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
～はじめての監査のために～

平成31年３月

（令和５年３月最終改正）

個人情報保護委員会事務局

目次

第１　はじめに

個人情報保護委員会は、「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）に基づき、地方公共団体等が特定個人情報等の適正な取扱いを確保するための具体的な指針として、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「ガイドライン」という。）を定めています。また、ガイドライン（別添１）特定個人情報に関する安全管理措置（以下「安全管理措置」という。）２Ｃｅにおいて、「監査責任者（地方公共団体等においては相当する者）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（地方公共団体等においては相当する者。以下同じ。）に報告する。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。」と規定されており、監査の実施が求められています。

特定個人情報等の監査については、様々な手法が考えられますが、本監査マニュアルは、保護責任者及び事務取扱担当者に対する自己点検を活用した内部監査手順を示すものであり、特に、監査が実施できていない団体において活用されることを期待し作成したものです。具体的な監査の流れについては、別添資料１「事務フロー」に示しているため、当該フロー図を参照しながら読み進めることを推奨します。

なお、本監査マニュアルに記述した構成や項目等は参考として示したものであり、地方公共団体等において、監査項目、監査方法等を実情に応じて変更し、監査を実施することを妨げるものではありません。

第２　監査体制の構築

ガイドライン安全管理措置２Ｃａにおいて、「監査責任者の設置及び責任の明確化」が求められているため、取扱規程等において監査責任者とその責務について規定する必要があります。

また、監査責任者が単独で監査を実施することは困難であることから、監査を実施する者（以下「監査担当者」という。）を指定することが考えられます。特定個人情報等の監査は、情報システム、電子媒体、文書等が対象となるため、監査担当者として、番号制度所管課の職員だけでなく、情報システム及び文書管理の所管課の職員を加えることも有効です。

第３　監査計画の策定

特定個人情報等の監査を効率的かつ効果的に行うために、監査計画を策定する

ことが有効です。監査計画として、「中期計画」及び「年度計画」を策定することが考えられます。

⑴　中期計画

監査の対象となる課（個人番号利用事務又は個人番号関係事務を実施している課を含め、特定個人情報等を取り扱う全ての課）について、単年度内で全て監査を実施することが困難である場合も考えられます。そのような場合には、一定の期間（例えば、３年から５年程度）で全ての課に対して監査が実施できるよう、中期計画を策定することが有効です。別添資料２「監査計画」の「特定個人情報等に関する中期監査計画」の記載例を参考に、適宜作成することが望まれます。

⑵　年度計画

年度計画は、中期計画を基に年度内での被監査課、実施時期等を記載するものですが、例えば、漏えい等事案の発生等を理由に、中期計画では当該年度で監査を実施する予定ではなかった課を監査すること等も考えられます。年度計画の作成については、別添資料２「監査計画」の「令和〇〇年度　特定個人情報等に関する監査計画」の記載例を参考にしてください。

第４　監査の実施

⑴　自己点検の活用

自己点検については、保護責任者及び事務取扱担当者自らが特定個人情報等の取扱いの見直しを図ることを意識付けることができるとともに、被監査課における特定個人情報等の取扱状況を効率的に把握することができるため有効です。また、自己点検の結果を基に、監査当日に何を確認するかを事前に決めておくことで、監査時間の短縮、被監査課の負担軽減を図ることができ、監査を効率的かつ効果的に実施することができると考えられます。

監査の実施に当たっては、事前に別添資料３－１「特定個人情報等の取扱いに関する自己点検チェックリスト（保護責任者用）」及び別添資料３－２「特定個人情報等の取扱いに関する自己点検チェックリスト（事務取扱担当者用）」に基づき、被監査課の保護責任者及び事務取扱担当者に対して自己点検の実施を依頼します。なお、当該チェックリストの項目は、初めて特定個人情報等の監査を行う場合を想定して作成したものであり、当該チェックリストの項目のみを確認すれば足りるというものではありません。地方公共団体等において、組織の体制、運用状況等を考慮して適宜追加、修正する必要があります。

また、特定個人情報等の取扱状況を把握することや、その結果を受けて必要に応じ随時の監査を実施することができることから、被監査課以外の課においても自己点検を実施することも有効です。

このほか、当該チェックリストを用いた監査の手法としては、当該チェックリストを監査チェックリストと位置づけ、自己点検を実施せずに現地の状況を確認する方法も考えられます。

⑵ 規程の確認

確認すべき規程としては、各地方公共団体等内における共通ルールとして策定された規程と、各課で策定された事務マニュアル等が考えられます。

共通ルールとしての規程については、特定個人情報等を取り扱う全ての課に適用される重要な規程であることから、その時点における法令等に沿ったものとなっているか、規定すべき事項の漏れや各課の運用に合わない規定がないかどうかなどを確認する必要があります。別添資料４「番号制度所管課用チェックリスト」は、共通ルールとしての規程の整備状況についての確認のために作成したものです。

各課で策定された事務マニュアル等については、法令等や共通ルールとしての規程に反した規定がないか、規定すべき事項の漏れや各課の運用に合わない規定がないかどうかなどを確認する必要があります。

※参考

共通ルールとしての規程の整備状況について、地方公共団体等自ら確認することに加え、近隣の市区町村と相互に確認し合うなど、外部の客観的な視点で確認を受けることも有効です。

⑶ 監査当日

監査担当者は、独立した立場で、かつ客観的な視点で監査を実施することが求められることに留意しましょう。

監査の実施については、基本的には自己点検チェックリストの回答のとおり運用が行われているかを確認することとなりますが、被監査課の職員に対するヒアリングのみでなく、現地において目視で確認しましょう。例えば、常に施錠することとなっている書庫が確実に施錠されているか確認することや、特定個人情報等が含まれている情報システムへのアクセス権を画面上で確認すること等が考えられます。

また、当該チェックリストについて、保護責任者の回答と、事務取扱担当者の回答に食い違いがある場合には、被監査課内で特定個人情報の取扱いに関する認識が統一されているかを確認することも重要です。

第５　監査実施後

⑴　監査結果報告書の作成

監査を実施するだけでなく、実施した結果を受けて必要に応じて取扱規程等や安全管理措置を見直す必要があります。そのため、監査責任者は、監査結果報告書を作成して総括責任者に報告し、総括責任者は、必要に応じて、番号制度所管課及び特定個人情報等を取り扱う課に対して、取扱規程等や安全管理措置の見直しを指示する必要があります。

総括責任者への報告に当たっては、別添資料５「監査結果報告書作成例」を参考にしてください。

監査結果報告書を作成する前に、どのような改善方法があるのかを被監査課と議論し、現場の効率性と安全性のバランスがとれた改善を行うことが重要です。

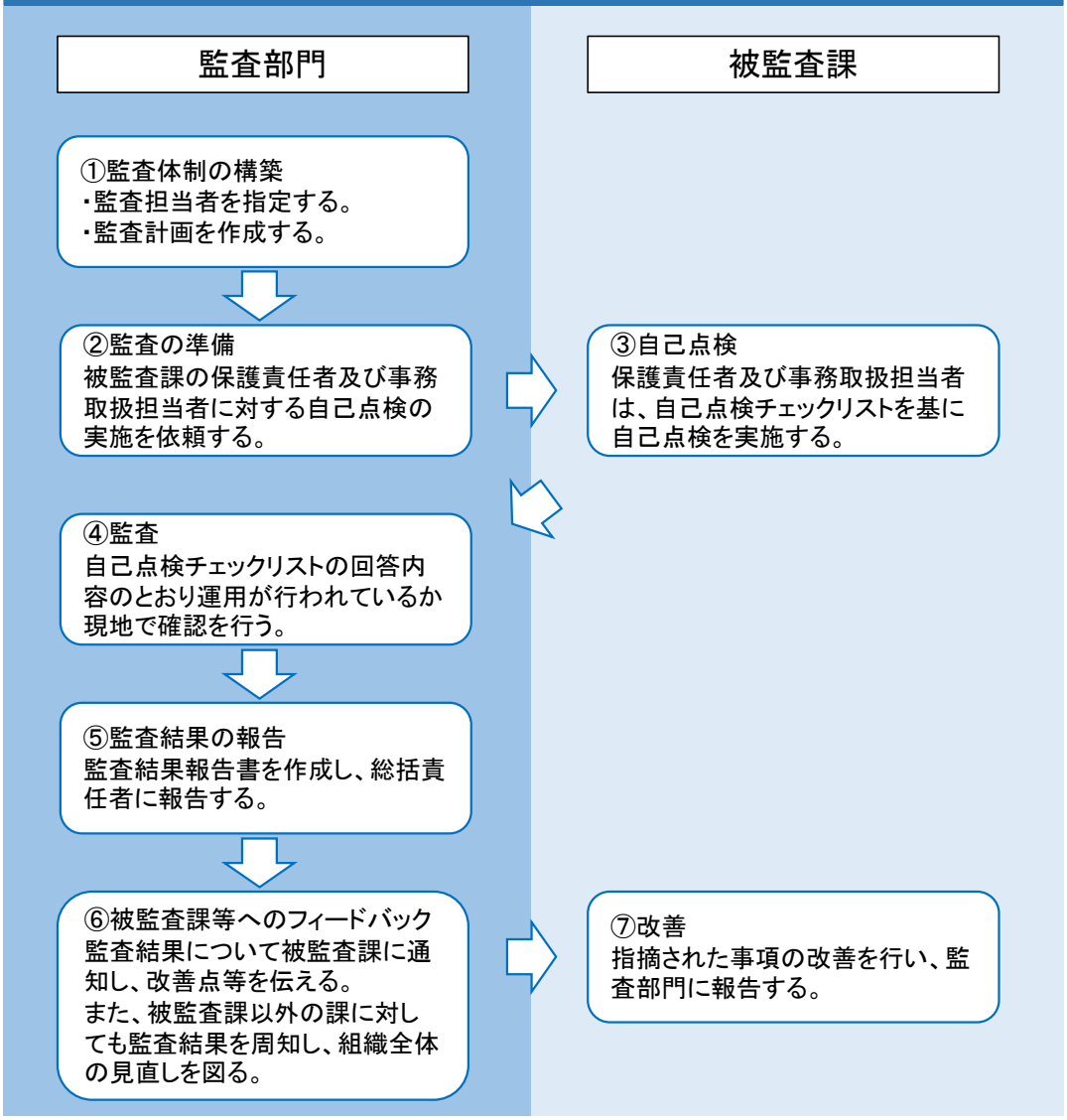
また、改善の必要がある事項のみでなく、被監査課独自の良い取組についても報告書に記載し、特定個人情報等を取り扱う課に対して周知することで、組織全体の安全管理措置の向上につながることが考えられます。

⑵　改善状況のフォローアップ

ガイドライン安全管理措置２Ｃｅにおいて、特定個人情報等の監査の実施が求められている趣旨としては、特定個人情報等の取扱状況を把握した上で、取扱規程等に不備があれば当該規程等を改正し、また、取扱規程等に沿った運用が行われていなければ運用の改善を図るなど、安全管理措置の見直し等を行うことにあります。そのため、監査で指摘した事項について、改善案のとおり対応が執られているか、後日監査担当者が確認する必要があります。なお、日々の業務により改善が後回しになることを防ぐため、改善する期日を被監査課に明示させることが重要です。

別添資料1

自己点検チェックリストを活用した監査の流れ



番号制度所管課用チェックリストの利用方法

担当課での運用状況等とは別に、組織全体に係る規程や体制の整備、教育研修等についてガイドラインが遵守されているか確認する必要があります。当該チェックリストを参考に、組織として講ずべき安全管理措置が講じられているか確認してください。

別添資料２

【中期監査計画ひな形】

令和　　年　　月　　日

部

課

特定個人情報等に関する中期監査計画

監査計画

年度	被監査課
令和●年度	
令和●年度	
令和●年度	
令和●年度	
令和●年度	

なお、総括責任者は、上記の監査に加えて、漏えい等事案の発生等を踏まえ、必要に応じて随時監査を実施することとする。

以　上

【監査計画記載例】

令和○○年○○月○○日
○○○○○部
○○○○○課

令和○○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	被監査課	・○○課（原課） ・○○課（○○システム所管課）
4	監査方法	・自己点検結果の確認 ・○○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
5	監査実施日程	令和○○年○○月○○日～令和○○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

別添資料3－1

特定個人情報等の取扱いに関する
自己点検チェックリスト（保護責任者用）

記入年月日：	所属名：	氏名：

NO.	管理段階	確認事項	回答欄	参考条文等
1	取得	課内の職員は、本人や代理人から個人番号の提供を受ける場合等に、本人確認を行っているか。		・番号法第16条 ・ガイドライン第４－３－(5)
2	取得	課内において、番号法上、個人番号の取得が認められている事務以外で、個人番号を取得していることがないか。		・番号法第20条 ・ガイドライン第４－３－(4)
3	利用	課内の職員は、書類又は電子媒体を持ち運ぶ際に、封緘等の措置を講じているか。講じている場合、どのような方法であるか。		・ガイドライン 安全管理措置2Ec
4	利用	情報システムについて、課内の職員に対して業務上必要な範囲を超えたアクセス権の付与を行っていないか。		・ガイドライン 安全管理措置2Fa
5	利用	情報システムの利用状況等の記録に関して、定期に及び必要に応じ随時に分析等を行っているか。		・ガイドライン 安全管理措置2Cb
6	保存	課内の職員は、書類又は電子媒体について、業務終了後、施錠可能なキャビネット等に保管し、施錠しているか。		・ガイドライン 安全管理措置2Eb
7	保存	キャビネット等の鍵について、適切に管理しているか。		・ガイドライン 安全管理措置2Eb
8	提供	課内の職員は、書類等を交付や送付する際に、誤交付や誤送付をしないための措置を講じているか。講じている場合、どのような方法であるか。		・番号法第12条
9	提供	課内の職員は、電子媒体を提供する場合、電子媒体にパスワードを設定するなど、漏えい等を防ぐための措置を講じているか。		・ガイドライン 安全管理措置2Ec
10	提供	課内の職員は、書類を対面又は郵送で提供する場合、発送日等を記録しているか。		・ガイドライン 安全管理措置2Cb
11	廃棄	課内の職員は、書類を廃棄する場合、シュレッダーにて裁断する等、復元できない方法により廃棄しているか。		・ガイドライン 安全管理措置2Ed
12	廃棄	課内において、既に保存期間を満了し、廃棄又は削除すべき特定個人情報等を保存していないか。		・ガイドライン 安全管理措置2Ed
13	廃棄	課内の職員は、廃棄した記録を保存しているか。また、廃棄の作業を委託する場合には、委託先が確実に廃棄したことについて、証明書等により確認しているか。		・ガイドライン 安全管理措置2Ed

別添資料3－1

特定個人情報等の取扱いに関する
自己点検チェックリスト（保護責任者用）

14	その他	課内の特定個人情報等を取り扱う事務について、規程、マニュアル等があるか。（ある場合、その名称を記入。）		・ガイドライン 安全管理措置2B
15	その他	課内の職員は、書類やPC画面を周りから見える状態で離席していないか。		・ガイドライン 安全管理措置2Ea
16	その他	申請窓口等において、書類やPC画面が、外部の人（市民等）から容易に見える状態にないか。		・ガイドライン 安全管理措置2Ea
17	その他	情報システムへのログイン時等の認証について、課内の職員は、パスワードを記載した付箋をPCに貼るなど、他人が容易にログインできるような状況にしていないか。		・ガイドライン 安全管理措置2Fb
18	その他	今年度、課内の事務取扱担当者に対して、特定個人情報等に関する研修（課内研修を含む。）を行っている、又は受講させているか。未実施である場合は、いつ頃実施する予定であるか。		・ガイドライン 安全管理措置2Db
19	その他	今年度、課における特定個人情報等の適切な管理に関する保護責任者に対する研修を受講しているか。受講していない場合、いつ頃受講する予定であるか。		・ガイドライン 安全管理措置2Db
20	その他	課内において、特定個人情報の漏えい等事案が発生した場合、どこに報告すればよいか把握しているか。		・ガイドライン 安全管理措置2Cd
21	その他	個人番号利用事務等を委託する際に、委託先において自団体と同等の安全管理措置が講じられるか確認しているか。具体的には何を確認しているか。		・ガイドライン第4－2－(1) 1B
22	その他	委託先における特定個人情報の取扱状況を把握しているか。把握している場合、どのような方法で把握しているのか。		・ガイドライン第4－2－(1) 1B
23	その他	個人番号利用事務等の再委託が行われている場合、どのような方法で再委託の許諾を行っているか。		・ガイドライン第4－2－(1) 2A
24	その他	外国において特定個人情報等を取り扱う場合、当該外国の個人情報の保護に関する制度等を把握しているか。その上で、特定個人情報等の安全管理のために必要かつ適切な措置を講じているか。		・ガイドライン 安全管理措置2G

別添資料３－２

特定個人情報等の取扱いに関する
自己点検チェックリスト（事務取扱担当者用）

記入年月日：	所属名：	氏名：

NO.	管理段階	確認事項	回答欄	参考条文等
1	取得	本人や代理人から個人番号の提供を受ける場合等に、本人確認を行っているか。		・番号法第16条 ・ガイドライン第４－３－(5)
2	取得	番号法上、個人番号の取得が認められている事務以外で、個人番号を取得していることがないか。		・番号法第20条 ・ガイドライン第４－３－(4)
3	利用	書類又は電子媒体を持ち運ぶ際に、封緘等の措置を講じているか。講じている場合、どのような方法であるか。		・ガイドライン 安全管理措置2Ec
4	利用	情報システムについて、業務上必要な範囲を超えてアクセスできるようになっていないか。		・ガイドライン 安全管理措置2Fa
5	利用	情報システムの利用状況等の記録に関して、分析等が行われていることを知っているか。		・ガイドライン 安全管理措置2Cb
6	保存	書類又は電子媒体について、業務終了後、施錠可能なキャビネット等に保管し、施錠しているか。		・ガイドライン 安全管理措置2Eb
7	保存	キャビネット等の鍵について、適切に管理しているか。		・ガイドライン 安全管理措置2Eb
8	提供	書類等を交付や送付する際に、誤交付や誤送付をしないための措置を講じているか。講じている場合、どのような方法であるか。		・番号法第12条
9	提供	電子媒体を提供する場合、電子媒体にパスワードを設定するなど、漏えい等を防ぐための措置を講じているか。		・ガイドライン 安全管理措置2Ec
10	提供	書類を対面又は郵送で提供する場合、発送日等を記録しているか。		・ガイドライン 安全管理措置2Cb
11	廃棄	書類を廃棄する場合、シュレッダーにて裁断する等、復元できない方法により廃棄しているか。		・ガイドライン 安全管理措置2Ed
12	廃棄	既に保存期間を満了し、廃棄又は削除すべき特定個人情報等を保存していないか。		・ガイドライン 安全管理措置2Ed
13	廃棄	廃棄した記録を保存しているか。また、廃棄の作業を委託する場合には、委託先が確実に廃棄したことについて、証明書等により確認しているか。		・ガイドライン 安全管理措置2Ed
14	その他	自身が従事する特定個人情報等を取り扱う事務について、規程、マニュアル等があるか。（ある場合、その名称を記入。）		・ガイドライン 安全管理措置2B

別添資料3－2

特定個人情報等の取扱いに関する
自己点検チェックリスト（事務取扱担当者用）

15	その他	離席時に、書類やPC画面を周りから見える状態にしていないか。		・ガイドライン 安全管理措置2Ea
16	その他	申請窓口等において、書類やPC画面が、外部の人（市民等）から容易に見える状態にないか。		・ガイドライン 安全管理措置2Ea
17	その他	情報システムへのログイン時等の認証について、パスワードを記載した付箋をPCに貼るなど、他人が容易にログインできるような状況になっていないか。		・ガイドライン 安全管理措置2Fb
18	その他	今年度、特定個人情報等に関する研修（課内研修を含む。）を受講しているか。まだ受講していない場合、いつ頃受講する予定であるか。		・ガイドライン 安全管理措置2Db
19	その他	特定個人情報の漏えい等事案が発生した場合、どこに報告すればよいか把握しているか。		・ガイドライン 安全管理措置2Cd
20	その他	個人番号利用事務等を委託する際に、委託先において自団体と同等の安全管理措置が講じられるか確認しているか。具体的には何を確認しているか。		・ガイドライン第4－2－(1) 1B
21	その他	委託先における特定個人情報の取扱状況を把握しているか。把握している場合、どのような方法で把握しているのか。		・ガイドライン第4－2－(1) 1B
22	その他	個人番号利用事務等の再委託が行われている場合、どのような方法で再委託の許諾を行っているか。		・ガイドライン第4－2－(1) 2A
23	その他	外国において特定個人情報等を取り扱う場合、当該外国の個人情報の保護に関する制度等を把握しているか。その上で、特定個人情報等の安全管理のために必要かつ適切な措置を講じているか。		・ガイドライン 安全管理措置2G

番号制度所管課用チェックリスト

別添資料4

記入年月日:

ガイドライン項番		チェック	確認事項	参照先（根拠規程等）	補足説明
安全管理措置 2A 基本方針の策定	－	□	基本方針を策定しているか		・基本方針の策定は義務ではないが、組織としての安全管理に係る方針を明確にすることは重要である。
安全管理措置 2B 取扱規程等の見直し等	－	□	実施機関の共通ルールとして、特定個人情報等を取り扱うための規程の策定・見直しをしているか		・共通ルールとしての規程があれば、監査時にその規程に従った運用が行われているか確認し、各課で規程を作成している場合は、その内容に従った運用が行われているか確認する。
安全管理措置 2C 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		・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		
	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、利用目的等を記録し、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しているか。		
	d 漏えい等事案に対応する体制等の整備	□	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		・漏えい等した情報に係る本人の数に関わらず、個人情報保護委員会へ報告する。
		□	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		
	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		
		□	監査の実施により改善すべき事項が見つかった際に、改善状況を確認しているか		
安全管理措置 2D 人的安全管理措置	b 事務取扱担当者等の教育	□	特定個人情報等に関する教育研修に係る規程を整備しているか		・新規採用（非常勤職員等を含む。）時や異動等に伴う随時の研修を実施する必要がある。 ・未受講者へのフォローアップ等を行うために、研修を実施する課が、受講すべき職員の受講状況を記録しておくことが重要である。 ・各課で伝達研修等のフォローアップを行っている場合、番号制度所管課がフォローアップの記録を確認することが重要である。 ・サイバーセキュリティに関する研修については、対象者全員に毎年度実施することが番号法で義務付けられている。
		□	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ファイル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に違反した場合の対処の規程を整備しているか		
安全管理措置 2E 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（管理区域）を明確にしているか		
		□	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	□	書庫への保管の際のルールを設けているか		
	c 電子媒体等の取扱いにおける漏えい等の防止	□	許可された電子媒体又は機器等以外のものについて使用の制限等を行っているか		
安全管理措置 2F 技術的安全管理措置	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		・各課で管理しているのであれば、監査時に確認する。
		□	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		
安全管理措置 2G 外的環境の把握	－	□	外国において特定個人情報等を取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、特定個人情報等の安全管理のために必要かつ適切な措置を講じているか		・外国にある拠点で特定個人情報を取り扱う場合、外国にある第三者に特定個人情報の取扱いを委託する場合、外国にある第三者が提供するクラウドサービスを利用して特定個人情報を取り扱う場合等が考えられる。 ・外国にある第三者に特定個人情報の取扱いを委託する場合は、当該委託先における安全管理措置について、必要かつ適切な監督を行う必要がある。
その他	ガイドライン第4－2－(1)委託の取扱い	□	委託契約書のひな形に、ガイドライン上求められている次の事項を盛り込んでいるか。 (1) 秘密保持義務 (2) 事業所内からの特定個人情報の持ち出しの禁止 (3) 特定個人情報の目的外利用の禁止 (4) 再委託における条件 (5) 漏えい等事案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の返却又は廃棄 (7) 特定個人情報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) 委託先に対して実地の監査、調査等を行うことができる規定		・ひな形に盛り込むことで各課での契約時に記載漏れを防ぐことができる。

別添資料５

【監査結果報告書作成例】

令和○○年○○月○○日
監査責任者　○○　○○

令和○○年度　特定個人情報等の取扱いに関する監査結果報告書

「令和○○年度特定個人情報等の取扱いに関する監査計画」に関する監査結果は、次のとおりである。

１　監査の対象
○○課

２　監査の実施日
令和○○年○○月○○日～○○月○○日

３　監査担当者
○○課　○○　○○、○○　○○

４　指摘事項等

⑴　特定個人情報等を含む書類の管理

ア　指摘事項

○○市特定個人情報等取扱要領において、「特定個人情報等を含む書類については、所定のキャビネット等に施錠した上で保管する。」旨、規定されているところ、○○課における事務取扱担当者１名が、特定個人情報等を含む書類を、個人の机に保管していた。

イ　改善案

○○課の保護責任者と協議した結果、○○課における全事務取扱担当者に対し、○○市特定個人情報等取扱要領を通読させた上で、今回の指摘事項を共有し、同様の取扱いをしないよう指示した。

⑵　・・・

以　上