（別紙）

「特定個人情報及び個人情報等の取扱いについて（指導及び報告等の求め）」
における指導事項の改善状況報告書

1　本人確認の措置（番号法第16条）

⑴　指導事項

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付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。

⑵　改善状況

地方公共団体における支援窓口でのログアウト忘れ防止のための対策が必ずしも十分ではなかったと認識しています。

そこで令和５年６月23日にログアウト忘れ防止機能を搭載することで、システム面では所要の対応を了したと認識しています。

なお、非システム面での対応も強化すべく、令和５年11月上旬に地方公共団体向けに事務連絡を発出し、その中で、「ログアウトの徹底」に向けて、支援窓口の支援員自身によるログアウト忘れの確認を要請する予定です。

2　安全管理措置

⑴保有個人情報の漏えい等発生時における報告体制（個人情報保護法第66条第１項））

①　指導事項

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の改善を行うこと。

② 改善状況

漏えい又は漏えいのおそれがある場合のデジタル庁内の対応について、個人情報保護法及び内部規程の理解に欠けていたと認識しています。

そこで、次の６つの対応や取組を実施済又は実施する予定です。

１）人的体制の整備

デジタル庁内で個人情報保護を担当する部署の人員の充実に取り組みました。

まず、令和５年９月１日付で個人情報保護に関し専門的な知見を有する方をデジタル庁参与に任命し、個人情報保護全般に関する指導・助言をいただくこととしたところです。

次に、参与任命と同時期に、従前は個人情報保護担当は職員２名が他業務との兼務体制であったものを専従職員３名を配置する体制に改め、併せて、庁内のプライバシーデザイナー３名を新たに個人情報保護担当としたところです。

このほか令和５年10月より、外部の弁護士を活用することとし、個人情報保護に関する企画・立案、職員の教育・研修、監査スキームの構築などを行う際に助言・指導をいただくこととして、法令順守に基づいた個人情報保護を行える体制を構築しました。

以上の人的体制の整備に伴い、参与をヘッドとして、弁護士、プライバシーポリシーデザイナー３名、個人情報保護担当参事官１名、専従職員３名の計９名からなる「個人情報保護対策チーム（以下「対策チーム」という。）」を令和５年10月11日に発足し、庁内各部署が個人情報保護に関する専門的な相談や指導その他必要助言などを受けることが出来る体制としたところです。

この対策チームを有効に活用し、新たな制度やシステムの構築の際、個人情報保護の観点を、より一層組み込んでいく考え方（プライバシー・バイ・デザイン（Privacy-by-design））の徹底を図ってまいります。

２）庁内の責任体制の明確化

「デジタル庁の保有する個人情報管理規程（訓令）」の抜本的見直しを行いました。

従来の規程では、個人情報漏えい等の事案が発生した場合の庁内報告体制は、現場の担当参事官である保護管理者から直接、総括保護管理者たる戦略・組織担当の統括官に報告されることとなっていましたが、各システムを所管する各グループ統括官にも、個人情報保護の対象事案の事実

関係を共有することを明確にする等の体制を整備した形で規程の見直しを行い、令和５年10月31日付で改正を行いました。

３）情報共有体制の整備

情報共有体制の整備として報告経路（レポートライン）の明確化に関する次の２つの取組を前後して行っています。

１つには、個人情報保護に特化した取組として、個人情報漏えいのおそれがある場合に備えて、デジタル庁全職員が常時確認することが可能なデジタル庁ポータルサイトに「個人情報漏洩のおそれがある事案が発生した場合」とする掲示を令和５年10月13日に新設し、同時に全職員へ周知しました。

これにより、情報セキュリティインシデント報告フローに基づきインシデント対応総括CSIRTへ報告を行うとともに、個人情報管理者及び対策チームへの速やかな報告が実現することとなり、更なる報告体制の強化を図ったところです。

併せて、本対応により漏えい等事案が発生した場合は必要に応じて個人情報保護委員会への報告が必要なことが、当該掲示の新設により事案発生時にも職員が改めて確認できるようになりました。

２つ目として、個人情報の漏えい等を含めた庁内のリスク事案発生に備えて、令和５年６月26日の段階でデジタル庁内に組織における迅速な情報共有のための「リスク事案ホットライン」を設置しました。

この取組は、デジタル監やデジタル審議官などの幹部を含むリスク事案ホットラインのメーリングリストを新たに整備し、個人情報の漏えいのおそれがある事案等のリスク事案を認知した者は、担務リーダーに即時報告をすることとし、報告を受けた担務リーダーは、当該メーリングリストに連絡することとして、デジタル庁の幹部職員への事案の迅速な共有を図ることとしたものです。

加えて、必要に応じてデジタル大臣を含む政務が参加する庁内幹部会議の場で当該情報の共有等を行うこととしたところであり、デジタル庁内での事案等の情報の横展開を実現することとしております。

４）個人情報保護に関する庁内周知

デジタル監をはじめとする幹部職員から全職員に向けて個人情報保護に関する周知を次のとおり行いました。

デジタル監から、２週間に１度程度、「直近の出来事と情報共有」ということで全職員向けに情報発信していますが、9月から10月までにかけて

は個人情報保護の重要性や研修の受講について触れたところです。

また、令和５年９月28日に開催された大臣等政務３役と全職員が参加するオール・ハンズ・ミーティングにおいて、庁内の責任体制の明確化等を目的とした規程改正を行うことや個人情報保護に関する研修の重要性と全職員が研修を受講する必要があることについて、個人情報保護担当参事官から周知しました。

さらに、令和５年10月31日実施のオール・ハンズ・ミーティングにおいて、デジタル審議官から個人情報保護の重要性を喚起し、対策チームと個人情報保護に関わる情報を共有して、個人情報保護に適切に対応するよう指示を行ったところです。

５）研修の実施

個人情報保護に関する研修を次のように実施済又は実施する予定です。

ア）公金口座誤登録事案を教訓とした研修

「特定個人情報及び個人情報等の取扱いについて（指導及び報告等の求め）」の１⑵アにあるような誤登録事案への対応を教訓とした、研修資料（グループディスカッション向け）を作成する予定としています【令和５年末】。その中で、組織内での適時適切な情報共有の重要性について言及するとともに、全職員へ周知徹底することとしています。

イ）個人情報等保護に関する研修の実施

令和５年８月７日に全職員を対象として、個人情報保護委員会作成の「個人情報の適正な取扱いのための研修資料」を用いて研修を行い、大臣からデジタル庁全職員が漏れなく受講を修了するようにとの指示もあり、デジタル監からも受講を促す連絡を行ったところから令和５年10月20日までにデジタル庁全職員が受講を修了しておりますので、個人情報保護制度の基礎について、及び個人情報の漏えい等が発生した場合は個人情報保護委員会へ報告が必要なことについて、全職員に正しく理解させたところです。

また、令和５年度の「保有個人情報を取扱う情報システムの管理に関する事務に従事する職員」に対する研修は、デジタル庁において作成した研修資料により実施し、「保有個人情報の取扱いに従事する職員」及び「保護管理者及び保護担当者」に対する研修は、個人情報保護委員会作成の研修資料により研修を行いましたが、令和６年度に向けて、令和５年度末までに最新の法改正の状況やデジタル庁で実際に起こった情

報漏えい事案等を反映させたデジタル庁独自の研修資料を作成するなど、研修の内容の充実と強化に努めてまいります。（※　特定個人情報についても同じ。）

なお、令和５年度のこれらの研修については、令和５年10月20日時点で受講対象となる職員全員が受講を修了しております。

ウ）計画的な研修の実施

今後は、毎年度末までに翌年度における研修計画を策定し「保有個人情報の取扱いに従事する職員」に対する研修については、全職員に対して保有個人情報の取扱い等に関する必要な研修を実施するとともに、「保護管理者及び保護担当者」に対しては、担当する現場における保有個人情報の適切な管理のための研修を実施し、計画的な研修の実施と受講対象者全員が確実に受講完了するようにします。

６）職員の意識改革と個人情報保護の継続的な取組

今回の規程改正を受け、規程を全職員に周知する際に、各グループにおける個人情報の取扱いについて、特にトラブル、異例・特異な扱い、手続きの変更、リスクの判明・顕在化などがあった場合には、直ちに対策チームに一報を入れること、その場合は、当該グループ担当と対策チームが連携しつつ、対策チームが必要な指示を行うことを明記した個人情報保護担当参事官通知（以下「参事官通知」という。）を令和５年中に発出することとしており、日常の個人情報保護の執行に関する留意事項を全職員に周知することとしています。

また、本通知にはこの他に例えば、漏えい等の事案に応じて個人情報保護委員会への報告を行うことや必要に応じて関係機関との連携を図ること、また事案に応じては対外的な情報発信が必要であることや同様の漏えい等事案を防止するために必要な対策の検討が必要であること、特定個人情報保護評価への反映が必要なことについて注記し、漏えい等事案が発生した場合にデジタル庁として取り組む必要があるポイントとなる事柄を全職員に対して周知します。

本通知は新たに周知が必要となった事項等が判明し又は生じた場合には、適時適切な見直しを行うこととし、個人情報保護が継続的な取組となるようにします。

⑵取扱手順の見直し（番号法第12条）

① 指導事項

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こと。

② 改善状況

窓口支援を行う地方公共団体に対して、ログアウト忘れ防止に係る注意喚起が必ずしも十分ではなかったと認識しています。

そこで令和５年５月23日に、地方公共団体向けに事務連絡を発出し、その中で、マイナポイント支援窓口の利用者へのログアウトの働きかけの徹底を依頼しています。その上で、十分な対応を確保する観点から改めて検討した結果、令和５年11月上旬に地方公共団体向けに事務連絡を発出し、その中で「ログアウトの徹底」に向けて、支援窓口の支援員自身によるログアウト忘れの確認についても要請する予定です。

⑶個人情報保護委員会に対する漏えい等の報告（個人情報保護法第68条第１項）

① 指導事項

番号法及び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こと。

② 改善状況

漏えい又は漏えいのおそれがある場合の個人情報保護委員会への報告対応について、個人情報保護法の理解に欠けていたと認識しています。

そこで、次の２つの対応や取組を実施又は実施する予定です。

１）情報共有体制の整備

「情報セキュリティインシデント対応手順書」に個人情報保護法施行規則第43条各号に掲げる事態が発生した場合は、個人情報保護委員会に報告を行う旨の記述を追記し、令和５年10月27日にデジタル庁内の情報共有ツールにて全職員に周知するほか、個人情報保護委員会への報告ルートを記載した報告フローを令和５年９月27日にデジタル庁内の情報共有ツールにて、全職員に周知を行いました。

これらの対応手順書や報告フローは、デジタル庁ポータルサイトに資料を掲示し、全職員が常時確認できるようにしており、個人情報の漏えい

時等には個人情報保護委員会へ報告が必要である旨、全職員への周知と対応の徹底を図りました。

２）研修の実施

ア）公金口座誤登録事案を教訓とした研修

「特定個人情報及び個人情報等の取扱いについて（指導及び報告等の求め）」の１⑵ウにあるような漏えい等の報告に係る対応を教訓とした、研修資料（グループディスカッション向け）を作成する予定です【令和５年末】。その中で、個人情報保護委員会への速やかな漏えい等の報告の重要性について言及するとともに、全職員へ周知徹底することとしています。

イ）個人情報等保護に関する研修の実施

令和５年８月７日に全職員を対象として、個人情報保護委員会作成の「個人情報の適正な取扱いのための研修資料」を用いて研修を行いましたので、個人情報保護制度の基礎について、及び個人情報の漏えい等が発生した場合は個人情報保護委員会へ報告が必要なことについては、職員の理解を醸成したところです。

また、令和５年度の本研修については、大臣からデジタル庁全職員が漏れなく受講を修了するようにとの指示があり、デジタル監からも受講を促す連絡を行ったことから令和５年10月20日までにデジタル庁全職員が受講を修了しております。

なお、令和５年度の「保有個人情報を取扱う情報システムの管理に関する事務に従事する職員」に対する研修は、デジタル庁において作成した研修資料により実施し、「保有個人情報の取扱いに従事する職員」及び「保護管理者及び保護担当者」に対する研修は、個人情報保護委員会作成の研修資料により研修を行いましたが、令和６年度に向けて、令和５年度末までに最新の法改正の状況やデジタル庁で実際に起こった情報漏えい事案等を反映させたデジタル庁独自の研修資料を作成するなど、研修の内容の充実と強化に努めてまいります。

ウ）計画的な研修の実施

今後は毎年度末までに翌年度における研修計画を策定し「保有個人情報の取扱いに従事する職員」に対する研修については、全職員に対して、保有個人情報の取扱い等に関する必要な研修を実施するとともに、

「保護管理者及び保護担当者」に対しては、担当する現場における保有個人情報の適切な管理のための研修を実施し、計画的な研修の実施と受講対象者全員が確実に受講完了するようにします。

3　特定個人情報保護評価（番号法第27条及び第28条）

⑴　指導事項

特定個人情報保護評価制度の趣旨及び当委員会の「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。」等の指摘に鑑み、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。

⑵　改善状況

環境変化に応じて特定個人情報保護評価書の見直しを行うことへの意識が必ずしも十分ではなかったと認識しています。

そこで特定個人情報ファイルを所有する担当部署に対して、特定個人情報保護評価書が個人情報保護委員会にて承認されて以後、特定個人情報ファイルを取り扱う事務に係る環境の変化や想定していなかったリスク事案等が発生した場合においては、直ちに対策チームに情報を共有するように、当該担当部署の職員に対して、啓発及び周知徹底を図るとともに令和５年中に発出することとしている参事官通知においても、明記することとしております。これにより、担当部署と対策チームの両者において、特定個人情報保護評価書の見直し・検討が必要となる旨の確認を行うこととしました。

また、個人情報保護委員会作成の「特定個人情報保護評価指針」の第５・４「特定個人情報保護評価書の見直し」にあるように、１年に１回、公表している特定個人情報保護評価書については、記載事項を実態に照らして見直し、変更が必要か否かを検証します。その際は、当該評価書を担当する部署と対策チームが共に評価・検討を行うことし、その旨は、令和５年中に発出することとしている参事官通知にも明記することとしております。

4　その他（デジタル庁における個人情報保護に関する監査の充実について）

今回、個人情報保護委員会から指導を受けた事項については、上記１から

３までにおいて、その対応策等を御報告したところですが、これらの対応策等の実効性や継続性を担保し、形骸化しない取組が必要と考えています。こうした観点からデジタル庁の保有個人情報に関する実効性のある「監査と点検」が特に重要であると認識しております。

このため、次の対応や取組を実施済又は実施する予定です。

１）個人情報保護監査チームの発足

個人情報保護の専従職員のほか、セキュリティ担当、プライバシーデザイナー及び弁護士を含む「個人情報保護監査チーム（以下「監査チーム」という。）」を令和５年10月31日に発足させました。

この監査チームは、保有個人情報ファイルの担当部署等の監査や関係システムの運用等を委託する委託先に対する担当部署が行う監査・点検についてのサポート等を行うこととしております。

２）自己点検を兼ねた実態調査の実施

「デジタル庁で個人情報ファイル簿を現に保有する担当に対する実態確認」を実施し、内部監査に向けて庁内各々における個人情報保護の取組状況を確認しました。これは、今後の内部監査の実施に向けての現状把握と監査時に注目すべき事項を事前に把握する目的で実施したものです。既にデジタル庁が保有する11の個人情報ファイル全てについて、担当部署からの回答が提出されました。

３）監査の実施

令和５年度中に現在保有する特定個人情報ファイル４つの全てと個人情報ファイル1つの計５ファイルの監査を実施します。

また、令和６年９月末までに保有する残りの６つの個人情報ファイルの監査を実施します。これら令和６年９月までに実施する監査については、個人情報保護委員会が提供している「地方公共団体等における特定個人情報等に関する監査実施マニュアル」や「（参考）監査チェックリスト・監査資料」を参考に「デジタル庁の保有する個人情報等管理規程」の順守状況を確認します。

なお、令和６年10月以降は、定期的かつ計画的な内部監査を実施し、及び監査の内容についても継続的に見直しと充実を図ってまいります。

さらに監査の実施においては、上記２⑴②１）でも御説明した通り外部の弁護士から指導を受けることなども検討してまいります。

４）関係システムの委託先に対する監査・点検のサポート

委託契約によって、保有個人情報ファイル等のデータをシステム処理している場合に、担当部署が委託先を監査・点検するときは、監査チームがサポートを行うとともに、担当部署が行った監査・点検の結果については、監査チームに共有することとし、監査チームがその内容を確認することで監査・点検の質的実効性を担保します。

５）ログ分析のサポート

委託契約によって、保有個人情報ファイル等のデータをシステム処理している場合に、担当部署が委託先にログの分析を行わせる場合には、次の５つのポイントは必須の分析項目としてログ分析を行うようにします。

ⅰ）不自然な曜日時間帯に個人情報を参照していないか

ⅱ）通常とは異なる端末を使用していないか

ⅲ）権限が付与されていない操作で個人情報を取得しようとしていないか

ⅳ）通常行う必要がない操作で個人情報を取得していないか

ⅴ）同一の個人情報を何度も参照していないか

なお、担当部署は委託先から受領したログの分析結果について、その分析内容の妥当性等を独自に確認するとともに、ログの分析結果については監査チームに共有することとし、監査チームがその内容を確認することでログ分析の質的実効性を担保します。

以上