「個人情報」と「特定個人情報」
～正しい理解のために～

平成31年２月
個人情報保護委員会事務局

本資料の記載について

本資料において、関係法令等は次の略称を用いる。

- 個人情報の保護に関する法律（平成15年５月30日法律第57号）　⇒　個人情報保護法
- 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５月31日法律第27号）　⇒　番号法

また、法律の条文は次の例のとおり表記する。

（例）　個人情報の保護に関する法律　第23条第１項第１号　⇒　個人情報保護法§23Ⅰ①

本資料において、用いる記号は、それぞれ次のとおりである。

✓　・・・全体に共通するポイントを記載する際に用いる。

■　・・・「個人情報」及び「個人情報保護法」に関するポイントを記載する際に用いる。

◘　・・・「マイナンバー（個人番号）」、「特定個人情報」及び「番号法」に関するポイントを記載する際に用いる。

はじめに

- 番号法における「特定個人情報」は、個人情報保護法における「個人情報」よりも厳格な各種の保護措置が設けられている。例えば、利用目的、再委託、第三者への提供に関する制限等については、後述のとおり差異がある。
- 一方で、安全管理措置については、法律上求められている基本的な要素は共通しており、ガイドラインが求める個々の安全管理措置についても、基本的に差異はない（詳細について、P11及び巻末資料参照）。

１．個人情報保護法と番号法の関係

【法律の目的】

- ✓ 個人情報保護法は、個人情報の有用性に配慮しつつ、個人の権利利益を保護するための法律
- ✓ 番号法は、行政を効率化し、国民の利便性を高め、公平・公正な社会を実現するために必要な事項を定めるほか、特定個人情報等の取扱いについて、個人情報保護法等の特例を定めるための法律

【ポイント】

- ✓ 個人情報保護法は、民間事業者における「個人情報」の取扱いルール等を定めている。
- ✓ 一方、番号法は、マイナンバー（個人番号）や特定個人情報（マイナンバー（個人番号）を含む個人情報）の取扱いについて、個人情報保護法の特例を定めている。
- ✓ 次ページのとおり、生存する方のマイナンバー（個人番号）は、「個人情報」に該当するため、その取扱いについて、個人情報保護法の適用を受けるが、番号法で個人情報保護法と異なる定めがされている場合は、番号法が優先的に適用される。

【マイナンバー（個人番号）の取扱いについて、個人情報保護法と番号法のどちらが適用されるか？】

- ● 番号法に、個人情報保護法と異なる規定がある場合
  → 当該番号法の規定が適用
- ● 上記以外（番号法に特則が定められていない場合）
  → 個人情報保護法の規定が適用

2．個人情報と特定個人情報（個人情報保護法§２Ⅰ、番号法§2Ⅷ）

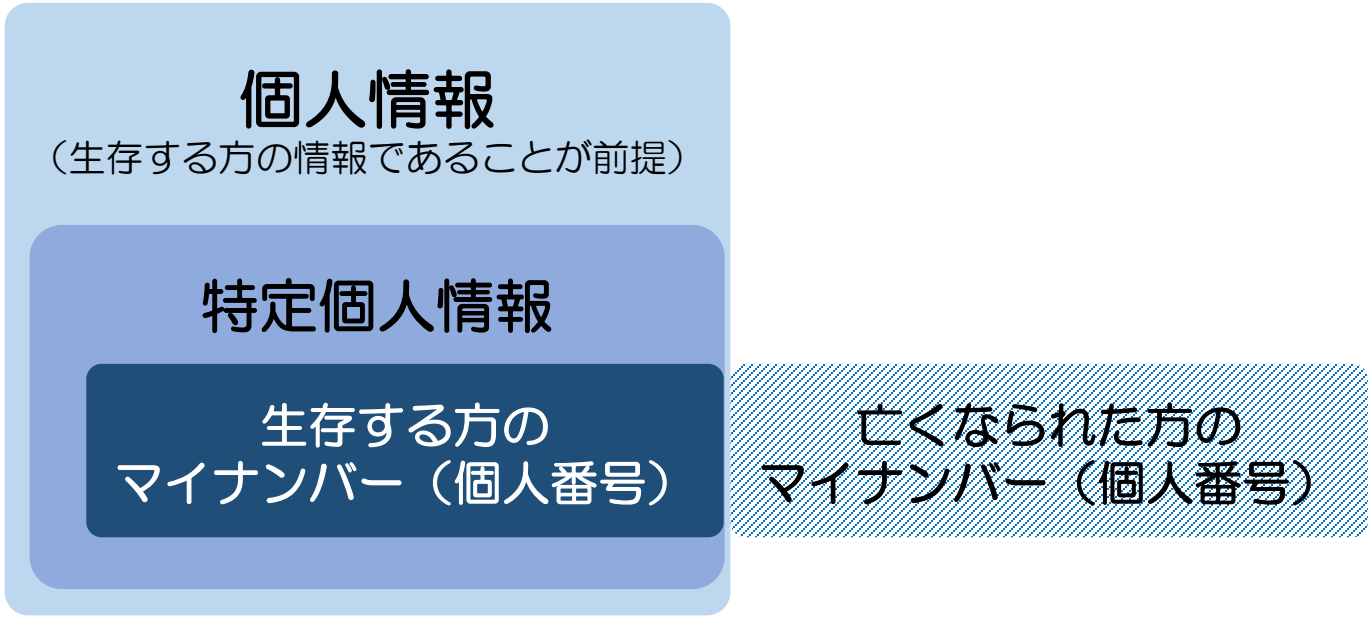
【ポイント】

- ✓ マイナンバー（個人番号）は、個人情報に該当する。
  （※ただし、生存する方の情報である場合）
- ✓ 特定個人情報とは、マイナンバー（個人番号）を含む個人情報をいう。

↓

- ✓ 生存する方のマイナンバー（個人番号）は、「個人情報」に該当する。
- ✓ 亡くなられた方のマイナンバー（個人番号）は、「個人情報」に該当しない。

※個人情報保護法において、「個人情報」は「生存する個人に関する情報」であることが前提となっている。



３．個人情報、個人データと特定個人情報等に関するルールの主な違い

① 利用目的

・・・個人情報は利用範囲に特に制限はなく、事業者が自由に利用目的を決められるが、特定個人情報は利用範囲が「税・社会保障・災害対策」に限定されており、その範囲内で利用目的を決める必要がある。

② 不要となった情報の取扱い

・・・個人データは遅滞なく消去するよう努めることとされている。一方、特定個人情報については、所管法令で定められている保存期間を経過した場合には、できるだけ速やかに廃棄又は削除しなければならないとされている。

③ 第三者提供ができる場合

・・・個人データは本人の同意があれば第三者提供ができるが、特定個人情報は第三者提供ができる場合が限定されている。

④ 第三者に提供した場合・第三者から提供を受けた場合の記録作成等の要否

・・・個人データは原則記録作成等が必要であるが、特定個人情報については、第三者提供できる場合が限定的なので、記録作成等が必要な場面が想定されていない。

⑤ 委託

・・・委託先の監督が必要である点で共通しているが、特定個人情報については、再委託する場合、最初の委託者の許諾が必要である。

⑥ 安全管理措置

・・・基本的な要素は共通している。

⑦ 漏えい等が発生した場合の対応

・・・基本的には同じであるが、特定個人情報は一定の場合には個人情報保護委員会への報告が法律上の義務とされている。

４．利用目的

【ポイント】

■　個人情報は、利用範囲に特に制限はなく、自由に利用目的を決められる。

□　特定個人情報は、利用範囲が「税・社会保障・災害対策」に限定されており、その範囲内で利用目的を決める必要がある。

【解説】

①個人情報については、利用範囲に特に制限はないが、個人情報を取り扱うに当たっては、その利用目的をできる限り特定しなければならない（個人情報保護法§15Ⅰ）。また、あらかじめ本人の同意を得ないで、特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない（個人情報保護法§16ⅠⅡ）とされており、本人の同意を得れば、特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱うことができる。

②特定個人情報については、利用範囲が「税・社会保障・災害対策」に限定されており（番号法§9）、その範囲内で利用目的を特定しなければならない（個人情報保護法§15Ⅰ）。また、特定された利用目的の達成に必要な範囲を超えて、特定個人情報を取り扱ってはならない（番号法§30Ⅲ、個人情報保護法§16ⅠⅡ）とされており、本人の同意があったとしても、特定された利用目的の達成に必要な範囲を超えた利用はできない。

5．不要となった個人情報・特定個人情報の取扱い

【ポイント】

■ 不要となった個人データは、遅滞なく消去するよう努めなければならない。

□ 不要となった特定個人情報は、法令で決められた保存期間を経過すれば、廃棄又は削除しなければならない。

【解説】

①個人データ（個人情報をデータベース化したものを構成する個人情報）は、利用する必要がなくなったときは、遅滞なく消去するよう努めなければならない（個人情報保護法§19）。

②特定個人情報は、番号法§19各号のいずれかに該当する場合を除き、収集し、又は保管してはならない（番号法§19、§20）とされており、事務を処理する必要がなくなった場合で、所管法令において定められている保存期間を経過した場合には、個人番号をできるだけ速やかに廃棄又は削除しなければならない（マイナンバーガイドライン第4－3－(3)）。

６．第三者提供の制限

【ポイント】

■ 個人データは、本人の同意があれば、第三者に提供できる。また、法令に基づく場合や人の生命・身体・財産の保護に必要な場合等は、本人の同意を得ずに提供できる。
※その他、オプトアウトによる提供の場合（個人情報保護法§23Ⅱ）や、委託、事業承継又は共同利用（個人情報保護法§23Ⅴ）の場合も、提供に当たって本人の同意は不要。

□ 特定個人情報は、本人同意の有無は関係なく、番号法§19各号に掲げる場合のみ提供できる。

【解説】

①個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない（個人情報保護法§23Ⅰ）。
(ア)法令に基づく場合
(イ)人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
(ウ)公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
(エ)国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

②特定個人情報については、第三者提供の制限（個人情報保護法§23）を適用除外とした上で、番号法§19各号に該当する場合のみ提供することができる。

7．第三者に提供する際・第三者から提供を受ける際の記録義務等

【ポイント】

■ 個人データを第三者に提供したときは、記録を作成し保存しなければならない。

■ 個人データを第三者から提供される場合は、相手方の氏名や、取得経緯等を確認し、記録を作成し保存しなければならない。

□ 特定個人情報は、第三者に提供できる場合が限定されているので、記録の作成等は不要

【解説】

①個人情報取扱事業者は、個人データを第三者に提供したときは、当該個人データを提供した年月日、当該第三者の氏名又は名称その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない（個人情報保護法§25Ⅰ）。

②個人情報取扱事業者は、第三者（注）から個人データの提供を受けるに際しては、次に掲げる事項の確認を行わなければならない（個人情報保護法§26Ⅰ）。

(ア)当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者（法人でない団体で代表者又は管理人の定めのあるものにあっては、その代表者又は管理人）の氏名

(イ)当該第三者による当該個人データの取得の経緯

（注）第三者は、個人情報取扱事業者がこの確認を行う場合において、当該確認に係る事項を偽ってはならない（個人情報保護法§26Ⅱ）。

③ただし、①②いずれも当該個人データの提供が法令に基づく場合等（個人情報保護法§23Ⅰ①②③④）又は委託、事業承継若しくは共同利用（個人情報保護法§23Ⅴ①②③）のいずれかに該当する場合はこの限りでない（個人情報保護法§25Ⅰ、§26Ⅰ）。

④特定個人情報については、提供できる場合が限定されているので、第三者に提供する場合・提供を受ける場合の記録の作成等が義務付けられていない（番号法§30Ⅲにより個人情報保護法§25、§26の適用除外）。

8. 委託

【ポイント】

- ■ 個人データの取扱いを委託する場合は、委託を受けた者に対する必要かつ適切な監督を行わなければならない。
- □ 特定個人情報の取扱いを委託する場合は、委託を受けた者に対する必要かつ適切な監督を行わなければならない。また、再委託する場合は、最初の委託者の許諾が必要である。

【解説】

①個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない（個人情報保護法§22）。

②特定個人情報の取扱いの全部又は一部を委託する者は、特定個人情報の安全管理が図られるよう、当該委託を受けた者に対する必要かつ適切な監督を行わなければならない（番号法§11）。また、委託をした者の許諾を得た場合に限り、その全部又は一部の再委託をすることができる（番号法§10Ⅰ）。

9. 安全管理措置

【ポイント】

✓ 個人情報保護法が求める安全管理措置と、番号法が求める安全管理措置とでは、その基本的な要素（漏えい、滅失又はき損の防止その他の安全管理のために必要かつ適切な措置）は共通しており、ガイドラインが求める個々の安全管理措置についても、その基本的な要素は共通している。

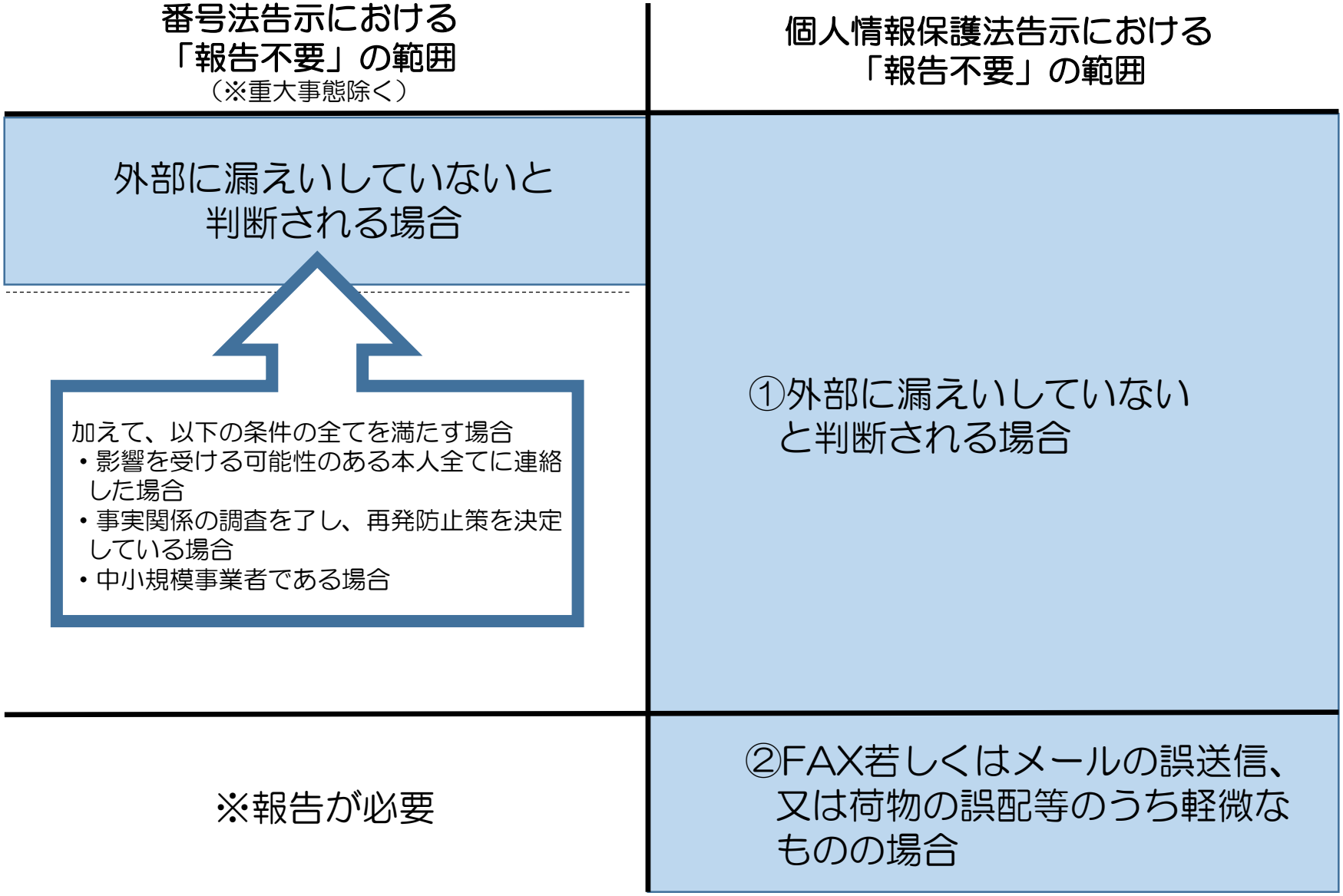
	個人情報保護法の 安全管理措置	番号法の 安全管理措置
内容	■個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない（個人情報保護法§20）。 ※具体的な内容及び手法例（中小特例含む。）は、ガイドライン（通則編）で、組織的・人的・物理的・技術的等の観点から示している。	□個人番号の漏えい、滅失又は毀損の防止その他の個人番号の安全管理のために必要かつ適切な措置を講じなければならない（番号法§12）。 ※具体的な内容及び手法例（中小特例含む。）は、ガイドライン（事業者編）で、組織的・人的・物理的・技術的等の観点から示している。

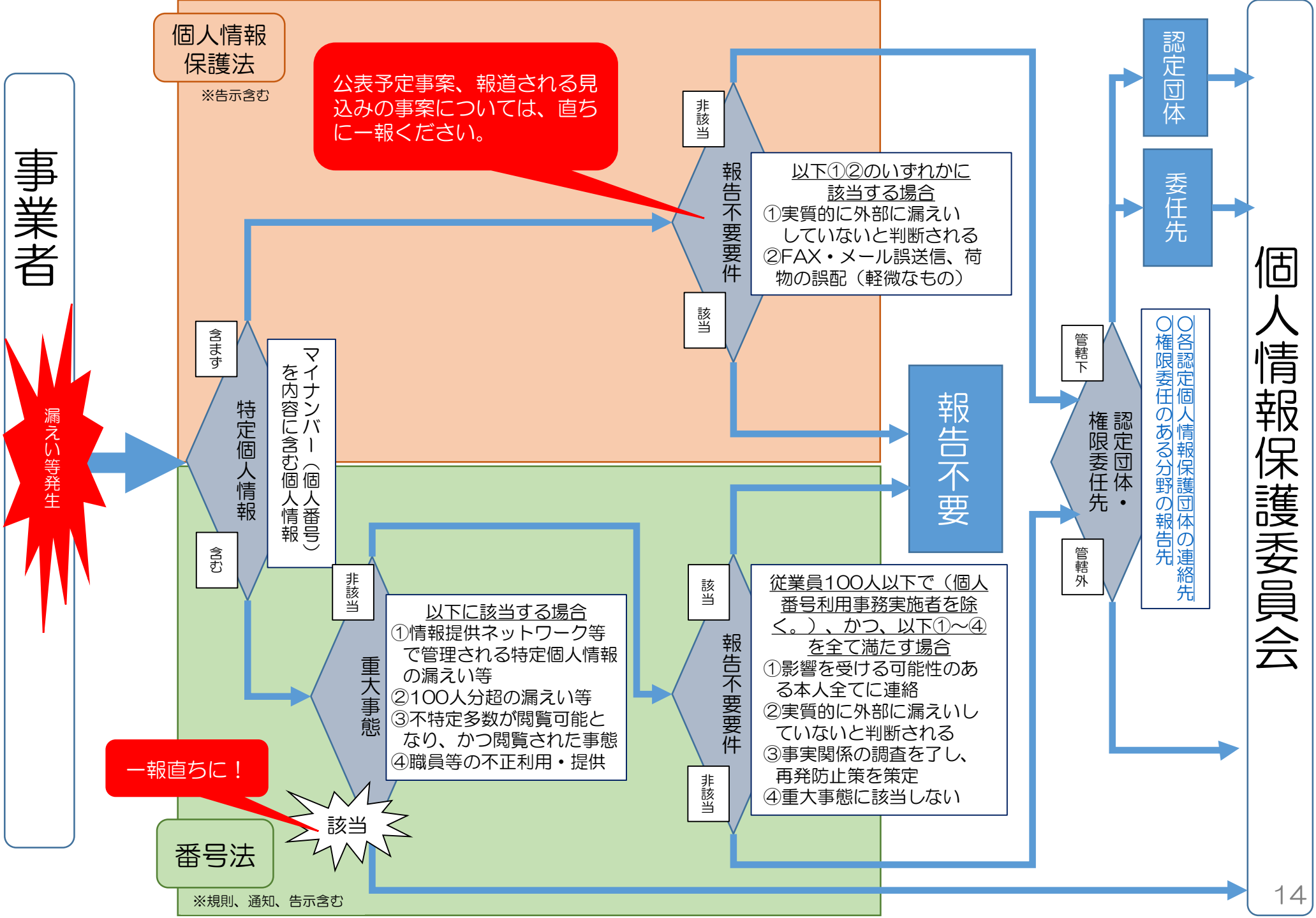
10. 漏えい等が発生した場合の対応

規定項目	番号法、 番号法漏えい規則	番号法漏えい対応告示	個人情報保護法漏えい対応告示
対象事案	【重大事態(§29の4、規則)】 ・情報提供NWS等で管理される特定個人情報の漏えい等 ・100人分超の漏えい等 ・不特定多数が閲覧可能となり、かつ閲覧された事態 ・職員等の不正利用・提供	【重大事態以外】 ・漏えい事案その他の番号法違反の事案又は番号法違反のおそれのある事案	・個人データの漏えい、滅失又は毀損 ・匿名加工情報の作成に用いた個人情報から削除した記述等、個人識別符号（マイナンバー（個人番号）を除く）、§36Ⅰの規定により行った加工の方法に関する情報の漏えい ・これらのおそれ
求められる対応	○以下を報告する。 ・概要及び原因 ・特定個人情報の内容 ・再発防止のためにとった措置 ・その他報告様式所定の事項	○以下の事項について、必要な措置を講ずることが望ましい。 ・事業者内部における報告、被害拡大防止 ・事実関係の調査、原因の究明 ・影響範囲の特定 ・再発防止策の検討・実施 ・影響を受ける可能性のある本人への連絡等 ・事実関係及び再発防止策等の公表 ○委員会等へ報告するよう努める。	
報告先	個人情報保護委員会 （第一報は直ちに報告するよう努める。※1）	原則、個人情報保護委員会 ・認定団体の対象事業者は、認定団体 ・権限委任分野の事業者は、委任先省庁	
報告が不要となる場合	なし	※2	※3

※1　番号法漏えい対応告示により、重大事態に該当する事案（おそれを含む）が発覚した場合は、直ちに報告するよう求めている。
※2　従業員100人以下で（個人番号利用事務実施者を除く。）、かつ、①～④全てをみたす（①影響を受ける可能性のある本人全てに連絡、②実質的に外部に漏えいしていないと判断される、③事実関係の調査を了し、再発防止策を決定、④重大事態に該当しない）。
※3　①②のいずれかに該当する場合（①実質的に外部に漏えいしていないと判断される、②FAX・メール誤送信、荷物誤配（軽微なもの））

（参考）漏えい等が発生した場合の報告が不要となる基準（軽微基準）の比較




事業者
漏えい等発生
個人情報保護法
※告示含む
公表予定事案、報道される見込みの事案については、直ちに一報ください。
特定個人情報
含まず
含む
マイナンバー（個人番号）を内容に含む個人情報
非該当
該当
報告不要要件
以下①②のいずれかに該当する場合
①実質的に外部に漏えいしていないと判断される
②FAX・メール誤送信、荷物の誤配（軽微なもの）
重大事態
非該当
該当
以下に該当する場合
①情報提供ネットワーク等で管理される特定個人情報の漏えい等
②100人分超の漏えい等
③不特定多数が閲覧可能となり、かつ閲覧された事態
④職員等の不正利用・提供
報告不要要件
該当
非該当
従業員100人以下で（個人番号利用事務実施者を除く。）、かつ、以下①～④を全て満たす場合
①影響を受ける可能性のある本人全てに連絡
②実質的に外部に漏えいしていないと判断される
③事実関係の調査を了し、再発防止策を策定
④重大事態に該当しない
報告不要
一報直ちに！
該当
番号法
※規則、通知、告示含む
認定団体・権限委任先
管轄下
管轄外
認定団体
委任先
○各認定個人情報保護団体の連絡先
○権限委任のある分野の報告先
個人情報保護委員会

【巻末資料】個人情報保護法と番号法の安全管理措置の対比

○組織的安全管理措置①

※赤字箇所が実質的な差異（手法の例示を除く。）

個人情報保護法 の安全管理措置	番号法 の安全管理措置
個人情報取扱事業者は、組織的安全管理措置として、次に掲げる措置を講じなければならない。 (1)組織体制の整備 安全管理措置を講ずるための組織体制を整備しなければならない。 ＜手法の例示＞ (組織体制として整備する項目の例) ・個人データの取扱いに関する責任者の設置及び責任の明確化 ・個人データを取り扱う従業者及びその役割の明確化 ・上記の従業者が取り扱う個人データの範囲の明確化 ・法や個人情報取扱事業者において整備されている個人データの取扱いに係る規律に違反している事実又は兆候を把握した場合の責任者への報告連絡体制 ・個人データの漏えい等の事案の発生又は兆候を把握した場合の責任者への報告連絡体制 ・個人データを複数の部署で取り扱う場合の各部署の役割分担及び責任の明確化	事業者は、特定個人情報等の適正な取扱いのために、次に掲げる組織的安全管理措置を講じなければならない。 a 組織体制の整備 安全管理措置を講ずるための組織体制を整備する。 ≪手法の例示≫ ＊ 組織体制として整備する項目は、次に掲げるものが挙げられる。 ・事務における責任者の設置及び責任の明確化 ・事務取扱担当者の明確化及びその役割の明確化 ・事務取扱担当者が取り扱う特定個人情報等の範囲の明確化 ・事務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の責任者への報告連絡体制 ・情報漏えい等事案の発生又は兆候を把握した場合の従業者から責任者等への報告連絡体制 ・特定個人情報等を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化
(2)個人データの取扱いに係る規律に従った運用 あらかじめ整備された個人データの取扱いに係る規律に従って個人データを取り扱わなければならない。 なお、整備された個人データの取扱いに係る規律に従った運用の状況を確認するため、利用状況等を記録することも重要である。 ＜手法の例示＞ 個人データの取扱いに係る規律に従った運用を確保するため、例えば次のような項目に関して、システムログその他の個人データの取扱いに係る記録の整備や業務日誌の作成等を通じて、個人データの取扱いの検証を可能とすることが考えられる。 ・個人情報データベース等の利用・出力状況 ・個人データが記載又は記録された書類・媒体等の持ち運び等の状況 ・個人情報データベース等の削除・廃棄の状況（委託した場合の消去・廃棄を証明する記録を含む。） ・個人情報データベース等を情報システムで取り扱う場合、担当者の情報システムの利用状況（ログイン実績、アクセスログ等）	b 取扱規程等に基づく運用 取扱規程等に基づく運用を行うとともに、その状況を確認するため、特定個人情報等の利用状況等を記録する。 ≪手法の例示≫ ＊ 記録する項目としては、次に掲げるものが挙げられる。 ・特定個人情報ファイルの利用・出力状況の記録 ・書類・媒体等の持ち運びの記録 →「持ち運び」については、P19c参照 ・特定個人情報ファイルの削除・廃棄記録 ・削除・廃棄を委託した場合、これを証明する記録等 ・特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況（ログイン実績、アクセスログ等）の記録

○組織的安全管理措置②

個人情報保護法 の安全管理措置	番号法 の安全管理措置
(3)個人データの取扱状況を確認する手段の整備 個人データの取扱状況を確認するための手段を整備しなければならない。 ＜手法の例示＞ 例えば次のような項目をあらかじめ明確化しておくことにより、個人データの取扱状況を把握可能とすることが考えられる。 ・個人情報データベース等の種類、名称 ・個人データの項目 ・責任者・取扱部署 ・利用目的 ・アクセス権を有する者　等	c 取扱状況を確認する手段の整備 特定個人情報ファイルの取扱状況を確認するための手段を整備する。 なお、取扱状況を確認するための記録等には、特定個人情報等は記載しない。 ≪手法の例示≫ ＊ 取扱状況を確認するための記録等としては、次に掲げるものが挙げられる。 ・特定個人情報ファイルの種類、名称 ・責任者、取扱部署 ・利用目的 ・削除・廃棄状況 ・アクセス権を有する者
(4)漏えい等の事案に対応する体制の整備 漏えい等の事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備しなければならない。 なお、漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である(※)。 (※)個人情報取扱事業者において、漏えい等の事案が発生した場合等の対応の詳細については、別に定める(4(漏えい等の事案が発生した場合等の対応)参照)。 ＜手法の例示＞ 漏えい等の事案の発生時に例えば次のような対応を行うための、体制を整備することが考えられる。 ・事実関係の調査及び原因の究明 ・影響を受ける可能性のある本人への連絡 ・個人情報保護委員会等への報告 ・再発防止策の検討及び決定 ・事実関係及び再発防止策等の公表　等	d 情報漏えい等事案に対応する体制の整備 情報漏えい等の事案の発生又は兆候を把握した場合に、適切かつ迅速に対応するための体制を整備する。 情報漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である。 ≪手法の例示≫ ＊ 情報漏えい等の事案の発生時に、次のような対応を行うことを念頭に、体制を整備することが考えられる。 ・事実関係の調査及び原因の究明 ・影響を受ける可能性のある本人への連絡 ・委員会又は事業所管大臣等への報告 ・再発防止策の検討及び決定 ・事実関係及び再発防止策等の公表

○組織的安全管理措置③

個人情報保護法 の安全管理措置	番号法 の安全管理措置
(5)取扱状況の把握及び安全管理措置の見直し 　個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない。 ＜手法の例示＞ ・個人データの取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施する。 ・外部の主体による監査活動と合わせて、監査を実施する。	e 取扱状況の把握及び安全管理措置の見直し 　特定個人情報等の取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組む。 ≪手法の例示≫ ＊ 特定個人情報等の取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施することが考えられる。 ＊ 外部の主体による他の監査活動と合わせて、監査を実施することも考えられる。

○人的安全管理措置

個人情報保護法 の安全管理措置	番号法 の安全管理措置
個人情報取扱事業者は、人的安全管理措置として、次に掲げる措置を講じなければならない。また、個人情報取扱事業者は、従業者に個人データを取り扱わせるに当たっては、法第21条に基づき従業者に対する監督をしなければならない（3-3-3（従業者の監督）参照）。 ○従業者の教育 　従業者に、個人データの適正な取扱いを周知徹底するとともに適切な教育を行わなければならない。 ＜手法の例示＞ ・個人データの取扱いに関する留意事項について、従業者に定期的な研修等を行う。 ・個人データについての秘密保持に関する事項を就業規則等に盛り込む。	事業者は、特定個人情報等の適正な取扱いのために、次に掲げる人的安全管理措置を講じなければならない。 a 事務取扱担当者の監督 　事業者は、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。 b 事務取扱担当者の教育 　事業者は、事務取扱担当者に、特定個人情報等の適正な取扱いを周知徹底するとともに適切な教育を行う。 ≪手法の例示≫ ＊ 特定個人情報等の取扱いに関する留意事項等について、従業者に定期的な研修等を行うことが考えられる。 ＊ 特定個人情報等についての秘密保持に関する事項を就業規則等に盛り込むことが考えられる。

○物理的安全管理措置①

個人情報保護法 の安全管理措置	番号法 の安全管理措置
個人情報取扱事業者は、物理的安全管理措置として、次に掲げる措置を講じなければならない。 (1)個人データを取り扱う区域の管理 個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域(以下「管理区域」という。)及びその他の個人データを取り扱う事務を実施する区域(以下「取扱区域」という。)について、それぞれ適切な管理を行わなければならない。 ＜手法の例示＞ (管理区域の管理手法の例) ・入退室管理及び持ち込む機器等の制限等 なお、入退室管理の方法としては、ICカード、ナンバーキー等による入退室管理システムの設置等が考えられる。 (取扱区域の管理手法の例) ・間仕切り等の設置、座席配置の工夫、のぞき込みを防止する措置の実施等による、権限を有しない者による個人データの閲覧等の防止	事業者は、特定個人情報等の適正な取扱いのために、次に掲げる物理的安全管理措置を講じなければならない。 a 特定個人情報等を取り扱う区域の管理 特定個人情報ファイルを取り扱う情報システム(サーバ等)を管理する区域(以下「管理区域」という。)を明確にし、物理的な安全管理措置を講ずる。 また、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。)について、事務取扱担当者等以外の者が特定個人情報等を容易に閲覧等できないよう留意する必要がある。 ≪手法の例示≫ ＊ 管理区域に関する物理的安全管理措置としては、入退室管理及び管理区域へ持ち込む機器等の制限等が考えられる。 ＊ 入退室管理方法としては、ICカード、ナンバーキー等による入退室管理システムの設置等が考えられる。 ＊ 取扱区域に関しては、間仕切り等の設置、座席配置の工夫、のぞき込みを防止する措置等を講ずることが考えられる。
(2)機器及び電子媒体等の盗難等の防止 個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、適切な管理を行わなければならない。 ＜手法の例示＞ ・個人データを取り扱う機器、個人データが記録された電子媒体又は個人データが記載された書類等を、施錠できるキャビネット・書庫等に保管する。 ・個人データを取り扱う情報システムが機器のみで運用されている場合は、当該機器をセキュリティワイヤー等により固定する。	b 機器及び電子媒体等の盗難等の防止 管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる。 ≪手法の例示≫ ＊ 特定個人情報等を取り扱う機器、電子媒体又は書類等を、施錠できるキャビネット・書庫等に保管することが考えられる。 ＊ 特定個人情報ファイルを取り扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定すること等が考えられる。

○物理的安全管理措置②

個人情報保護法 の安全管理措置	番号法 の安全管理措置
(3)電子媒体等を持ち運ぶ場合の漏えい等の防止 個人データが記録された電子媒体又は書類等を持ち運ぶ場合、容易に個人データが判明しないよう、安全な方策を講じなければならない。 なお、「持ち運ぶ」とは、個人データを管理区域又は取扱区域から外へ移動させること又は当該区域の外から当該区域へ移動させることをいい、事業所内の移動等であっても、個人データの紛失・盗難等に留意する必要がある。 ＜手法の例示＞ ・持ち運ぶ個人データの暗号化、パスワードによる保護等を行った上で電子媒体に保存する。 ・封緘、目隠しシールの貼付けを行う。 ・施錠できる搬送容器を利用する。	c 電子媒体等の取扱いにおける漏えい等の防止 特定個人情報等が記録された電子媒体又は書類等を持ち運ぶ場合、容易に個人番号が判明しないよう、安全な方策を講ずる。 「持ち運ぶ」とは、特定個人情報等を管理区域又は取扱区域から外へ移動させること又は当該区域の外から当該区域へ移動させることをいい、事業所内での移動等であっても、特定個人情報等の紛失・盗難等に留意する必要がある。 ≪手法の例示≫ ＊ 特定個人情報等が記録された電子媒体を安全に持ち運ぶ方法としては、持ち運ぶデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用、追跡可能な移送手段の利用等が考えられる。ただし、行政機関等に法定調書等をデータで提出するに当たっては、行政機関等が指定する提出方法に従う。 ＊ 特定個人情報等が記載された書類等を安全に持ち運ぶ方法としては、封緘、目隠しシールの貼付、追跡可能な移送手段の利用等が考えられる。
(4)個人データの削除及び機器、電子媒体等の廃棄 個人データを削除し又は個人データが記録された機器、電子媒体等を廃棄する場合は、復元不可能な手段で行わなければならない。 また、個人データを削除した場合、又は、個人データが記録された機器、電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存することや、それらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて証明書等により確認することも重要である。 ＜手法の例示＞ （個人データが記載された書類等を廃棄する方法の例） ・焼却、溶解、適切なシュレッダー処理等の復元不可能な手段を採用する。 （個人データを削除し、又は、個人データが記録された機器、電子媒体等を廃棄する方法の例） ・情報システム（パソコン等の機器を含む。）において、個人データを削除する場合、容易に復元できない手段を採用する。 ・個人データが記録された機器、電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等の手段を採用する。	d 個人番号の削除、機器及び電子媒体等の廃棄 個人番号関係事務又は個人番号利用事務を行う必要がなくなった場合で、所管法令等において定められている保存期間等を経過した場合には、個人番号をできるだけ速やかに復元不可能な手段で削除又は廃棄する。 →ガイドライン第４－３－(3)B参照 個人番号若しくは特定個人情報ファイルを削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存する。また、これらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認する。 ≪手法の例示≫ ＊ 特定個人情報等が記載された書類等を廃棄する場合、焼却又は溶解、復元不可能な程度に細断可能なシュレッダーの利用、個人番号部分を復元不可能な程度にマスキングすること等の復元不可能な手段を採用することが考えられる。 ＊ 特定個人情報等が記録された機器及び電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を採用することが考えられる。 ＊ 特定個人情報等を取り扱う情報システム又は機器等において、特定個人情報ファイル中の個人番号又は一部の特定個人情報等を削除する場合、容易に復元できない手段を採用することが考えられる。 ＊ 特定個人情報等を取り扱う情報システムにおいては、保存期間経過後における個人番号の削除を前提とした情報システムを構築することが考えられる。 ＊ 個人番号が記載された書類等については、保存期間経過後における廃棄を前提とした手続を定めることが考えられる。

○技術的安全管理措置①

個人情報保護法 の安全管理措置	番号法 の安全管理措置
個人情報取扱事業者は、情報システム（パソコン等の機器を含む。）を使用して個人データを取り扱う場合（インターネット等を通じて外部と送受信等する場合を含む。）、技術的安全管理措置として、次に掲げる措置を講じなければならない。 (1)アクセス制御 担当者及び取り扱う個人情報データベース等の範囲を限定するために、適切なアクセス制御を行わなければならない。 ＜手法の例示＞ ・個人情報データベース等を取り扱うことのできる情報システムを限定する。 ・情報システムによってアクセスすることのできる個人情報データベース等を限定する。 ・ユーザーIDに付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる従業者を限定する。	事業者は、特定個人情報等の適正な取扱いのために、次に掲げる技術的安全管理措置を講じなければならない。 a アクセス制御 情報システムを使用して個人番号関係事務又は個人番号利用事務を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う。 ≪手法の例示≫ ＊ アクセス制御を行う方法としては、次に掲げるものが挙げられる。 ・ 特定個人情報ファイルを取り扱うことのできる情報システム端末等を限定する。 ・ 各情報システムにおいて、アクセスすることのできる特定個人情報ファイルを限定する。 ・ ユーザーIDに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を事務取扱担当者に限定する。
(2)アクセス者の識別と認証 個人データを取り扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない。 ＜手法の例示＞ （情報システムを使用する従業者の識別・認証手法の例） ・ユーザーID、パスワード、磁気・ICカード等	b アクセス者の識別と認証 特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する。 ≪手法の例示≫ ＊ 事務取扱担当者の識別方法としては、ユーザーID、パスワード、磁気・ICカード等が考えられる。

○技術的安全管理措置②

個人情報保護法 の安全管理措置	番号法 の安全管理措置
(3)外部からの不正アクセス等の防止 個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。 ＜手法の例示＞ ・情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する。 ・情報システム及び機器にセキュリティ対策ソフトウェア等(ウイルス対策ソフトウェア等)を導入し、不正ソフトウェアの有無を確認する。 ・機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 ・ログ等の定期的な分析により、不正アクセス等を検知する。	c 外部からの不正アクセス等の防止 情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する。 ≪手法の例示≫ ＊ 情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断することが考えられる。 ＊ 情報システム及び機器にセキュリティ対策ソフトウェア等(ウイルス対策ソフトウェア等)を導入し、不正ソフトウェアの有無を確認することが考えられる。 ＊ 機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とすることが考えられる。 ＊ ログ等の分析を定期的に行い、不正アクセス等を検知することが考えられる。
(4)情報システムの使用に伴う漏えい等の防止 情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用しなければならない。 ＜手法の例示＞ ・情報システムの設計時に安全性を確保し、継続的に見直す(情報システムのぜい弱性を突いた攻撃への対策を講ずることも含む。)。 ・個人データを含む通信の経路又は内容を暗号化する。 ・移送する個人データについて、パスワード等による保護を行う。	d 情報漏えい等の防止 特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる。 ≪手法の例示≫ ＊ 通信経路における情報漏えい等の防止策としては、通信経路の暗号化等が考えられる。 ＊ 情報システム内に保存されている特定個人情報等の情報漏えい等の防止策としては、データの暗号化又はパスワードによる保護等が考えられる。