恩納村

特定個人情報等取扱マニュアル

作成者	恩納村役場　総務課
作成日	平成２９年１１月３０日
最終更新日	

目　　次

Ⅰ　基本事項【管理規程第１章関連】

１　目的

平成 28 年１月より、マイナンバー（以下「個人番号」という。）及び特定個人情報（個人番号を含んだ個人情報）の取扱いがはじまり、住民等の税や社会保障、災害対策の事務に加え、源泉徴収事務や支払調書作成事務等で、多くの職員が個人番号を取り扱うこととなった。

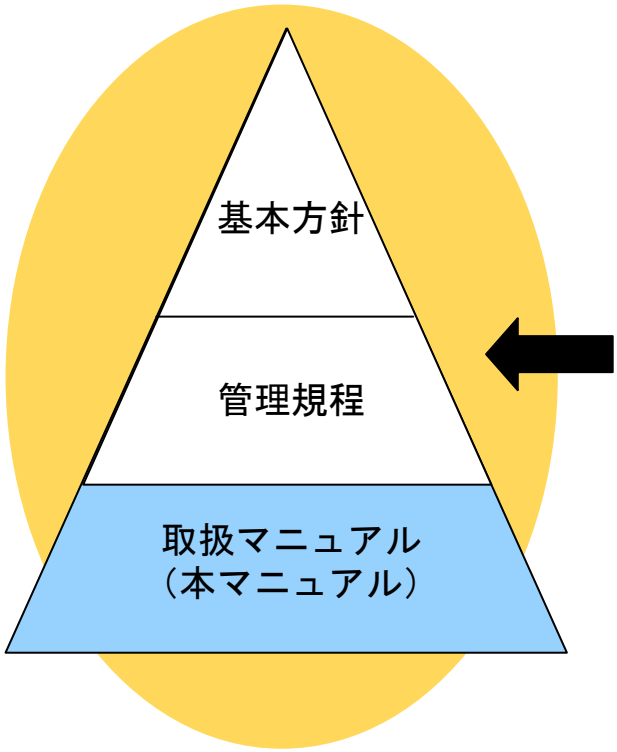
そのため、個人番号を取り扱う事務においては、個人番号の漏えいや滅失等の防止をはじめ、個人番号の適切な管理のために必要な措置を講ずることが求められている。

また、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。）や恩納村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に基づく個人番号の利用及び特定個人情報の提供に関する条例（平成 27 年恩納村条例第 25 号。以下「番号利用・提供条例」という。）、恩納村個人情報保護条例（平成 15 年恩納村条例第 10 号。以下「個人情報保護条例」という。）において、個人番号及び特定個人情報（以下「特定個人情報等」という。）の厳格な取扱いが定められている。

これらを踏まえ、すべての職員が特定個人情報等の取り扱いについて正しく理解し、安全で適切な制度運用を行うことを目的に、本マニュアルを作成する。

２　概要

（１）　全体像と関係する主な法令等



【関係する主な法令等】

- 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（番号法）
- 恩納村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に基づく個人番号の利用及び特定個人情報の提供に関する条例（番号利用・提供条例）
- 恩納村個人情報保護条例（個人情報保護条例）
- 恩納村個人情報保護条例施行規則（平成 15 年恩納村規則第 16 号）
- 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・地方公共団体等編）（平成 26 年特定個人情報保護委員会告示第６号）
- 恩納村情報セキュリティポリシー

（２）　番号法と個人情報保護条例との関係

番号法は、特定個人情報等の取扱いに関して、個人情報の保護に関する法律（平成 15 年法律第 57 号）、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。）及び独立行政法人等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 59 号。以下「独立行政法人等個人情報保護法」という。）の３つの法律（以下「一般法」という。）の特例を規定した特別法であることから、番号法は一般法の規定に優先して適用される。

地方公共団体においては、一般法の位置付けが個人情報保護条例となるため、特定個人情報等に関する番号法の規定は、個人情報保護条例の規定に優先して適用されるが、特定個人情報等に関して番号法に特段の規定がない事項については、個人情報保護条例の規定が適用されることとなる。

（３）　特定個人情報等の取扱いに関するポイント

特定個人情報等を取り扱ううえで、個人情報保護条例における個人情報の取扱いと大きく異なる点は、番号法により、特定個人情報等を取り扱うことのできる範囲が限定されていることにある。番号法においては、個人番号の利用範囲及び提供の要求について制限されているほか、特定個人情報の提供、収集及び保管並びに特定個人情報ファイルの作成についても、その範囲が制限されている。

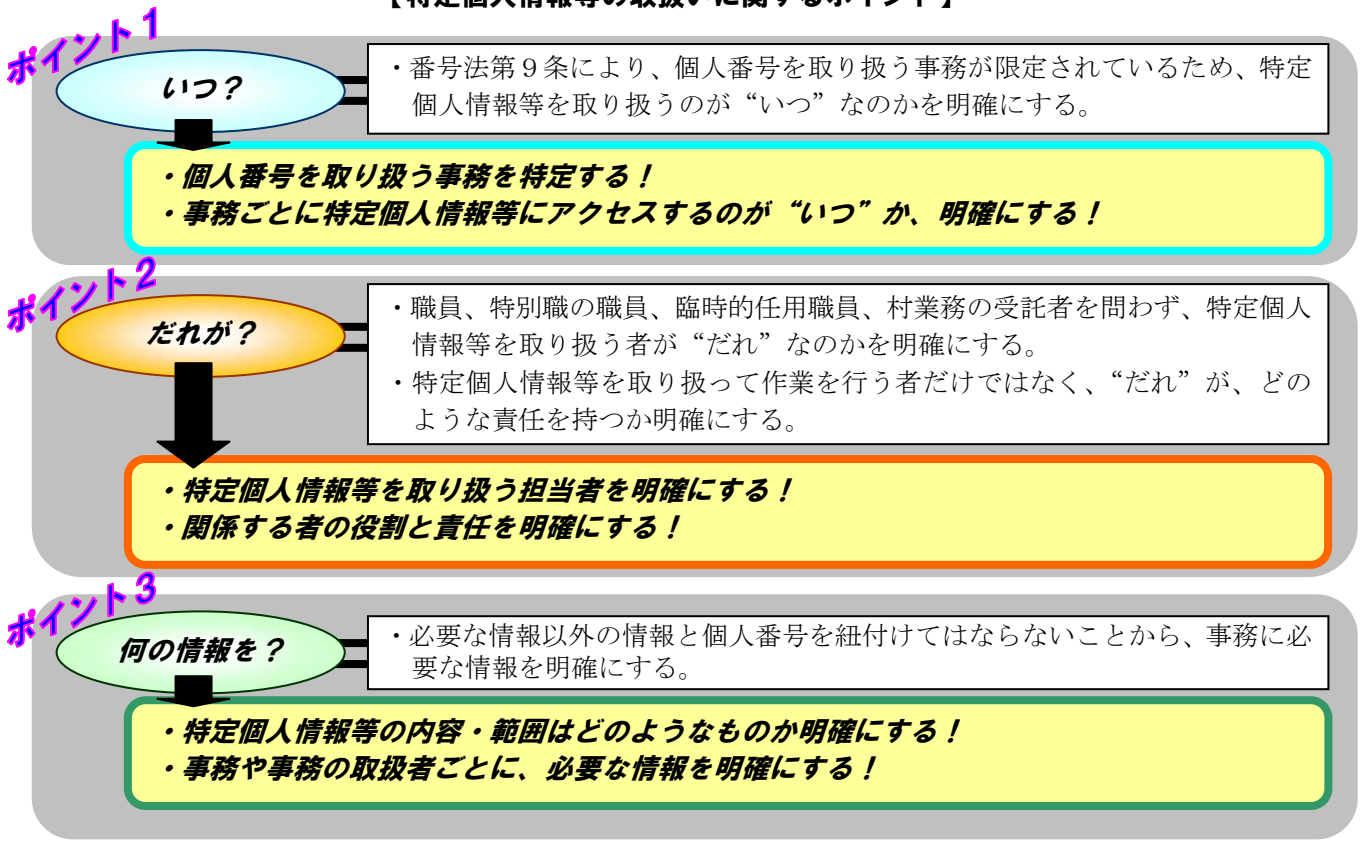
【特定個人情報等の取扱いに関する番号法の主な規定】

番号法	内容
第９条	（利用範囲） ・番号法に明記された事務の処理に関して保有する特定個人情報ファイルにおいて個人情報を効率的に検索し、及び管理するために必要な限度で個人番号を利用することができる。
第 15 条	（提供の求めの制限） ・番号法第 19 条各号のいずれかに該当して特定個人情報の提供を受けることができる場合を除き、他人（自己と同一の世帯に属する者以外の者をいう。第 20 条において同じ。）に対し、個人番号の提供を求めてはならない。
第 19 条	（特定個人情報の提供の制限） ・番号法に明記された場合を除き、特定個人情報の提供をしてはならない。
第 20 条	（収集等の制限） ・番号法第 19 条各号のいずれかに該当する場合を除き、特定個人情報（他人の個人番号を含むものに限る。）を収集し、又は保管してはならない。
第 28 条	（特定個人情報ファイルの作成の制限） ・番号法第 19 条第 11 号から第 14 号までのいずれかに該当して特定個人情報を提供し、又はその提供を受けることができる場合を除き、個人番号利用事務等を処理するために必要な範囲を超えて特定個人情報ファイルを作成してはならない。

【収集又は保管に関する留意事項】
・番号法第 15 条及び第 20 条において、他人とは「自己と同一の世帯に属する者以外の者」であり、子、配偶者等の自己と同一の世帯に属する者の特定個人情報等は、同法第 19 条各号のいずれかに該当しなくても、収集又は保管することができると解される。

そのため、特定個人情報等の取扱いについては、“いつ”、“だれ”が“何の情報”を取り扱うかを明確にしてくことが必要となる。

【特定個人情報等の取扱いに関するポイント】



３　適用範囲

（１）　実施機関の職員

個人情報保護条例第２条第７号に規定する実施機関（村長（水道事業管理者の職務を行う村長を含む。）、議会、教育委員会、選挙管理委員会、農業委員会、固定資産評価審査委員会及び監査委員）の職員（非常勤職員及び臨時職員を含む。）をいう。

（２）　委託先及び再委託先（再々委託先以降を含む。）

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。）の全部又は一部を委託する場合には、委託先において、村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う。

また、委託先において、個人番号利用事務等の全部又は一部が再委託される場合には、委託先又は村自らが、村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う。

なお、再委託先が再々委託を行う場合以降も、同様である。

４　用語の定義

（１）　個人情報

個人に関する情報（事業を営む個人の当該事業に関する情報を除く。）であって、特定の個人が識別され、又は識別され得るものをいう。

（２）　個人番号

番号法第７条第１項又は第２項の規定により、住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。

（３）　特定個人情報

個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報をいう。

（４）　特定個人情報ファイル

個人番号をその内容に含む個人情報ファイルをいう。

【参考：個人情報ファイルの定義（行政機関個人情報保護法第２条第４項）】

４　この法律において「個人情報ファイル」とは、保有個人情報を含む情報の集合物であって、次に掲げるものをいう。
（１）　一定の事務の目的を達成するために特定の保有個人情報を電子計算機を用いて検索することができるように体系的に構成したもの
（２）　前号に掲げるもののほか、一定の事務の目的を達成するために氏名、生年月日、その他の記述等により特定の保有個人情報を容易に検索することができるように体系的に構成したもの

（５）　個人番号利用事務

行政機関、地方公共団体、独立行政法人等その他の行政事務を処理する者が番号法第９条第１項又は第２項の規定によりその保有する特定個人情報ファイルにおいて個人情報を効率的に検索し、及び管理するために必要な限度で個人番号を利用して処理する事務をいう。

（６）　個人番号関係事務

番号法第９条第３項の規定により個人番号利用事務に関して行われる他人の個人番号を必要な限度で利用して行う事務をいう。

（７）　個人番号利用事務実施者

個人番号利用事務を処理する者及び個人番号利用事務の全部又は一部の委託を受けた者をいう。

（８）　個人番号関係事務実施者

個人番号関係事務を処理する者及び個人番号関係事務の全部又は一部の委託を受けた者をいう。

５　罰則の強化

行政機関個人情報保護法、独立行政法人等個人情報保護法、住民基本台帳法（昭和 42 年法律第 81 号)、国家公務員法（昭和 22 年法律第 120 号）及び地方公務員法（昭和 25 年法律第 261 号）においては、正当な理由なく個人情報ファイルを提供したとき、不正な利益を図る目的で保有個人情報を提供又は盗用したとき、職務上知り得た秘密を漏えい又は盗用したとき等に罰則が科されることとされているが、番号法においては、類似の刑の上限が引き上げられるなど、罰則が強化されている（番号法第 51 条から第 58 条まで)。

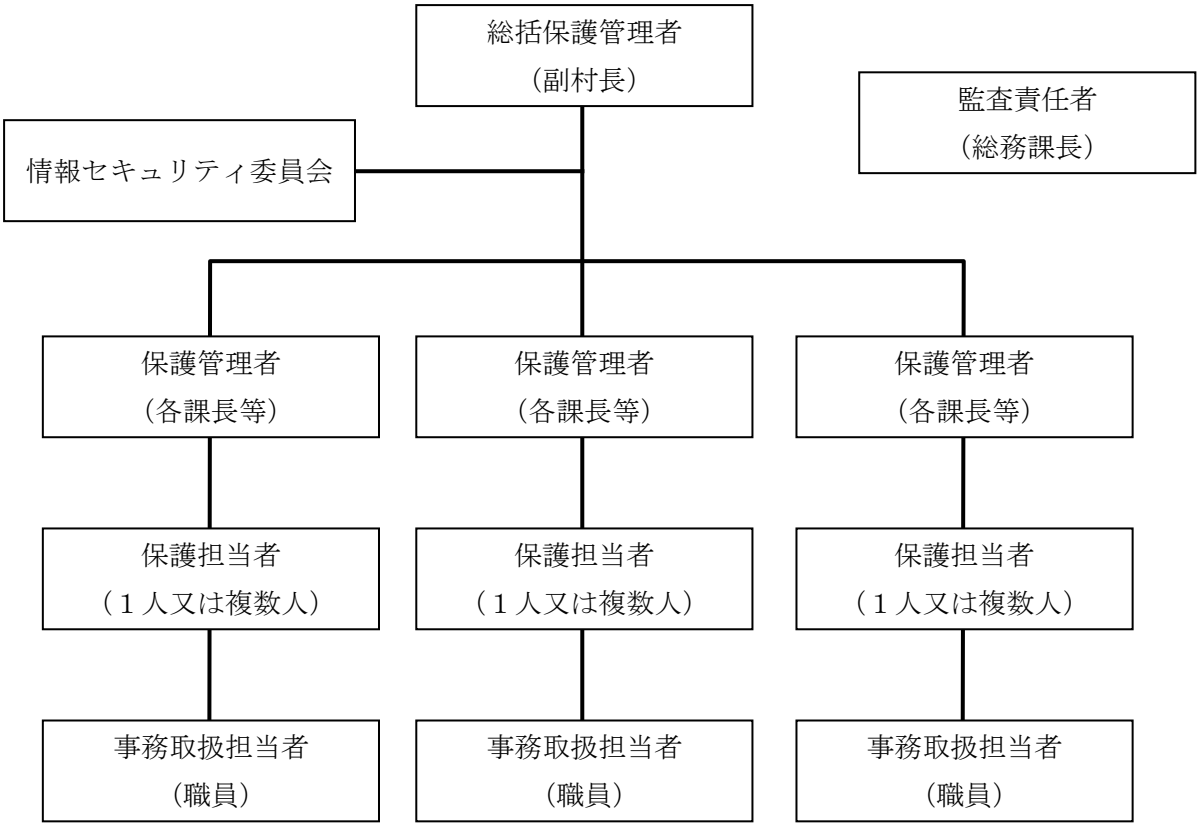
【罰則規定】

行為	番号法	同種法律における類似規定の罰則	
		行政機関個人情報保護法【個人情報保護条例】	住民基本台帳法
個人番号利用事務等に従事する者又は従事していた者が、正当な理由なく、特定個人情報ファイルを提供	**４年以下の懲役若しくは 200 万円以下の罰金又は併科（第 51 条）**	２年以下の懲役又は 100 万円以下の罰金（第 53 条【規定なし】)	－
上記の者が、不正な利益を図る目的で、個人番号を提供又は盗用	**３年以下の懲役若しくは 150 万円以下の罰金又は併科（第 52 条）**	１年以下の懲役又は 50 万円以下の罰金（第 54 条【規定なし】)	２年以下の懲役又は 100 万円以下の罰金（第 42 条）
情報提供ネットワークシステムの事務に従事する者又は従事していた者が、情報提供ネットワークシステムに関する秘密を漏えい又は盗用	**同上（第 53 条）**	－	同上（第 42 条）
人を欺き、人に暴行を加え、人を脅迫し、又は財物の窃取、施設への侵入、不正アクセス等により個人番号を取得	**３年以下の懲役又は 150 万円以下の罰金（第 54 条）**	－	－
職員が、職権を濫用して、専らその職務の用以外の用に供する目的で、特定個人情報等が記録された文書等を収集	**２年以下の懲役又は 100 万円以下の罰金（第 55 条）**	１年以下の懲役又は 50 万円以下の罰金（第 55 条【規定なし】)	－
個人情報保護委員会から命令を受けた者が、個人情報保護委員会の命令に違反	**２年以下の懲役又は 50 万円以下の罰金（第 56 条）**	－	１年以下の懲役又は 50 万円以下の罰金（第 43 条）
個人情報保護委員会に対する虚偽の報告、虚偽の資料提出、検査拒否等	**１年以下の懲役又は 50 万円以下の罰金（第 57 条）**	－	30 万円以下の罰金（第 46 条､第 47 条）
偽りその他不正の手段により個人番号カード等を取得	**６月以下の懲役又は 50 万円以下の罰金（第 58 条）**	－	30 万円以下の罰金（第 46 条）

Ⅱ　管理体制【管理規程第２章関連】

１　管理体制

特定個人情報等の適正な取扱いを図るため、次の管理体制を整備する。



２　総括保護管理者

（１）　総括保護管理者の設置

総括保護管理者は、副村長をもって充て、村長を補佐し、村における特定個人情報等の管理に関する事務を総括する任に当たる。

副村長は、恩納村情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）に規定された最高情報セキュリティ責任者（Chief Information Security Officer）でもあり、情報セキュリティポリシーと連携した管理体制を整備する。

（２）　総括保護管理者の所掌事項

総括保護管理者は、特定個人情報等の取扱いに関する次の事項を所掌する。

① 保護管理者、保護担当者、事務取扱担当者及び職員に対する必要かつ適切な監督

② 保護管理者、保護担当者、事務取扱担当者及び職員に対する教育研修の実施

③ 情報セキュリティ委員会の設置及び開催

④ 特定個人情報等の漏えい、滅失又は毀損等（以下「情報漏えい等」という。）の事案に係る事実関係及び再発防止策の公表

⑤ 監査又は点検の結果等を踏まえた評価及び見直し

３　保護管理者

（１）　保護管理者の設置

保護管理者は、特定個人情報等を取り扱う各課等の長（又はこれに代わる者）をもって充て、各課等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。

具体的には、村長（水道事業管理者の職務を行う村長を含む。）、議会、教育委員会、選挙管理委員会、農業委員会、固定資産評価審査委員会及び監査委員の各部局において、個人番号利用事務等を所管する部署の長等が該当する。

なお、法定調書の作成や共済組合等の事務を処理している場合は、個人番号関係事務に該当することに留意する。

（２）　保護管理者の所掌事項

保護管理者は、特定個人情報等の取扱いに関する次の事項を所掌する。

① 特定個人情報等を情報システムで取り扱う場合の当該情報システムの管理者との連携

② 特定個人情報等を取り扱う職員及びその役割の指定（事務取扱担当者の明確化）

③ 事務取扱担当者が取り扱う特定個人情報等の範囲の指定

④ 事務取扱担当者に対する必要かつ適切な監督

⑤ その他、所管する特定個人情報等に係る安全管理措置の実施

（３）　保護管理者が整備すべき組織体制

保護管理者は、次に掲げる組織体制を整備する。

① 事務取扱担当者が恩納村特定個人情報等の取扱いに関する管理規程（平成 29 年恩納村規程第７号。以下「管理規程」という。）等に違反している事実又は兆候を把握した場合の職員から保護管理者への報告連絡体制

② 特定個人情報等の情報漏えい等の事案の発生又は兆候を把握した場合の職員から保護管理者等への報告連絡体制

③　特定個人情報等を複数の課等で取り扱う場合の各課等の任務分担及び責任の明確化

④　特定個人情報等の情報漏えい等の事案の発生又は兆候を把握した場合の対応体制

４　保護担当者

（１）　保護担当者の設置

保護担当者は、特定個人情報等を取り扱う各課等に１人又は複数人置くこととし、当該課等の保護管理者が指定する。

（２）　保護担当者の所掌事項

保護担当者は、保護管理者を補佐し、各課等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。

５　監査責任者

（１）　監査責任者の設置

監査責任者は、総務課長をもって充て、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。

（２）　監査責任者の所掌事項

監査責任者は、特定個人情報等の管理の状況について、定期に又は随時に監査を行い、その結果を総括保護管理者に報告する。

６　事務取扱担当者

（１）　事務取扱担当者の明確化

保護管理者は、特定個人情報等を取り扱う職員及びその役割を指定するとともに、各事務取扱担当者が取り扱う特定個人情報等の範囲を指定する。

【参考：事務取扱担当者の明確化】

部署名（○○課、○○係等）、事務名（○○事務担当者）等により、担当者が明確になれば十分であると考えられます。
ただし、部署名等により事務取扱担当者の範囲が明確化できない場合には、事務取扱担当者を指名する等を行う必要があると考えられます。

資料：個人情報保護委員会事務局「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・地方公共団体等編）の概要」平成 28 年１月版

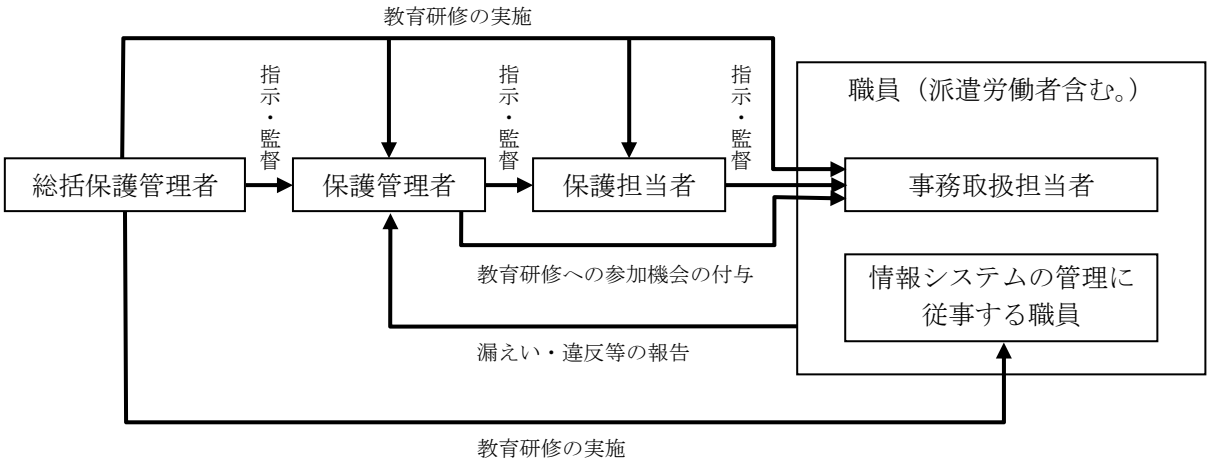
7　情報セキュリティ委員会

（1）　情報セキュリティ委員会の設置

総括保護管理者は、特定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、情報セキュリティ委員会を設け、定期に又は随時に開催する。

Ⅲ　教育研修・職員の責務【管理規程第３章・第４章関連】

１　教育研修・職員の責務のフロー



２　総括保護管理者の役割

総括保護管理者は、保護管理者及び保護担当者に対し、課等の現場における特定個人情報等の適切な管理のための教育研修を実施する。

また、管理規程及び本マニュアルを遵守し、特定個人情報等の適正な取扱いが周知徹底されるよう、事務取扱担当者及び情報システムの管理に従事する職員に対して啓発を行うとともに、定期的に教育研修を実施し、特定個人情報等が管理規程及び本マニュアルに基づき適正に取り扱われるよう、職員に対して、必要かつ適切な監督を行う。

【教育研修の例】
- 特定個人情報等の適正な取扱いについて理解を深め、特定個人情報等の保護に関する意識の高揚を図るための啓発や研修（事務取扱担当者向け）
- 情報システムの管理、運用及びセキュリティ対策に関する研修（情報システムの管理に従事する職員）
- 各課等における特定個人情報等の適正な管理のための教育研修（保護管理者、保護担当者向け）

３　保護管理者の役割

保護管理者は、当該課等の事務取扱担当者に対し、総括保護管理者が実施する教育研修への参加の機会を与える等の必要な措置を講ずる。

また、特定個人情報等が管理規程及び本マニュアルに基づき適正に取り扱われるよう、当該課等の職員を監督する。

４　保護担当者の役割

保護担当者は、保護管理者の指示に基づき「３　保護管理者の役割」を補佐する。

５　派遣労働者の位置付け

特定個人情報等の取扱いに従事する派遣労働者についても、職員と同様、特定個人情報等の適切な管理のための教育研修を実施するなど、必要な措置を講ずる。

６　職員の責務

事務取扱担当者は、個人情報保護条例及び番号法の趣旨に則り、関連する法令及び規程等の定め、並びに総括保護管理者、保護管理者及び保護担当者の指示に従い、特定個人情報等を取り扱わなければならない。

職員は、特定個人情報等の情報漏えい等の事案の発生又は兆候を把握した場合及び事務取扱担当者が管理規程等に違反している事実又は兆候を把握した場合は、速やかに保護管理者に報告しなければならない。

Ⅳ　特定個人情報等の取扱い【管理規程第５章関連】

１　アクセス制限

（１）　アクセス権限の範囲の限定

保護管理者は、特定個人情報等にアクセスする権限を有する職員とその権限の内容を、当該職員が業務を行ううえで必要最小限の範囲に限る。

【具体例】
・ファイルサーバ上に特定個人情報ファイルを保存するフォルダを作成し、許可された職員のみが、そのフォルダを開くことができるようにするなどの措置を講ずる。

（２）　権限のない職員のアクセス禁止

アクセス権限を有しない職員は、特定個人情報等にアクセスしてはならない。

【具体例】
・アクセス権限を有しない職員は、アクセス権限を有する職員のユーザーID とパスワードを使用してアクセスしてはならない。
・アクセス権限を有しない職員は、アクセス権限を有する職員の PC を一時的に使用してアクセスしてはならない。
・アクセス権限を有する職員は、アクセス権限を有しない職員にパスワードを教えたり、自分の PC を使用させたりしてはならない。

（３）　目的外アクセスの禁止

事務取扱担当者は、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特定個人情報等にアクセスしてはならない。

【具体例】
・住基ネットを使って芸能人の住所を調べたり、業務上必要がないにもかかわらず、住民の所得情報を参照したりするなどの行為をしてはならない。

２　複製等の制限

事務取扱担当者が業務上の目的で特定個人情報等を取り扱う場合であっても、特定個人情報等の取扱いは、当該行為を行うことができる場合を限定して行わなければならない。

保護管理者は、次に掲げる行為について、事務取扱担当者を適切に監督し、事務取扱担当者は、保護管理者の指示に従って行う。

（１）　特定個人情報等の複製

事務取扱担当者は、所定の手続がない場合、特定個人情報等を複写・複製してはならない。

所定の手続以外の方法で特定個人情報等を複写・複製する場合は、保護管理者の書面による承認を得なければならない。

【複製等の例】
・PC 上でのデータファイル等の電磁的な複製、USB メモリ等への電磁的な複製
・データファイル等の紙文書への印刷
・紙文書や台帳のコピー

（２） 特定個人情報等の送信

事務取扱担当者は、特定個人情報等の電子メール送信を基本的に LGWAN で接続されている機関間に限るものとし、インターネットメール等で扱ってはならない。

特定個人情報等が記載された紙文書の移動及び FAX 送信は、移動・送信先の間違いなどが起こらないようにし、移動・送信の記録が残る方法で送信しなければならない。

【送信等の例】
・電子メールでの送信、紙文書の FAX 送信
・紙文書の他の課等への移動

（３） 特定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出し

事務取扱担当者は、特定個人情報等が記録されている媒体を外部へ送付する場合、データの暗号化やパスワード設定を施したうえで、簡易書留等の追跡可能な方法を利用する。

また、特定個人情報等が記録されている媒体を外部へ持ち出す場合、持出し中の紛失、盗難、盗み見等の危険があるため、事務取扱担当者は、持ち出すデータの暗号化やパスワード設定を施したうえで、施錠可能な容器に入れて移送する。

【媒体の外部への送付又は持出しの例】
・USB メモリ等による庁外への持出し
・DVD、CD 等の他機関や委託業者への送付

（４） その他、特定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

事務取扱担当者は、特定個人情報等の適切な管理に支障を及ぼすおそれがあると認められるときは、当該特定個人情報等の取扱いの可否について、保護管理者に確認し、その指示に基づき特定個人情報等を取り扱う。

３ 誤りの訂正等

事務取扱担当者は、特定個人情報等の内容に誤り等を発見した場合には、保護管理者の指示に従い、訂正等を行う。事務及び項目にもよるが、中間サーバにも情報が登録されるため、強制修正や職権修正を行うとデータの整合性が失われる可能性があることから、訂正等は個人の判断のみで行わず、必ず保護管理者の指示に従って行うようにする。

保護管理者は、特定個人情報ファイルを複数の事務で利用している場合、当該特定個人情報ファイルの内容の誤りを訂正したら、当該特定個人情報ファイルを利用している課等に訂正を行ったことを知らせる。

また、保護管理者は、特定個人情報等の内容に誤りを発見した場合は、その発生原因

を調査し、再発防止手段をとる。

４　媒体の管理等

事務取扱担当者は、保護管理者の指示に従い、特定個人情報等が記録されている USB メモリ等及び紙文書等の盗難又は紛失等を防止するために、定められた場所に保管する。必要があると認めるときは、耐火金庫への保管、施錠等を行う。

また、特定個人情報等が記録された USB メモリ等及び紙文書等を庁舎内で移動する場合についても、盗難又は紛失等に留意する。

（１）　媒体の管理方法等

① 特定個人情報等を取り扱う USB メモリ等及び紙文書等を管理する場合は、定められた施錠可能な書棚等で厳重に保存管理する。

② 特に必要がある場合は、特定個人情報等が記録された媒体を耐火金庫へ保管し、施錠するなどの措置をとる。

③ 保護管理者は、書棚や耐火金庫等の鍵を管理するとともに、鍵の使用状況及び媒体の使用状況について、記録を作成し、保存する。

５　廃棄等

特定個人情報等は、必要な範囲のみで活用し、不要となった時点で、速やかに情報の削除又は記録された媒体（端末及びサーバに内蔵されているものを含む。）の廃棄を行わなければならない。

事務取扱担当者は、恩納村文書取扱規程（平成 14 年恩納村規定第８号。以下「文書取扱規程」という。）に定める保存期間を経過するなど、特定個人情報等が記録された媒体が不要となった場合には、保護管理者の指示に従って、当該特定個人情報等の復元又は判読が不可能な方法により、当該情報の削除又は当該媒体の廃棄を行う。

なお、特定個人情報等の削除又は記録された媒体の廃棄を行った場合、盗難又は紛失等との区別に有効なことから、その記録を作成し、保存することとする。削除又は廃棄を委託する場合、委託先が確実に削除又は廃棄したことについて、証明書等によって確認する。

【不要になった媒体の例】
・PC、サーバに内蔵されたハードディスクドライブ
・紙文書（出力帳票等の印刷物、申請書、簿冊等）
・個人番号を記載したメモ等
・特定個人情報等が入力されたデータファイル（Excel ファイル等）
・USB メモリ、DVD、CD、MO、磁気テープその他のメディア等の可搬媒体
・取り外し可能なハードディスク等の媒体
・映像、録音、その他の記録

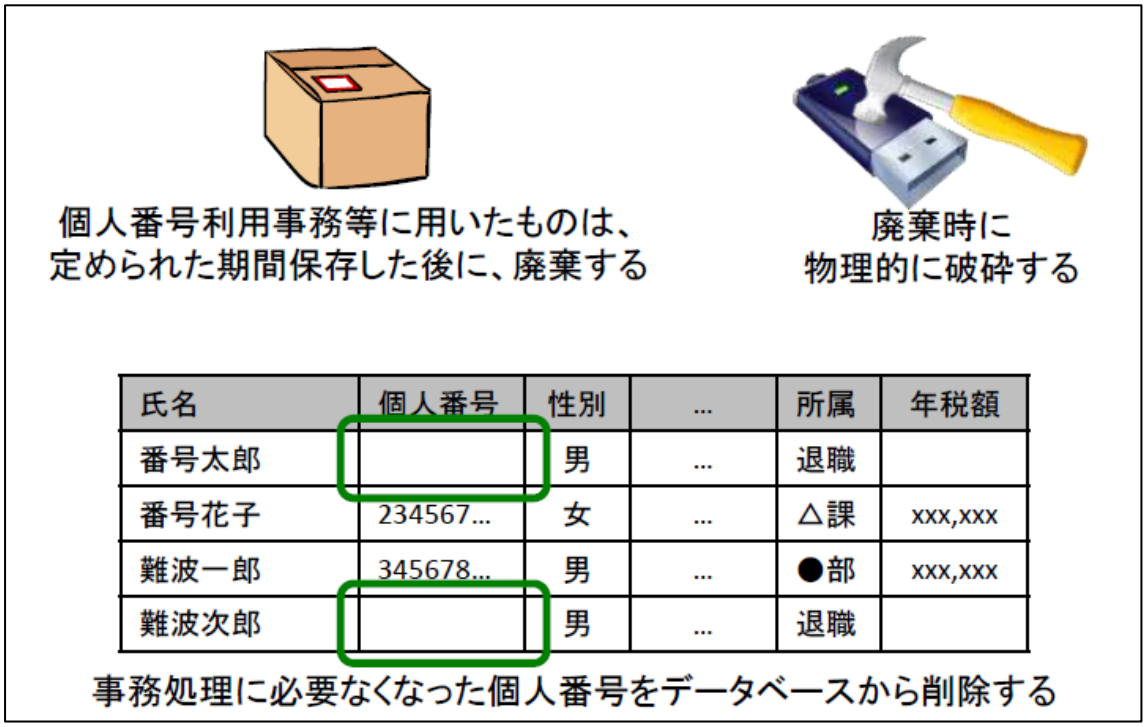
（１）　**廃棄方法等**

①　紙文書及びメモ等を廃棄する場合、マイクロカットシュレッダー（縦横２方向に裁断し、特に裁断サイズの小さいシュレッダー）を使用するか、焼却・溶解処理を行う。

②　電子媒体等を廃棄する場合、専用のデータ完全削除ソフトを利用する、専用装置（消磁装置等）でデータを消去する又は媒体を物理的に破壊するなどの措置を講ずる。

③　特定個人情報の個人番号部分を削除する場合は、個人番号を復元できないようにマスキングするなどの措置を講ずる。

④　個人番号が記載された紙文書等については、保存期間経過後における廃棄を前提とした手続をあらかじめ定める。



資料：個人情報保護委員会事務局「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・地方公共団体等編）の概要」平成 28 年１月版

６　特定個人情報等の取扱状況の記録

保護管理者は、特定個人情報ファイルの取扱状況を確認する手段を整備して、特定個人情報等の利用及び保管等の取扱状況について記録する。

具体的には、特定個人情報ファイルの利用及び保管等の取扱状況ついて、次の項目について記録し、保存する。システム上で管理でき、取扱状況を確認できる場合は、それを管理台帳とみなすことができる。

なお、取扱状況を確認するための記録には、特定個人情報等自体は記載しない。

（１）　記録項目

①　特定個人情報ファイルの名称

②　特定個人情報ファイルを利用した部署及び事務取扱担当者名

③　特定個人情報ファイルの利用目的

④　特定個人情報ファイルに記録される項目及び本人として記録される個人の範囲

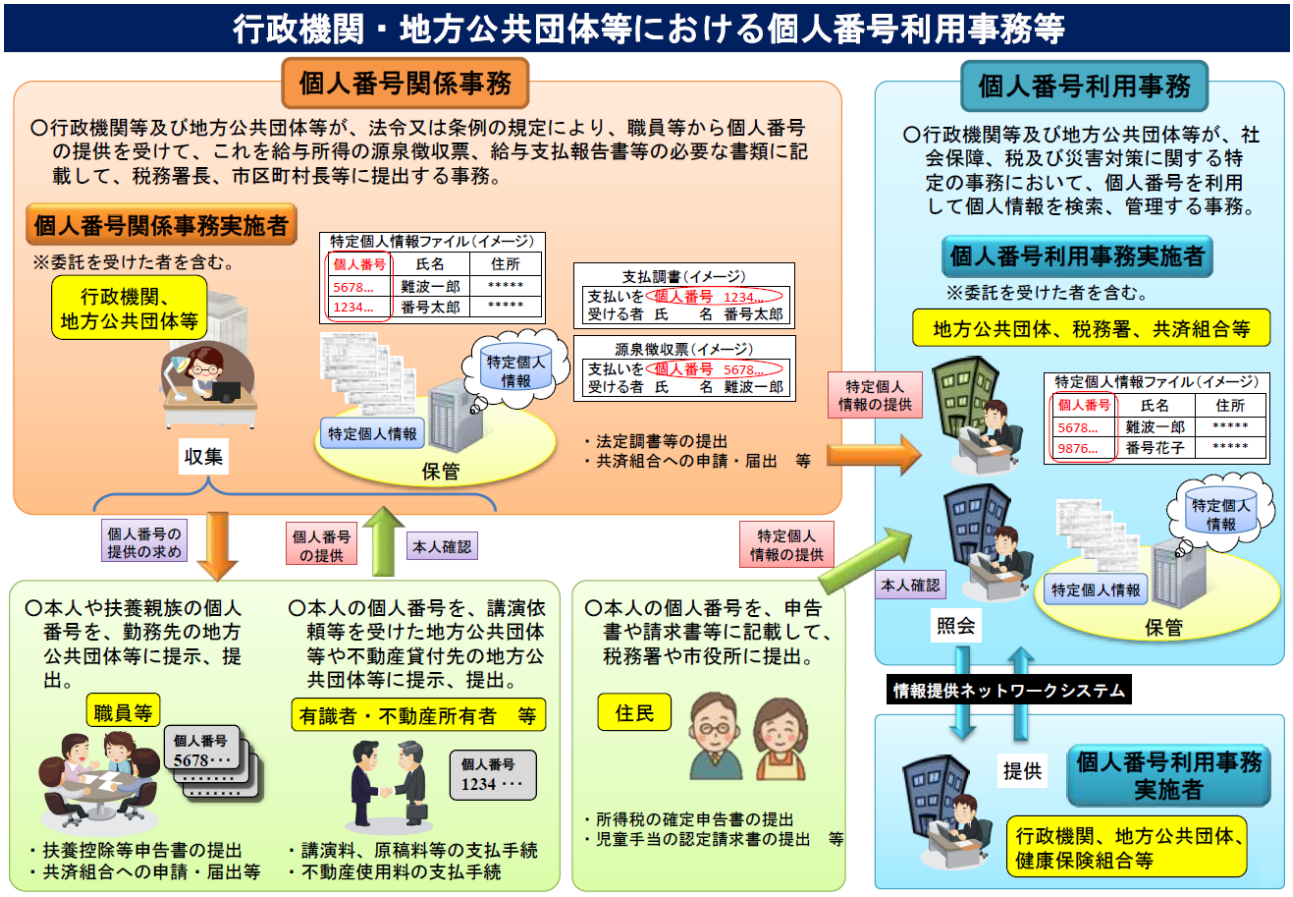
⑤　特定個人情報ファイルに記録される特定個人情報等の収集方法

⑥　その他必要な事項

７　個人番号の利用の制限

個人番号を利用することができる範囲については、番号法第９条において、社会保障、税及び災害対策に関する特定の事務（番号法に基づき、番号利用・提供条例で定めた事務を含む。）に限定されている。本来の利用目的以外の目的で例外的に特定個人情報等を利用することができる範囲についても、同様に定められている。

そのため、個人番号の利用は、基本的に個人番号利用事務等に限定し、目的外利用を行ってはならない。



資料：個人情報保護委員会事務局「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・地方公共団体等編）の概要」平成 28 年１月版

【参考：個人番号利用事務（番号法第９条第１項及び第２項等）】

・番号法別表第１に掲げられた事務（第９条第１項）と、同法第９条第２項に基づき、村が定めた番号利用・提供条例で掲げられた事務を指す（※事務件数が膨大なため、事務の掲載は省略している。）。

【参考：個人番号関係事務（番号法第９条第３項）】

・村が実施する個人番号関係事務は、大きく次の２つに分けることができる。

↓

【職員及び職員の扶養家族等の個人番号に関連する事務】

個人番号関係事務のうち、職員及び職員の扶養家族等の個人番号に関連する事務は、次のとおり（※「職員」とは、雇用関係にある職員（再任用職員、臨時職員、嘱託職員を含む。）及び特別職を含み、その他雇用関係にない者は含まない。）。

① 源泉徴収関連事務（扶養控除等申告書、配偶者特別控除申告書含む。）
② 給与支払報告書作成事務
③ 給与支払報告特別徴収に係る給与所得者異動届出書作成事務
④ 特別徴収の異動申請書作成事務
⑤ 健康保険、厚生年金、共済年金の申請・請求事務
⑥ 健康保険、厚生年金、企業年金の届出事務
⑦ 国民年金第三号届出事務
⑧ 雇用保険、労災保険証明書作成事務
⑨ 雇用保険、労災保険届出事務
⑩ 雇用保険、労災保険申請・請求事務
⑪ 上記①から⑩までの事務以外の関連事務

【職員以外の個人に係る個人番号に関連する事務】

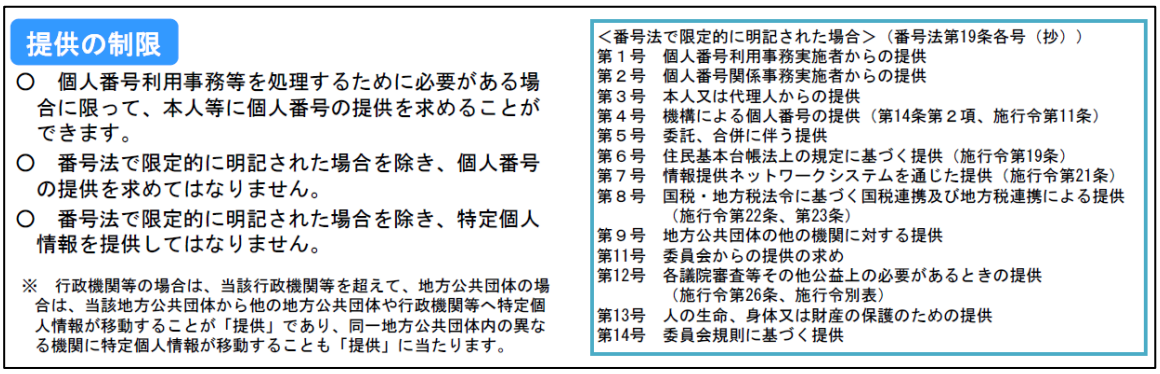
個人番号関係事務のうち、職員以外の個人に係る個人番号に関連する事務は次のとおり。

① 源泉徴収票作成事務（賃金、委員報酬、個人に支払う管理料等の委託料、選挙管理者・立会人、消防団員報酬等）
② 報酬・料金等の支払調書作成事務（講師謝金、個人事業主である弁護士・司法書士・土地家屋調査士・建築士等報酬）
③ 不動産の使用料等の支払調書作成事務（同一人に対する年間支払額が 15 万円を超えるもの）
④ 不動産等の譲受けの対価の支払調書作成事務（同一人に対する年間支払額が 100 万円を超えるもの）
⑤ 上記事務に関連する事務

８　個人番号の提供の求めの制限

個人番号の提供を求めることができる状況は、番号法第 15 条において、同法第 19 条に基づき特定個人情報の提供を受けることができる場合のみと定められている。

そのため、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限定的に明記された場合を除き、個人番号の提供を求めてはならない。



資料：個人情報保護委員会事務局「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・地方公共団体等編）の概要」平成 28 年１月版

なお、村では、番号法第 19 条第９号（及び番号法第９条第２号）に基づき番号利用・提供条例を定めているため、村長部局➡教育委員会部局への情報提供が可能となっている。

９　特定個人情報ファイルの作成の制限

特定個人情報ファイルの作成については、番号法第 19 条第 11 号から第 14 号のいずれかに該当して特定個人情報を提供する場合か、又は提供を受けることができる場合を除き、個人番号利用事務等を処理するために必要な範囲を超えて特定個人情報ファイルを作成してはならないと、番号法第 28 条に定められている。

そのため、事務取扱担当者は、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。

10　特定個人情報等の収集及び保管の制限

番号法第 19 条各号のいずれかに該当する場合を除き、特定個人情報等を収集又は保管してはならないことが、番号法第 20 条において定められている。

そのため、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等、番号法に基づく提供を受けた場合を除き、特定個人情報等を収集又は保管してはならない。

（１）　収集の制限について

「収集」とは、「集める意思を持って自己の占有に置くこと」であり、例えば、人から個人番号を記載したメモを受け取ることや人から聞き取った個人番号をメモすることなど、直接取得する場合のほか、端末の画面上に表示させた個人番号を書き取ることやプリントアウトすることなどを含む。ただし、特定個人情報等の提示を受け、単に個人番号を見ただけの場合は、「収集」に当たらない。

個人番号利用事務等以外の事務においては、個人番号カードを本人確認書類として利用することはできるが、カードの個人番号が記載された部分をコピーするなどの行為は「収集」に該当するため、行ってはならない。

（２）　保管の制限について

特定個人情報等は、番号法で限定的に明記された事務を処理するために収集又は保管されるものであるため、該当する事務を行ううえで必要がある場合に限り、特定個人情報等を保管し続けることができる。文書取扱規程に定めのある文書等については、定められた期間保管することとなる。

一方、それらの事務を処理する必要がなくなった場合で、文書取扱規程により定められている保存期間を経過した場合は、特定個人情報等を速やかに廃棄又は削除しなければならない。例えば、人から聞き取った個人番号のメモ等は、特定個人情報ファイルへの記載等の必要な処理が終了した時点で、速やかに復元又は判読が不可能な方法により、廃棄しなければならない。

11　取扱区域

特定個人情報等の情報漏えい等を防止するため、特定個人情報等を取り扱う事務を実施する区域を「取扱区域」として、特定個人情報ファイルを取り扱う情報システムを管理する区域を「管理区域」として、それぞれ明確にし、物理的な安全管理措置を講ずる。

（１）　取扱区域

取扱区域は、事務取扱担当者以外の往来が少ない場所に配置し、事務取扱担当者の座席は、背後に壁がある位置など、背後からのぞき見される可能性が少ない場所に配置するとともに、必要に応じてパーティション等を設置する。取扱区域において、事務取扱担当者は、クリアデスク・クリアスクリーン（離席時に、紙

文書やUSBメモリ等を机の上に放置しない、PCのログオフを行うなど。）を徹底するとともに、特定個人情報等が記録された媒体を施錠できる書棚等で保管する。

また、受付窓口等においても、隣席の紙文書等が見えないように工夫するとともに、特定個人情報等が表示される端末の画面がのぞける配置にならないように注意する。

（２） 管理区域

管理区域においては、入退管理や持ち込む機器等の制限等の措置を講ずるなど、情報セキュリティポリシーに従い、必要な物理的安全管理措置を講ずる。

Ⅴ　情報システムにおける安全の確保等【管理規程第６章関連】

１　アクセス制御

特定個人情報等にアクセスする権限を有する職員及びその権限の内容の範囲は、保護管理者によって限定される。そのため、保護管理者は、パスワードやICカード等によって職員の権限を識別する機能を設定するなど、アクセス制御のために必要な措置を講ずる。

（１）　アクセス制御の方法

保護管理者は、アクセス制御のために、次の措置を講ずる。

① 個人番号と紐付けてアクセスできる情報の範囲を、アクセス制御により限定する。

② 特定個人情報ファイルを取り扱う情報システム等を、アクセス制御により限定する。

③ 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利用できる者を事務取扱担当者に限定する。

④ 特定個人情報ファイルへのアクセス権を付与すべき者を最少化する。

⑤ アクセス権を有する者に付与する権限を最小化する。

⑥ 情報システムの管理者権限を有するユーザーであっても、情報システムの管理上、特定個人情報ファイルの内容を知らなくてもよい場合は、特定個人情報ファイルへ直接アクセスできないようにアクセス制御をする。

⑦ 特定個人情報ファイルを取り扱う情報システムに導入したアクセス制御機能の脆弱性等を定期的に検証する。

（２）　アクセス権の設定

① アクセス管理できるシステムで特定個人情報等を管理している場合

事務ごと、職員ごとにアクセス権を設定して管理し、アクセス権は保護管理者が決定する。異動、退職等のために職員のステータスが変更になる場合、保護管理者は、職員のステータス変更後、直ちにアクセス権を変更する。

② ファイルサーバ内で特定個人情報等を管理している場合

保護管理者は、事務ごとに許可された職員のみがアクセスできるように、ファイルサーバ内のフォルダを設定する。フォルダ構成についても、特定個人情報等へのアクセス管理が可能となるように設定する。

新規フォルダを作成する場合は、保護管理者の指示のもと、行わなければならない。

③ スタンドアロンシステムで特定個人情報等を管理している場合

保護管理者は、スタンドアロンシステムにアクセスできるユーザーID 及びパ

スワードを設定する。

（３） ICカード等の取扱い

職員は、自己の管理するICカード等に関し、次の事項を遵守しなければならない。

① 業務上必要がない場合、ICカード等をカードリーダー等から抜いておく。

② ICカード等を紛失した場合、速やかに保護管理者に報告する。

保護管理者は、報告を受け次第、直ちに当該ICカード等を使用したアクセス権限を停止するなどの措置を講ずる。

③ 保護管理者は、ICカード等の切替えを行う場合は、現行のICカード等を確実に回収し、物理的に破壊するなど、復元が不可能な方法により、廃棄しなければならない。

（４） ユーザーIDの取扱い

職員は、自己の管理するユーザーID に関し、次の事項を遵守しなければならない。

① 自己の管理するユーザーIDは、他人に利用させてはならない。

② 共用IDを利用する場合は、共用IDの利用者以外に利用させてはならない。

（５） パスワードの取扱い

職員は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

① パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

② パスワードは十分な長さとし、文字列は、他人が想像しにくいものとする。

③ パスワードが流出したおそれがある場合は、保護管理者に直ちに報告するとともに、速やかに当該パスワードを変更する。

④ パスワードは、定期に又は随時に変更する。ただし、それ以前に使用したことのあるパスワードは使用してはならない。

⑤ 複数の情報システムを利用する職員は、複数のシステム間で同一のパスワードを使用してはならない。

⑥ 初期設定のパスワードは、最初のログイン後に必ず変更する。

⑦ 端末のパスワードの記憶機能を利用してはならない。また、パスワードを付箋に記して机に貼っておくなど、第三者が容易に閲覧できる場所にパスワードを残してはならない。

⑧ 職員同士でパスワードを共有してはならない。

２　アクセス記録

保護管理者は、特定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。）を一定期間保存するとともに、アクセス記録を定期的に分析し、特定個人情報等への不適切なアクセスがないかを確認する。

また、アクセス記録の改ざん、窃取又は不正な削除の防止のために必要な措置を講ずる。

（１）　特定個人情報等へのアクセスが記録できるシステムでアクセスログを記録する場合

①　情報システムのアクセスログは、データの修正ができない媒体に保存し、管理する。

②　アクセスログを保存した媒体は、施錠可能な書棚等で保管し、管理する。

（２）　特定個人情報等へのアクセスが記録できないシステムでアクセスログを記録する場合

①　特定個人情報等へのアクセス状況を記録する管理簿を作成し、事務取扱担当者は、特定個人情報等へアクセスした場合、アクセス記録を管理簿に記録する。

②　管理簿には、“いつ”、“だれ”が、“何の情報”にアクセスし、どのような処理を行ったのかを記録する。

（３）　簿冊（紙ファイル等）で特定個人情報等を管理している場合

①　管理簿を作成し、簿冊の利用等の状況を記録する。

②　管理簿には、“いつ”、“だれ”が、“何の情報”にアクセスし、どのような処理を行ったのかを記録する。

３　アクセス状況の監視

保護管理者は、特定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を設定するとともに、当該設定の定期的確認等の対策を講じ、特定個人情報等への不適切なアクセスを随時監視する。

４　管理者権限の設定

特定個人情報等を取り扱う情報システムの管理者権限の特権は、事務取扱担当者の権限に比べて、不正に窃取された場合の被害が大きくなる。

そのため、保護管理者は、特定個人情報等を取り扱う情報システムの管理者権限の特権を付与されたユーザーID を利用する者を必要最小限にするとともに、当該ユーザーID

のパスワードの漏えい等が発生しないよう、ユーザーID 及びパスワードを厳重に管理する。

また、保護管理者は、特権を付与されたユーザーID 及びパスワードの管理をより強化するため、職員の端末等のパスワードよりも短期的にパスワード変更を行うなどの措置を講ずる。

５　外部からの不正アクセスの防止

保護管理者は、特定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、次の措置を講ずる。

① 特定個人情報等を取り扱う情報システムと外部ネットワーク（又はその他の情報システム）との接続を必要最低限に限定し、可能な限り接続ポイントを減らす。

② 特定個人情報等を取り扱う情報システムと外部ネットワーク（又はその他の情報システム）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。

③ 定期に又は随時にログ等の分析を行い、不正アクセス等を検知する。

④ 不正アクセス等の被害にあった場合であっても、被害を最小化する仕組み（ネットワークの遮断やシステムの停止等）を導入し、適切に運用する。

⑤ 必要に応じて、インターネットから独立するなどのセキュリティ対策を踏まえたシステム構築や運用体制の整備を行う。

６　不正プログラムによる情報漏えい等の防止

保護管理者は、不正プログラムによる特定個人情報等の情報漏えい等の防止のため、次の措置を講ずる。

① 特定個人情報等を取り扱う情報システム及び端末等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）を導入する。

② 導入したセキュリティ対策ソフトウェア等を利用し、入出力データにおける不正プログラムの有無を確認する。

③ 端末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を活用し、ソフトウェア等を常に最新の状態に保つ。

④ 情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等やソフトウェアのインストール等）を防止するために必要な措置を講ずる。

７　情報システムにおける特定個人情報等の処理

情報システムにおける特定個人情報等を取り扱ううえで、一時的に加工等の処理を行うために複製等を行う場合、事務取扱担当者は、その対象を必要最小限に限定し、処理

終了後は、不要となった特定個人情報等を速やかに消去する。

また、一時的な加工等の処理のために複製等を行った特定個人情報等が消去されずに残っていた場合、定められた管理方法によって管理される可能性が低いため、保護管理者は、事務取扱担当者の使用した特定個人情報等の内容に応じて、随時、消去等の実施状況を重点的に確認する。

８　暗号化

特定個人情報等をインターネット等により外部と送受信する場合、通信経路における情報漏えい等を防止するため、通信経路の暗号化等の措置を講ずる。

また、特定個人情報等が記録された媒体を持ち出す場合や外部へ送付する場合は、必要に応じて、暗号化又はパスワードの設定等を行うとともに、暗号鍵及びパスワードの運用管理、パスワードに用いる文字の種類や桁数等の要素を考慮して、不正に入手した者が容易に復元できないようにする。

９　記録機能を有する機器及び媒体の接続制限

特定個人情報等の情報漏えい等の防止のため、スマートフォンや USB メモリ等の記録機能を有する機器及び媒体を情報システム端末等へ接続する場合は、あらかじめ保護管理者の許可を得る。

基本的には、あらかじめ接続を許可された記録媒体等のみを使用することとし、個人所有のスマートフォンや USB メモリ等は、特定個人情報等を取り扱う情報システム端末には、決して接続してはならない。

10　端末の限定

保護管理者は、特定個人情報等の処理を行う端末を限定するとともに、当該端末を使用する者を事務取扱担当者に限定する。端末を限定することで、情報セキュリティ対策の範囲を限定できるとともに、集中的に対策を講ずることが可能となる。

11　端末の盗難防止等

特定個人情報等の処理を行う端末については、施錠可能な書棚等での保管やセキュリティワイヤー等による固定等、盗難又は紛失防止のための措置を講ずる。

また、特定個人情報等の処理を行う端末を有する執務室については、施錠管理等の対策を講ずる。

12　端末の外部持出し等

特定個人情報等の処理を行う端末については、保護管理者の許可がない限り、外部へ持ち出し、又は外部から持ち込んではならない。

なお、スマートフォンや USB メモリ等の記録機能を有する機器及び媒体についても、同様とする。

13　第三者の閲覧防止

特定個人情報等の処理を行う端末を使用する場合は、特定個人情報等が第三者に閲覧されることがないようにする。

また、特定個人情報等が記録された媒体を使用する場合も、同様とする。

（１）　クリアスクリーン

① 長時間の離席時は、PC の電源をオフにし、短時間の離席時は、PC をロックする。

② 一定時間以上情報システムを利用しない場合は、情報システムからログオフする。

③ PC 起動時にはパスワードの設定を行い、定期的にパスワードを変更する。

④ パスワード等を記録し、PC 周辺に貼っておくなどの行為はしてはならない。

（２）　クリアデスク

① 離席時は、個人番号が記載された紙文書をキャビネット等に収納するとともに、特定個人情報等が記録された媒体を PC 等から取り外し、同様にキャビネット等に収納する。

② 事務取扱担当者の離席時は、個人番号が記載されたメモ等を事務取扱担当者の机の上に放置せず、事務取扱担当者の在席時に直接手渡す。

③ 帰宅時は、使用した PC の電源をオフにし、紙文書及び媒体等は、施錠可能な書棚等に収納する。

（３）　その他

① コピー機、FAX、プリンタ等に特定個人情報等を出力した紙文書を放置してはならない。

② 特定個人情報等が記録された媒体の郵送等による送付時及び FAX・電子メール等による送信時には、誤送信防止のため、必ず宛先を確認する。

③ 業務目的以外で、庁内のあらゆる場所を撮影してはならない。

④ 電話等による、なりすましに注意する。

14　入力情報の照合等

事務取扱担当者は、情報システムに特定個人情報等を入力した場合、誤入力防止のため、入力原票と入力内容との照合を必ず行う。

また、情報システムで特定個人情報等を取り扱う場合、処理前後の当該特定個人情報等の内容を確認するとともに、必要に応じて、既存の特定個人情報等との照合等を行い、誤入力されたものでないかを確認する。

15　バックアップ

保護管理者は、特定個人情報等の重要度に応じて、バックアップを作成し、分散管理をするために、次の措置を講ずる。

① スタンドアロンシステムに記録されている情報については、定期的にバックアップを実施する。

② 大容量の保存媒体にバックアップする場合は、年度ごとに保存媒体を区分してデータを保存する。

③ データの修正ができない媒体に、バックアップデータを保存する。

④ 各保存媒体には、媒体の識別番号等を付番するとともに、管理簿を作成し、管理状況が分かるようにする。

⑤ バックアップのタイミングは、事務ごとに事務取扱担当者が決め、保護管理者の承認を得て、文書化しておく。

⑥ バックアップは２セット作成し、別の場所で保管する。

16　情報システム設計書等の管理

特定個人情報等の情報漏えい等の防止のため、保護管理者は、特定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、適切に保管し、複製を制限するとともに、文書取扱規程に定める保存期間が経過するなど、不要になった場合には、復元又は判読が不可能な方法により廃棄する。

Ⅵ　電算室等の安全管理【管理規程第７章関連】

１　入退管理

（１）　入退記録等

保護管理者は、特定個人情報等を取り扱う基幹的なサーバ等の機器を設置する室その他の区域（以下「電算室等」という。）に立ち入る権限を有する者を限定する。

電算室等に立ち入る際には、保護管理者に用件を報告して許可を得るものとし、保護管理者は、電算室等への入退状況を管理簿に記録する。

職員及び外部委託事業者は、電算室等に立ち入る場合、身分証明書等を携行し、保護管理者の求めに応じ、これを提示しなければならない。

電算室等に立ち入る権限を有する者以外の部外者が、保護管理者の許可を得て電算室等に立ち入る場合は、立入権限を有する職員が立ち会うものとし、職員と外見上区別できる措置を講じなければならない。

電算室等への持込み、利用及び持出しが可能な媒体等は、保護管理者の許可を得たもののみとし、持込み、利用及び持出しの状況について管理簿に記録したうえで、必要に応じて、媒体等の検査を実施する。

特定個人情報等が記録された媒体を保管するための施設についても、同様の措置を講ずる。

（２）　出入口の特定化等

保護管理者は、必要に応じて、電算室等の出入口を限定することによる入退管理の容易化、所在表示の制限等の措置を講じ、電算室等に立ち入る権限を有する者以外の部外者が、電算室等に近づくリスクの軽減を図る。

（３）　認証機能等の設定等

保護管理者は、必要に応じて、電算室等や特定個人情報等が記録された媒体を保管するための施設の出入口にパスワードやICカード等による認証機能を設定するとともに、パスワード等の管理に関する定めを整備し、セキュリティ対策を実施する。

２　電算室等の管理

（１）　不正な侵入への備え

保護管理者は、電算室等に施錠装置、警報装置、監視設備を設置するなどの措置を講じ、外部からの不正な侵入を防止する。

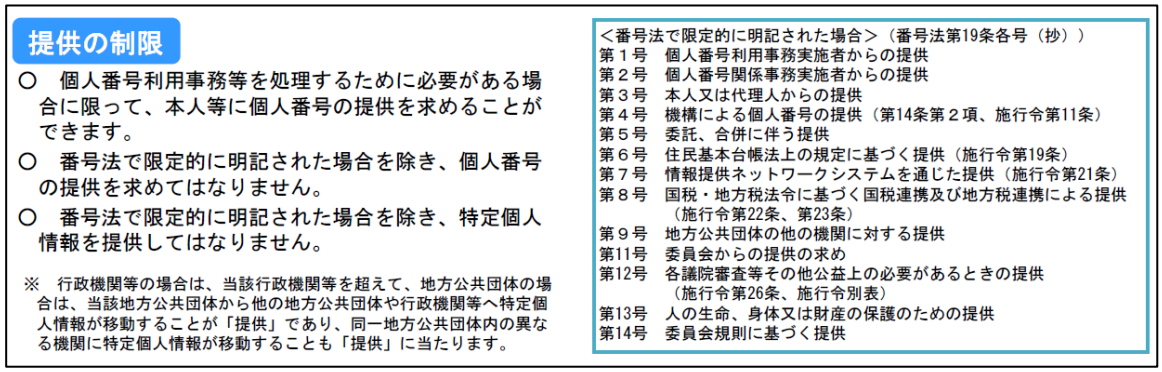
（２）　災害等への備え

保護管理者は、電算室等に、転倒及び落下防止等の耐震対策、防火対策、防煙対策、防水対策等を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講じ、災害等に備える。

Ⅶ　特定個人情報等の提供及び業務の委託等【管理規程第８章関連】

１　特定個人情報等の提供

特定個人情報等を提供することができるのは、番号法第 19 条各号に定められている場合に限り、それ以外の場合、特定個人情報等を提供することはできない。



資料：個人情報保護委員会事務局「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・地方公共団体等編）の概要」平成 28 年１月版

（１）　「提供」の意義

地方公共団体から他の地方公共団体や行政機関等へ特定個人情報等が移動することが「提供」であり、同一地方公共団体内の異なる機関に特定個人情報等が移動することも「提供」に当たる。一方、同一地方公共団体内の同一機関間で特定個人情報等が移動することは「利用」に当たる。

（２）　「提供」に当たらない場合

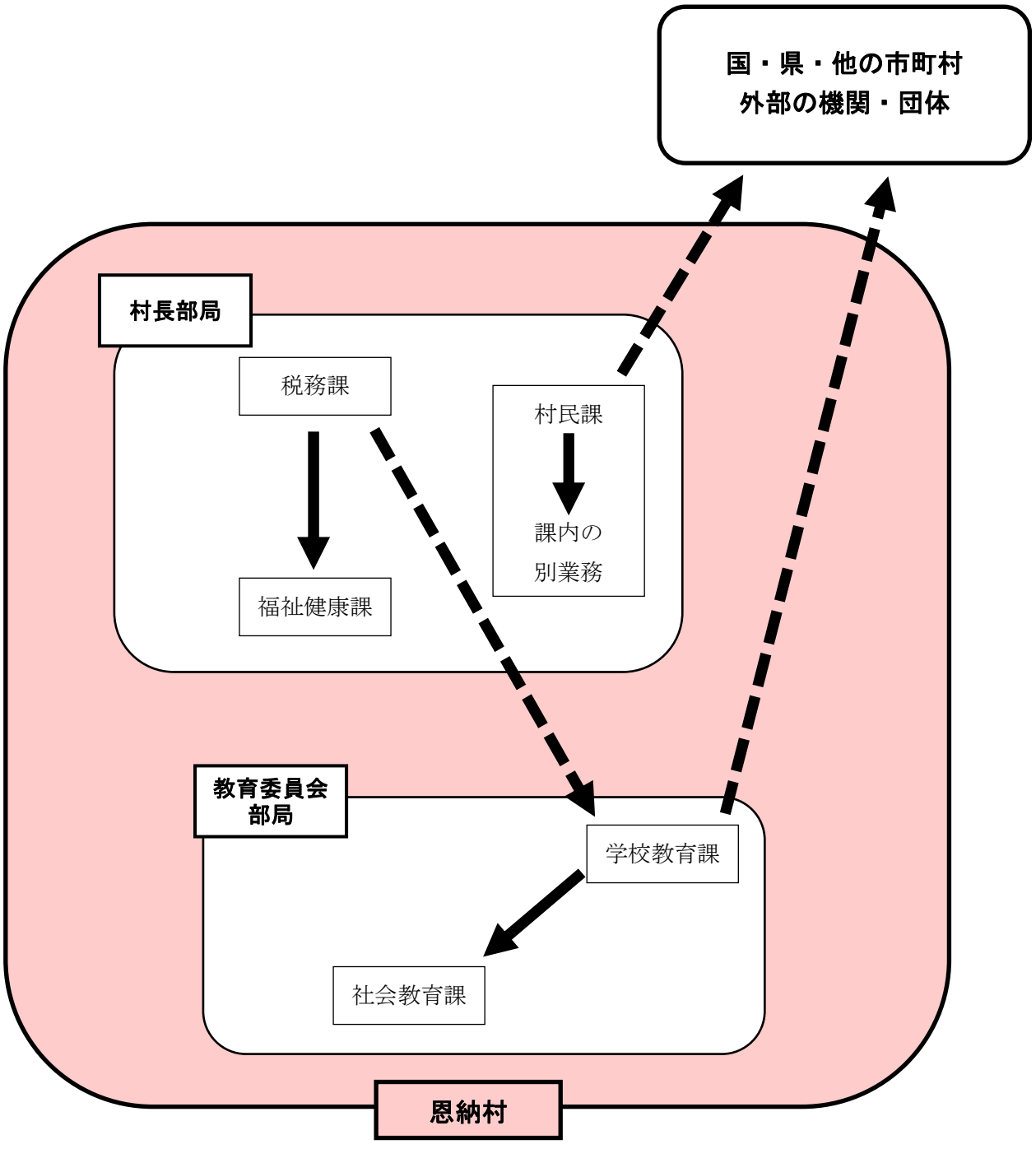
村長部局の税務課から、同じ村長部局の福祉健康課に特定個人情報等が移動する場合は、同じ村長部局内での移動であるため、「提供」には当たらず、「利用」となる。

（３）　「提供」に当たる場合

村長部局の税務課から、教育委員会部局に特定個人情報等が移動する場合は、同一地方公共団体内の異なる機関に特定個人情報等が移動することから、「提供」に当たる。

なお、この場合、番号法第 19 条第７号に基づく情報連携によらず、教育委員会部局が特定個人情報等の提供を受けるためには、同条第９号に基づき、村長部局から教育委員会部局に対し、特定個人情報等を提供する旨の条例を定める必要がある。

【参考：利用と提供のイメージ図】



※特定個人情報等の流れ

利用

提供

２　業務の委託等

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、番号法に基づき村が果たすべき安全管理措置と同等の措置が講じられなければならない。

保護管理者は、そのために必要かつ適切な監督を行わなければならない。

（１）　委託先の適切な選定

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、番号法に基づき村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、保護管理者は、あらかじめ、次の事項を確認する。

①　委託先の設備
②　技術水準
③　従業者（従業員のほか、取締役、監査役、理事、監事、派遣社員等を含む。）に対する監督・教育の状況
④　その他委託先の経営環境等

（２）　委託先に安全管理措置を遵守させるために必要な契約の締結

委託先と交わす契約書には、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、業務従事者の管理及び実施体制、特定個人情報等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する。

①　秘密保持義務
②　事業所内からの特定個人情報等の持出しの禁止
③　特定個人情報等の利用範囲の限定と目的外利用の禁止
④　再委託における条件
⑤　漏えい事案等が発生した場合の委託先の責任
⑥　委託契約終了後の特定個人情報等の返却又は廃棄
⑦　特定個人情報等を取り扱う従業者の明確化
⑧　従業者に対する監督・教育
⑨　契約内容の遵守状況について報告を求める規定
⑩　村が必要と認めるとき、委託先に対して実地の調査を行うことができる規定等

（３）　委託先における特定個人情報等の取扱状況の把握

委託先において、適切に特定個人情報等が取り扱われているか、また、番号法に基づき村が果たすべき安全管理措置と同等の措置が講じられているか、定期的に確認する必要がある。

委託先から、定期的に契約内容の遵守状況について報告を受けるとともに、年１回以上の定期的検査や必要に応じて実地調査を実施し、委託先における特定個人情報等の管理状況を確認する。

なお、委託先からの報告や委託先に対する検査、調査の結果に応じて、改善要求等の措置を講ずる。

（４） 再委託の取扱いと管理

① 再委託及び再々委託について

個人番号利用事務等の全部又は一部の委託を受けた者は、委託元である村の許諾を得た場合に限り、当該事務の再委託を行うことができる。

再委託先が、再々委託を行うことも可能だが、その場合にも、同様に、委託元である村の許諾が必要となる。

② 再委託の許諾

委託先が再委託を行う場合には、再委託先において、番号法に基づき村が果たすべき安全管理措置と同等の措置が講じられることを確認したうえで、再委託の諾否を判断する。

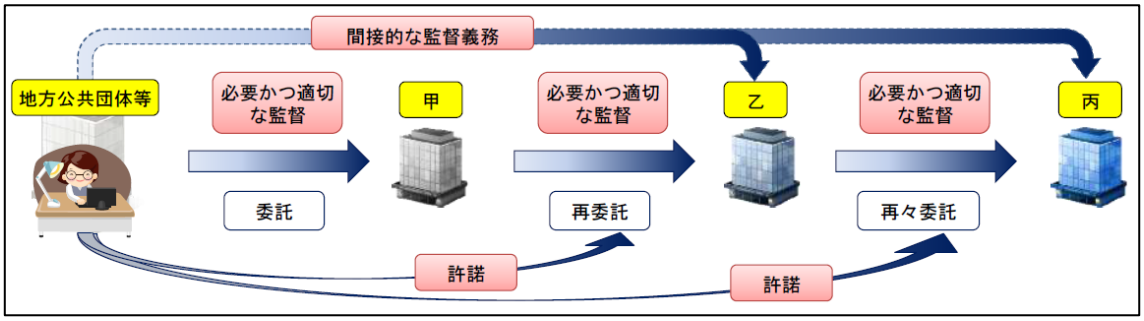
委託先は、村が委託先に対して講ずるのと同様の措置を、再委託先に対して講ずる。

③ 再委託先の監督

村が、委託先に対して、村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うのと同様に、委託先は再委託先に対して、再委託先は再々委託先に対して、それぞれ直前の委託元が必要かつ適切な監督を行う義務を負う。

ただし、村は、再委託、再々委託の諾否を判断するだけでなく、委託先が再委託先に対して、再委託先が再々委託先に対して、それぞれ必要かつ適切な監督を行っているかどうかを監督する義務を負う。

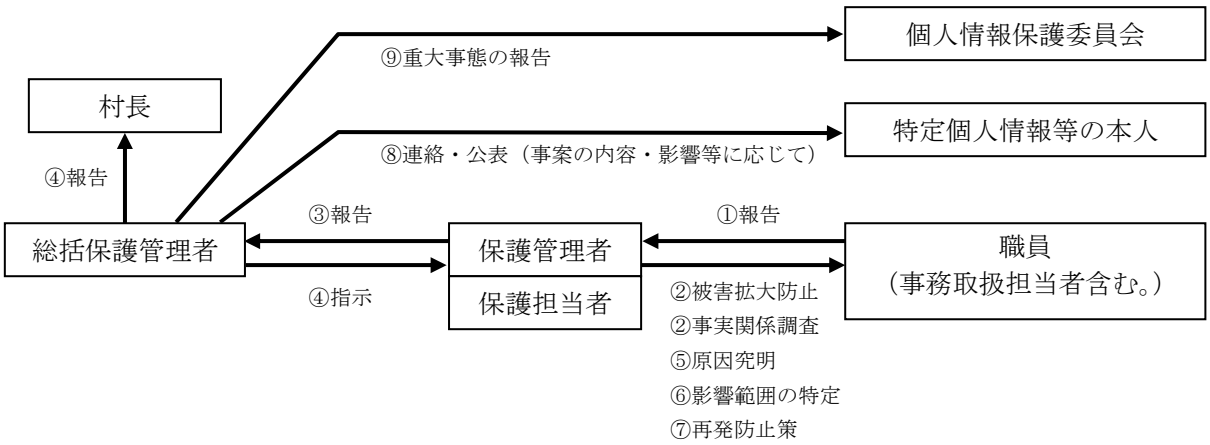
そのため、村は、再委託先、再々委託先に対しても、間接的に監督する義務を負うこととなる。



資料：個人情報保護委員会事務局「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・地方公共団体等編）の概要」平成 28 年１月版

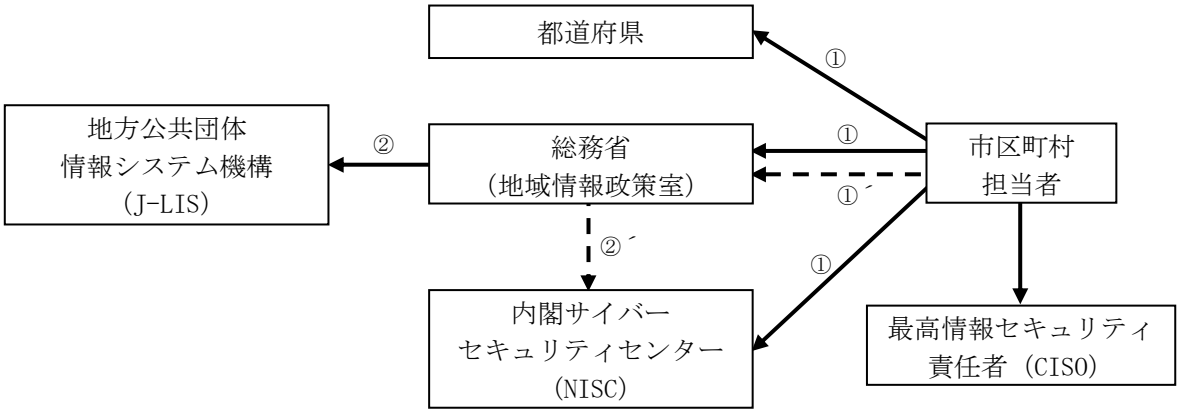
Ⅷ　安全確保上の問題への対応【管理規程第９章関連】

１　特定個人情報等の情報漏えい等事案の連絡体制



※　特に重大な事案の場合は、個人情報保護委員会、総務省の規則又は告示、情報セキュリティポリシーの規定に従い、判断する。

【参考：地方公共団体が検知した情報セキュリティインシデント連絡ルート（H29.7.1 改定予定）】



①　情報セキュリティインシデントが発生した市区町村（指定都市を含む。）は、対応状況について都道府県、総務省、内閣サイバーセキュリティセンター（NISC）及び市区町村最高情報セキュリティ責任者（CISO）に報告する。

②　総務省は、必要に応じて、地方公共団体情報システム機構（J-LIS）に情報提供する（サイバー攻撃（と考えられる事案を含む。）に係るものについては、すべて情報提供する。）。

【留意事項】
- LGWAN（～lg.jp）を利用して報告する場合は、パスワード不要。
- LGWAN を利用しない場合（地域ドメインで報告）は、内閣サイバーセキュリティセンター（NISC）への同報は不可（総務省経由）。
- 都道府県から市区町村の情報セキュリティインシデント報告の転送は不要。
- 報告のあった情報セキュリティインシデントに対する内閣サイバーセキュリティセンター（NISC）からの内容確認は、総務省が窓口となる。

２　事案の報告及び再発防止措置、公表等

特定個人情報等の情報漏えい等の事案の発生又は兆候を把握した場合及び事務取扱担当者が管理規程等に違反している事実又は兆候を把握した場合、次の手順により必要な措置を講ずる。

（１）　組織内における報告、被害の拡大防止

特定個人情報等の情報漏えい等の事案の発生又は兆候を把握した場合及び事務取扱担当者が管理規程等に違反している事実又は兆候を把握した場合、職員は、当該特定個人情報等を管理する保護管理者に直ちに報告する。

報告を受けた保護管理者は、被害の拡大防止のために必要な措置を速やかに講ずる。特に、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端末等からLANケーブルを抜くなどの措置は、直ちに行う（職員に行わせることを含む。）ものとする。

（２）　事実関係の調査、原因の究明

保護管理者は、事実関係（事案の発生した経緯、被害状況等）を調査し、総括保護管理者に報告する。ただし、特に重大と認める事案が発生した場合には、直ちに総括保護管理者に事案の内容等について報告する。

総括保護管理者は、事実関係の報告を受けた場合、事案の内容等に応じて、その内容、経緯、被害状況等を、速やかに村長に報告する。

保護管理者は、事実関係を調査し、番号法違反又は番号法違反のおそれが把握できた場合には、原因の究明を行う。

（３）　影響範囲の特定

保護管理者は、原因究明によって明らかになった事実関係による問題の影響範囲を特定する。

（４）　再発防止策の検討・実施

保護管理者は、事案の発生原因を踏まえ、再発防止策を検討し、速やかに実施する。

（５）　影響を与える可能性のある本人への連絡等

総括保護管理者は、事案の内容等に応じて、二次被害の防止、類似事案の発生回避等の観点から、事実関係等について、速やかに、影響を与える可能性のある本人に電話又は郵便等で連絡し、又は村ホームページに特定個人情報等の情報漏えい等の事案の発生と対応状況等を掲載するなど、本人が容易に知り得る状態に置く。

（６）　事実関係、再発防止策等の公表

総括保護管理者は、事案の内容等に応じて、二次被害の防止、類似事案の発生回避等の観点から、事実関係及び再発防止策等について、速やかに公表する。

（７）　個人情報保護委員会への報告

特定個人情報等の情報漏えい等、その他番号法違反の事案又は番号法違反のおそれのある事案を把握した場合、総括保護管理者は、事実関係及び再発防止策等について、速やかに、個人情報保護委員会に報告する。

また、番号法第 28 条の４の規定に基づき、「特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則」（平成 27 年特定個人情報保護委員会規則第５号）第２条に規定する特定個人情報ファイルに記録された特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態（以下「重大事態」という。）に該当する事案については、重大事態に該当する事案又はそのおそれのある事案が発覚した時点で、直ちにその旨を、個人情報保護委員会に報告する。

なお、個人情報保護委員会への報告は、「特定個人情報の漏えい等報告について（行政機関、独立行政法人等、地方公共団体等用様式）」により行うものとする。

【参考：重大事態に該当する事案】

（特定個人情報の安全の確保に係る重大な事態）

第２条　番号法第 28 条の４に規定する特定個人情報ファイルに記録された特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態は、次に掲げる事態とする。

（１）　次に掲げる特定個人情報が漏えい（不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）第２条第４項に規定する不正アクセス行為をいう。）による漏えいその他番号法第 19 条各号に該当しない特定個人情報の提供を含む。）し、滅失し、又は毀損した事態

イ　情報提供ネットワークシステム及びこれに接続された電子計算機に記録された特定個人情報

ロ　個人番号利用事務実施者が個人番号利用事務を処理するために使用する情報システムにおいて管理される特定個人情報

ハ　行政機関、地方公共団体、独立行政法人等及び地方独立行政法人が個人番号関係事務を処理するために使用する情報システム並びに行政機関、地方公共団体、独立行政法人等及び地方独立行政法人から個人番号関係事務の全部又は一部の委託を受けた者が当該個人番号関係事務を処理するために使用する情報システムにおいて管理される特定個人情報

（２）　次に掲げる特定個人情報に係る本人の数が 100 人を超える事態

イ　漏えいし、滅失し、又は毀損した特定個人情報

ロ　番号法第９条の規定に反して利用された個人番号を含む特定個人情報

ハ　番号法第 19 条の規定に反して提供された特定個人情報

（３）　個人番号利用事務実施者又は個人番号関係事務実施者の保有する特定個人情報ファイルに記録された特定個人情報を電磁的方法により不特定多数の者が閲覧することができる状態となり、かつ、その特定個人情報が閲覧された事態

（４）　不正の目的をもって、個人番号利用事務実施者又は個人番号関係事務実施者の保有する特定個人情報ファイルに記録された特定個人情報を利用し、又は提供した者がいる事態

資料：「特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則」より抜粋・編集

【重大事態が発生した場合の個人情報保護委員会への報告のフロー】

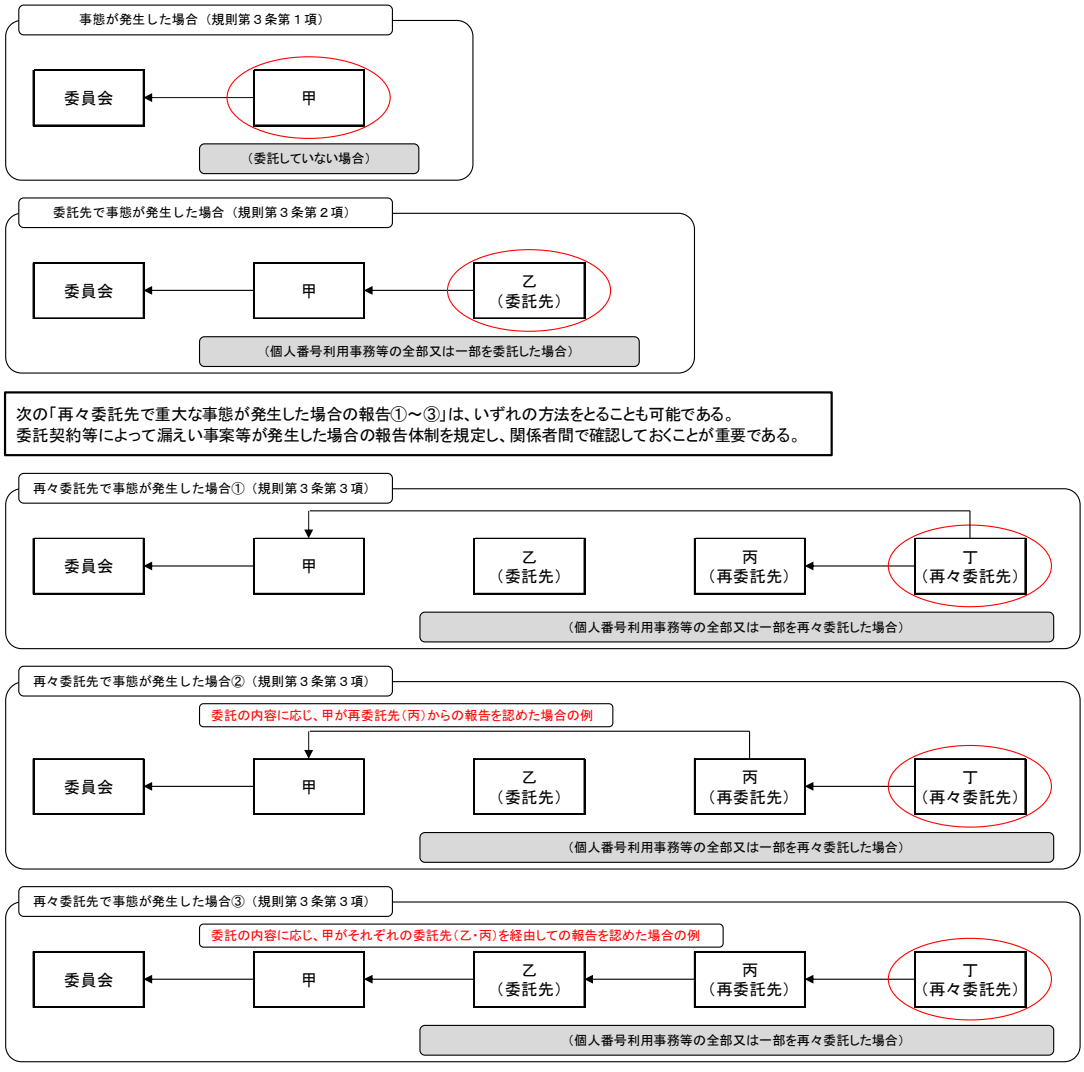
重大事態が発生した場合、個人情報保護委員会への報告は、村（甲）が行う。

個人番号利用事務等の全部又は一部を委託していて、委託先で重大事態が発生した場合、委託先（乙）は、委託元である村（甲）へ報告し、村（甲）は、個人情報保護委員会へ報告することになる。

委託先（乙）が再委託をして、再委託先（丙）で重大事態が発生した場合、再委託先（丙）は、自らの委託元である委託先（乙）及び村（甲）への報告義務を有するが、再委託先（丙）から村（甲）への報告は、委託の内容に応じ、委託先（乙）を経由して行うことが可能である。

そのため、再委託先（丙）で重大事態が発生した場合の個人情報保護委員会への報告体制は、「再委託先（丙）→委託先（乙）、再委託先（丙）→村（甲）→個人情報保護委員会」と「再委託先（丙）→委託先（乙）→村（甲）→個人情報保護委員会」の２パターンが想定される。

再委託先（丙）以降で重大事態が発生した場合の報告体制については、事前に関係者間で報告体制を確認しておく必要がある。



【様式：特定個人情報の漏えい等報告について】

（表面）

行政機関、独立行政法人等、地方公共団体等用様式

平成　　年　　月　　日

個人情報保護委員会　御中

組織名
担当部署
担当者
所在地
連絡先（TEL：　　）

特定個人情報の漏えい等報告について

（特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態等）

番号法違反の事案又は番号法違反のおそれのある事案について報告します。

（第一報の際に①～⑥は記載必須事項です。）

①事態の類型 ※重大事態に該当する事案又はそのおそれのある事案の該当する項目を選択してください。（複数選択可）	【重大事態（そのおそれのある事案を含む）の該当の有無】 □　該当する　　□　該当しない 【※「該当する」を選択した場合のみ記載】 □　第一報（告示に基づく報告）　□　確報（規則第３条に基づく報告） 【重大事態（そのおそれのある事案を含む）の類型】 □　情報提供ネットワークシステム又は個人番号利用事務を処理する情報システムで管理される特定個人情報の漏えい等が起こった。 □　個人番号関係事務を処理するために使用する情報システムで管理される特定個人情報の漏えい等が起こった。 □　漏えい等した特定個人情報の本人の数が 101 人以上である。 □　電磁的方法により、不特定多数の人が閲覧できる状態となった。 □　職員等（従業員等）が不正の目的で利用し、又は提供した。
②事態の概要 ※発覚日、判明している発生原因も含む	
③漏えい等した情報の内容	
④漏えい等した特定個人情報の本人の数	（　　）人 ※ 発覚した時点で把握した概数を記載
⑤漏えい等が発生した事務の名称	【個人番号利用事務・個人番号関係事務の該当】 □　個人番号利用事務 □　個人番号関係事務 【特定個人情報保護評価の実施の有無】 □　実施　（義務付けられる評価の種類：　　） □　義務付けられない 【事務名　※　特定個人情報保護評価計画管理書の「事務の名称」を記載】 （　　） ※「個人番号利用事務」を選択した場合のみ記載
⑥公表（予定）	【事案の公表】 □　あり（予定も含む）　公表（予定）　　年　月　日 □　なし　　□　未定 【公表方法　※「あり（予定も含む）」を選択した場合のみ記載】 □　ＨＰに掲載　□　記者会見　□　記者クラブ等への資料配布 □　その他（　　）

（裏面）

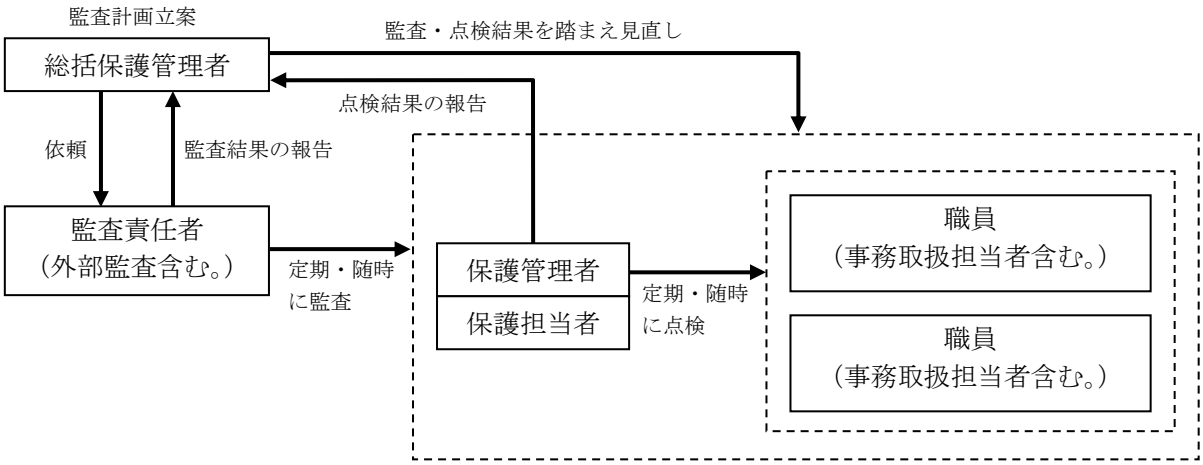
行政機関、独立行政法人等、地方公共団体等用様式

⑦本人への連絡等の状況	
⑧再発防止策等	
⑨その他	

※　第一報から記載を変更した箇所には、変更した記載に下線を引いてください。

Ⅸ　監査及び点検の実施【管理規程第 10 章関連】

１　監査、点検のフロー



２　監査

監査責任者は、特定個人情報等の管理の状況について、定期に又は随時に監査（外部監査を含む。）を行い、その結果を総括保護管理者に報告する。

① 監査責任者は、監査の目的を明確にし、監査体制を確立したうえで、監査計画に基づき、監査を実施する。

② 情報システムの運用・保守等を事業者に委託している場合、監査責任者は、特定個人情報等の取扱いに関する安全管理措置の遵守について、必要に応じ、監査を実施する。

③ 監査責任者は、点検結果をとりまとめ、総括保護管理者に報告する。

④ 保護管理者は、特定個人情報等の管理の状況について改善が必要な場合は、監査結果を踏まえ、必要な見直しを行う。

３　点検

保護管理者は、各課等における特定個人情報等の記録媒体、処理経路、保管方法等について、定期に又は随時に点検を行い、必要があると認めるときは、その結果を総括保護管理者に報告する。

① 保護管理者は、点検の目的を明確にし、点検体制を確立したうえで、点検を実施する。

② 情報システムの運用・保守等を事業者に委託している場合、保護管理者は、特定個人情報等の取扱いに関する安全管理措置の遵守について、必要に応じ、点検を実施する。

③　保護管理者は、点検結果をとりまとめ、総括保護管理者に報告する。
④　職員は、特定個人情報等の記録媒体、処理経路、保管方法等について改善が必要な場合、点検結果を踏まえ、必要な見直しを行う。

４　評価及び見直し

特定個人情報等の管理の状況等に関する監査及び点検の結果等を踏まえ、総括保護管理者及び保護管理者等は、恩納村特定個人情報等の安全管理に関する基本方針（以下「基本方針」という。）、管理規程及び本マニュアル（以下「基本方針等」という。）について実効性等の観点から評価し、必要があると認めるときは、その見直しを行う。

監査及び点検の結果等を踏まえ、不備がなかった場合であっても、情報技術の進展等によって、安全管理措置等が陳腐化していると考えられる場合は、基本方針等の見直しを行う必要があることに留意する。

（１）　評価項目

特定個人情報等の安全管理措置に関する評価は、次の項目について行う。

①　組織における安全管理措置の遵守状況
②　業務における安全管理措置の遵守状況
③　安全管理措置の形骸化及び情報技術の進展等による陳腐化等を含む有効性の状況
④　安全管理措置対策に要するコストや効率化の状況

（２）　評価の実施

特定個人情報等の安全管理措置の評価は、定期的な実施のほか、脅威の変化や組織体制の変更、新たな対策技術の導入等、特定個人情報等の安全管理措置に重大な影響を与える事項の変更に応じて実施する。

（３）　見直しの実施

評価の結果、改定の必要があると認められた場合、基本方針等の見直しを行う。

見直しには、基本方針等の内容改定のほか、新たな対策の追加、不要となった対策の廃止を含むものとする。

（４）　情報セキュリティ委員会の承認

基本方針等は、情報セキュリティ委員会の承認を受け、見直しを行う。

（５）　安全管理措置の職員への周知

見直しを行った基本方針等は、特定個人情報等の安全管理措置にかかわるすべての職員に、速やかに周知する。