デジタル庁の保有する個人情報管理規程

（令和３年９月１日
デジタル庁訓令第30号）

第１章　総則

（目的）

第１条　この規程は、デジタル庁の保有する個人情報及び個人番号の適切な管理に関して必要な事項を定めることを目的とする。

（用語の定義）

第２条　この規程における用語の定義は、「行政機関の保有する個人情報の保護に関する法律」（平成１５年法律第５８号。以下「行政機関個人情報保護法」という。）第２条及び「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２条の定めるところによる。

第２章　管理体制

（総括個人情報管理者）

第３条　デジタル庁に、総括個人情報管理者１人を置き、デジタル庁の保有する個人情報及び個人番号の保護に関する事務を担当する統括官（以下「個人情報保護等担当統括官」という。）をもって充てる。

２　総括個人情報管理者は、デジタル庁における保有個人情報及び個人番号（以下「保有個人情報等」という。）の管理に関する事務を総括する任に当たる。

（個人情報管理者）

第４条　デジタル庁に、個人情報管理者を置く。

２　個人情報管理者は、デジタル庁の保有する個人情報の保護に関する事務を担当する参事官（以下「個人情報保護担当参事官」という。）をもって充てる。

３　個人情報管理者は、デジタル庁における保有個人情報（特定個人情報を除く。本項、第６条、第９条、第１８条、第３７条及び第３９条において同じ。）の適切な管理を確保する任に当たる。保有個人情報を情報システムで取り扱う場合、個人情報管理者は、当該情報システムの管理者と連携して、その任に当たる。

（特定個人情報等管理者）

第５条　デジタル庁に、特定個人情報等管理者を置く。

２　特定個人情報等管理者は、その担当する事務において、デジタル庁の保有する特定個人情報及び個人番号（以下「特定個人情報等」という。）を取り扱う参事官（以下「特定個人情報等取扱参事官」という。）をもって充てる。

３　特定個人情報等管理者は、デジタル庁における特定個人情報等の適切な管理を確

保する任に当たる。特定個人情報等を情報システムで取り扱う場合、特定個人情報等管理者は、当該情報システムの管理者と連携して、その任に当たる。

（個人情報取扱主任）

第６条　デジタル庁に、個人情報取扱主任を置き、個人情報管理者が指名する職員をもって充てる。

２　個人情報取扱主任は、個人情報管理者を補佐し、デジタル庁における保有個人情報の管理に関する事務を担当する。

（特定個人情報等取扱主任）

第７条　デジタル庁に、特定個人情報等取扱主任を置き、特定個人情報等管理者が指名する職員をもって充てる。

２　特定個人情報等取扱主任は、特定個人情報等管理者を補佐し、デジタル庁における特定個人情報等の管理に関する事務を担当する。

（特定個人情報等取扱担当者）

第８条　デジタル庁において、特定個人情報等を取り扱う場合には、特定個人情報等管理者は、特定個人情報等を取り扱う職員（以下「特定個人情報等取扱担当者」という。）を指名し、総括個人情報管理者が別に定めるところにより、当該特定個人情報等取扱担当者が個人番号を取り扱う事務の範囲及び取り扱う特定個人情報等の範囲を指定する。

（監査責任者）

第９条　デジタル庁に、監査責任者２人を置き、保有個人情報に関する監査については、デジタル庁の職員の任免、給与、懲戒、服務その他の人事並びに教養及び訓練に関する事務を担当する参事官を、特定個人情報等に関する監査については、個人情報保護担当参事官をもって充てる。

２　監査責任者は、それぞれ保有個人情報又は特定個人情報等の管理の状況について監査する任に当たる。

（保有個人情報等の適切な管理のための会議）

第１０条　総括個人情報管理者は、保有個人情報等の管理に係る重要事項の決定、連絡・調整等を行うため必要があると認めるときは、関係職員を構成員とする会議を開催することができる。

第３章　教育研修

第１１条　総括個人情報管理者は、保有個人情報等の取扱いに従事する職員（派遣労働者を含む。以下同じ。）に対し、保有個人情報等の取扱いについて理解を深め、個人情報及び個人番号の保護に関する意識の高揚を図るための啓発その他を目的として必要な教育研修を実施する。

２　総括個人情報管理者は、保有個人情報等を取り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し、保有個人情報等の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を実施する。

３ 総括個人情報管理者は、個人情報管理者及び特定個人情報等管理者（以下「個人

情報管理者等」という。）並びに個人情報取扱主任及び特定個人情報等取扱主任（以下「個人情報取扱主任等」という。）に対し、現場における保有個人情報等の適切な管理のための教育研修を実施する。

４　個人情報管理者等は、デジタル庁の職員に対し、保有個人情報等の適切な管理のために、総括個人情報管理者の実施する教育研修への参加の機会を付与する。

第４章　職員の責務

第１２条　職員は、行政機関個人情報保護法及び番号法の趣旨に則り、関連する法令及びこの規程並びに総括個人情報管理者、個人情報管理者等及び個人情報取扱主任等の指示に従い、保有個人情報等を取り扱わなければならない。

第５章　保有個人情報等の取扱い

（アクセス制限）

第１３条　個人情報管理者等は、個人識別の容易性（匿名化の程度等）、要配慮個人情報の有無、漏えい等が発生した場合に生じ得る被害の性質・程度などを考慮し、保有個人情報等の秘匿性等その内容に応じて、当該保有個人情報等にアクセスする（紙等に記録されている保有個人情報等に接する行為を含む。以下同じ。）権限を有する職員の範囲と権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限らなければならない。

２　アクセス権限を有しない職員は、保有個人情報等にアクセスしてはならない。

３　職員は、アクセス権限を有する場合であっても、業務上の目的以外の目的で保有個人情報等にアクセスしてはならない。

（複製等の制限）

第１４条　職員が業務上の目的で保有個人情報等を取り扱う場合であっても、個人情報管理者等は、次に掲げる行為については、当該保有個人情報等の秘匿性等その内容に応じて、当該行為を行うことができる場合を限定し、職員は、個人情報管理者等の指示に従い行わなければならない。

一　保有個人情報等の複製

二　保有個人情報等の送信

三　保有個人情報等が記録されている媒体の外部への送付又は持ち出し

四　その他保有個人情報等の適切な管理に支障を及ぼすおそれのある行為

（誤りの訂正等）

第１５条　職員は、保有個人情報等の内容に誤り等を発見した場合には、個人情報管理者等の指示に従い、訂正等を行わなければならない。

（媒体の管理等）

第１６条　職員は、個人情報管理者等の指示に従い、保有個人情報等が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、耐火金庫への保管、施錠等を行わなければならない。

（廃棄等）

第１７条　職員は、保有個人情報等又は保有個人情報等が記録されている媒体（端末及びサーバに内蔵されているものを含む。）が不要となった場合には、個人情報管理者等の指示に従い、当該保有個人情報等の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行わなければならない。

（保有個人情報等の取扱状況の記録）

第１８条　個人情報管理者は、保有個人情報の秘匿性等その内容及び必要に応じて、台帳等を整備して、当該保有個人情報の利用及び保管等の取扱いの状況について記録しなければならない。

２　特定個人情報等管理者は、特定個人情報ファイルを保有する場合は、総括個人情報管理者が別に定めるところにより、台帳等を整備して、当該特定個人情報ファイルの利用及び保管等の取扱状況について記録しなければならない。

（個人番号の利用の制限）

第１９条　特定個人情報等管理者は、個人番号の利用に当たり、番号法があらかじめ定めた事務に限定する。

（特定個人情報の提供の求めの制限）

第２０条　職員は、個人番号利用事務又は個人番号関係事務（以下「個人番号利用事務等」という。）を処理するために必要な場合その他番号法で定める場合を除き、個人番号の提供を求めてはならない。

（特定個人情報ファイルの作成の制限）

第２１条　職員は、個人番号利用事務等を処理するために必要な場合その他番号法で定める場合を除き、特定個人情報ファイルを作成してはならない。

（特定個人情報等の収集・保管の制限）

第２２条　職員は、番号法第１９条各号のいずれかに該当する場合を除き、他人の個人番号を含む個人情報を収集又は保管してはならない。

（特定個人情報等の取扱区域）

第２３条　特定個人情報等管理者は、特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）を明確にし、物理的な安全管理措置を講ずる。

第６章　情報システムにおける安全の確保等

（アクセス制御）

第２４条　個人情報管理者等は、保有個人情報等（情報システムで取り扱うものに限る。以下第３０条を除き、この章において同じ。）の秘匿性等その内容に応じて、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講じなければならない。

２　個人情報管理者等が前項の措置を講じる場合には、パスワード等の管理に関する規程を定めるとともに、パスワード等の読取防止等を行うために必要な措置を講じなければならない。パスワード等の管理に関する規程は、必要に応じて見直しを行う。

（アクセス記録）

第２５条　個人情報管理者等は、保有個人情報等の秘匿性等その内容及び必要に応じて、当該保有個人情報等へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存しなければならない。

２　個人情報管理者等は、必要に応じてアクセス記録を分析するものとする。

３　個人情報管理者等は、アクセス記録の改ざん、窃取又は不正な消去等の防止のために必要な措置を講じなければならない。

（アクセス状況の監視）

第２５条の２ 個人情報管理者等は、保有個人情報等の秘匿性等その内容及びその量に応じて、当該保有個人情報等への不適切なアクセスの監視のため、保有個人情報等を含むか又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能の設定、当該設定の定期的確認等の必要な措置を講じなければならない。

（管理者権限の設定）

第２５条の３ 個人情報管理者等は、保有個人情報等の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化及び内部からの不正操作等の防止のため、当該特権を最小限とする等の必要な措置を講じなければならない。

（外部からの不正アクセスの防止）

第２６条　個人情報管理者等は、保有個人情報等を取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォールの設定による経路制御等の必要な措置を講じなければならない。

（不正プログラムによる漏えい等の防止）

第２７条　個人情報管理者等は、不正プログラムによる保有個人情報等の漏えい、滅失又は毀損等の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講じなければならない。

（情報システムにおける保有個人情報等の処理）

第２８条　職員は、保有個人情報等について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去する。個人情報管理者等は、当該保有個人情報等の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認する。

（暗号化）

第２９条　個人情報管理者等は、保有個人情報等の秘匿性等その内容に応じて、暗号化のために必要な措置を講じなければならない。職員は、これを踏まえ、その処理する保有個人情報等について、当該保有個人情報等の秘匿性等その内容に応じて、適切に暗号化を行う。

（入力情報の照合等）

第３０条　職員は、情報システムで取り扱う保有個人情報等の重要度に応じて、入力

原票と入力内容との照合、処理前後の当該保有個人情報等の内容の確認、既存の保有個人情報等との照合等を行う。

（バックアップ）

第３１条　個人情報管理者等は、保有個人情報等の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講じなければならない。

（情報システム設計書等の管理）

第３２条　個人情報管理者等は、保有個人情報等に係る情報システムの設計書、構成図等の文書について外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講じなければならない。

（端末の限定）

第３３条　個人情報管理者等は、保有個人情報等の秘匿性等その内容に応じて、その処理を行う端末を限定しなければならない。

（端末の盗難防止等）

第３４条　個人情報管理者等は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講じなければならない。

２　職員は、個人情報管理者等が必要があると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。

（第三者の閲覧防止）

第３５条　職員は、端末の使用に当たっては、保有個人情報等が第三者に閲覧されることがないようにしなければならない。

（記録機能を有する機器・媒体の接続制限）

第３６条　個人情報管理者等は、保有個人情報等の秘匿性等その内容に応じて、当該保有個人情報等の情報漏えい等の防止のため、スマートフォン、ＵＳＢメモリ等の記録機能を有する機器・媒体の情報システム端末等への接続の制限（当該機器の更新への対応を含む。）等の必要な措置を講ずる。

第７章　保有個人情報等の提供及び業務の委託等

（保有個人情報の提供）

第３７条　個人情報管理者は、行政機関個人情報保護法第８条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、原則として、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について書面を取り交わさなければならない。

２　個人情報管理者は、行政機関個人情報保護法第８条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善要求等の措置を講じることができる。

３　個人情報管理者は、行政機関個人情報保護法第８条第２項第３号の規定に基づき

行政機関又は独立行政法人等に保有個人情報を提供する場合において、必要があると認めるときは、前二項に規定する措置を講じることができる。

（特定個人情報等の提供）

第３８条　職員は、番号法で限定的に明記された場合を除き、特定個人情報等を提供してはならない。

（保有個人情報の取扱いに係る業務の委託等）

第３９条　保有個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないようにしなければならない。また、契約書に、次に掲げる事項を明記するとともに、委託先における責任者等及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認しなければならない。

一　個人情報に関する秘密保持、目的外利用の禁止等の義務

二　再委託（再委託先が委託先の子会社（会社法（平成１７年法律第８６号）第２条第１項第３号に規定する子会社をいう。）である場合も含む。本号、第３項及び第４０条において同じ。）の制限又は事前承諾等再委託に係る条件に関する事項

三　個人情報の複製等の制限に関する事項

四　個人情報の漏えい等の事案の発生時における対応に関する事項

五　委託終了時における個人情報の消去及び媒体の返却に関する事項

六　違反した場合における契約解除、損害賠償責任その他必要な事項

２　保有個人情報の取扱いに係る業務を外部に委託する場合には、委託する業務に係る保有個人情報の秘匿性等その内容やその量等に応じて、委託先における管理体制及び実施体制や個人情報の管理の状況について、少なくとも年１回以上、原則として実地検査により確認しなければならない。

３　委託先において、保有個人情報の取扱いに係る業務が再委託される場合には、委託先に第１項の措置を講じさせるとともに、再委託される業務に係る保有個人情報の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが前項の措置を実施しなければならない。保有個人情報の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。

４　保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記しなければならない。

５　保有個人情報を提供又は業務委託する場合には、漏えい等による被害発生のリスクを低減する観点から、提供先の利用目的、委託する業務の内容、保有個人情報の秘匿性等その内容などを考慮し、必要に応じ、氏名を番号に置き換える等の匿名化措置を講ずる。

（特定個人情報等の取扱いに係る業務の委託等）

第４０条　個人番号利用事務等の全部又は一部を委託する場合には、委託先において、番号法に基づきデジタル庁が果たすべき安全管理措置と同等の措置が講じられる

か否かについて、あらかじめ確認しなければならない。
２　個人番号利用事務等の全部又は一部の委託をする際には、「委託を受けた者」において、デジタル庁が果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行わなければならない。
３　個人番号利用事務等の全部又は一部の「委託を受けた者」が再委託をする際には、委託をする個人番号利用事務等において取り扱う特定個人情報の適切な安全管理が図られることを確認した上で再委託の諾否を判断する。

第８章　安全確保上の問題への対応

（事案の報告及び再発防止措置）

第４１条　保有個人情報等の漏えい、滅失又は毀損等の事案の発生又は兆候を把握した場合及び特定個人情報等取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合等、安全確保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等を管理する個人情報管理者等（個人情報管理者等が不在等により報告等が困難な場合かつ特に重大と認める事案が発生した場合には、総括個人情報管理者）に報告しなければならない。
２　個人情報管理者等は、被害の拡大防止又は復旧等のために必要な措置を速やかに講じなければならない。ただし、外部からの不正アクセスや不正プログラムの感染が疑われる当該端末等のＬＡＮケーブルを抜くなど、被害拡大防止のため直ちに行い得る措置については、直ちに行う（職員に行わせることを含む。）ものとする。
３　個人情報管理者等は、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。ただし、特に重大と認める事案が発生した場合には、直ちに総括個人情報管理者に当該事案の内容等について報告しなければならない。
４　総括個人情報管理者は、前項の規定に基づく報告を受けた場合には、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を内閣総理大臣に速やかに報告しなければならない。
５　個人情報管理者等は、事案の発生した原因を分析し、再発防止のために必要な措置を講じなければならない。

（公表等）

第４２条　事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報等の本人への対応等の措置を講じる。公表を行う事案については、当該事案の内容、経緯、被害状況等について、速やかに総務省（行政管理局）及び個人情報保護委員会に情報提供を行う。

第９章　監査及び点検の実施

（監査）

第４３条　監査責任者は、保有個人情報等の適切な管理を検証するため、第２章から

第８章に規定する措置の状況を含む当該行政機関における保有個人情報等の管理の状況について、必要に応じ監査を行い、その結果を総括個人情報管理者に報告する。

（点検）

第４４条　個人情報管理者等は、自ら管理責任を有する保有個人情報等の記録媒体、処理経路、保管方法等について、必要に応じ点検を行い、必要があると認めるときは、その結果を総括個人情報管理者に報告する。

（評価及び見直し）

第４５条　この規程等については、監査又は点検の結果等を踏まえ、実効性等の観点から評価し、必要があると認めるときは、その見直し等の措置を行う。

第１０章　その他

（細則）

第４６条　この規程に定めるもののほか、この規程の実施のための手続その他について必要な事項は、別に定める。

附　則

この訓令は、令和３年９月１日から施行する。