公金受取口座登録の際、ログアウト漏れにより前の利用者の個人情報の漏えいが起こりうると予測していたことを示している。もっとも、デジタル庁は、この時点で、このようなリスクへの対応につき組織的な検討を経ることなく、前記手順書の送付以外の対応を、特段行うことはなかった。

さらに、同年7月、豊島区の支援端末で誤登録が発生（前記第2の2(1)）したことを認知し、その後も立て続けに同種事案が生じたこと（前記第2の2(2)・(3)）

¹⁸ 特定個人情報保護評価指針 第10-1(2)。

¹⁹ 特定個人情報保護評価指針 第1-2。

で、ログアウト漏れのリスクが顕在化した時点においても、デジタル庁は、そのリスク対策等の見直しにつき、組織的な検討をしなかった。

- ウ これに関し、デジタル庁は、「マイナポイント第二弾」に加え、前記誤登録の発生によっても、公金受取口座登録に関する事務内容を変更していないことから、前記手順書の送付の他にリスク対策等の見直しは必要ないと判断したものである。

デジタル庁が前記判断に至ったことは、デジタル庁が本件事案に対する早期対応を行う契機を失した要因の一つともいえる。すなわち、デジタル庁は、事態を組織的かつ多角的に検討し、共用端末におけるログアウトが徹底されていないという実務上の実態から生じる誤登録のリスクと、これが頻発することにより大規模な漏えい事態を発生させるリスクを、正しく認識した上でその対策等の見直し・検討を行うべきであったが、これを実施しておらず、当委員会の指摘に適う対応の実施状況について、その検証が必要である。

- エ 以上のことから、特定個人情報保護評価制度の趣旨及び当委員会の前記指摘に鑑み、デジタル庁は、前記評価書に記載したリスク対策につき不断の見直し・検討を行うとともに、今後、リスクを変動させ得る事実関係の変更が生じ、当該変更に応じたリスク対策を講ずる際などには、必要な特定個人情報保護評価を適時・適切に実施する体制を、有効に機能させることが求められる。

以 上

別 添 資 料

- 1 時系列表（別紙1）
- 2 公金受取口座登録フロー概要（別紙2）