地方公共団体等における
特定個人情報等取扱要領等

平成３１年４月

個人情報保護委員会事務局

資料一覧及び補足説明

1. 資料一覧

No	資料	活用想定
①	特定個人情報等取扱要領（例）	取扱規程等の見直し等を行っていない場合
	様式第１号（事務取扱担当者）	事務取扱担当者が明確になっていない場合
	様式第２号（研修計画）	研修計画を策定していない場合
	様式第３号（取扱区域）（平成 30 年９月削除）	
	様式第４号（監査計画）	監査を実施していない場合
	様式第５号（事務マニュアル）	管理段階ごとに安全管理措置を盛り込んでいない場合
②	研修出欠リスト	研修の未受講者を把握等していない場合
③	監査チェックリスト（基礎編）	監査を実施していない場合
④	漏えい報告体制（フロー）	漏えい等の報告体制を整備していない場合
⑤	特定個人情報等の取扱いに関する特記事項（例）	委託契約書等に特定個人情報等の取扱いを規定していない場合

2. 資料の補足説明

【全体】

- 当該資料は、参考として示すものであるため、当該資料に基づき特定個人情報等を取り扱わなければならないということではありません。適宜、修正するなどして、活用してください。

【特定個人情報取扱要領（例)】

- 本要領を策定せず、情報セキュリティポリシーを見直す方法等も考えられます。なお、情報セキュリティポリシーのみで運用する場合は、情報資産の範囲に文書（窓口で受け取った申請書等）が含まれていないと考えられますので、当該取扱いに留意が必要です。
- 本要領の米印の部分において、具体的な説明をしています。

【様式第１号】

- 「特定個人情報の適正な取扱いに関するガイドライン」の特有の事項として、事務取扱担当者や取扱区域の明確化等がありますが、課ごとに明確化の方法が異なる場合や一部の課において策定していない場合がありましたので、組織内で統一的なものとなるよう様式を示しています。

【様式第２号】【研修出欠リスト】

- 番号法第 29 条の２で求められているサイバーセキュリティ研修は、研修計画をあらかじめ策定すること、特定個人情報ファイルを取り扱う事務に従事する者の全てに対して研修することなどが求められているため、留意する必要があります。

【様式第４号】【監査チェックリスト（基礎編)】

- 監査の実効性を担保するため、監査計画の様式を示しています。
- 監査項目については、今回送付する「監査チェックリスト（基礎編)」のほかに、「地方公共団体等における監査のためのチェックリスト（個人情報保護委員会)」、「地方公共団体における情報セキュリティ監査に関するガイドライン（総務省)」等を参考にしてください。

【漏えい報告体制（フロー)】

- 各団体内において、「情報セキュリティに関する統一的な窓口」に情報が集約され、当該窓口から外部の機関に報告することを想定しています。
- 当該報告フローに、「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の整備」も併せて明記しています。

特定個人情報等取扱要領　（例）

平成●年●月●日

第１章　総則

（趣旨）

第１条　本要領は、行政手続における特定の個人を識別する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。）及び「●●条例」（平成●年●第●号。以下「個人情報保護条例」という。）に定めるところにより、特定個人情報の取扱いに関し必要な措置を定めるものとする。

（定義）

第２条　用語の意義は、番号法第２条及び個人情報保護条例第●条に定めるところによる。 ※必要に応じて、個人情報保護条例第●条を削除したり、個人情報保護法等を追記したりする。

第２章　管理体制

※第３条～第６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・地方公共団体等編）（以下「ＧＬ」という。）安全管理措置２Ｃａに対応

（総括責任者）

第３条　総括責任者を一人置くこととし、副●長をもって充てる。総括責任者は、実施機関の長を補佐し、各機関における個人番号及び特定個人情報（以下「特定個人情報等」という。）の管理に関する事務を総括する任に当たる。

（保護責任者）

第４条　個人番号利用事務等を実施する課室等に、保護責任者を一人置くこととし、当該課室等の長又はこれに代わる者をもって充てる。保護責任者は、各課室等における特定個人情報等を適切に管理する任に当たる。

（監査責任者）

第５条　監査責任者を一人置くこととし、●●をもって充てる。監査責任者は、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。

（事務取扱担当者の指定等）

第６条　特定個人情報等を取り扱う職員（以下「事務取扱担当者」という。）及びその役割を明確化し、事務取扱担当者を別に定める様式（様式第１号）により指定する。

※様式第１号は、指定については、部署名や事務名でもよいため、個人単位と部署単位の例を記載している。

２　事務取扱担当者が取り扱う特定個人情報等の範囲を明確化する。

３　次に掲げる組織体制を整備する。

（１）事務取扱担当者が本要領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

（２）特定個人情報等の漏えいその他の番号法違反（以下「情報漏えい等」という。）の事案又はおそれのある事案を把握した場合の対応体制並びに関係部署及び関係機関へ

の報告連絡体制　※ＧＬ安全管理措置２Ｃｄにも対応

※「特定個人情報の漏えい事案等が発生した場合の報告フロー」などを活用する。

（３）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

※第６条、第 10 条等は、組織として体制整備をして欲しいため、「保護責任者は」等の主語をあえて記載していない。

（事務取扱担当者の監督）　※ＧＬ安全管理措置２Ｄａに対応

第７条　総括責任者及び保護責任者は、特定個人情報等が本要領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。

第３章　教育研修　※ＧＬ安全管理措置２Ｄｂに記載

第８条　総括責任者及び保護責任者は、事務取扱担当者に対し、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その他必要な教育研修を行う。また、事務取扱担当者のうち特定個人情報ファイルを取り扱う事務に従事する者に対し、番号法第 29 条の２に定めるサイバーセキュリティの確保に関する事項その他の事項に関する研修を行う。

２　総括責任者及び保護責任者は、特定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、特定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行う。

３　総括責任者は、保護責任者に対し、課室等における特定個人情報等の適切な管理のために必要な教育研修を行う。

４　教育研修については、教育研修への参加の機会を付与するとともに、研修未受講者に対して再受講の機会を付与する等の必要な措置を講ずる。

５　総括責任者は、教育研修を行うに当たり、研修計画（様式第２号）を策定し、研修計画に基づき教育研修を実施する。

第４章　特定個人情報等の取扱い　※番号法の規定（利用制限等）は、本要領に記載していない。

（特定個人情報等の取扱状況の記録）　※ＧＬ安全管理措置２Ｃｂ、Ｃｃに対応

第９条　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、当該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。

（取扱区域）　※ＧＬ安全管理措置２Ｅａ、Ｅｂ、Ｅｃに対応

第 10 条　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。）においては、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ほか、書類等の盗難又は紛失等を防止するために施錠可能な場所への保管等の物理的な安全管理措置を講ずる。

※保管等の「等」は、「書類等を持ち運ぶ必要が生じた場合には、容易に個人番号が判明しないよう安全な方策を講ずる。」を指す。

（廃棄等）　※ＧＬ安全管理措置２Ｅｄに対応

第 11 条　特定個人情報等が記録された書類等について、文書管理に関する規程等によっ

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復元不可能な手段で削除又は廃棄する。

2　個人番号又は特定個人情報ファイルを削除又は廃棄した場合には、その記録を保存する。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。

（委託先の監督）　※ＧＬ第４－２－(1)に対応

第 12 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●●自ら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、あらかじめ確認する。

2　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、契約書等に特定個人情報等の特記事項を定めるなどし、委託先に安全管理措置を遵守させるための必要な契約を締結する。※「特定個人情報等の取扱いに関する特記事項（例）」などを活用する。

3　個人番号利用事務等の全部又は一部を委託した場合、委託先における特定個人情報の取扱状況を把握する。

4　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する場合には、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。

※番号法第10条「個人番号利用事務又は個人番号関係事務の全部又は一部の委託を受けた者は、当該個人番号利用事務等の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。」を前提としている。

（情報資産）　※ＧＬ安全管理措置２Ｆｃに対応（第３項を除く。）

第 13 条　個人番号利用事務の実施に当たり接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守する。

2　個人番号利用事務において使用する情報システムについて、インターネットから独立する等の高いセキュリティ対策を踏まえたシステム構築や運用体制整備を行う。

3　その他の情報資産の取扱いについては、●●情報セキュリティポリシーの例による。

※ＧＬ安全管理措置２に対応「地方公共団体等は、安全管理措置を講ずるに当たり、（略）地方公共団体等において策定した情報セキュリティポリシー等を遵守することを前提とする。」

※本要領は、「情報セキュリティ対策基準の例文」と同等の規定があることを前提とする。

第５章　監査の実施

（監査）　※ＧＬ安全管理措置２Ｃｅに対応

第 14 条　監査責任者は、特定個人情報等の管理の状況について、定期に及び必要に応じ随時に監査（外部監査及び他部署等による点検を含む。）を行い、その結果を総括責任者に報告する。

2　監査責任者は、監査を行うに当たり、監査計画（様式第４号）を立案し、総括責任者の承認を得る。

（評価及び見直し）

第 15 条　総括責任者は、監査の結果等を踏まえ、必要があると認めるときは、本要領等

の見直し等の措置を講ずる。

第６章　事務の流れの整理　※ＧＬ安全管理措置２Ｂに対応

第 16 条　個人番号利用事務等の範囲等を明確にした上で、別に定める様式（様式第５号）により個人番号利用事務等の流れを整理し、管理段階ごとに安全管理措置を織り込む。

※範囲等の「等」は、本要領第６条に規定する特定個人情報等の範囲、事務取扱担当者を指す。

※様式第５号について、複数の事務をまとめて作成することも考えられる。

附則

この規程は、平成●年●月●日から施行する。

特定個人情報等取扱要領（平成●年●●●第●号）

様式第１号（第６条関係）

平成　年　月　日

事務取扱担当者一覧（個人単位）

	部	課	氏名	役職	事務	備考
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

注：適宜、行を追加すること

（日本工業規格Ａ列４番）

様式第１号（第６条関係）

平成　年　月　日

事務取扱担当者一覧（部署単位）

	部	課	事務	備考
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

注：適宜、行を追加すること

（日本工業規格Ａ列４番）

様式第２号（第８条関係）

平成　年　月　日

部

課

平成　　年度　特定個人情報等に関する研修計画

No.	実施時期	研修名	対象者	実施方法	備考
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

注：適宜、行を追加すること

（日本工業規格Ａ列４番）

【記載例】

平成○○年○○月○○日
○○○○○部
○○○○○課

平成○○年度　特定個人情報等に関する研修計画

No.	実施時期	研修名	対象者	実施方法	備考
1	平成○○年○○月○○日	特定個人情報の適正な取扱いについて（保護責任者用）	保護責任者（課室長）	研修形式（座学）	管理職・マネジメント研修の一部として、当該研修を実施する
2	平成○○年○○月○○日	特定個人情報の適正な取扱いについて（事務取扱担当者用）	事務取扱担当者	上記１の伝達研修 研修形式（座学）	・保護責任者が課内の事務取扱担当者に研修を実施する ・番号法第 29 条の２に定めるサイバーセキュリティの確保に関する事項を含む
3	平成○○年○○月○○日 ～平成○○年○○月○○日	マイナンバーシステム管理者研修	事務取扱担当者のうち情報システムの管理に関する事務に従事する職員	ｅラーニング	ｅラーニング受講後、理解度テストを実施する
4	・・・				
5	・・・				

様式第４号（第 14 条関係）

平成　　年　　月　　日

部

課

平成　　年度　特定個人情報等に関する監査計画

１．監査計画

1	監査目的	
2	監査範囲	
3	被監査部門	
4	監査方法	
5	監査実施日程	
6	監査実施体制	
7	適用基準	

２．監査結果のフォローアップ

総括責任者は、監査の結果等を踏まえ、必要があると認めるときは、取扱規程等の見直し等の措置を講ずることとする。

以　上

（日本工業規格Ａ列４番）

【記載例】

平成○○年○○月○○日
○○○○○部
○○○○○課

平成○○年度　特定個人情報等に関する監査計画

１．監査計画

1	監査目的	○○業務に関して、取扱規程等に基づく運用状況及び特定個人情報等の管理状況について、確認する。
2	監査範囲	・○○業務 ・○○システム
3	被監査部門	・○○課（原課） ・○○課（○○システム所管課）
4	監査方法	・○○課における取扱規程等に基づく運用状況の確認 ・○○課における特定個人情報等の管理状況の確認 ・○○システム、マシン室の確認 ・自己点検結果の確認
5	監査実施日程	平成○○年○○月○○日～平成○○年○○月○○日
6	監査実施体制	監査責任者　　○○　○○ 監査人　　○○　○○
7	適用基準	・○○市　特定個人情報等取扱規程 ・○○市　情報セキュリティポリシー

２．監査結果のフォローアップ

総括責任者は、監査の結果等を踏まえ、必要があると認めるときは、取扱規程等の見直し等の措置を講ずることとする。

以　上

様式第５号（第 16 条関係）

平成　　年　　月　　日

部

課

特定個人情報等の取扱いに関する事務マニュアル

（　　に関する事務）

各事務手続の実施にあたっては、特定個人情報等取扱要領を遵守する。

区　分	概　要（主な留意点等）

注：適宜、行を追加すること

（日本工業規格Ａ列４番）

【記載例】

平成○○年○○月○○日
○○○○部
○○○○課

特定個人情報等の取扱いに関する事務マニュアル

（○○に関する事務）

各事務手続の実施にあたっては、特定個人情報等取扱要領を遵守する。

区　分	概　要（主な留意点等）
①取得	申請書等に記載されたマイナンバーについて、本人確認を行い、個人番号を取得する。 ※情報提供ネットワークシステムによる地方税情報の入手に関して、法令又は条例により質問検査権及び担保措置の規程がない場合は、本人同意が必要となるため、留意すること。
②情報システムへの個人番号を含むデータ入力の方法	入力作業を行う場合には、のぞき見や書類の紛失等の情報漏えい等、申請書等に記載された情報の誤入力等に十分注意する。
③保管方法	個人番号が記載された書類及び電磁的記録媒体は、取扱区域内の施錠可能なキャビネットに保管する。
④委託	情報システムの保守・管理のための委託にあたり、「特定個人情報等の取扱いに関する特記事項」を踏まえた契約等を締結した上で、委託先に対する必要かつ適切な監督を行う。
⑤削除・廃棄	情報システムについては、保存期間の経過等により、保存の必要がなくなったときに、速やかに個人番号を削除し、削除状況を第三者が確認する。 書類及び電磁的記録媒体については、保存期間の経過等により、保存の必要がなくなったときに、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。

【研修出欠リスト】

平成▲年▲月▲日現在

No.	職員名	職員区分	採用年月日 異動年月日	研修一覧					備考
				○○研修	△△研修	■■研修	■■研修	●●研修	
				○月○日	△月△日	■月■日	□月□日	●月●日	
1	●●　××	非常勤	●●年●月●日	○	×	×	○	×	■■研修については、□月□日に再受講したものである。
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									

注：適宜、行を追加すること

監査チェックリスト（基礎編）

項番	大分類	小分類	チェック	確認事項	補足説明
A	基本方針の策定	周知していることを確認する場合には、自己点検などを利用することが考えられる。	□	基本方針を策定しているか	✔基本方針の策定は義務付けられてはいないが、特定個人情報等に関する安全管理に係る方針を明確にすることにより職員への教育研修、意識付けなどに利用できる。 ✔既存の個人情報保護方針等の見直しで対応することも考えられる。 ✔周知は職場内メールや掲示板等を利用することが考えられる。
				（策定している場合、以下もチェック）	
			□	事務取扱担当者等の関係者に周知しているか	
B	取扱規程等の見直し等	特定個人情報等を取り扱う事務フローに沿って具体的な取扱いを定める取扱規程等を策定等する必要がある。	□	特定個人情報を取り扱うための規程の策定・見直しをしているか	✔既存の個人情報を取り扱うための規程等に特定個人情報に関する取扱いルールを追記するなどの方法も考えられる。 ☞取扱規程等と情報セキュリティポリシー等の情報セキュリティ関係規程の内容に矛盾はないか。 ✔周知は職場内メールや掲示板等を利用することが考えられる。
			□	情報セキュリティの規程について、相互に関連性を示す文書管理体系となっているか	
			□	事務取扱担当者等の関係者に周知しているか	
		取得	□	取得する際の規程を整備しているか	☞住民等から個人番号が記載された申請書を受理する際の本人確認（身元確認、番号確認）等の手順を定めているか。 ☞特定個人情報を取得する際に紛失や毀損が生じないような手順を定めているか。 ☞不要な個人番号を取得しないための確認（個人番号記載不要の申請書に個人番号が記載されていないか）等の手順を定めているか。 ☞特定個人情報を取得（紙媒体、電子媒体）した場合、台帳（システムを含む。以下同じ。）等に記録することとしているか。
			□	取得に係る運用はどのようになっているか	
			□	目的外の取得についてリスク対策を講じているか	
		利用	□	利用する際の規程を整備しているか	☞個人番号を利用する際の具体的な手順を業務マニュアル等で定めているか。 ✔不正利用を防止する対策としては「アクセスできる者の限定」、「アクセスできるファイルの限定」、「アクセスログのチェック」等が考えられる。
			□	利用に係る運用はどのようになっているか	
			□	不正利用についてのリスク対策を講じているか	
		保存	□	保存する際の規程を整備しているか	☞特定個人情報が記載された書類・電子媒体等の保管ルール（保管方法、保管期限等）を定めているか。 ☞特定個人情報が記載された書類・電子媒体等の保管状況が台帳等に記載されているか。
			□	保存に係る運用はどのようになっているか	
		提供	□	提供する際の規程を整備しているか	☞個人番号を提供する際の具体的な手順を業務マニュアル等で定めているか（個人番号が記載された住民票の写しを交付する場合等を含む）。 ☞特定個人情報を提供した場合、台帳等に記録することとしているか。
			□	提供に係る運用はどのようになっているか	
		削除・廃棄	□	削除・廃棄する際の規程を整備しているか	☞特定個人情報が記載された書類・電子媒体等の削除・廃棄のルール（廃棄方法、保管期限等）を定めているか。 ☞特定個人情報が記載された書類・電子媒体等の削除・廃棄の実績が台帳等に記載されているか。
			□	削除・廃棄に係る運用はどのようになっているか	

C	組織的安全管理措置	a 組織体制の整備	□	総括責任者（機関に１人）を設置し、役割・責任を明確にしているか	☞左記の各事項を規程等で明確にしているか。 ✔各責任者や担当者の設置については、個人名ではなく役職名や係名で明確化することも考えられる。 ✔情報漏えい等事案に係る報告連絡体制は、報告ルートの途上に不在者があっても総括責任者や最高情報セキュリティ責任者まで迅速に報告される体制としておくことが重要である。
			□	保護責任者（個人番号を利用する課室等に各１人）を設置し、役割・責任を明確にしているか	
			□	監査責任者を設置し、役割・責任を明確にしているか	
			□	事務取扱担当者を設置し、役割を明確にしているか	
			□	事務取扱担当者が取り扱う特定個人情報等の範囲を明確にしているか	
			□	情報漏えい等事案の発生又は兆候を把握した場合の報告連絡体制を整備しているか	
		b 取扱規程等に基づく運用	□	特定個人情報ファイルの利用、データの出力状況を記録しているか	☞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ているかどうかを確認しているか。 ✔記録を保存することは、取扱規程等の遵守、情報漏えい等事案の発生の抑制、監査、情報漏えい等事案の再発防止策の策定等に際し、有用である。 ✔記録が改ざん、不正な削除等がされないように保護責任者（又は保護責任者が指名する者等）が記録を管理するなどの手法が考えられる。
			□	特定個人情報等が記載された書類、電子媒体等の持ち運び（持ち出し、持ち帰り）について記録しているか	
			□	特定個人情報ファイルの削除・廃棄について記録しているか	
			□	特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者のシステムの利用状況（ログイン実績、アクセスログ等）を記録しているか	
			□	上記の記録を一定期間保存しているか	
			□	上記の記録を定期及び必要に応じ随時に分析等しているか	
			□	上記の記録について、改ざん、窃取、不正な削除の防止のために必要な措置を講じているか	
		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名称を定め、記録しているか	✔個人情報ファイル簿を作成している場合は、その内容を見直し、特定個人情報ファイル管理簿とすることも考えられる。 ✔記録することは、監査により取扱状況を確認する際に有用である。 ☞取扱状況を確認するための記録に個人番号を記載していないか。
			□	特定個人情報ファイルを利用する事務を行う組織（部署）名を記録しているか	
			□	特定個人情報ファイルの利用目的を記録しているか	
			□	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を記録しているか	
		d 情報漏えい等事案に対応する体制等の整備 ●漏えい等した情報に係る本人の数にかかわらず、個人情報保護委員会への漏えい等報告は必須。	□	情報漏えい等事案が発覚した際の組織内の報告・連絡体制を明確にし、周知しているか	✔情報漏えい等の発生時に被害が最小限にとどまるようにあらかじめ体制を整備しておく必要がある。 ☞情報漏えい等が発生した場合、事実関係の調査、原因究明、漏えい等の影響を受ける可能性のある本人への連絡、再発防止策等を速やかに行う体制・手順等が整備されているか。
			□	個人情報保護委員会その他の関係機関へ報告する体制を明確化し、周知しているか	
			□	不正アクセス、標的型攻撃等の被害を受けた場合の対応について定期的に確認又は訓練等を行っているか	
		e 取扱状況の把握及び安全管理措置の見直し	□	監査に係る規程を整備しているか	✔監査担当部署がない場合は、特定個人情報等が規程に則して取り扱われているかなどについて、他部署とクロスチェックするなどの手法も考えられる。 ☞監査担当部署（監査実施部署）と取扱規程等の改定等を所管する部署が連携するなど取扱規程等の見直し等を行う体制が整備されているか。
			□	監査の計画（監査の観点、監査周期等）を策定しているか	
			□	監査結果を総括責任者に報告しているか	
			□	監査結果を踏まえ、取扱規程等の見直し等をしているか	

D	人的安全管理措置	a 事務取扱担当者の監督	□	総括責任者及び保護責任者は事務取扱担当者が適正に特定個人情報等を取り扱っているか適切に監督しているか	
		b 事務取扱担当者等の教育 ●(※)は番号法で実施が義務付けられた研修。	□	特定個人情報等の保護に関する教育研修に係る規程を整備しているか	☞教育研修に係る規程において研修の受講が必要な者を明確にしているか。 ✔未受講者へのフォロー等を行うために、研修を開催する部署等が受講が必要な職員の受講状況を記録しておくことが重要である。 ☞新規採用（非常勤職員等を含む）時や異動に伴う随時の研修を実施しているか。 ✔集合研修に参加した職員は自分が所属する部署の職員に研修内容を確実に伝達する必要がある。 ✔各種の業務関係研修に併せて研修を行うことも考えられる。
			□	事務取扱担当者や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て教育研修を実施しているか	
			□	保護責任者に対して教育研修を実施しているか	
			□	未受講者に対して、再度の教育研修を実施するなどのフォローを行っているか	
			□	サイバーセキュリティの確保に関する事項その他の事項に関する研修を計画し実施しているか(※)	
			□	サイバーセキュリティに関する研修を特定個人情報を取り扱う事務に従事する職員全員に概ね１年ごとに実施しているか(※)	
		c 法令・内部規程違反等に対する厳正な対処	□	法令又は内部規程等の違反した場合の対処の規程を整備しているか	
			□	法令又は内部規程等の違反した職員がいた場合、厳正に対処しているか	
E	物理的安全管理措置	a 特定個人情報等を取り扱う区域の管理	□	特定個人情報等を取り扱う事務を実施する区域（取扱区域）では、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に留意しているか	✔取扱区域は、実際に事務を行っている課室等のスペースや特定個人情報等が記載されている書類等が保管されている書庫などが該当する。 ✔管理区域において、入室する権限を有する者を定めたり、入退室の記録を残すなどの措置を講ずるほか、施錠装置、監視設備の設置等の措置を講ずる。
			□	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（管理区域）は明確になっているか	
			□	管理区域への入退室管理を行っているか	
			□	管理区域へ持ち込む機器等の制限等を行っているか	
		b 機器及び電子媒体等の盗難等の防止	□	機器、電子媒体の盗難等の防止の措置を講じているか	☞書類、機器、電子媒体等を施錠できるキャビネットや書庫で保管しているか。 ☞情報システム機器をセキュリティワイヤー等で固定しているか。
			□	書類の盗難等の防止の措置を講じているか	
		c 電子媒体等の取扱いにおける漏えい等の防止	□	電子媒体又は機器等の使用・接続制限等を行っているか	☞**電子媒体等の**使用申請・許可等を行っているか。 ☞持ち運ぶ際には、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、封緘等の搬送方法や持出し手続等を行っているか。
			□	電子媒体又は書類等持ち運ぶ際に個人番号が容易に判明しないような措置を講じているか	
		d 個人番号の削除、機器及び電子媒体の廃棄	□	削除又は廃棄の規程を整備しているか	✔文書管理規程等の中に規定が設けられていても差し支えない。 ✔書類等を廃棄する場合、焼却・溶解、復元不可能な程度に裁断可能なシュレッダーの利用や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が考えられる。 ✔機器や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や物理的な破壊等が考えられる。
			□	削除又は廃棄は規程に則して適切に行われているか	
			□	委託している場合、委託先が確実に削除又は廃棄したことを証明書等を取得して確認しているか	

F	技術的安全管理措置	a アクセス制御	□	情報システムを使用する場合、使用可能な端末、事務取扱担当者、特定個人情報ファイルの範囲を限定しているか	☞アクセス権限が付与される者を最小化しているか（不必要な者に付与していないか）。 ☞アクセス権限が付与された者がアクセスできるファイルの範囲を最小化しているか（アクセス不要なファイルにアクセスする権限を付与していないか）。
			□	人事異動等があった場合、漏れなくアクセス権限の削除等が行われているか	
		b アクセス者の識別と認証	□	情報システムにアクセスするための識別・認証を行っているか	✔事務取扱担当者の識別方法としては、ユーザID、パスワード、生体情報等が考えられる。 ☞パスワード等を記載したメモ等を他人の目に触れるところに貼付等していないか。
		c 不正アクセス等による被害の防止等	□	外部等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ているか	✔外部ネットワークと接続する場合、接続箇所にファイアーウォール等を設置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。 ☞不正アクセス等の被害に遭った場合、被害を最小化する仕組み（ネットワークの遮断等）を導入し、周知しているか。 ☞システムへのアクセスログ等を分析（業務時間外のアクセス、大量なデータの送信の有無の確認等）しているか。
			□	情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守しているか	
			□	個人番号利用事務において使用する情報システムについて、インターネットから独立する等の高いセキュリティ対策を踏まえたシステム構築や運用体制を構築しているか	
		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、情報漏えい等を防止するための措置を講じているか	✔外部に送信する際、送信先等に誤りはないか確認する手順を盛り込むことが考えられる。 ☞外部に送信する場合、暗号化等の措置を講じているか。 ☞機器や電子媒体等に保存する場合等の暗号化又はパスワードによる秘匿化に当たっては、暗号鍵及びパスワードに用いる文字数や文字の種類等を考慮しているか（大文字・小文字、数字を混在させる等）。
			□	特定個人情報ファイルを機器又は電子媒体に保存する場合、暗号化等により秘匿しているか	

特定個人情報の漏えい事案等が発生した場合の報告フロー

市町村内

【情報セキュリティに関する統一的な窓口】

課名　　：

担当者名：

TEL　　：

FAX　　：

・個人情報保護委員会へ報告する者
・県へ報告する者（住基、税関係）
・CISOに報告する者
統一する！！

原課において、どのような場合に報告しなければならないか（漏えい事案等が何に該当するか）周知しておくことが必要です。
（例）
・内部不正
・不正アクセス
・書類等の誤交付
・データの誤削除
・書類等の紛失
・メール誤送信　など

【内部フロー】

原課 → 窓口 → CISO

※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も同様とする。

個人情報保護委員会

重大事態に該当するか？

≪重大事態≫
① 情報提供ネットワークシステム等又は個人番号利用事務・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が漏えい等した事態
② 漏えい等した特定個人情報に係る本人の数が100人を超える事態
③ 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、かつ閲覧された事態
④ 職員等が不正の目的をもって、特定個人情報を利用し、又は提供した事態

YES

発覚した時点で直ちに第一報を報告

報告手段：**電話にて報告した後、委員会ウェブサイトに設置している報告フォームから報告**
※不正プログラム等による情報漏えい等の場合はFAX
※報告フォームによる報告が困難な場合のみ、別紙様式により電子メールで報告

事態の収束、再発防止策の確定

速やかに確報を個人情報保護委員会へ報告

NO

速やかに確報を報告

報告手段：原則　**委員会ウェブサイトに設置している報告フォーム**
例外　不正プログラム等による情報漏えい等の場合FAX
報告フォームによる報告が困難な場合は、別紙様式により電子メールで報告

注意点：重大な事態又はそのおそれのある事案について、報道発表する場合は、事前に資料を個人情報保護委員会へ提出

都道府県

【都道府県】
課名　　：
担当者名：
TEL　　：
FAX　　：
E－mail　：

総務省からの事務連絡に従い、都道府県の担当者にも連絡する必要がある。

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 ※重大な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 ※概要については、時系列で記載するとともに、発生原因及び発覚の経緯も明記すること。	【発生日】　　年　　月　　日 【発覚日】　　年　　月　　日 【概　要】
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 ※ 重大事態に該当する場合は、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（　　）
⑦本人への連絡等の状況 ※連絡した場合は、完了日も記載すること。	
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。

特定個人情報等の取扱いに関する特記事項（例）

第１条（特定個人情報等の保護に関する法令等の遵守）

受託者（以下「乙」という。）は、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。）、個人情報保護委員会が定める特定個人情報の適正な取扱いに関するガイドライン（以下「ガイドライン」という。）に基づき、本特定個人情報等の取扱いに関する特記事項（以下「特記事項」という。）を遵守しなければならない。また、これらのほか、｛*地方公共団体*｝(以下「甲」という。)の定める｛*個人情報保護条例*｝、｛*情報セキュリティポリシー*｝及び｛*情報セキュリティ実施手順*｝に基づき、特記事項を遵守しなければならない。

第２条（責任体制の整備）

乙は、特定個人情報及び個人番号（以下「特定個人情報等」という。）の安全管理について、内部における責任体制を構築し、その体制を維持しなければならない。

第３条（作業責任者等の届出）

1　乙は、特定個人情報等の取扱いに係る作業責任者及び作業従事者を定め、書面により甲に報告しなければならない。

2　乙は、特定個人情報等の取扱いに係る作業責任者及び作業従事者を変更する場合の手続を定めなければならない。

3　乙は、作業責任者を変更する場合は、事前に書面により甲に申請し、その承認を得なければならない。

4　乙は、作業従事者を変更する場合は、事前に書面により甲に報告しなければならない。

5　作業責任者は、特記事項に定める事項を適切に実施するよう作業従事者を監督しなければならない。

6　作業従事者は、作業責任者の指示に従い、特記事項に定める事項を遵守しなければならない。

第４条（取扱区域の特定）

1　乙は、特定個人情報等を取り扱う場所（以下「取扱区域」という。）を定め、業務の着手前に書面により甲に報告しなければならない。

2　乙は、取扱区域を変更する場合は、事前に書面により甲に申請し、その承認を得なければならない。

3　乙は、甲が指定した場所へ持ち出す場合を除き、特定個人情報等を定められた場所から持ち出してはならない。

第５条（教育の実施）

1　乙は、特定個人情報等の保護、情報セキュリティに対する意識の向上、特記事項における作業従事者が遵守すべき事項その他本委託業務の適切な履行に必要な教育及び研修を、作業従事者全員に対して実施しなければならない。

2　乙は、前項の教育及び研修を実施するに当たり、実施計画を策定し、実施体制を確立しなければならない。

第６条（守秘義務）

1　乙は、本委託業務の履行により直接又は間接に知り得た特定個人情報等を第三者に漏らしてはならない。契約期間満了後又は契約解除後も同様とする。

2　乙は、本委託業務に関わる作業責任者及び作業従事者に対して、秘密保持に関する誓約書を提出させなければならない。

第７条（再委託）

1　乙は、本委託業務を第三者へ委託（以下「再委託」という。）してはならない。

2　乙は、本委託業務の一部をやむを得ず再委託する必要がある場合は、再委託先の名称、再委託する理由、再委託して処理する内容、再委託先において取り扱う情報、再委託先における安全性及び信頼性を確保する対策並びに再委託先に対する管理及び監督の方法を明確にした上で、業務の着手前に、書面により再委託する旨を甲に申請し、その承認を得なければならない。

3　前項の場合、乙は、再委託先に本契約に基づく一切の義務を遵守させるとともに、甲に対して、再委託先の全ての行為及びその結果について責任を負うものとする。

4　乙は、再委託先との契約において、再委託先に対する管理及び監督の手続及び方法について具体的に規定しなければならない。

5　乙は、再委託先に対して本委託業務を委託した場合は、その履行状況を管理・監督するとともに、甲の求めに応じて、管理・監督の状況を甲に対して適宜報告しなければならない。

第８条（派遣労働者等の利用時の措置）

1　乙は、本委託業務を派遣労働者、契約社員その他の正社員以外の労働者に行わせる場合は、正社員以外の労働者に本契約に基づく一切の義務を遵守させなければならない。

2　乙は、甲に対して、正社員以外の労働者の全ての行為及びその結果について責任を負うものとする。

第９条（特定個人情報等の管理）

乙は、本委託業務において利用する特定個人情報等を保持している間は、ガイドラインに定める各種の安全管理措置を遵守するとともに、次の各号の定めるところにより、特定個人情報等の

管理を行わなければならない。

一　個人番号を取り扱う事務、特定個人情報等の範囲及び同事務に従事する作業従事者を明確化し、取扱規程等を策定すること。

二　組織体制の整備、取扱規程等に基づく運用、取扱状況を確認する手段の整備、情報漏えい等事案に対応する体制の整備、取扱状況の把握及び安全管理措置の見直しを行うこと。

三　事務取扱担当者の監督・教育を行うこと。

四　特定個人情報等を取り扱う区域の管理、機器及び電子媒体等の盗難等の防止、電子媒体等の取扱いにおける漏えい等の防止、個人番号の削除・機器及び電子媒体等の廃棄を行うこと。

五　アクセス制御、アクセス者の識別と認証、外部からの不正アクセス等の防止、情報漏えい等の防止を行うこと。

第 10 条（提供された特定個人情報等の目的外利用及び第三者への提供の禁止）

乙は、本委託業務において利用する特定個人情報等について、本委託業務以外の目的で利用してはならない。また、第三者へ提供してはならない。

第 11 条（受渡し）

乙は、甲乙間の特定個人情報等の受渡しに関しては、甲が指定した手段、日時及び場所で行った上で、甲に特定個人情報等の預り証を提出しなければならない。

第 12 条（特定個人情報等の返還又は廃棄）

1　乙は、本委託業務の終了時に、本委託業務において利用する特定個人情報等について、甲の指定した方法により、返還又は廃棄を実施しなければならない。

2　乙は、本委託業務において利用する特定個人情報等を消去又は廃棄する場合は、事前に消去又は廃棄すべき特定個人情報等の項目、媒体名、数量、消去又は廃棄の方法及び処理予定日を書面により甲に申請し、その承諾を得なければならない。

3　乙は、特定個人情報等の消去又は廃棄に際し甲から立会いを求められた場合は、これに応じなければならない。

4　乙は、本委託業務において利用する特定個人情報等を廃棄する場合は、当該情報が記録された電磁的記録媒体の物理的な破壊その他当該特定個人情報等を判読不可能とするのに必要な措置を講じなければならない。

5　乙は、特定個人情報等の消去又は廃棄を行った後、消去又は廃棄を行った日時、担当者名及び消去又は廃棄の内容を記録し、書面により甲に対して報告しなければならない。

第 13 条（定期報告及び緊急時報告）

1　乙は、甲から、特定個人情報等の取扱いの状況について報告を求められた場合は、直ちに報

告しなければならない。

2　乙は、特定個人情報等の取扱いの状況に関する定期報告及び緊急時報告の手順を定めなければならない。

第 14 条（監査及び調査）

1　甲は、本委託業務に係る特定個人情報等の取扱いについて、本契約の規定に基づき必要な措置が講じられているかどうか検証及び確認するため、乙及び再委託先に対して、監査又は調査を行うことができる。

2　甲は、前項の目的を達するため、乙に対して必要な情報を求め、又は本委託業務の処理に関して必要な指示をすることができる。

第 15 条（事故時の対応）

1　乙は、本委託業務に関し特定個人情報等の漏えい等の事故（番号法違反又はそのおそれのある事案を含む。）が発生した場合は、その事故の発生に係る帰責の有無に関わらず、直ちに甲に対して、当該事故に関わる特定個人情報等の内容、件数、事故の発生場所、発生状況等を書面により報告し、甲の指示に従わなければならない。

2　乙は、特定個人情報等の漏えい等の事故が発生した場合に備え、甲その他の関係者との連絡、証拠保全、被害拡大の防止、復旧、再発防止の措置を迅速かつ適切に実施するために、緊急時対応計画を定めなければならない。

3　甲は、本委託業務に関し特定個人情報等の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる。

第 16 条（契約解除）

1　甲は、乙が本特記事項に定める義務を履行しない場合は、本特記事項に関連する委託業務の全部又は一部を解除することができる。

2　乙は、前項の規定による契約の解除により損害を受けた場合においても、甲に対して、その損害の賠償を請求することはできないものとする。

第 17 条（損害賠償）

乙の故意又は過失により、甲に対する損害を発生させた場合は、乙は、甲に対して、その損害を賠償しなければならない。