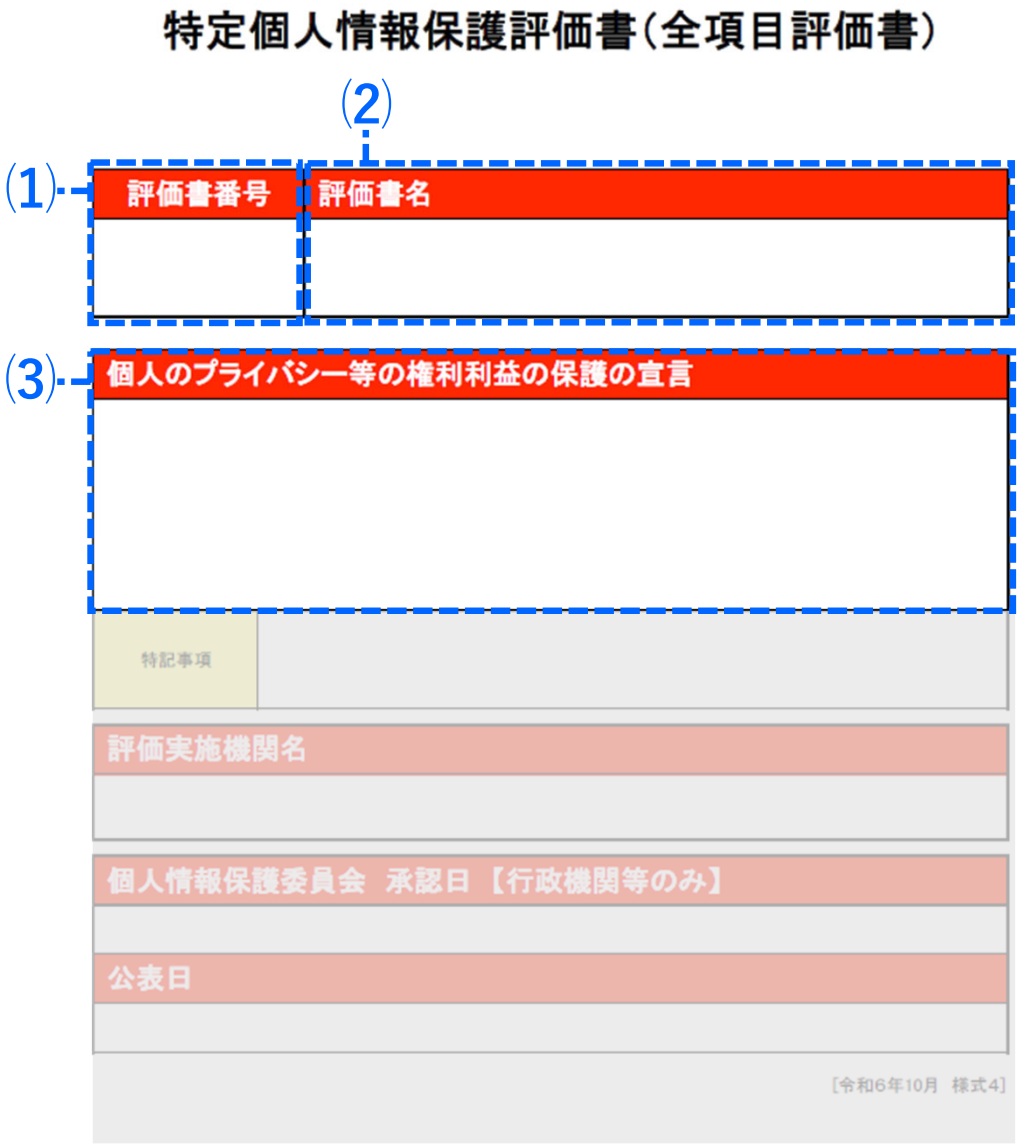
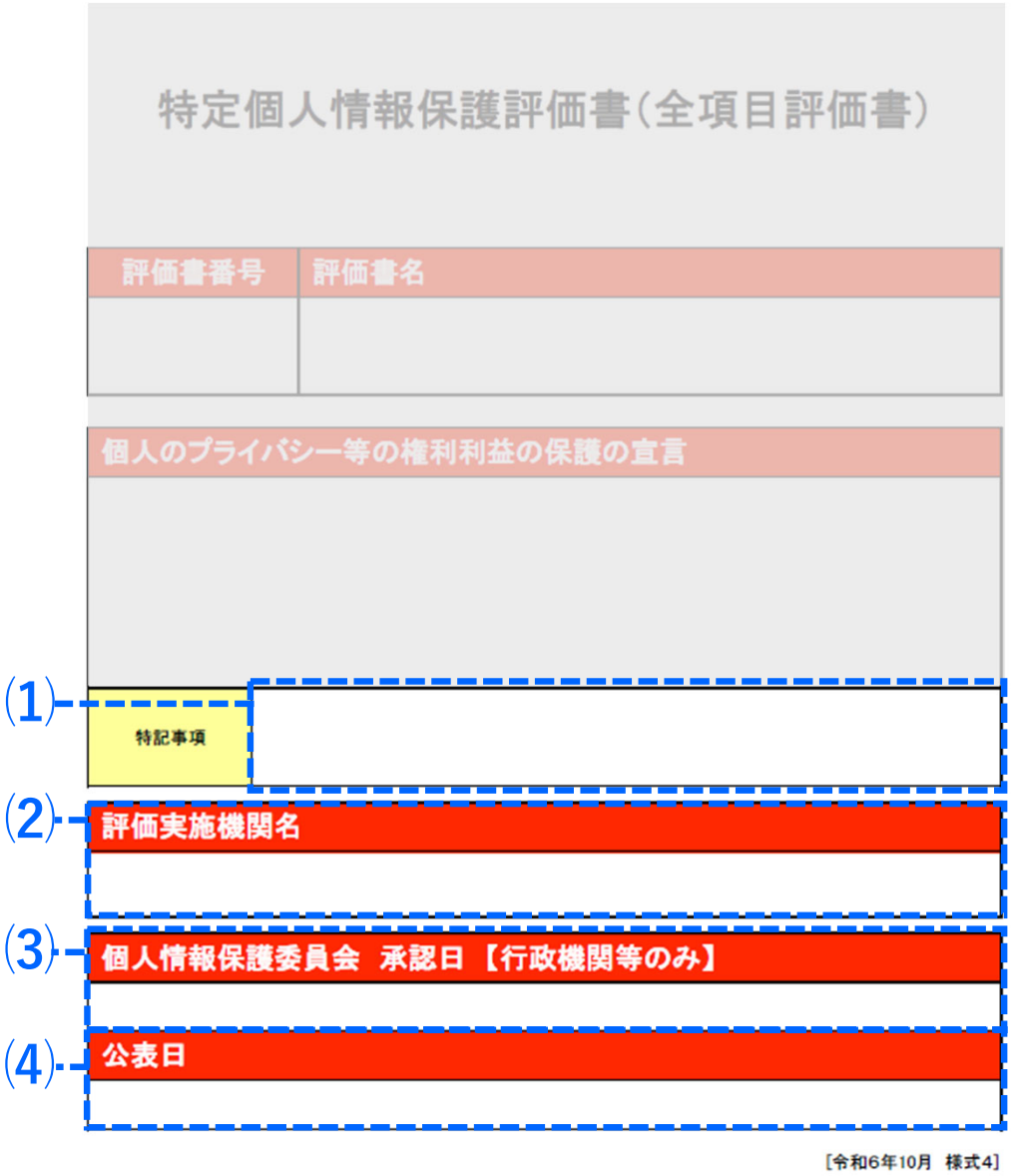
この記載要領は、令和６年５月27日公布の特定個人情報保護評価指針（以下「指針」という。）に沿ったものです。今後、個人情報保護委員会事務局により改訂される可能性があることに御留意ください。



(1)	○　評価書番号は、特定個人情報保護評価計画管理書（以下「計画管理書」という。）の「評価書番号」欄に記載する番号と同じものを記載してください。
(2)	○　評価書名には、特定個人情報保護評価（以下「評価」という。）の対象の事務の内容が分かる名称を記載してください。事務やシステムの名称をそのまま用いる必要はなく、実態に応じて、評価書の内容を推察できる名称としてください。 ○　評価は、原則として、法令上の事務（番号法別表に掲げる事務）を単位として実施するものですが、評価実施機関のシステムや事務の執行状況等によっては、別表の項ごとでは評価書の記載が困難な場合や、別表の複数の項をまとめて記載した方が分かりやすい場合などが考えられるため、評価実施機関の判断で、別表の事務を分割又は統合した事務を単位に、１つの評価書を作成することを可能としています。 ○　評価対象の事務の実施をやめるなどした場合は、評価書名に続けて事務の実施をやめるなどした日を【●年●月●日終了】と記載してください。事務の実施をやめるなどした日から少なくとも３年間は評価書を公表する必要があります。
(3)	○　評価の結果、評価対象の事務において、特定個人情報ファイルの取扱いに際し、個人のプライバシー等の権利利益に影響を与え得る特定個人情報の漏えいその他の事態を発生させるリスクを認識し、このようなリスクを軽減するための適切な措置を講じていることを確認の上、宣言してください。



(1)	○　評価対象の事務において評価実施機関が実施しているリスク対策のうち、特に力を入れて取り組んでいること等、特記して一般に向けて積極的に情報提供したいものがある場合は、記載してください。特記すべきものがなければ、「なし」又は無記入で構いません。
(2)	○　評価書を提出する評価実施機関の名称を記載してください（例：●●大臣、 ●●庁長官、 ●●県知事、 ●●市長、 ●●市教育委員会、独立行政法人●●等）。 【☆行政機関にとっては事前通知事項です（個人情報保護法第74条第１項第２号）。】 ○　評価実施機関（評価対象の事務について評価の実施が義務付けられる者）が複数存在する場合は、取りまとめの評価実施機関が評価書を作成・提出するとともに、「Ⅰ６．他の評価実施機関」に取りまとめ以外の全ての評価実施機関の名称を記載してください。
(3)	○　評価書を個人情報保護委員会（以下「委員会」という。）が承認した日を記載してください。承認日は委員会から通知されます。 ○　委員会による審査・承認のために評価書を提出する時点では空欄のままで提出し、委員会から通知を受けた後、公表する前に記載してください。
(4)	○　行政機関等は、評価の実施・再実施に伴い委員会による審査・承認のために評価書を提出する時点では空欄のままで提出し、委員会の承認を受けた後、公表する前に記載してください。修正に伴う場合は、評価書を委員会に提出するときに、公表する日を記載してください。 ○　地方公共団体等は、評価の実施・再実施又は修正に伴い評価書を委員会に提出するときに、公表する日を記載してください。 ○　評価書の記載内容は、原則として、公表日時点のものとしてください。事前評価という評価の性質上、公表日時点での想定に基づいて記載することになります。

Ⅰ　基本情報

1. 特定個人情報ファイルを取り扱う事務

(1) ①事務の名称

(2) ②事務の内容 ※

(3) ③対象人数 [　　]

＜選択肢＞
1) 1,000人未満　2) 1,000人以上1万人未満
3) 1万人以上10万人未満　4) 10万人以上30万人未満
5) 30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム

システム1

①システムの名称

②システムの機能

③他のシステムとの接続

[　]情報提供ネットワークシステム　[　]庁内連携システム
[　]住民基本台帳ネットワークシステム　[　]既存住民基本台帳システム
[　]宛名システム等　[　]税務システム
[　]その他　（　　）

システム2～5

システム6～10

システム11～15

システム16～20

○　Ⅰは、評価対象の事務の全体像を把握するために記載するものです。
○　様式中に※が付されている各項目への変更は、重要な変更に該当するため、変更する前に評価を再実施する必要があります。ただし、これらの項目の変更であっても、個人のプライバシー等の権利利益に影響を与え得る特定個人情報の漏えいその他の事態を発生させるリスクを相当程度変動させるものではないと考えられる変更又は当該リスクを明らかに軽減させる変更の場合は、重要な変更には当たらないため再実施する必要はありません。

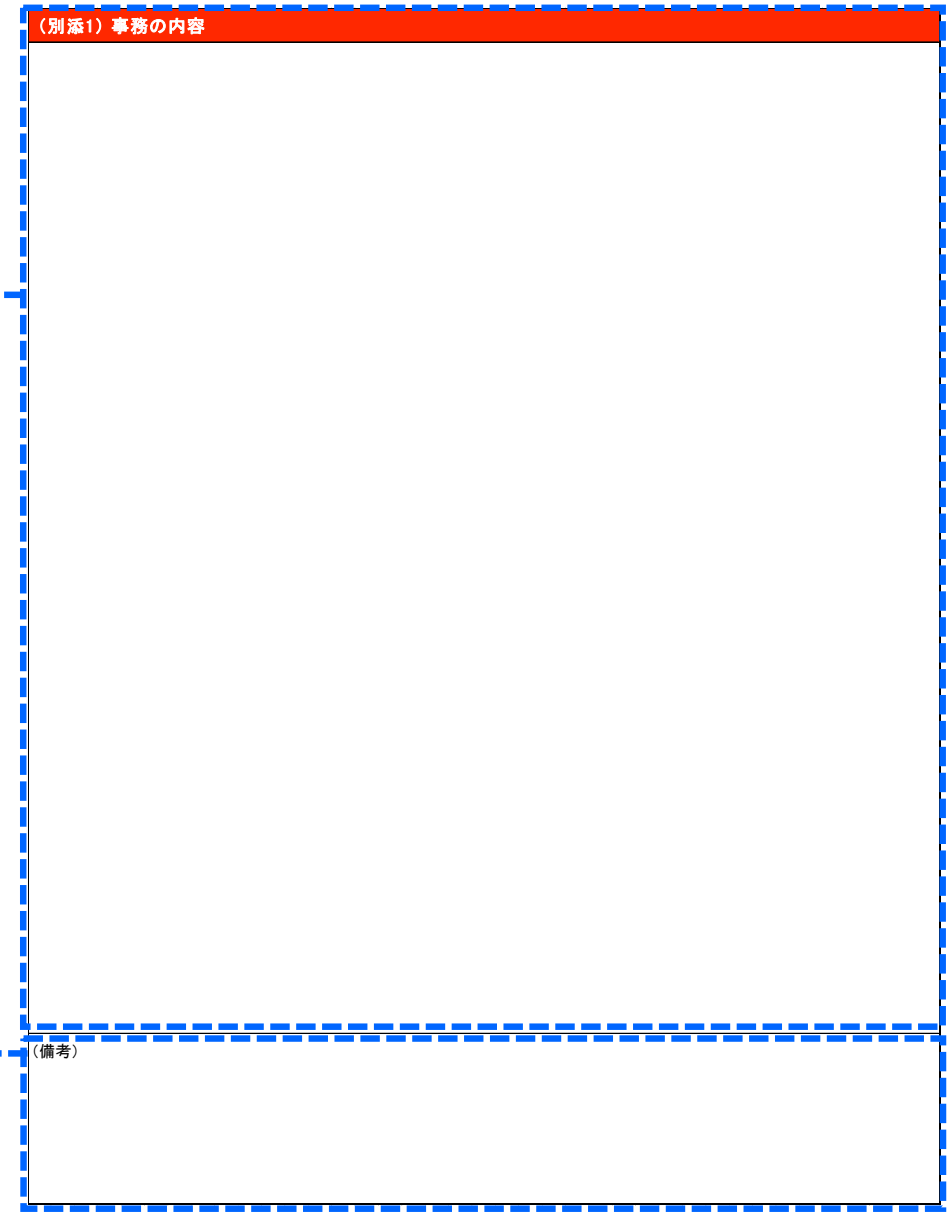
(1)	○　評価対象の事務の名称を記載してください。計画管理書の「事務の名称」欄に記載する名称と同じものを記載してください。
(2)	○　評価対象の事務全体の概要及びその中で特定個人情報ファイルを使用して実施する事務の具体的な内容を記載してください。 ○　さらに、特定個人情報の流れが分かる事務フロー図を別添１に記載してください。 ※　文字数により、セルの表示に収まりきらない（文字が見切れてしまう）場合については、「別添●●を参照。」などと記載の上、当該項目の内容がわかる資料を作成し、評価書の添付資料として併せて提出・公表するなどしてください（以下全ての項目について、同じです。）。
(3)	○　評価対象の事務の対象人数を選んでください。基礎項目評価書の「Ⅱ　1．対象人数」欄と同じものを選択してください。ただし、評価の実施が義務付けられない事務で、任意で評価を行う場合、基礎項目評価書の「1,000人未満(任意実施）」ではなく、評価を行う事務の対象人数を選択してください。

(1)	○　評価対象の事務において使用するシステムの名称を記載してください。計画管理書の「システムの名称」欄に記載する名称と同じものを記載してください。
(2)	○　このシステムが実現する機能の名称とその概要を記載してください。
(3)	○　このシステムと接続して情報（特定個人情報に限らない。）をやりとりするシステムを全て選択してください（目視、紙又は電子記録媒体を介したやりとりは含まない。）。「その他」を選択する場合はシステムの名称を記載してください。 ○　宛名システム等とは、個人番号と既存の内部番号（宛名番号）の対照テーブルなどを用い複数の事務で個人番号を共通して参照するシステムであり、例えば、地方公共団体における団体内統合宛名システムのことです。
(4)	○　評価対象の事務において複数のシステムを使用する場合は、システム２～20の記載欄を「再表示」することにより、その事務を実施する上でのシステムの重要性の順に、それぞれのシステムについて同様に記載してください。 ○　評価対象の事務において使用するシステムの数が21以上の場合は、評価書にはシステム20まで記載し、残りのシステムについて同様に記載した添付資料を併せて提出・公表してください。

(1)	○　評価対象の事務において取り扱う特定個人情報ファイルの名称を記載してください。正式な名称がない場合は、主な記録項目、事務を実施する上での使用目的等に基づく名称を作成し、記載してください。データベース名などでも構いませんが、特定個人情報ファイルの内容を推察できる名称としてください。【☆行政機関にとっては事前通知事項です（個人情報保護法第74条第１項第１号）。】 ○　複数の特定個人情報ファイルを取り扱う場合は、全ての特定個人情報ファイルの名称を記載してください。その際、各特定個人情報ファイルの名称の前に「１．２．３．・・・」と通し番号を付してください。II、IIIのそれぞれ「１．特定個人情報ファイル名」において、そのシートで記載する特定個人情報ファイルの名称を記載する際に、この通し番号とともに記載してください。 ○　特定個人情報ファイルの保有をやめた場合又は対象人数が1,000人未満となった場合は、特定個人情報ファイル名に続けて、保有をやめた場合は【●年●月●日　保有終了】、1,000人未満となった場合は【●年●月●日　対象人数1,000人未満となる】と記載してください。【☆行政機関にとっては事前通知事項です（個人情報保護法第74条第３項）。】
(2)	○　特定個人情報ファイルを取り扱うことが評価対象の事務を実施する上で必要であることを、具体的な事務の流れに即して説明してください。 ○　複数の特定個人情報ファイルを取り扱う場合は、必要に応じて、それぞれの特定個人情報ファイルについて記載してください。
(3)	○　評価対象の事務において特定個人情報ファイルを取り扱うことにより、期待されるメリットについて幅広く記載してください。 ○　複数の特定個人情報ファイルを取り扱う場合は、必要に応じて、それぞれの特定個人情報ファイルについて記載してください。

(1)	○　評価対象の事務において個人番号を利用する法令上の根拠を記載してください。番号法別表の事務については、別表の項の番号を記載してください（主務省令の名称及び条項を記載する必要はありません。）。別表以外の番号法の規定、住民基本台帳法第７条等の番号法以外の国の法令の規定又は番号法第９条第２項に基づく条例の規定を根拠とする場合は、法令名及び条項を記載してください。評価実施時に条例が制定されていない場合には、「○○に関する条例案」等と記載しても構いません。条例制定後、必要に応じて、評価書の修正又は評価の再実施を行ってください。

(2)	○　情報提供ネットワークシステムによる情報連携を実施するか否かを選択してください。主務省令が制定されていない等の理由により、評価実施時点で情報連携を実施するか否かを決定できない場合は、「未定」を選択し、決定した後に評価の再実施又は評価書の修正を行い、再度提出・公表してください。
(3)	○　法令上の根拠には、情報提供ネットワークシステムによる情報連携ができる根拠規定を記載してください。根拠規定の記載について、番号法第19条第８号に基づく情報連携を行う場合は、利用特定個人情報省令第２条の表の項の番号を記載してください（主務省令の正式名称及び第３条以降の条項を記載する必要はありません。）。条例に基づく独自事務について情報連携を行う場合は、番号法第19条第９号と記載してください。 ［例］番号法第19条第8号に基づく主務省令第２条の表○○○の項 ※　情報提供ネットワークシステムを通じた利用特定個人情報の提供ができる根拠規定及び照会ができる根拠規定を区別して記載してください。
(4)	○　評価の実施を担当する部署の名称及び所属長の役職名を記載してください。部署については、計画管理書の「担当部署」欄に記載する部署名と同じものを記載してください。 ○　（計画管理書の表紙に記載した）評価実施機関において実施する評価に関連する全ての事務の取りまとめを担当する部署ではなく、評価対象の事務に知見を有し、実際に評価を実施する部署です。複数の部署が共同で評価を実施する場合は、複数の部署の名称、所属長の役職名を記載してください。
(5)	○　評価実施機関（評価対象の事務について評価の実施が義務付けられる者）が複数存在し、取りまとめの評価実施機関が評価書を作成・提出する場合に、取りまとめ以外の全ての評価実施機関の名称を記載してください。



(1)	○　直接入力はせず、表計算ソフトウェアその他の事務処理で用いられる一般的なソフトウェアを用いて作成した事務フロー図を、オブジェクト・図として貼り付けてください。なお、マイナンバー保護評価システムの評価書の提出の際にエラーが発生する場合は、事務フロー図に隠れるように文字を入力してください。 ○　評価対象の事務について、以下の点に注意しながら事務フローを図示してください。 ・・・事務に関わる者（事務担当部署、委託先、転入者・受給者・入居者といった国民・住民等）、事務において使用するシステム、事務において取り扱う情報（特定個人情報に限らない。）の流れを明記してください。その際、色を変えるなどして特定個人情報の流れとそれ以外の情報の流れを区別してください。 ・・・事務の流れが分かるように、事象が起きる順に番号を付けるなどして記載してください（例．①入居申込、②収入要件確認など）。 ※　事務に複数の行政手続がある場合で、当該手続ごとに別添１を複数作成する場合等は、マイナンバー保護評価システムでの提出時のエラーを防ぐため、このExcel内でシートのコピーをせずに、別途資料を作成し、評価書の添付資料として併せて提出・公表するなどしてください。
(2)	○　事務フロー図に関連して補足することがあれば、記載してください。

Ⅱ　特定個人情報ファイルの概要

(1)

1. 特定個人情報ファイル名

2. 基本情報

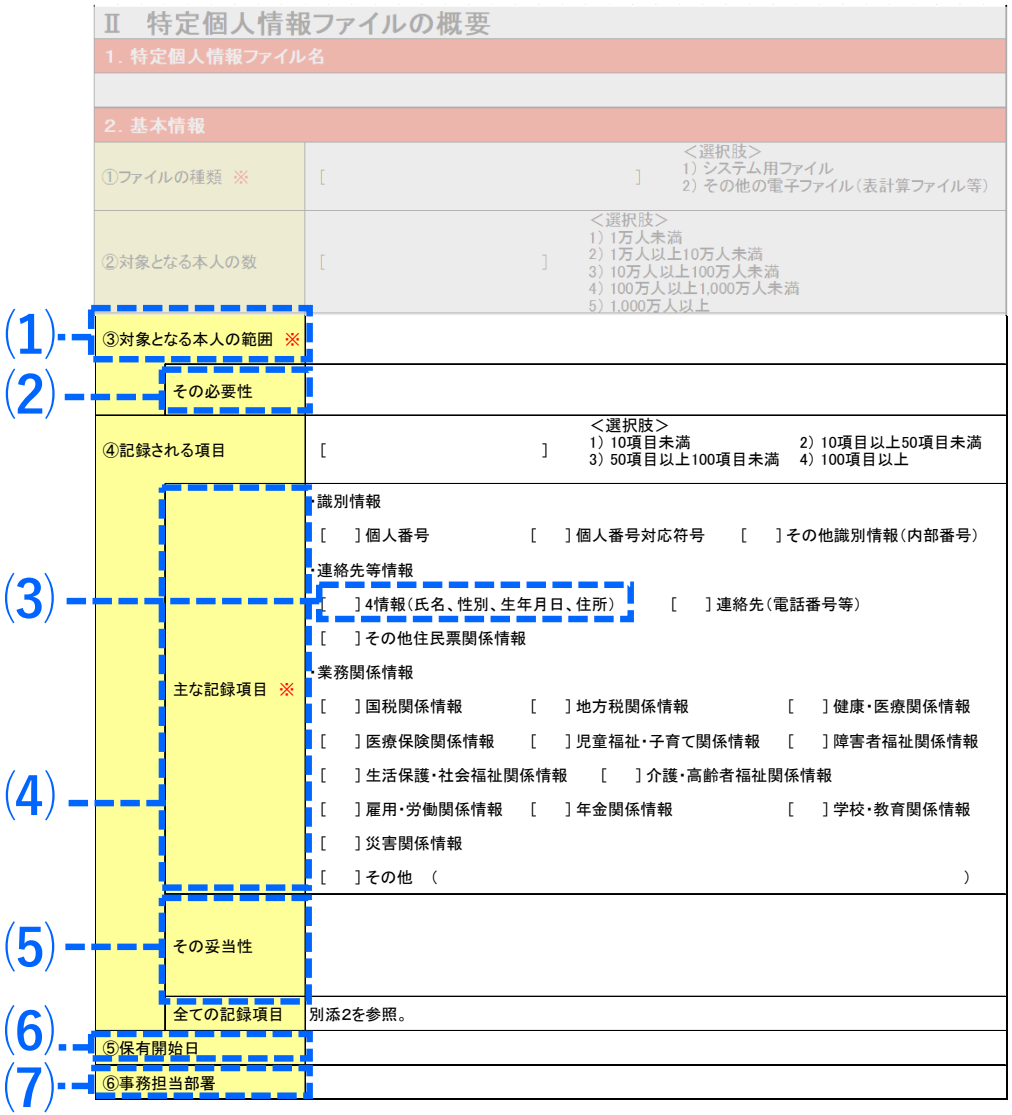
(2) ①ファイルの種類 ※	[　　] <選択肢> 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
(3) ②対象となる本人の数	[　　] <選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※	
その必要性	
④記録される項目	[　　] <選択肢> 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
主な記録項目 ※	・識別情報 [　]個人番号　[　]個人番号対応符号　[　]その他識別情報（内部番号） ・連絡先等情報 [　]4情報（氏名、性別、生年月日、住所）　[　]連絡先（電話番号等） [　]その他住民票関係情報 ・業務関係情報 [　]国税関係情報　[　]地方税関係情報　[　]健康・医療関係情報 [　]医療保険関係情報　[　]児童福祉・子育て関係情報　[　]障害者福祉関係情報 [　]生活保護・社会福祉関係情報　[　]介護・高齢者福祉関係情報 [　]雇用・労働関係情報　[　]年金関係情報　[　]学校・教育関係情報 [　]災害関係情報 [　]その他　（　　）
その妥当性	
全ての記録項目	別添2を参照。
⑤保有開始日	
⑥事務担当部署	

○　Ⅱは、評価対象の事務において取り扱う特定個人情報ファイルの内容と、その取扱いプロセスを把握するためのものです。これにより、対象人数が多い、記録項目が多い、使用者数が多い、特定個人情報ファイルの取扱いを委託・再委託している、保管期間が長い等、特定個人情報ファイルの特徴を把握することができ、それを踏まえて、Ⅲ において特定個人情報ファイルの取扱いプロセスにおけるリスク対策について検討することになります。

○　様式中に※が付されている各項目への変更は、重要な変更に該当するため、変更する前に評価を再実施する必要があります。ただし、これらの項目の変更であっても、リスクを相当程度変動させるものではないと考えられる変更又はリスクを明らかに軽減させる変更の場合は、再実施する必要はありません。（Ⅱ.2.③を除く）

○　評価対象の事務において複数の特定個人情報ファイルを取り扱う場合は、このシートをコピーして、全ての特定個人情報ファイルについてそれぞれ記載してください（１つの特定個人情報ファイルにつき１シートで記載してください。）。

(1)	○　このシートで記載する特定個人情報ファイルの名称を記載してください。 ○　その際、「Ⅰ　3．特定個人情報ファイル名」で記載した通し番号とともに記載してください。
(2)	○　手作業処理ファイルについて任意で記載する場合は、このExcelファイルには1又は2の選択肢を記載の上で提出し、公表用のPDFファイルを直接編集して、「手作業処理ファイル」とした上で、公表する必要があります。
(3)	○　特定個人情報ファイルの対象となる本人の数を選択してください。事務の対象人数とは異なります。



(1)	○　特定個人情報ファイルの対象となる本人の範囲について記載してください。 ○　特定個人情報ファイルに記録された者の一部についてのみ個人番号を保有し（例：契約者ファイルのうち一部の者についてのみ個人番号を保有する場合）、個人情報の対象となる本人の範囲と特定個人情報の対象となる本人の範囲が異なる場合は、それぞれ記載してください。【☆行政機関にとっては事前通知事項です（個人情報保護法第74条第１項第４号）。】
(2)	○　上記の範囲の本人の特定個人情報を特定個人情報ファイルにおいて保有することが事務を実施する上で必要な理由を記載してください。「法令に基づく」といった形式的な理由ではなく、評価対象の事務の内容に即して、実質的・具体的に記載してください。
(3)	○　４情報のうち記録しない項目がある場合は、「その妥当性」の欄にその旨を記載してください。 ※　なお、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等の一部を改正する法律（令和５年法律第48号）附則第１条第３号に掲げる規定の施行日以降は、様式中「４情報（氏名、性別、生年月日、住所）」が「５情報（氏名、氏名の振り仮名、性別、生年月日、住所）」に改正されます。
(4)	○　特定個人情報ファイルに記録される情報について、該当するものを全て選択してください。 ○　主な記録項目のうち「業務関係情報」とは、評価対象の事務を実施していく上での主たる情報です。例示されているものに該当しない場合は、「その他」を選択し、情報の内容を表す簡潔な名称を作成し、記載してください。
(5)	○　主な記録項目欄で選択した全ての情報について、保有する理由をそれぞれ記載してください。
(6)	○　行政機関においては、特定個人情報ファイルの保有開始日の年月日を記載してください。行政機関以外の評価実施機関の場合は、具体的な日が確定していなければ月単位の記載で構いません。 ○　特定個人情報ファイルの取扱いの重要な変更に先立って評価を再実施する時は、保有開始日に加えて、重要な変更の実施予定日を記載してください。 【☆行政機関にとっては保有開始日・重要な変更の実施予定日は事前通知事項です（個人情報保護法第74条第１項第11号・施行令第20条第1項第１号・第２号）。】
(7)	○　特定個人情報ファイルを取り扱う事務を所掌する課室等の名称を記載してください。行政機関においては、特定個人情報ファイルを保有しようとする者又は保有する者が複数存在する場合は、全ての評価実施機関における事務担当部署を記載してください。【☆行政機関にとっては事前通知事項です（個人情報保護法第74条第１項第２号）。】

(1)	○　特定個人情報ファイルに記録される特定個人情報をどこから入手するか該当するものを全て選択してください。【☆行政機関にとっては事前通知事項です（個人情報保護法第74条第１項第５号）。】 ○　評価実施機関内の他部署から個人情報として入手し、評価対象の事務の実施において個人番号と結び付き特定個人情報となる場合（特定個人情報の移転）も記載してください。なお、個人番号と結び付く個人情報の入手が移転によらない場合について、記載することを妨げるものではありません（以下、特定個人情報の入手に関する項目について同じ。）。
(2)	○　特定個人情報をどのように入手するか該当するものを全て選択してください。【☆行政機関にとっては事前通知事項です（個人情報保護法第74条第１項第５号）。】
(3)	○　特定個人情報を定期的に入手する場合は、「年１回、３月上旬」などと時期・頻度を記載してください。 ○　個別的な対応に際して入手する場合は、「申請を受けた都度」などと記載してください。再実施・評価書の修正の際には、「１年間に約○回」といった形で入手実績の概数を記載してください（１回に１人の情報を入手した場合も１回、１万人の情報を入手した場合も１回とします。）。 ○　特定個人情報を複数の入手元又は入手方法で入手している場合は、それぞれについて記載してください。
(4)	○　この入手方法、時期・頻度とした理由を記載してください。 ○　本人から入手する場合は、他の事務（評価実施機関内の他の部署が実施している事務も含みます。）で既に同一の情報を本人から入手していないか確認し、既に入手している場合は当該他の事務の担当部署から入手することができない理由を記載してください。
(5)	○　特定個人情報の入手の事実及び使用目的が本人にどのように示されているか記載してください。 ○　評価実施機関が本人に直接示していない場合であっても、法令に入手の根拠・使用目的に関する規定がある場合は、法令名及び条項を記載してください。

(1)	○　何のために特定個人情報を使用するか記載してください。【☆行政機関にとっては事前通知事項です（個人情報保護法第74条第１項第３号）。】 ○　番号法第９条第１項及び別表に基づく事務については、別表の文言をコピーするのではなく、より一般的な言葉で分かりやすく記載し、また、できる限り使用目的を特定してください（例えば、「介護保険給付の支給・保険料徴収」ではなく「被保険者資格の管理」「要介護度認定」「保険料賦課」と記載してください。）。
(2)	○　行政機関、独立行政法人等及び地方公共団体等については個人情報保護法第61条第３項、事業者については同法第17条第２項において個人情報の使用目的の変更が認められています。使用目的を変更する場合は、変更前の使用目的とともに、法令上の要件を満たし変更が妥当であることを記載してください。
(3)	○　評価対象の事務のために特定個人情報を使用する評価実施機関内の全ての部署の名称と使用者数（各部署の従業者の総数）を記載してください。委託先、提供先又は移転先の従業者は含みません。
(4)	○　特定個人情報ファイルに記録される情報を他から入手する際にどのような突合を行うか、この特定個人情報ファイルに記録された情報と他の情報をどのように突合するか、また、こうした突合を何のために行うか、具体的に記載してください。その際、上記の使用方法との対応関係を明示してください。
(5)	○　特定個人情報を用いた統計分析を行う場合は、どのような統計分析を行うか具体的に記載してください。
(6)	○　特定個人情報を使用することにより国民の権利利益に影響を与え得る決定（行政処分）を行う場合は、具体的に記載してください。
(7)	※　使用開始日については、日付として正しい入力値（yyyy/mm/dd）以外の入力を制御しています。そのため、正しい入力値以外（例えば、「●●法の施行後２年以内の政令で定める日」などの文字列）での公表が必要な場合は、提出処理の際のExcelファイルは正しい入力値を仮置きで記載したものを登録していただき、公表するＰＤＦファイルを直接編集して、使用開始日を文字列に修正するなどして、対応してください。

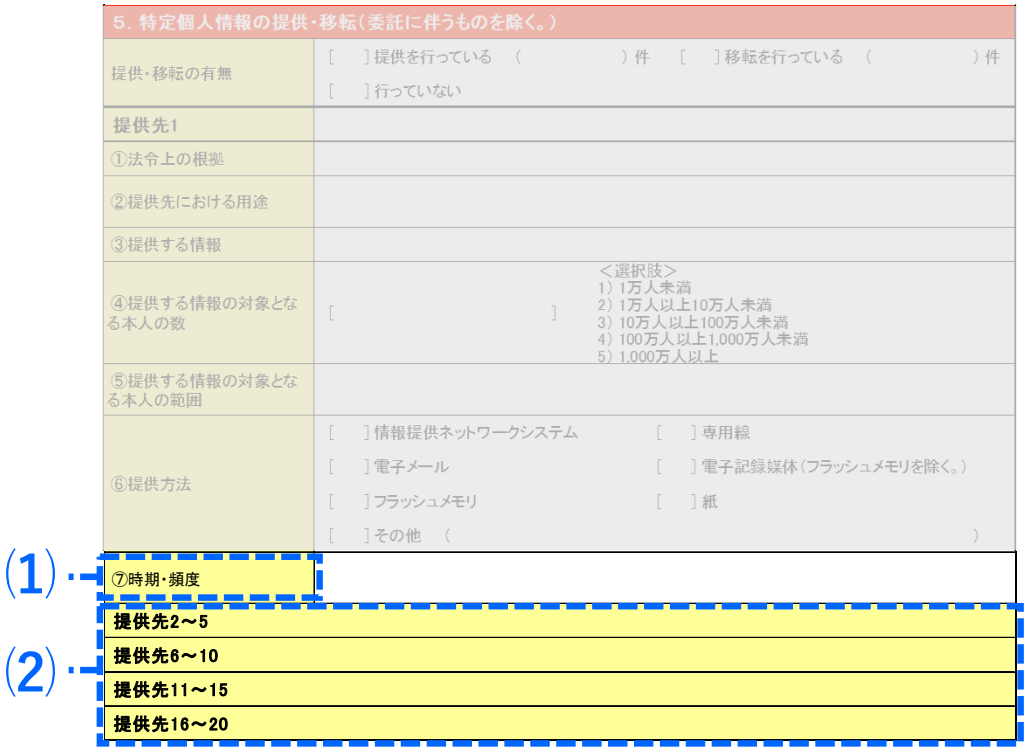
(1)	○　特定個人情報ファイルの取扱いを委託するかどうかを選択してください。 ○　委託する場合は、（委託先単位ではなく）委託事項単位で、件数を記載してください。
(2)	○　特定個人情報ファイルの取扱いを委託する事項（番号法上の委託）の名称を記載してください。正式な名称がない場合は、委託する事項の内容を表す簡潔な名称を作成し、記載してください。
(3)	○　委託先に上記の範囲の特定個人情報ファイルを取り扱わせることが必要な理由を記載してください。
(4)	○　委託先において特定個人情報ファイルを取り扱う者の数（従業者の総数）を選択してください。再委託する場合は、再委託先において特定個人情報ファイルを取り扱う者の数（従業者の総数）も含めて計上してください。
(5)	○　委託先を国民・住民等が確認できるか否か、確認できる場合はどのように確認できるか、確認できない場合はそのような取扱いが評価対象の事務を実施する上で必要な理由を記載してください。
(6)	○　委託先の名称を記載してください。【☆行政機関にとっては事前通知事項です（個人情報保護法第74条第１項第７号）。】 ○　委託契約の調達前であるなどの理由で、委託先事業者が未定である場合は、その旨を記入し、委託先が決定次第、速やかに評価書を修正し、提出・公表してください。

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※	[ ] （ ）件	<選択肢> 1）委託する　2）委託しない
委託事項1		
①委託内容		
②取扱いを委託する特定個人情報ファイルの範囲	[ ]	<選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
対象となる本人の数	[ ]	<選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
対象となる本人の範囲 ※		
その妥当性		
③委託先における取扱者数	[ ]	<選択肢> 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法	[ ]専用線　[ ]電子メール　[ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ　[ ]紙 [ ]その他 （ ）	
⑤委託先名の確認方法		
⑥委託先名		
再委託 ⑦再委託の有無 ※	[ ]	<選択肢> 1）再委託する　2）再委託しない
再委託 ⑧再委託の許諾方法		
再委託 ⑨再委託事項		
委託事項2～5		
委託事項6～10		
委託事項11～15		
委託事項16～20		

(1)	○　特定個人情報ファイルの取扱いを再委託するかどうかを選択してください。再委託しない場合は、⑧及び⑨を記載する必要はありません。 ○　現状では再委託を実施していない場合でも、今後、委託業者の繁忙や人的リソースの状況によって、再委託を行う可能性がある場合は、「再委託する」を選択してください。また、契約書の再委託条項等において、再委託ができる旨を規定しておく必要がありますので、御注意ください。
(2)	○　特定個人情報ファイルの取扱いを再委託するに当たって、どのような手続・方法によるかを記載してください。 ○　原則として再委託をしないこととしている場合は、その旨を記載してください。 ○　また、再委託を行う場合（可能性がある場合も含む。）は、番号法第10条等の観点から、再委託をする際に、事前許諾を行う方法、再委託先において特定個人情報の適切な安全管理措置が図られることを確認すること、再委託先の監督を行うこと等についても記載してください。 ○　評価実施機関が再委託を許諾する場合は、その判断基準について記載してください。
(3)	○　特定個人情報ファイルの取扱いを委託する事項が複数ある場合は、委託事項2～20の記載欄を「再表示」することにより、①再委託しているもの、②取扱いを委託する特定個人情報ファイルの対象となる本人の数、③委託先における取扱者数の多い順に、それぞれの委託事項について同様に記載してください。 ○　評価対象の事務において、特定個人情報ファイルの取扱いを委託する事項の数が21以上の場合は、この評価書には委託事項20まで記載し、残りの委託事項について同様に記載した添付資料を併せて提出してください。

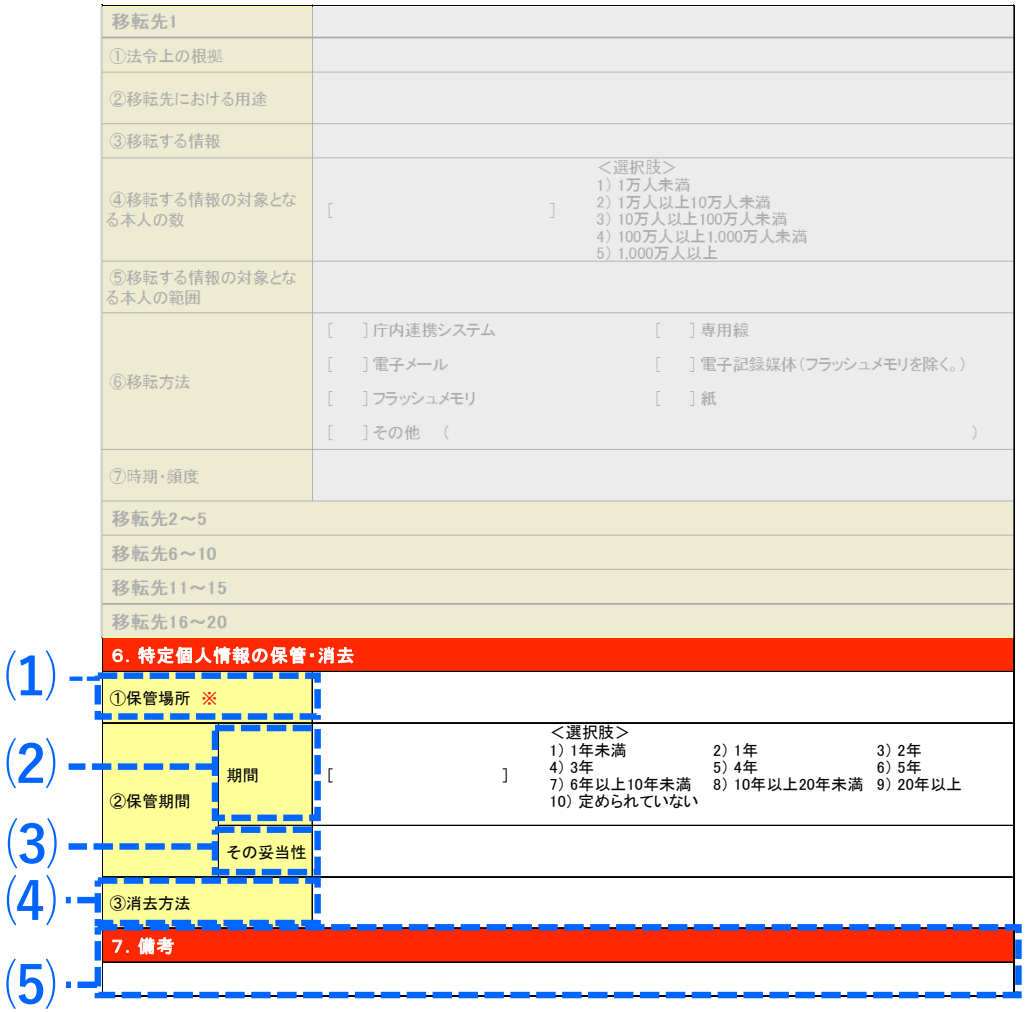
5. 特定個人情報の提供・移転（委託に伴うものを除く。）	
(1) 提供・移転の有無	[　]提供を行っている　（　　）件　[　]移転を行っている　（　　）件 [　]行っていない
(2) 提供先1	
(3) ①法令上の根拠	
(4) ②提供先における用途	
③提供する情報	
④提供する情報の対象となる本人の数	[　　]　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	
⑥提供方法	[　]情報提供ネットワークシステム　[　]専用線 [　]電子メール　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　[　]紙 [　]その他　（　　）
⑦時期・頻度	
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	

(1)	○　特定個人情報の評価実施機関外への提供又は評価実施機関内の他部署への移転を行うかどうかを選択してください。 ○　提供又は移転する場合は、提供先又は移転先単位で、それぞれ件数を記載してください。
(2)	○　特定個人情報の提供先を記載してください。【☆行政機関にとっては事前通知事項です（個人情報保護法第74条第１項第７号）。】 ○　特定個人情報の提供としては、番号法第19条各号で定められているものが想定されます。具体的には同条第８号の規定に基づき情報提供ネットワークシステムを使用して提供する場合、同条第11号に基づく条例に基づき、地方公共団体の機関が当該地方公共団体の他の機関に提供する場合等です。 ○　情報提供ネットワークシステムを使用して提供する場合は、利用特定個人情報提供省令（※）第２条の表の第一欄に掲げる者、例えば、「厚生労働大臣」「都道府県知事」「市町村長」「健康保険組合」を提供先として記載してください。ただし、提供の根拠となる同表の項が異なる場合は、提供先の名称が同じであっても、別々の提供先として記載してください（例えば、同表の11の項と20の項はいずれも市町村長が都道府県知事に地方税関係情報又は住民票関係情報を提供すると定めており、「提供先」はいずれも「都道府県知事」ですが、法令上の根拠が異なるため一方を提供先1、他方を提供先2として記載してください。）。 ※　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第十九条第八号に基づく利用特定個人情報の提供に関する命令（令和６年デジタル庁・総務省令第９号）をいう。以下同じ。
(3)	○　評価実施時に条例が制定されていない場合には、「●●に関する条例案」等と記載しても構いません。条例制定後、必要に応じて、評価書の修正又は再実施を行ってください。
(4)	○　提供した特定個人情報が、提供先において、いかなる目的で、どのように使用されることになるか、記載してください。



(1)	○　過去の実績から経常的に提供することが想定される場合は、その時期・頻度を記載してください。経常的に提供することが想定されない場合は、「照会を受けたら都度」と記載してください。 ○　再実施・評価書の修正の際には、「１年間に約●回」といった形で提供実績の概数を記載してください（１回に１人の情報を提供した場合も１回、１万人の情報を提供した場合も１回とします。）。
(2)	○　特定個人情報の提供先が複数ある場合は、提供先２～20の記載欄を「再表示」することにより、①提供する情報の対象となる本人の数、②提供の頻度の多い順に、それぞれの提供先について同様に記載してください。 ○　評価対象の事務において、特定個人情報の提供先の数が21以上の場合は、この評価書には提供先20まで記載し、残りの提供先について同様に記載した添付資料を併せて提出してください。

(1)	○　特定個人情報の移転先（評価実施機関内でこの評価書の評価対象の事務以外の事務を実施する部署）の名称を記載してください。【☆行政機関にとっては事前通知事項です（個人情報保護法第74条第１項第７号）。】
(2)	○　特定個人情報を移転する法令上の根拠を記載してください。番号法第９条第２項や条例が想定されます。評価実施時に条例が制定されていない場合には、「●●に関する条例案」等と記載しても構いません。条例制定後、必要に応じて、評価書の修正又は評価の再実施を行ってください。
(3)	○　移転した特定個人情報が、移転先において、いかなる目的で、どのように使用されることになるか、記載してください。
(4)	○　過去の実績から経常的に移転することが想定される場合は、その時期・頻度を記載してください。経常的に移転することが想定されない場合は、「照会を受けたら都度」と記載してください。 ○　再実施・評価書の修正の際には、「１年間に約●回」といった形で移転実績の概数を記載してください（１回に１人の情報を移転した場合も１回、１万人の情報を移転した場合も１回とします。）。
(5)	○　全ての移転先を記載することが困難な場合は、これまでの経緯を踏まえ、今後も経常的に移転することが予想されるものに限って記載しても構いません。 ○　特定個人情報の移転先が複数ある場合は、移転先2～20の記載欄を「再表示」することにより、①移転する情報の対象となる本人の数、②移転の頻度の多い順に、それぞれの移転先について同様に記載してください。 ○　評価対象の事務において、特定個人情報の移転先の数が21以上の場合は、この評価書には移転先20まで記載し、残りの移転先について同様に記載した添付資料を併せて提出してください。



(1)	○　特定個人情報の保管場所の態様及び保管場所への立入制限・アクセス制限について記載してください。 ○　クラウドサービスを利用する場合は、評価実施機関がクラウドサービス事業者の特定個人情報の保管場所の態様等について、詳細を把握することが困難だと思われますので、クラウドサービス選定時に用いている基準等を利用して記載することが考えられます。例えば、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等に定められた諸条件や「特定個人情報の適正な取扱いに関するガイドライン」等に定められた各種条件を満たしていること等を記載することが考えられます。
(2)	○　定めている特定個人情報ファイルの保管期間を記載してください。
(3)	○　上記の期間、保管することが妥当である理由を記載してください。
(4)	○　保管期間を経過した特定個人情報を消去する方法を記載してください。 ○　特定個人情報の消去を適切に行うために、実施することを記載してください。例えば、特定個人情報が記録された機器及び電子記録媒体等の消去・廃棄の方法や消去・廃棄の記録をとること等について、記載することが考えられます。また、これらの消去・廃棄を委託する場合には、委託先が消去・廃棄をしたことを確認する方法等について、記載することが考えられます。 ○　クラウドサービスを利用する場合は、特定個人情報の適切な消去について、評価実施機関が詳細を把握することが困難だと思われますので、第三者の監査機関による監査報告書等のレポートを利用し、廃棄・消去に係るプロセスを確認し、その内容を把握すること等を記載することが考えられます。 ○　既存システムからクラウドサービスへ移行する際は、既存のシステム環境に保管されていた特定個人情報の消去や機器の廃棄、クラウドサービス事業者における特定個人情報の消去等についての記載に留意が必要です。
(5)	○　上記以外にこの特定個人情報ファイルの取扱いに関して記載したい事項があれば、記載してください。

（別添2）特定個人情報ファイル記録項目

(1)

(1)	○　「Ⅱ　2．④主な記録項目」欄において選択・記載したものを含め、この特定個人情報ファイルに記録される全ての記録項目を記載してください。【☆行政機関にとっては事前通知事項です（個人情報保護法第74条第１項第４号）。】 ○　なお、記録項目をオブジェクト・画像として貼り付けたり、テキストボックスを利用したりする場合において、保護評価システムの評価書の提出の際にエラーが発生する場合は、画像等に隠れるように文字を入力してください。 ○　記録項目を記載する目的は、特定個人情報ファイルの内容を明らかにすることです。そのため、データベース内の項目名をそのまま記載しなければならないわけではなく、例えば、本人等から入手する情報を基に記録される項目とバッチ処理等のシステム処理のために用いる記録項目があると思われますが、前者の記録項目を分かりやすく記載することが考えられます。 ○　記録項目に要配慮個人情報が含まれるときは、その旨を記載してください。【☆行政機関にとっては事前通知事項です（個人情報保護法第74条第１項第６号）。】 ○　特定個人情報ファイルの種類がその他の電子ファイルであって、記録項目を個別具体的に事前に特定することが困難であるなど特段の事情がある場合には、具体的な項目を記載することまでは必ずしも求められませんが、特定個人情報ファイルに記録される情報の種類・内容等が分かるよう、できる限り具体的に記載することが求められます。 ※　文字数により、セルの表示に収まりきらない（文字が見切れてしまう）場合や、特定個人情報ファイルごとに記載を分けたい場合等は、マイナンバー保護評価システムでの提出時のエラーを防ぐため、この様式内でシートのコピーをせずに、別途資料を作成し、評価書の添付資料として併せて提出・公表するなどしてください。

(1)

Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※(7．リスク1⑨を除く。)

1．特定個人情報ファイル名

2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）

リスク1：　目的外の入手が行われるリスク		
対象者以外の情報の入手を防止するための措置の内容		
必要な情報以外を入手することを防止するための措置の内容		
その他の措置の内容		
リスクへの対策は十分か	[　　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2：　不適切な方法で入手が行われるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[　　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3：　入手した特定個人情報が不正確であるリスク		
入手の際の本人確認の措置の内容		
個人番号の真正性確認の措置の内容		
特定個人情報の正確性確保の措置の内容		
その他の措置の内容		
リスクへの対策は十分か	[　　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク4：　入手の際に特定個人情報が漏えい・紛失するリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[　　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置		

○　Ⅲは、評価対象の事務における特定個人情報ファイルの取扱いプロセスにおいて想定されるリスクへの対策について記載するものです。Ⅱの記載を踏まえ、例示されている各リスクに具体的にどのように対応しているかを確認することで、十分なリスク対策が実施されているかを検討します。
○　Ⅲ（1．及び7．リスク1⑨を除く。）に記載する内容への変更は、重要な変更に該当するため、変更する前に評価を再実施する必要があります。ただし、これらの項目の変更であっても、リスクを相当程度変動させるものではないと考えられる変更又はリスクを明らかに軽減させる変更の場合は、再実施する必要はありません。
○　評価対象の事務において複数の特定個人情報ファイルを取り扱う場合で、特定個人情報ファイルによってリスク対策が異なるものがある場合は、このシートをコピーしてリスク対策が共通する特定個人情報ファイルごとに、それぞれ記載してください。

(1)	○　このシートで記載する特定個人情報ファイルの名称を記載してください。リスク対策が共通する複数の特定個人情報ファイルについてまとめて記載することができます。その場合は、このシートで記載する全ての特定個人情報ファイルの名称を記載してください。 ○　その際、「Ⅰ　3．特定個人情報ファイル名」で記載した通し番号とともに記載してください。 【この項目の変更は、重要な変更には該当しません。】

Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。）

1．特定個人情報ファイル名

2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）

リスク1：　目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	
必要な情報以外を入手することを防止するための措置の内容	
その他の措置の内容	
リスクへの対策は十分か	[　　] <選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2：　不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[　　] <選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3：　入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	
個人番号の真正性確認の措置の内容	
特定個人情報の正確性確保の措置の内容	
その他の措置の内容	
リスクへの対策は十分か	[　　] <選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク4：　入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[　　] <選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	

■ マイナンバーガイドラインの主な参照箇所及び概要 ■

（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

第4−3−⑷ 収集・保管制限

○ 番号法で限定的に明記された場合を除き、特定個人情報を収集又は保管してはならない。

○ 番号法で限定的に明記された事務を処理する必要がなくなった場合で、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廃棄又は削除しなければならない。

（別添Ⅰ）特定個人情報に関する安全管理措置

2 講ずべき安全管理措置の内容

C 組織的安全管理措置

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し、その記録を一定の期間保存し、定期に及び必要に応じ随時に分析等するための体制を整備する。記録については、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とともに、分析等を行う。

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、次に掲げる項目を含めて記録する。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。

・特定個人情報ファイルの名称
・行政機関等の名称及び特定個人情報ファイルが利用に供される事務をつかさどる組織の名称
・特定個人情報ファイルの利用目的
・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特定個人情報ファイルに記録される個人の範囲
・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

e 取扱状況の把握及び安全管理措置の見直し

○ 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。

○ 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。

D 人的安全管理措置

a 事務取扱担当者の監督

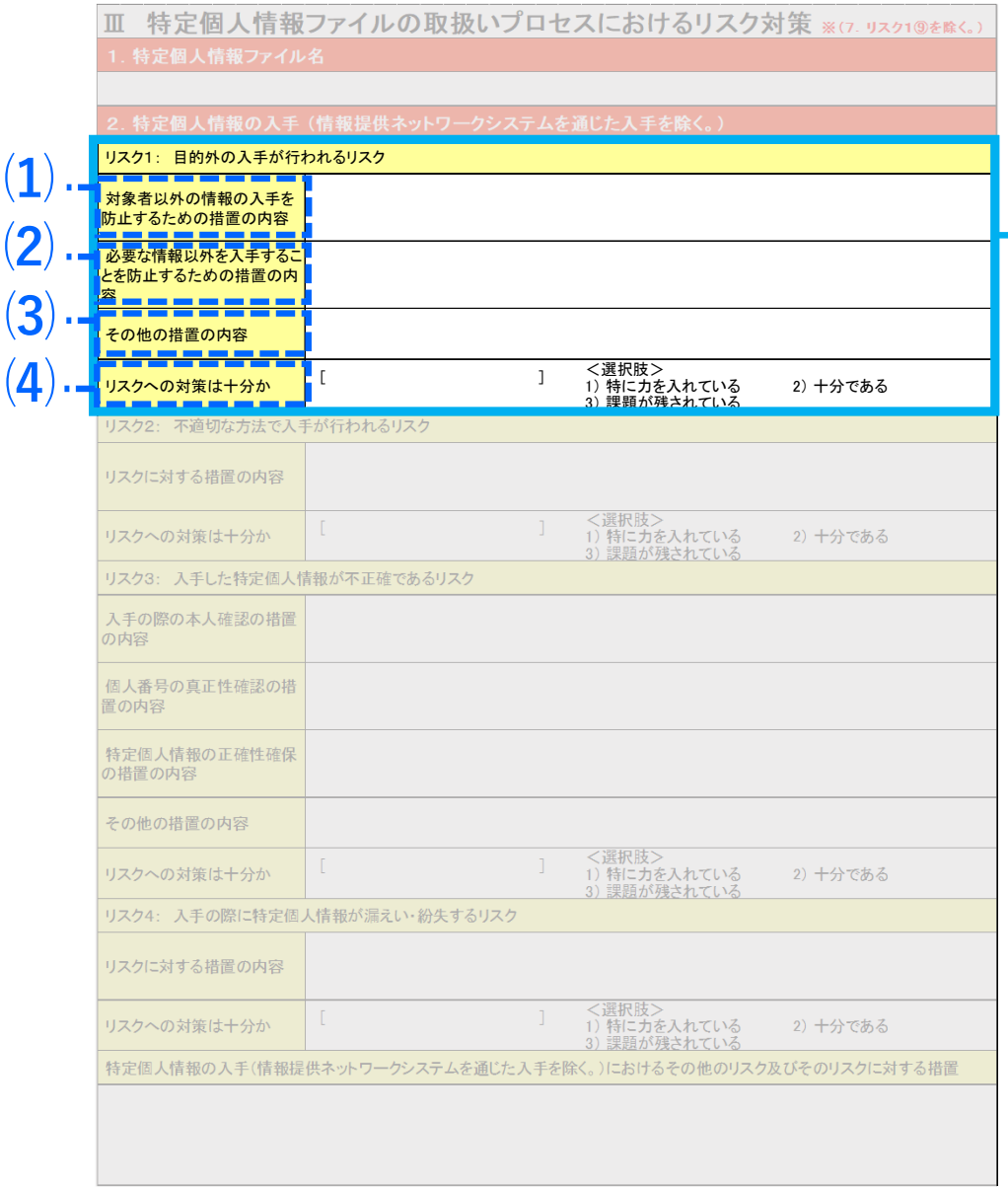
○ 総括責任者及び保護責任者は、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。

b 事務取扱担当者等の教育

○ 保護責任者は、部署内の事務取扱担当者等に特定個人情報の保護に関する必要な教育研修を行う。

・ 事務取扱担当者への教育研修
・ 情報システムの管理に関する事務に従事する職員への教育研修
・ 保護責任者に対する研修
・ 情報システムの管理に関する事務に従事する職員への教育研修
・ 特定個人情報ファイルを取り扱う事務に従事する者への研修
・ サイバーセキュリティに関する研修（具体的内容については、マイナンバーガイドラインを参照すること。）

※ 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。



■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

（別添Ⅰ）特定個人情報に関する安全管理措置
Ⅰ 安全管理措置の検討手順（抄）
A 個人番号を取り扱う事務の範囲の明確化
○ 行政機関等は、個人番号利用事務等の範囲を明確にしておかなければならない。
B 特定個人情報等の範囲の明確化
○ 行政機関等は、Aで明確化した事務において取り扱う特定個人情報等の範囲を明確にしておかなければならない。
C 事務取扱担当者の明確化
○ 行政機関等は、Aで明確化した事務に従事する事務取扱担当者を明確にしておかなければならない。
D･E（略）

2 講ずべき安全管理措置の内容
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して個人番号利用事務等を行う場合、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。

(1)	○ 評価対象の事務を遂行する上で必要な者以外の者の特定個人情報を入手しないよう、どのような対策を行っているか記載してください。
(2)	○ 評価対象の事務を遂行する上で必要な者に関する特定個人情報であっても、その事務を遂行する上で必要なもの以外の特定個人情報を入手しないよう、どのような対策を行っているか記載してください。
(3)	○ 上記で例示する以外に、目的外の特定個人情報の入手が行われるリスクに対応するための措置を講じている場合は、記載してください。
(4)	○ 上記を踏まえ、目的外の入手が行われるリスクに対して、十分な対策を行っていると評価する場合には「十分である」を選択し、十分に行っているとは評価できず、まだ課題が残されていると評価する場合には「課題が残されている」を選択してください。評価実施機関としてこのリスクへの対策に特に積極的に取り組んでいる場合は、「特に力を入れている」を選択してください。

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

第4−3−(5) 本人確認
○ 番号法、番号法施行令、番号法施行規則及び個人番号利用事務実施者（番号法第9条第3項の規定により情報提供用個人識別符号を利用する者を除く。）が認める方法に従い、適切に本人確認を行う（具体的な本人確認の方法については、マイナンバーガイドラインを参照すること。）。

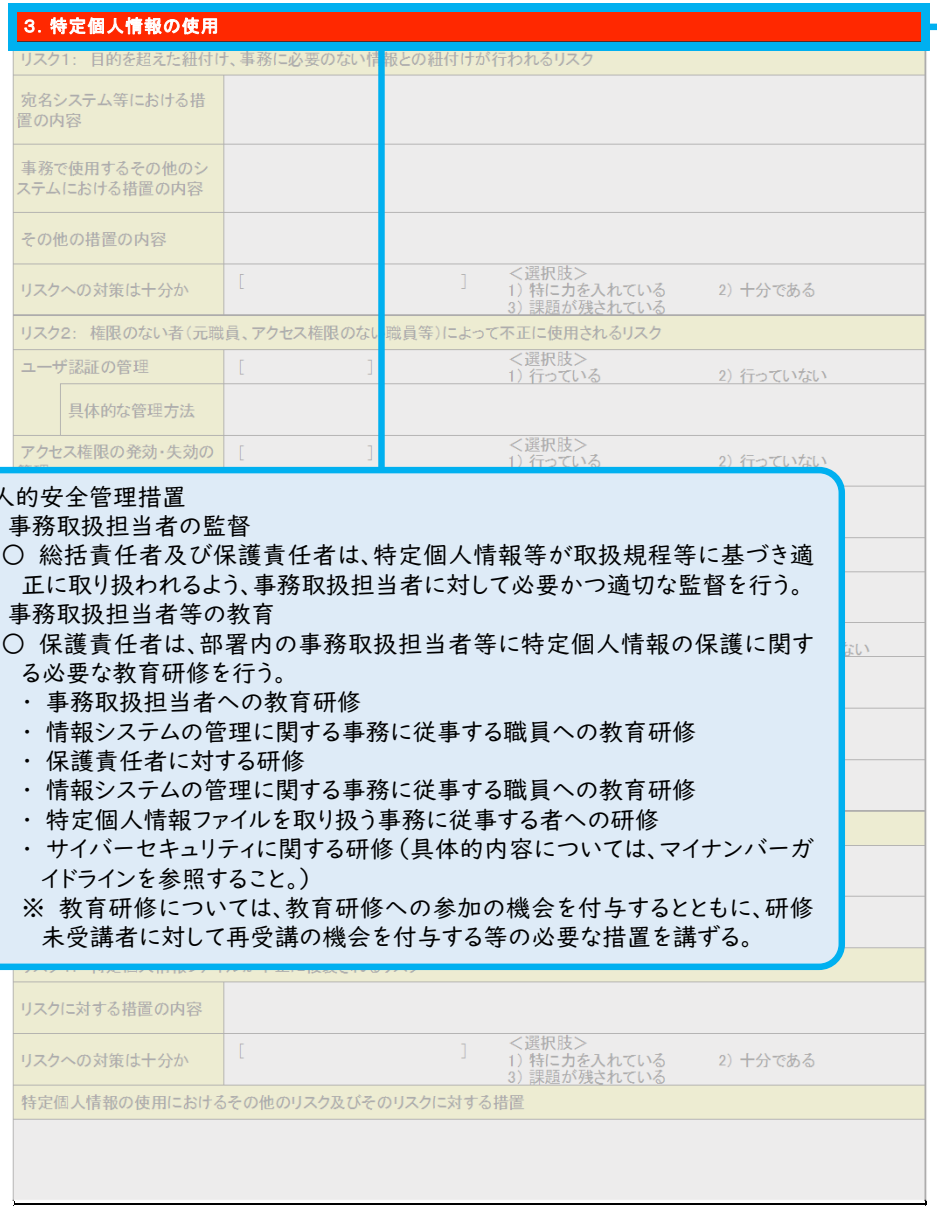
(1)	○ 特定個人情報の入手に際して、入手元が使用目的を認識できること、入手元に不必要な負担を負わせないこと、入手元から情報を詐取・奪取しないこと等、適切な方法で特定個人情報を入手するためにどのような措置を講じているか記載してください。
(2)	○ 番号法第16条には、本人から個人番号の提供を受けるときに、個人番号カードの提示もしくは通知カードと身分証明証の提示を受ける等の厳格な本人確認をするよう規定されています。評価対象の事務において特定個人情報を入手する際に、どのようにしてその特定個人情報が本人の情報であることを確認するか記載してください。
(3)	○ 入手した個人番号が本人の個人番号で間違いないことをどのようにして確認するか記載してください。
(4)	○ 特定個人情報を入手した後、その情報の正確性を保つためにどのようなことを行っているか記載してください。

(1)	○ 特定個人情報の入手に際して、情報の安全確保の観点から、情報漏えいや紛失のリスクを軽減するためにどのような措置を講じているか記載してください。
(2)	○ 特定個人情報の入手において、上記のリスク１～４以外に認識しているリスク及びそれらのリスクへの対策を記載してください。 ○ リスク１～４についての「リスクへの対策は十分か」の質問において「課題が残されている」を選択した場合は、今後の取組の概要、予定等、補足する事項があれば記載してください。

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

（別添１）特定個人情報に関する安全管理措置
２ 講ずべき安全管理措置の内容
E 物理的安全管理措置
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。また、電子媒体及び書類等の庁舎内の移動等において、紛失・盗難等に留意する。
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の必要な措置を講ずる。また、記録機能を有する機器の情報システム端末等への接続の制限等の必要な措置を講ずる。
○ 取扱規程等の手続に基づき、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。
○ 「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、庁舎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。

F 技術的安全管理措置
d 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、通信経路における漏えい等を防止するための措置を講ずる。
○ 特定個人情報ファイルを機器又は電子媒体等に保存する必要がある場合、原則として、暗号化又はパスワードにより秘匿する。



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、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 事務取扱担当者等の教育

○ 保護責任者は、部署内の事務取扱担当者等に特定個人情報の保護に関する必要な教育研修を行う。

- 事務取扱担当者への教育研修
- 情報システムの管理に関する事務に従事する職員への教育研修
- 保護責任者に対する研修
- 情報システムの管理に関する事務に従事する職員への教育研修
- 特定個人情報ファイルを取り扱う事務に従事する者への研修
- サイバーセキュリティに関する研修(具体的内容については、マイナンバーガイドラインを参照すること。)

※ 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。

■ マイナンバーガイドラインの主な参照箇所及び概要 ■

(※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。)

第4−1−(1) 個人番号の利用制限(抄)

○ 個人番号は、番号法があらかじめ限定的に定めた事務以外で利用することはできない。

○ 行政機関等が個人番号を利用するのは、個人番号利用事務(番号法別表に掲げられている事務及び番号法第9条第2項に基づいて条例で規定した事務)、個人番号関係事務(職員等の社会保障及び税等に関する手続書類の作成事務)、番号法第19条第13号から第17号までに基づき特定個人情報の提供を受けた目的を達成するために必要な限度で利用する事務に限られる。

第4−1−(2) 特定個人情報ファイルの作成の制限

○ 個人番号利用事務等を処理するために必要な場合、又は番号法第19条第13号から第17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、特定個人情報ファイルを作成してはならない。

第4−3−(4) 収集・保管制限

○ 番号法で限定的に明記された場合を除き、特定個人情報を収集又は保管してはならない。

○ 番号法で限定的に明記された事務を処理する必要がなくなった場合で、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廃棄又は削除しなければならない。

(別添1)特定個人情報に関する安全管理措置

2 講ずべき安全管理措置の内容

C 組織的安全管理措置

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し、その記録を一定の期間保存し、定期に及び必要に応じ随時に分析等するための体制を整備する。記録については、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とともに、分析等を行う。

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、次に掲げる項目を含めて記録する。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。

・特定個人情報ファイルの名称
・行政機関等の名称及び特定個人情報ファイルが利用に供される事務をつかさどる組織の名称
・特定個人情報ファイルの利用目的
・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特定個人情報ファイルに記録される個人の範囲
・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

e 取扱状況の把握及び安全管理措置の見直し

○ 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。

○ 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。

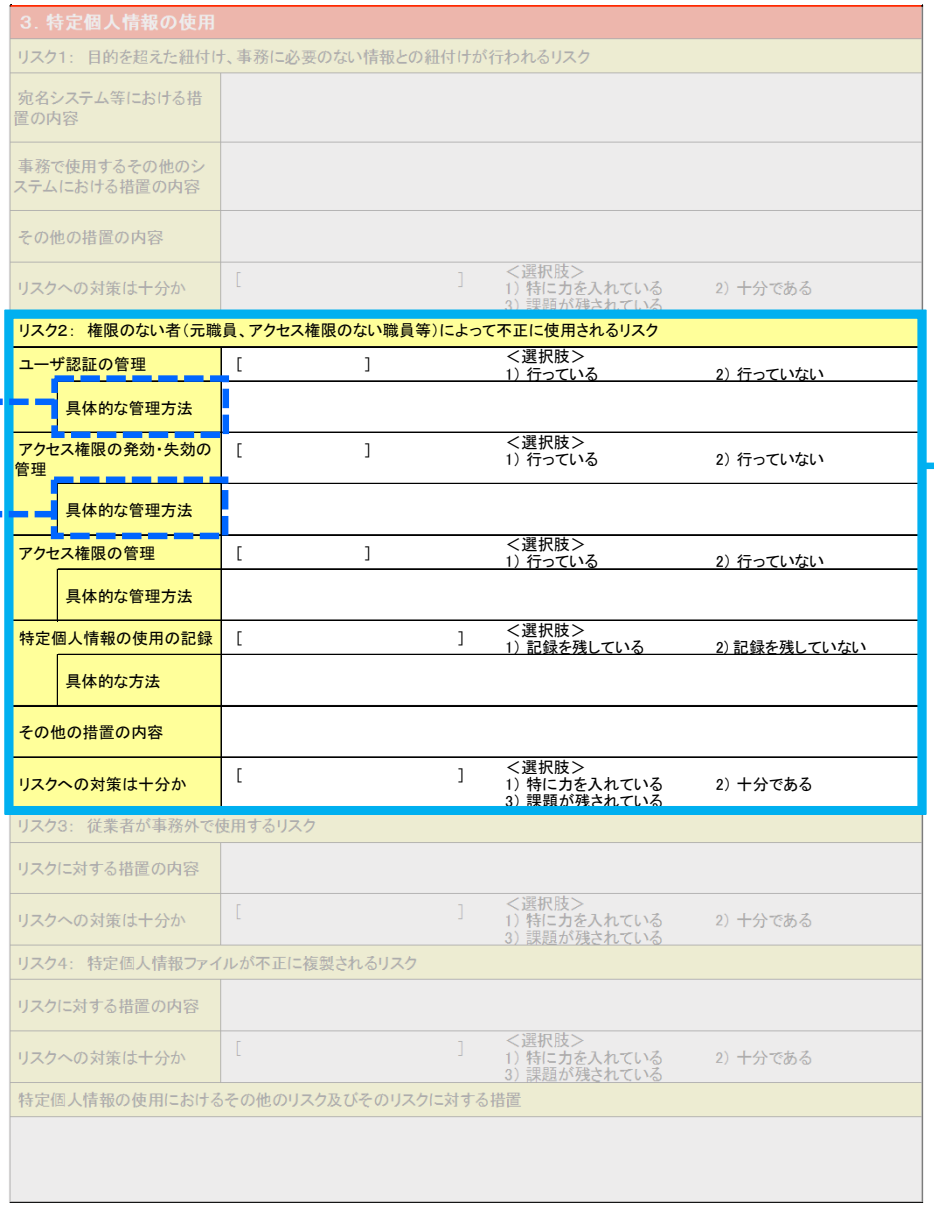
3. 特定個人情報の使用		
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容		
事務で使用するその他のシステムにおける措置の内容		
その他の措置の内容		
リスクへの対策は十分か	[ ]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理	[ ]	<選択肢> 1）行っている　2）行っていない
具体的な管理方法		
アクセス権限の発効・失効の管理	[ ]	<選択肢> 1）行っている　2）行っていない
具体的な管理方法		
アクセス権限の管理	[ ]	<選択肢> 1）行っている　2）行っていない
具体的な管理方法		
特定個人情報の使用の記録	[ ]	<選択肢> 1）記録を残している　2）記録を残していない
具体的な方法		
その他の措置の内容		
リスクへの対策は十分か	[ ]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 従業者が事務外で使用するリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク4： 特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		

(1)

(1)	
	○　特定個人情報が、使用目的を超えて取り扱われないよう、また、評価対象の事務に必要のない情報と併せて取り扱われないよう、どのような対策を行っているか記載してください（例えば、評価対象の事務に必要のない者の個人番号にアクセスできないようにする措置、評価対象の事務に必要のない情報にアクセスできないようにする措置について記載してください。）。 ○　その際、システム上の措置とその他の措置を分けて記載してください。さらに、システム上の措置の中でも、宛名システム等（個人番号と既存番号の対照テーブルなどを用い複数の事務で個人番号を共通して参照するシステム）における措置と、事務で使用するその他のシステムにおける措置に分けて記載してください。

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

（別添１）特定個人情報に関する安全管理措置
2 講ずべき安全管理措置の内容
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して個人番号利用事務等を行う場合、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。



3. 特定個人情報の使用		
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容		
事務で使用するその他のシステムにおける措置の内容		
その他の措置の内容		
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理	[ ]	<選択肢> 1) 行っている 2) 行っていない
具体的な管理方法		
アクセス権限の発効・失効の管理	[ ]	<選択肢> 1) 行っている 2) 行っていない
具体的な管理方法		
アクセス権限の管理	[ ]	<選択肢> 1) 行っている 2) 行っていない
具体的な管理方法		
特定個人情報の使用の記録	[ ]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法		
その他の措置の内容		
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 従業者が事務外で使用するリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク4： 特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		

(1)

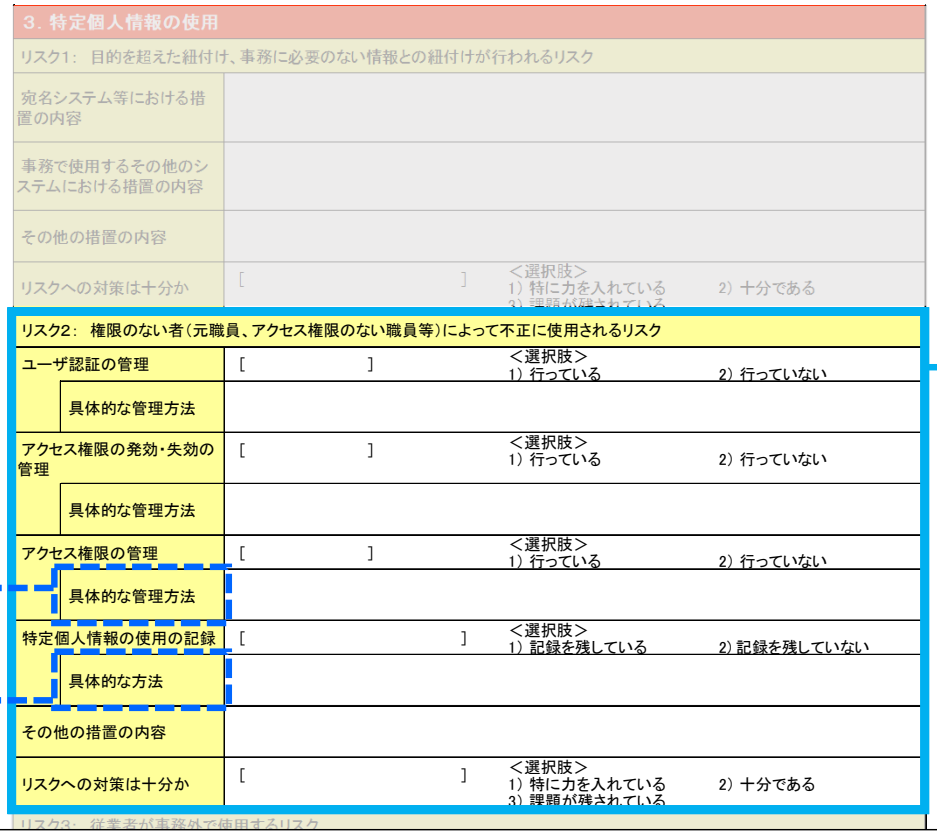
(2)

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

（別添１）特定個人情報に関する安全管理措置
２ 講ずべき安全管理措置の内容
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。管理区域において、入退室管理及び管理区域へ持ち込む機器等の制限等の措置を講ずる。
○ 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。
○ 基幹的なサーバ等の機器を設置する室等（以下「情報システム室等」という。）を区分して管理する場合は、情報システム室等について、次の①及び②に掲げる措置を講ずる。
① 入退室管理
情報システム室等に入室する権限を有する者を定めるとともに、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員の立会い等の措置を講ずる。
② 情報システム室等の管理
外部からの不正な侵入に備え、施錠装置、警報装置、監視設備の設置等の措置を講ずる。

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して個人番号利用事務等を行う場合、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。
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。

(1)	○ 特定個人情報にアクセスする際の認証を行う場合は、特定個人情報にアクセスするユーザの認証方法（ユーザIDとパスワードによる認証か、生体認証か、端末認証を行うかなど）、なりすましが行われないための対策について記載してください。 ○ 認証の管理を行わない場合、行わなくても権限のない者による不正な使用を防止できる理由を記載してください。
(2)	○ アクセス権限の発効・失効の管理を行う者による当該管理の適正性についてどのようにチェックをしているか（権限表の作成、定期的見直しなど）記載してください。



3. 特定個人情報の使用		
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容		
事務で使用するその他のシステムにおける措置の内容		
その他の措置の内容		
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている　2) 十分である 3) 課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理	[ ]	<選択肢> 1) 行っている　2) 行っていない
具体的な管理方法		
アクセス権限の発効・失効の管理	[ ]	<選択肢> 1) 行っている　2) 行っていない
具体的な管理方法		
アクセス権限の管理	[ ]	<選択肢> 1) 行っている　2) 行っていない
具体的な管理方法		
特定個人情報の使用の記録	[ ]	<選択肢> 1) 記録を残している　2) 記録を残していない
具体的な方法		
その他の措置の内容		
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている　2) 十分である 3) 課題が残されている
リスク3： 従業者が事務外で使用するリスク		

(1)

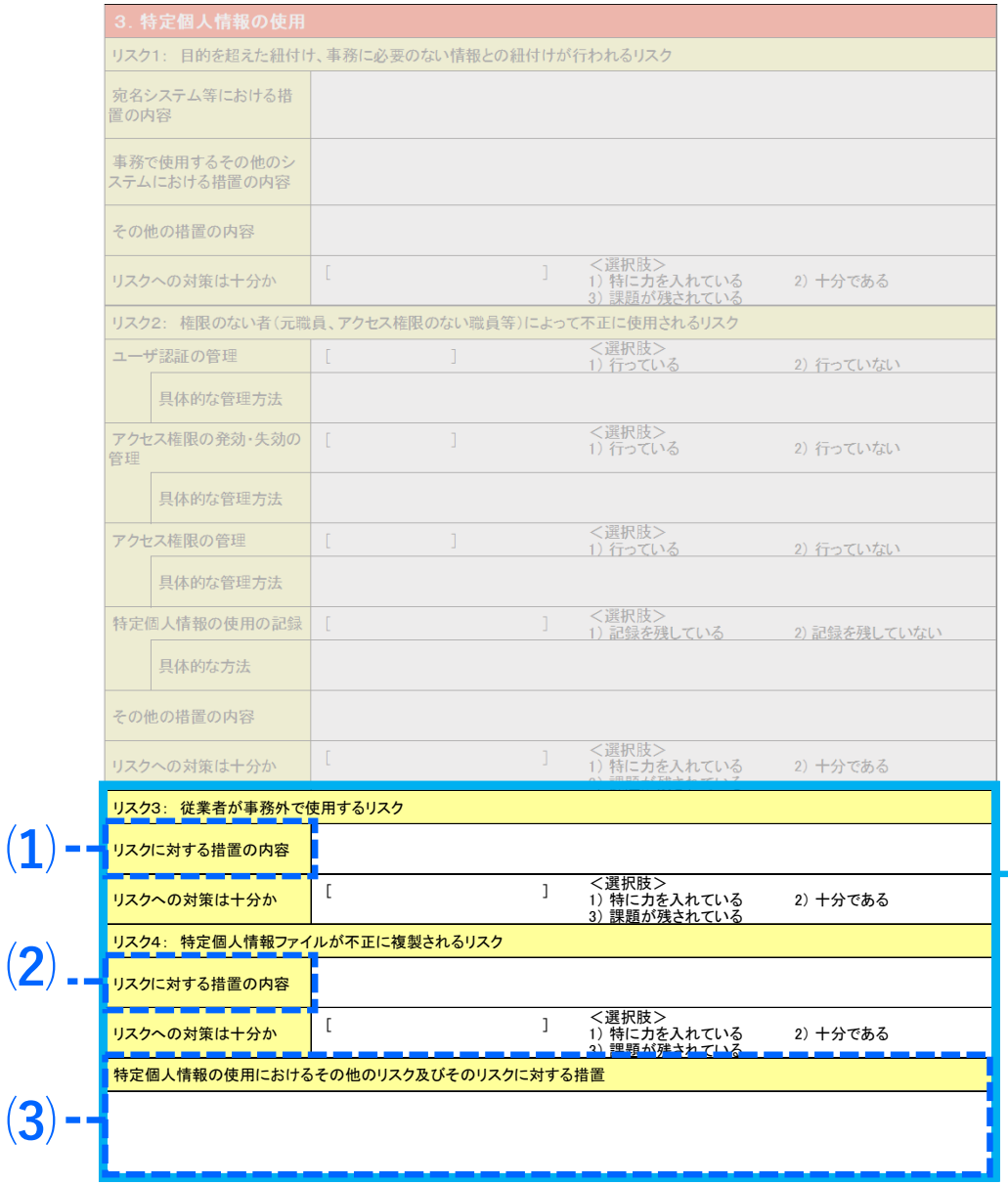
(2)

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

（別添１）特定個人情報に関する安全管理措置
２ 講ずべき安全管理措置の内容
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。管理区域において、入退室管理及び管理区域へ持ち込む機器等の制限等の措置を講ずる。
○ 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。
○ 基幹的なサーバ等の機器を設置する室等（以下「情報システム室等」という。）を区分して管理する場合は、情報システム室等について、次の①及び②に掲げる措置を講ずる。
① 入退室管理
情報システム室等に入室する権限を有する者を定めるとともに、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員の立会い等の措置を講ずる。
② 情報システム室等の管理
外部からの不正な侵入に備え、施錠装置、警報装置、監視設備の設置等の措置を講ずる。

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して個人番号利用事務等を行う場合、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。
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。

(1)	○ 特定個人情報ファイルを取り扱う者が正当なユーザであることを確認するための情報（ユーザID、パスワード等）の発効・失効の管理を行う場合は、以下の点について記載してください。 （１） 発効管理：事務上必要なユーザについてのみID等を発効するようにどのような手段を講じているか（権限発効のポリシー、申請・許可の流れ等を記載してください。）。更新権限者を不必要に増やさないためにどのような手段を講じているか。 （２） 失効管理：事務範囲の変更、異動、休職、退職など、事務上情報にアクセスする必要のなくなったユーザの権限を迅速に失効するためにどのような手段を講じているか（たとえば、権限失効の流れを記載してください。）。 ○ 発効・失効の管理を行わない場合、行わなくても権限のない者による不正な使用を防止できる理由を記載してください。
(2)	○ 特定個人情報ファイルに記録される特定個人情報の入手から消去までの各過程において、誰がどの特定個人情報を取り扱ったか、どの職員がアクセスに失敗したかなどについてログ等の記録を残しているかどうかを選択してください。 ○ 記録を残している場合は、具体的にどのような事項を記録するか、どの程度の単位で記録するか（操作者は個人まで特定するか、部署までか等）、どのような方法で記録するか、記録はどの程度の期間保管されるか、記録事項について分析・確認は行うか（分析・確認を行う場合は、分析・確認の時期、内容、方法）について記載してください。 ○ 記録を残していない場合は、残していなくても権限のない者による不正な使用を防止できる理由を記載してください。



(1)	○　従業者が特定個人情報ファイルを事務外で使用することは認められていません。従業者が事務外での使用を行わないことを確保するために、評価実施機関としてどのような措置を講じているか記載してください。
(2)	○　番号法第29条は、特定個人情報ファイルを作成できる範囲を限定的に定めています。評価対象の事務において特定個人情報ファイルを取り扱う者が不正に複製しないようにどのような措置を講じているか記載してください。
(3)	○　特定個人情報の使用において、上記のリスク１～４以外に認識しているリスク及びそれらのリスクへの対策を記載してください。 ○　リスク１～４についての「リスクへの対策は十分か」の質問において「課題が残されている」を選択した場合は、今後の取組の概要、予定等、補足する事項があれば記載してください。

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

（別添Ⅰ）特定個人情報に関する安全管理措置
2 講ずべき安全管理措置の内容
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、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 事務取扱担当者等の教育
○ 保護責任者は、部署内の事務取扱担当者等に特定個人情報の保護に関する必要な教育研修を行う。
・ 事務取扱担当者への教育研修
・ 情報システムの管理に関する事務に従事する職員への教育研修
・ 保護責任者に対する研修
・ 情報システムの管理に関する事務に従事する職員への教育研修
・ 特定個人情報ファイルを取り扱う事務に従事する者への研修
・ サイバーセキュリティに関する研修（具体的内容については、マイナンバーガイドラインを参照すること。）
※ 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。

E 物理的安全管理措置
c 電子媒体等の取扱いにおける漏えい等の防止 （抄）
○ 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の必要な措置を講ずる。また、記録機能を有する機器の情報システム端末等への接続の制限等の必要な措置を講ずる。

4. 特定個人情報ファイルの取扱いの委託			[　] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク			
(1) 情報保護管理体制の確認			
(2) 特定個人情報ファイルの閲覧者・更新者の制限	[　]	<選択肢> 1) 制限している	2) 制限していない
具体的な制限方法			
特定個人情報ファイルの取扱いの記録	[　]	<選択肢> 1) 記録を残している	2) 記録を残していない
具体的な方法			
特定個人情報の提供ルール	[　]	<選択肢> 1) 定めている	2) 定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法			
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法			
特定個人情報の消去ルール	[　]	<選択肢> 1) 定めている	2) 定めていない
ルールの内容及びルール遵守の確認方法			
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[　]	<選択肢> 1) 定めている	2) 定めていない
規定の内容			
再委託先による特定個人情報ファイルの適切な取扱いの確保	[　]	<選択肢> 1) 特に力を入れて行っている 3) 十分に行っていない	2) 十分に行っている 4) 再委託していない
具体的な方法			
その他の措置の内容			
リスクへの対策は十分か	[　]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置			

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

第4−2−(1) 委託の取扱い

○ 委託者（行政機関等）は、委託先において、番号法に基づき個人番号利用事務等を行う委託者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。

※ 委託者は、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しなければならない。また、委託先に対する監督義務だけではなく、再委託先に対しても間接的に監督義務を負うこととなる。

《必要かつ適切な監督》

① 委託先の適切な選定

② 委託先に安全管理措置を遵守させるための必要な委託契約の締結

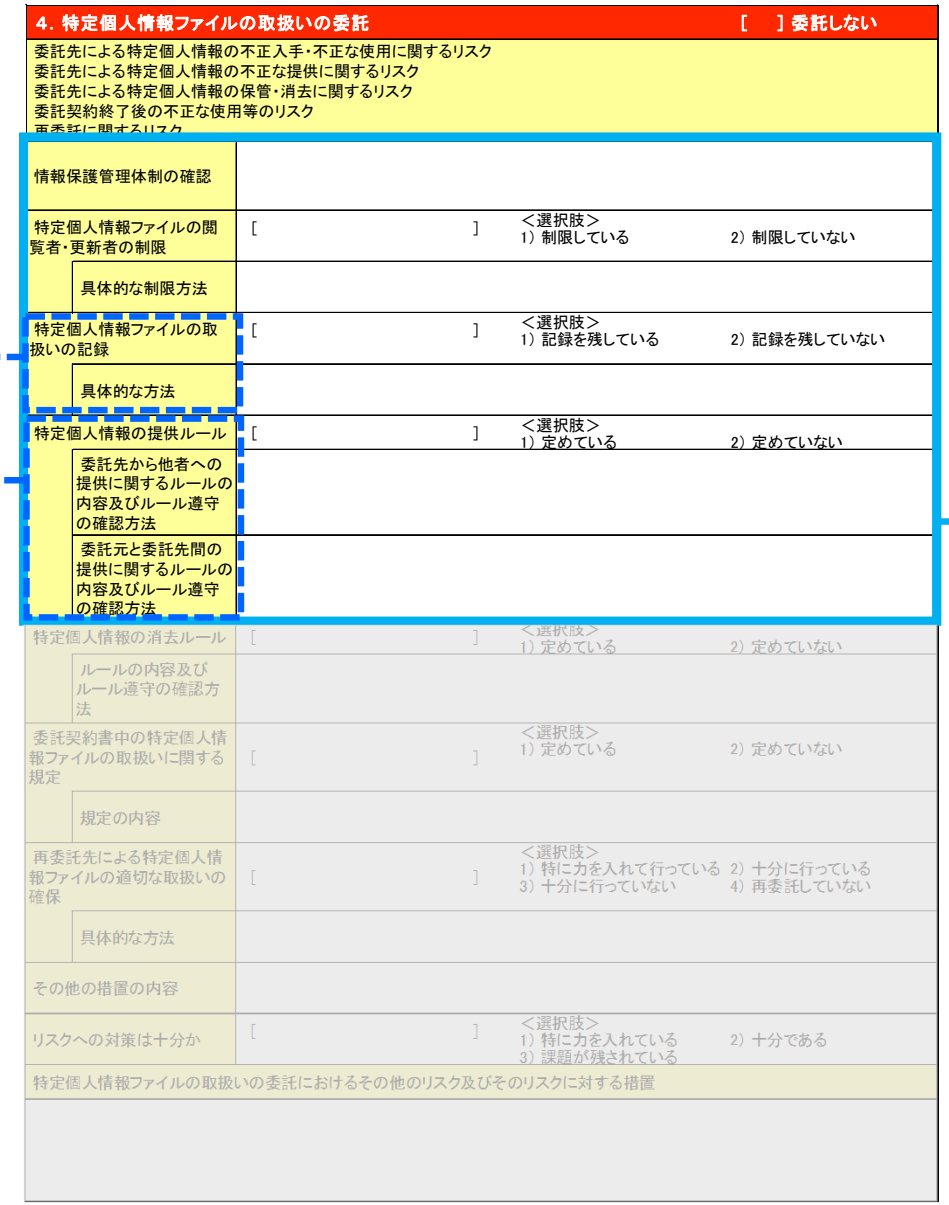
（契約に盛り込む必要がある内容）

・秘密保持義務
・委託する業務の遂行に必要な範囲を超える事業所内からの特定個人情報の持ち出しの禁止
・特定個人情報の目的外利用の禁止
・再委託における条件
・漏えい等事案が発生した場合の委託先の責任
・委託契約終了後の特定個人情報の返却又は廃棄
・特定個人情報を取り扱う従業者の明確化
・従業者に対する監督・教育
・契約内容の遵守状況について報告を求める規定
・必要があると認めるときに実地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の取扱状況の把握

○ 委託先が再委託する場合は、最初の委託者（行政機関等）の許諾を得た場合に限り、再委託をすることができます。再々委託以降も同様です。

(1)	○　委託先を決定する際に特定個人情報ファイルを適切に取り扱う委託先であることをどのように確認しているか、手続等について記載してください。 ○　また、委託先の決定後においても、特定個人情報ファイルの適切な取扱状況等を把握するために、必要に応じて実地の監査、調査等を行う等、契約締結後に情報保護管理体制の確認を行うこととしている場合は、その旨を記載することが考えられます。 ○　番号法上の委託に該当するクラウドサービスを利用する場合は、情報保護管理体制の詳細を把握することが困難だと思われますので、クラウドサービス選定時に用いている基準等を利用して記載することが考えられます。例えば、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等に定められた諸条件や「特定個人情報の適正な取扱いに関するガイドライン」等に定められた各種条件を満たしていること等を記載することが考えられます。
(2)	○　委託先において特定個人情報ファイルの閲覧者・更新者を必要最小限に制限しているかどうか選択してください。制限している場合は、具体的な措置について記載してください。



■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

第4−2−(1) 委託の取扱い

○ 委託者（行政機関等）は、委託先において、番号法に基づき個人番号利用事務等を行う委託者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。

※ 委託者は、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しなければならない。また、委託先に対する監督義務だけではなく、再委託先に対しても間接的に監督義務を負うこととなる。

《必要かつ適切な監督》

① 委託先の適切な選定

② 委託先に安全管理措置を遵守させるための必要な委託契約の締結

（契約に盛り込む必要がある内容）

・秘密保持義務
・委託する業務の遂行に必要な範囲を超える事業所内からの特定個人情報の持ち出しの禁止
・特定個人情報の目的外利用の禁止
・再委託における条件
・漏えい等事案が発生した場合の委託先の責任
・委託契約終了後の特定個人情報の返却又は廃棄
・特定個人情報を取り扱う従業者の明確化
・従業者に対する監督・教育
・契約内容の遵守状況について報告を求める規定
・必要があると認めるときに実地調査を行うことができる規定等

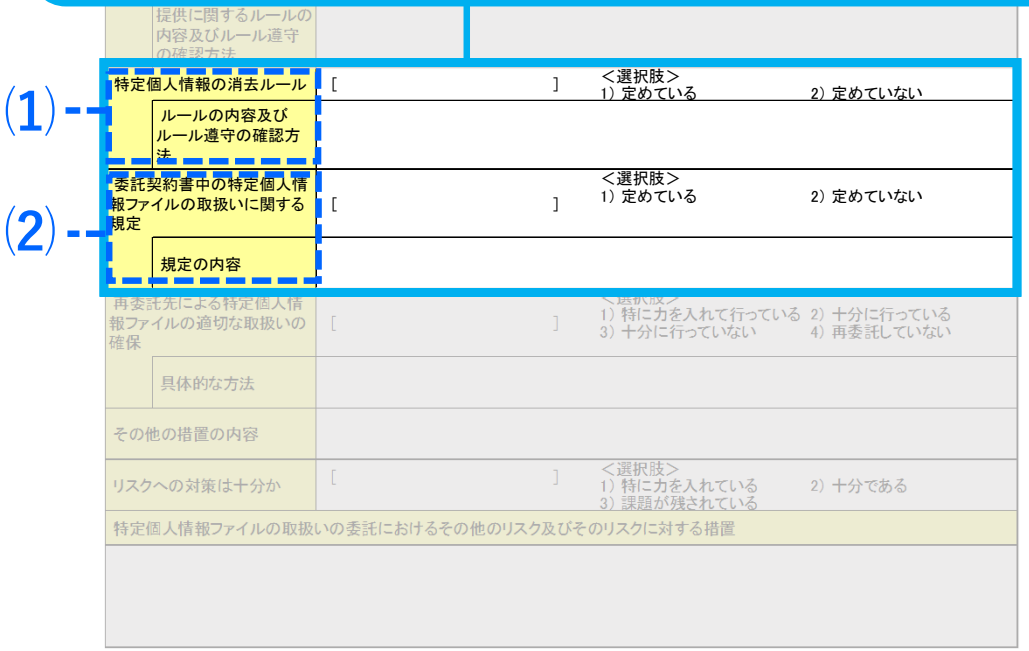
③ 委託先における特定個人情報の取扱状況の把握

○ 委託先が再委託する場合は、最初の委託者（行政機関等）の許諾を得た場合に限り、再委託をすることができます。再々委託以降も同様です。

(1)	○ 委託先における特定個人情報ファイルの取扱いについて、どの従業者がどの特定個人情報をどのように取り扱ったかの記録を残しているかどうかを選択してください。 ○ 記録を残している場合は、記録はどの程度の期間保存されるかを記載してください。 ○ 記録を残していない場合は、残していなくても権限のない者による不正な使用を防止できる理由を記載してください。
(2)	○ 委託先から他者への又は委託元から委託先への特定個人情報の提供に関するルールを定めているかどうかを選択してください。 ○ 定めている場合、それぞれどのようなルールであるか、どのようにしてルール遵守を確認するかを記載してください。 ○ そもそも委託先から他者への提供を認めていない場合、どのようにして提供されていないことを確認するかを記載してください。

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

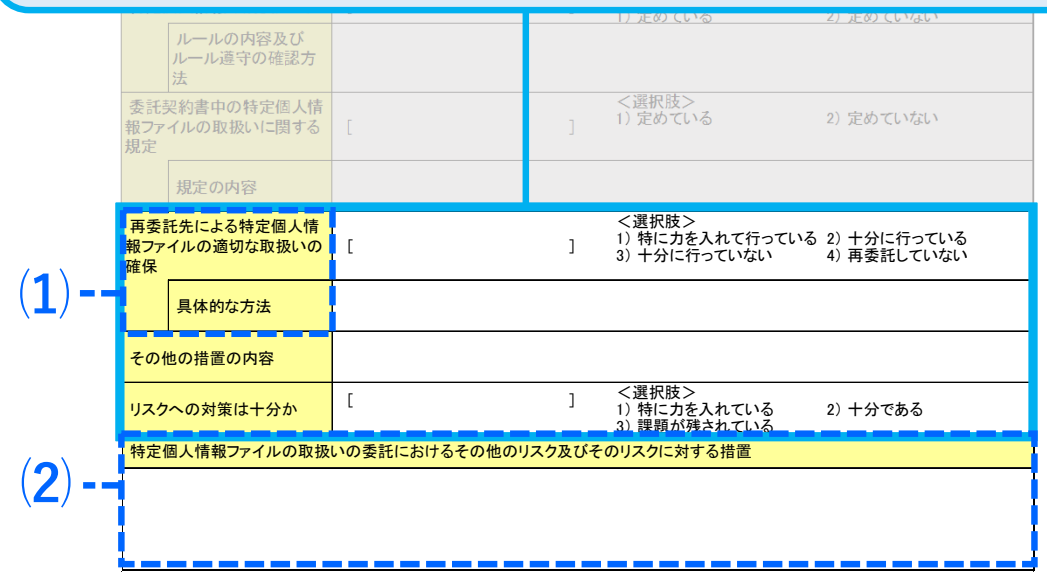
第4−2−(1) 委託の取扱い
○ 委託者（行政機関等）は、委託先において、番号法に基づき個人番号利用事務等を行う委託者が果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行わなければならない。
※ 委託者は、委託をする個人番号利用事務等において取り扱う特定個人情報の適切な安全管理が図られることを確認した上で再委託の諾否を判断しなければならない。また、委託先に対する監督義務だけではなく、再委託先に対しても間接的に監督義務を負うこととなる。
《必要かつ適切な監督》
① 委託先の適切な選定
② 委託先に安全管理措置を遵守させるための必要な委託契約の締結
（契約に盛り込む必要がある内容）
・秘密保持義務
・委託する業務の遂行に必要な範囲を超える事業所内からの特定個人情報の持ち出しの禁止
・特定個人情報の目的外利用の禁止
・再委託における条件
・漏えい等事案が発生した場合の委託先の責任
・委託契約終了後の特定個人情報の返却又は廃棄
・特定個人情報を取り扱う従業者の明確化
・従業者に対する監督・教育
・契約内容の遵守状況について報告を求める規定
・必要があると認めるときに実地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の取扱状況の把握
○ 委託先が再委託する場合は、最初の委託者（行政機関等）の許諾を得た場合に限り、再委託をすることができます。再々委託以降も同様です。



(1)	○ 委託先における特定個人情報の消去のルールを定めているかどうかを選択してください。 ○ 定めている場合は、どのようなルールを定めているか、どのようにしてルール遵守を確認するか、委託契約終了後の消去をどのように確認するかについて記載してください。
(2)	○ 委託先と締結する委託契約において、特定個人情報ファイルの取扱いに関して定めているかどうかを選択してください。また、定めている場合は、どのような規定を設けるか記載してください。 ○ 例えば、規定については、以下の内容が考えられます。 ・秘密保持義務 ・委託する業務の遂行に必要な範囲を超える事業所内からの特定個人情報の持ち出しの禁止 ・特定個人情報の目的外利用の禁止 ・再委託における条件 ・漏えい事案等が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の返却又は廃棄 ・特定個人情報を取り扱う従業者の明確化 ・従業者に対する監督・教育、契約内容の遵守状況についての報告を行うこと ・必要があると認めるときは、委託先に対して実地の監査、調査等を行うこと

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

第4−2−(1) 委託の取扱い
○ 委託者（行政機関等）は、委託先において、番号法に基づき個人番号利用事務等を行う委託者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。
※ 委託者は、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しなければならない。また、委託先に対する監督義務だけではなく、再委託先に対しても間接的に監督義務を負うこととなる。
《必要かつ適切な監督》
① 委託先の適切な選定
② 委託先に安全管理措置を遵守させるための必要な委託契約の締結
（契約に盛り込む必要がある内容）
・秘密保持義務
・委託する業務の遂行に必要な範囲を超える事業所内からの特定個人情報の持ち出しの禁止
・特定個人情報の目的外利用の禁止
・再委託における条件
・漏えい等事案が発生した場合の委託先の責任
・委託契約終了後の特定個人情報の返却又は廃棄
・特定個人情報を取り扱う従業者の明確化
・従業者に対する監督・教育
・契約内容の遵守状況について報告を求める規定
・必要があると認めるときに実地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の取扱状況の把握
○ 委託先が再委託する場合は、最初の委託者（行政機関等）の許諾を得た場合に限り、再委託をすることができます。再々委託以降も同様です。



(1)	○ 特定個人情報ファイルの取扱いを再委託している場合には、再委託先での適正な取扱いの確保のために行っている措置について記載してください。例えば、再委託先における特定個人情報ファイルの管理状況を定期的に点検している場合は、実施頻度、点検方法（訪問確認、セルフチェック）、点検後の改善指示の実施有無、改善状況のモニタリングの実施有無等を記載してください。
(2)	○ 特定個人情報ファイルの取扱いの委託において、上記のリスク以外に認識しているリスク及びそれらのリスクへの対策を記載してください。 ○ 上記「リスクへの対策は十分か」の質問において「課題が残されている」を選択した場合は、今後の取組の概要、予定等、補足する事項があれば記載してください。

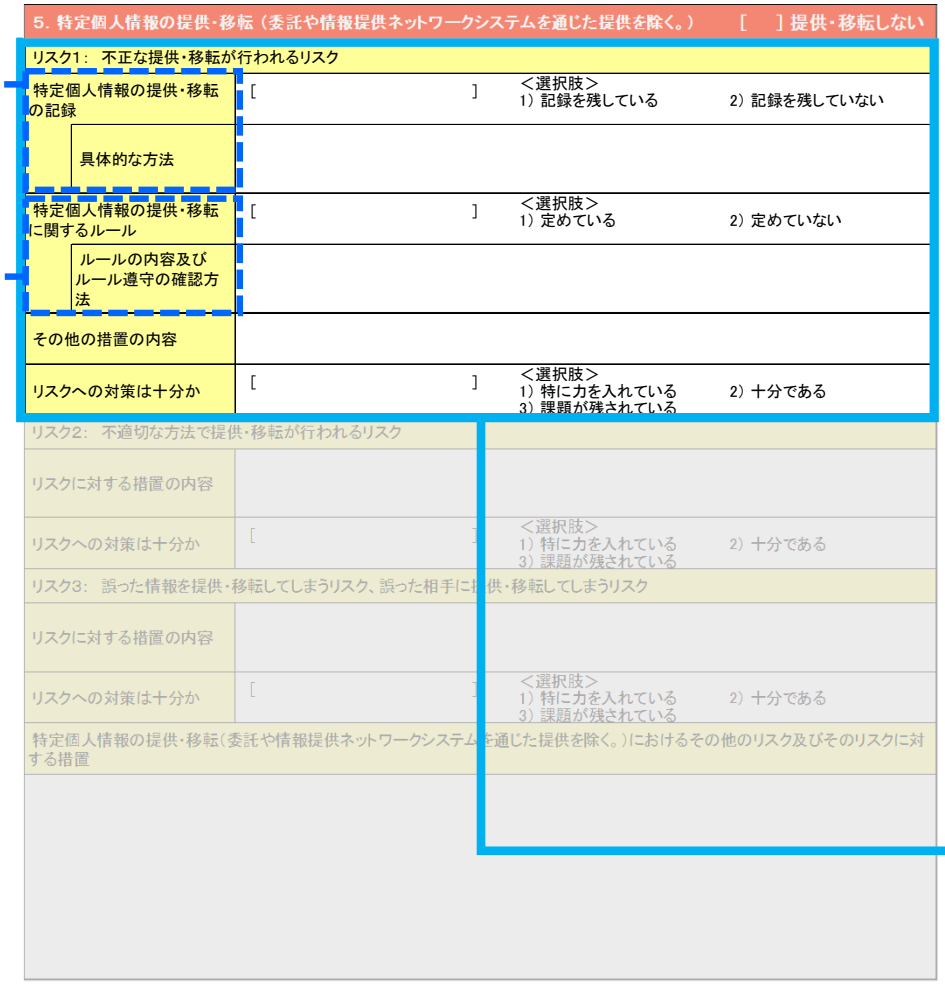
5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）	[　　] 提供・移転しない	
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[　　]	<選択肢> 1）記録を残している　2）記録を残していない
具体的な方法		
特定個人情報の提供・移転に関するルール	[　　]	<選択肢> 1）定めている　2）定めていない
ルールの内容及びルール遵守の確認方法		
その他の措置の内容		
リスクへの対策は十分か	[　　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[　　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[　　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

第4−3−(2) 個人番号の提供の求めの制限、特定個人情報の提供制限
○ 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。
○ 番号法で限定的に明記された場合を除き、特定個人情報を提供してはならない。

（別添Ⅰ）特定個人情報に関する安全管理措置
2 講ずべき安全管理措置の内容
C 組織的安全管理措置
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し、その記録を一定の期間保存し、定期に及び必要に応じ随時に分析等するための体制を整備する。記録については、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とともに、分析等を行う。
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、次に掲げる項目を含めて記録する。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。
・特定個人情報ファイルの名称
・行政機関等の名称及び特定個人情報ファイルが利用に供される事務をつかさどる組織の名称
・特定個人情報ファイルの利用目的
・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特定個人情報ファイルに記録される個人の範囲
・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
e 取扱状況の把握及び安全管理措置の見直し
○ 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。
○ 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。

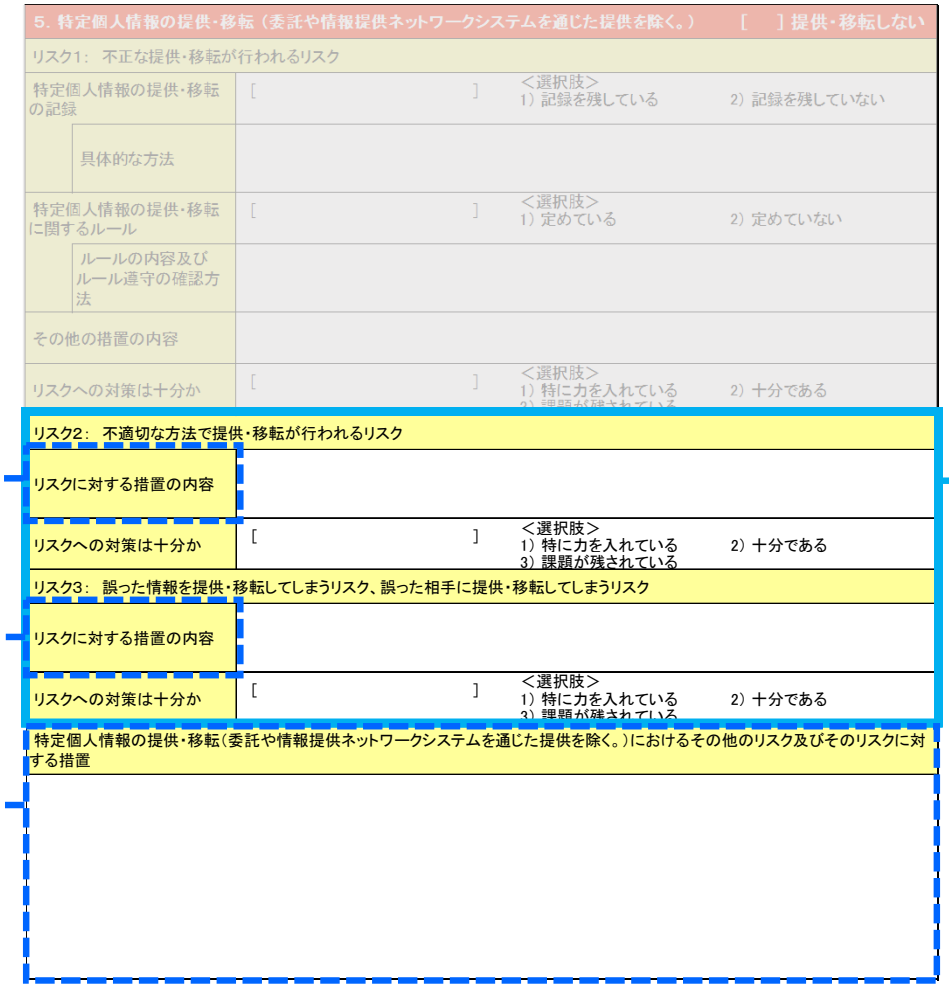
D 人的安全管理措置
a 事務取扱担当者の監督
○ 総括責任者及び保護責任者は、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。
b 事務取扱担当者等の教育
○ 保護責任者は、部署内の事務取扱担当者等に特定個人情報の保護に関する必要な教育研修を行う。
・ 事務取扱担当者への教育研修
・ 情報システムの管理に関する事務に従事する職員への教育研修
・ 保護責任者に対する研修
・ 情報システムの管理に関する事務に従事する職員への教育研修
・ 特定個人情報ファイルを取り扱う事務に従事する者への研修
・ サイバーセキュリティに関する研修（具体的内容については、マイナンバーガイドラインを参照すること。）
※ 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。



(1)	○　どの職員がどの特定個人情報をどのように提供又は移転したかについての記録を残しているかどうかを選択してください。 ○　記録を残している場合は、具体的にどのような事項を、どのような方法で記録するか、記録はどの程度の期間保存されるか、正当な提供・移転以外に不正がなされる可能性のある処理についてもすべて記録しているかについて記載してください。 ○　記録を残していない場合は、残していなくても特定個人情報が不正に提供又は移転されることを防止できる理由を記載してください。
(2)	○　特定個人情報の提供・移転に関するルールを定めているかどうかを選択してください。 ○　定めている場合は、どのようなルールを策定しているか、どのようにしてルール遵守を確認するかについて記載してください。

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

（別添１）特定個人情報に関する安全管理措置
2 講ずべき安全管理措置の内容
E 物理的安全管理措置
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の必要な措置を講ずる。また、記録機能を有する機器の情報システム端末等への接続の制限等の必要な措置を講ずる。
○ 取扱規程等の手続に基づき、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。
○ 「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、庁舎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。
d 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、通信経路における漏えい等を防止するための措置を講ずる。
○ 特定個人情報ファイルを機器又は電子媒体等に保存する必要がある場合、原則として、暗号化又はパスワードにより秘匿する。



■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

第4−3−(2) 個人番号の提供の求めの制限、特定個人情報の提供制限
○ 番号法で限定的に明記された場合を除き、個人番号の提供をしてはならない。

（別添１）特定個人情報に関する安全管理措置
2 講ずべき安全管理措置の内容
E 物理的安全管理措置
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の必要な措置を講ずる。また、記録機能を有する機器の情報システム端末等への接続の制限等の必要な措置を講ずる。
○ 取扱規程等の手続に基づき、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。
○ 「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、庁舎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。
F 技術的安全管理措置
d 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、通信経路における漏えい等を防止するための措置を講ずる。
○ 特定個人情報ファイルを機器又は電子媒体等に保存する必要がある場合、原則として、暗号化又はパスワードにより秘匿する。

(1)	○ 特定個人情報を提供・移転する際に、情報の安全が保たれない不適切な方法で行われないよう、特に情報漏えいや紛失のリスクを軽減するためにどのような措置を講じているか記載してください。また、提供先・移転先における特定個人情報の使途が法令に基づく適切なものであることを確認するための措置を講じているか記載してください。
(2)	○ 誤った特定個人情報を提供・移転したり、誤った相手に提供・移転してしまうと、提供・移転先で誤った情報をもとに処理することによる本人への不利益や、誤った相手による不正な使用のリスクが高まることになります。そのようなことが起こらないように、どのような措置を講じているか記載してください。
(3)	○ 特定個人情報の提供・移転において、上記のリスク１～３以外に認識しているリスク及びそれらのリスクへの対策を記載してください。 ○ リスク１～３についての「リスクへの対策は十分か」の質問において「課題が残されている」を選択した場合は、今後の取組の概要、予定等、補足する事項があれば記載してください。

6. 情報提供ネットワークシステムとの接続	[　] 接続しない（入手）	[　] 接続しない（提供）
リスク1：目的外の入手が行われるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[　]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2：安全が保たれない方法によって入手が行われるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[　]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3：入手した特定個人情報が不正確であるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[　]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

（別添Ⅰ）特定個人情報に関する安全管理措置
2 講ずべき安全管理措置の内容
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、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 事務取扱担当者等の教育
　　○ 保護責任者は、部署内の事務取扱担当者等に特定個人情報の保護に関する必要な教育研修を行う。
　　・ 事務取扱担当者への教育研修
　　・ 情報システムの管理に関する事務に従事する職員への教育研修
　　・ 保護責任者に対する研修
　　・ 情報システムの管理に関する事務に従事する職員への教育研修
　　・ 特定個人情報ファイルを取り扱う事務に従事する者への研修
　　・ サイバーセキュリティに関する研修（具体的内容については、マイナンバーガイドラインを参照すること。）
　　※ 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。

F 技術的安全管理措置
　d 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、通信経路における漏えい等を防止するための措置を講ずる。
　　○ 特定個人情報ファイルを機器又は電子媒体等に保存する必要がある場合、原則として、暗号化又はパスワードにより秘匿する。

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

第4−3−(3) 情報提供ネットワークシステムによる利用特定個人情報の提供
　○ 番号法で限定的に明記された場合を除き、利用特定個人情報を提供してはならない。

（別添Ⅰ）特定個人情報に関する安全管理措置
2 講ずべき安全管理措置の内容
C 組織的安全管理措置
　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し、その記録を一定の期間保存し、定期に及び必要に応じ随時に分析等するための体制を整備する。記録については、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とともに、分析等を行う。
　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、次に掲げる項目を含めて記録する。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。
　　・特定個人情報ファイルの名称
　　・行政機関等の名称及び特定個人情報ファイルが利用に供される事務をつかさどる組織の名称
　　・特定個人情報ファイルの利用目的
　　・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特定個人情報ファイルに記録される個人の範囲
　　・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
　e 取扱状況の把握及び安全管理措置の見直し
　　○ 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。
　　○ 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。

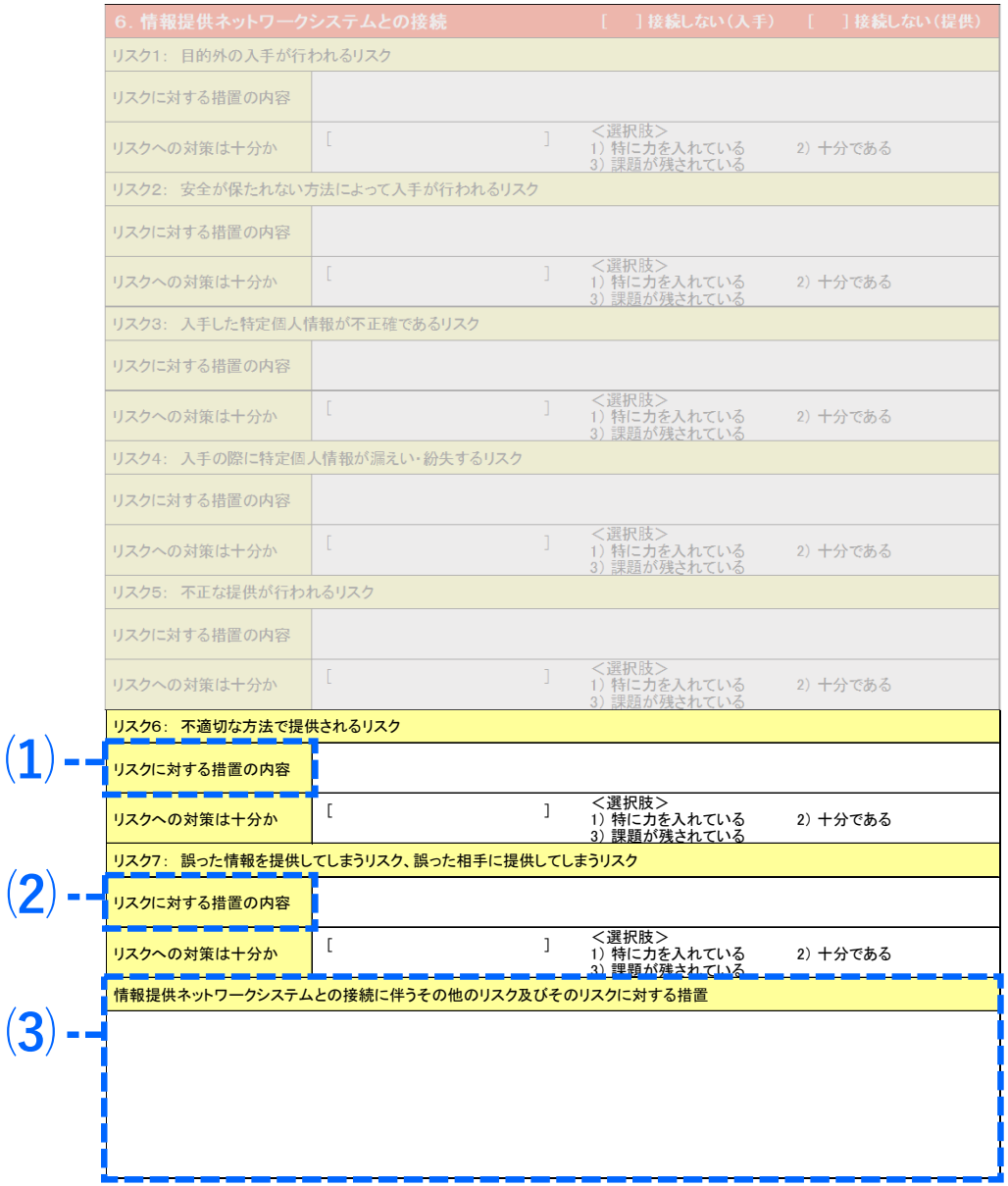
■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

第4−3−(4) 収集・保管制限（抄）
○ 番号法で限定的に明記された場合を除き、特定個人情報を収集又は保管してはならない。

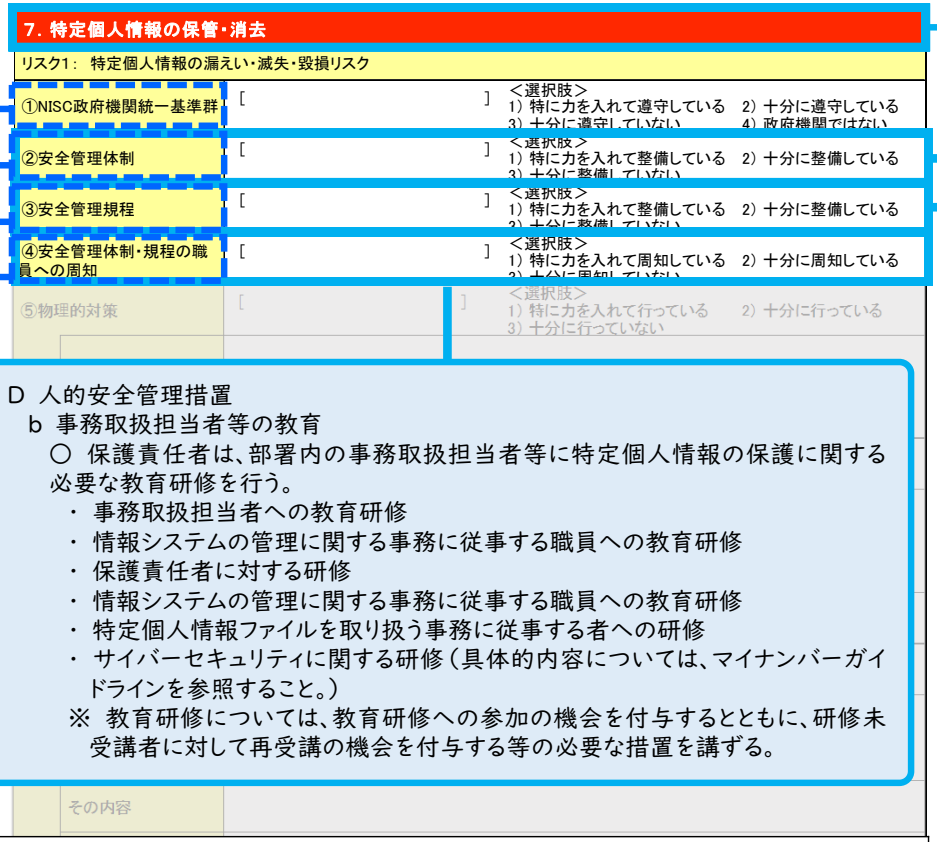
第4−3−(5) 本人確認
○ 番号法、番号法施行令、番号法施行規則及び個人番号利用事務実施者（番号法第9条第3項の規定により情報提供用個人識別符号を利用する者を除く。）が認める方法に従い、適切に本人確認を行う。
※ 具体的な本人確認の方法については、マイナンバーガイドラインを参照。

（別添1）特定個人情報に関する安全管理措置
2 講ずべき安全管理措置の内容
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して個人番号利用事務等を行う場合、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。
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。

(1)	○ 情報提供ネットワークシステムを通じて利用特定個人情報を入手する際に、目的外の入手が行われないために講じている措置を記載してください。
(2)	○ 情報提供ネットワークシステムを通じて利用特定個人情報を入手する際に、利用特定個人情報の安全が保たれない不適切な方法で特定個人情報を入手しないために、どのような対策を行っているか記載してください。
(3)	○ 情報提供ネットワークシステムを通じて利用特定個人情報を入手した後、その情報の正確性を保つためにどのような措置を講じているか記載してください。
(4)	○ 情報提供ネットワークシステムを通じて利用特定個人情報を入手する際に、情報漏えいや紛失のリスクを軽減するためにどのような措置を講じているか記載してください。
(5)	○ 情報提供ネットワークシステムを通じて提供する際に、利用特定個人情報の不正な提供が行われるリスクを軽減するために講じている措置を記載してください。



(1)	○　情報提供ネットワークシステムを通じて提供する際に、利用特定個人情報の提供方法が不適切とならないよう（特定個人情報の安全が保たれない方法で利用特定個人情報を提供・移転しないよう）、どのような措置を講じているか記載してください。
(2)	○　情報提供ネットワークシステムを通じて提供する際に、誤った利用特定個人情報を提供したり、誤った相手に提供してしまうと、提供先で誤った情報をもとに処理することによる本人への不利益や、誤った相手による不正な使用のリスクが高まることになります。そのようなことが起こらないように、どのような措置を講じているか記載してください。
(3)	○　情報提供ネットワークシステムとの接続に伴うリスクについて、上記のリスク１～７以外に認識しているリスク及びそれらのリスクへの対策を記載してください。 ○　リスク１～７についての「リスクへの対策は十分か」の質問において「課題が残されている」を選択した場合は、今後の取組の概要、予定等、補足する事項があれば記載してください。



D 人的安全管理措置
b 事務取扱担当者等の教育
○ 保護責任者は、部署内の事務取扱担当者等に特定個人情報の保護に関する必要な教育研修を行う。
・ 事務取扱担当者への教育研修
・ 情報システムの管理に関する事務に従事する職員への教育研修
・ 保護責任者に対する研修
・ 情報システムの管理に関する事務に従事する職員への教育研修
・ 特定個人情報ファイルを取り扱う事務に従事する者への研修
・ サイバーセキュリティに関する研修（具体的内容については、マイナンバーガイドラインを参照すること。）
※ 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。

(1)	○ 評価実施機関が政府機関の場合は、内閣サイバーセキュリティセンター（NISC）による政府機関等におけるサイバーセキュリティ対策のための統一基準群及びそれに基づく各府省庁ポリシーを遵守しているかどうかを選択してください。政府機関でない場合は、「政府機関ではない」を選択してください。
(2)	○ 特定個人情報の漏えい・滅失・毀損のリスクを想定した安全管理体制を整備しているかどうかを選択してください。
(3)	○ 評価実施機関の内規や条例等で漏えい・滅失・毀損を想定した情報セキュリティに関わる安全管理規程を整備しているかどうかを選択してください。
(4)	○ 特定個人情報の漏えい・滅失・毀損を想定した安全管理体制・規程を職員へ周知しているかどうかを選択してください。

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

第4−2−(2) 安全管理措置
○ 個人番号利用事務等実施者は、個人番号（生存する個人のものだけでなく死者のものも含む。）の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために必要な措置を講じなければならない。また、行政機関等は、保有個人情報である特定個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報である特定個人情報の適切な管理のために必要な措置を講じなければならない。
○ 個人のプライバシー等の権利利益に影響を与え得る特定個人情報の漏えいその他の事態を発生させるリスクを軽減するための措置として、特定個人情報保護評価書に記載した全ての措置を講ずるものとする。

（別添Ⅰ）特定個人情報に関する安全管理措置
2 講ずべき安全管理措置の内容
C 組織的安全管理措置
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。組織体制の整備として、次に掲げる事項を含める。
・ 総括責任者（機関等に各1名）の設置及び責任の明確化
・ 保護責任者（個人番号利用事務等を実施する課室等に各1名）の設置及び責任の明確化
・ 監査責任者の設置及び責任の明確化
・ 事務取扱担当者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
・ 特定個人情報等の取扱いにおける人的ミスの発生を防止するための確認体制の整備
・ 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
・ 個人番号の漏えい、滅失又は毀損等（以下「漏えい等」という。）事案の発生又は兆候を把握した場合の職員から責任者等への報告連絡体制の整備
・ 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
d 漏えい等事案に対応する体制等の整備
○ 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及び手順等を整備する。
○ 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。

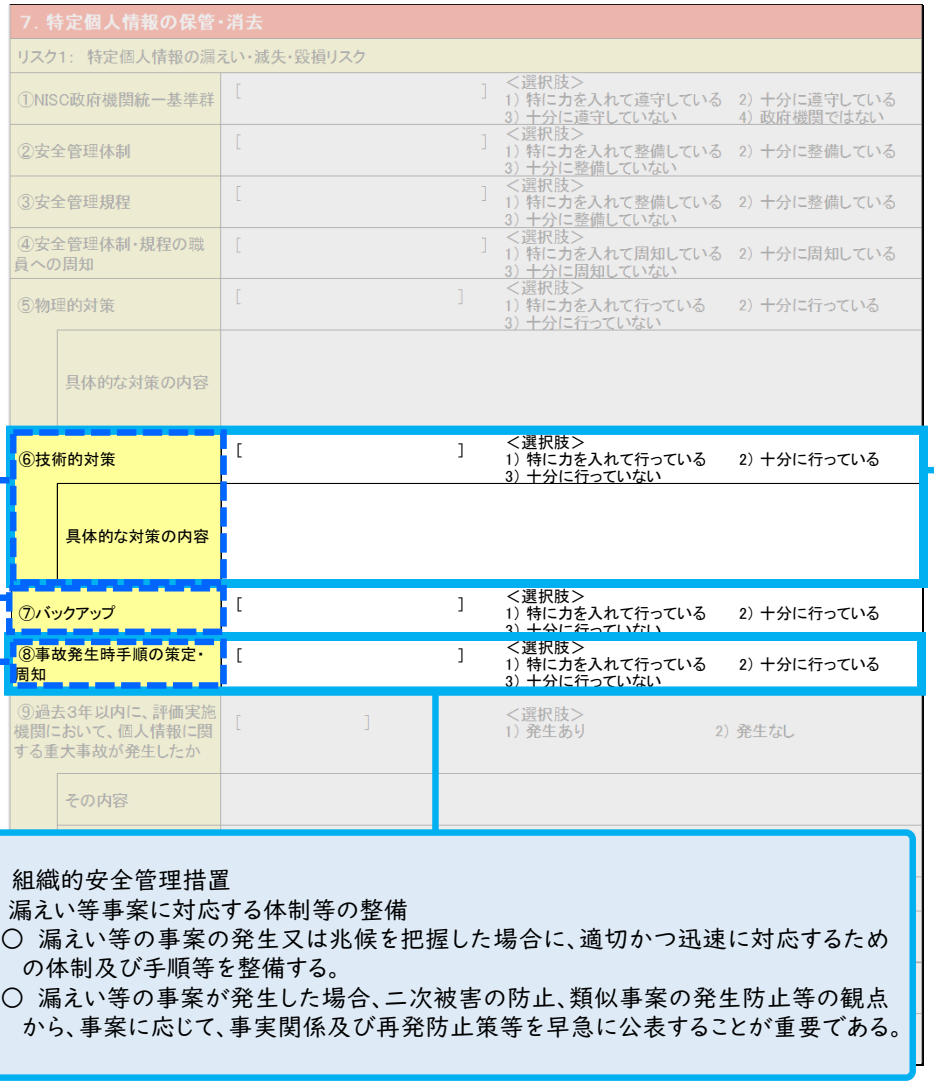
C 組織的安全管理措置
b 取扱規程等に基づく運用
○ 取扱規程等に基づく運用を行うとともに、その状況を確認するため、特定個人情報等の利用状況等を記録し、その記録を一定の期間保存し、定期に及び必要に応じ随時に分析等するための体制を整備する。記録については、改ざん、窃取又は不正な削除の防止のために必要な措置を講ずるとともに、分析等を行う。
e 取扱状況の把握及び安全管理措置の見直し
○ 監査責任者は、特定個人情報等の管理の状況について、定期に及び必要に応じ随時に監査（外部監査及び他部署等による点検を含む。）を行い、その結果を総括責任者に報告する。
○ 総括責任者は、監査の結果等を踏まえ、必要があると認めるときは、取扱規程等の見直し等の措置を講ずる。

(1)

(1)	○　クラウドサービスを利用する場合は、物理的対策について、評価実施機関が詳細を把握することが困難だと思われますので、クラウドサービス選定時に用いている基準等を利用して記載することが考えられます。例えば、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等に定められた諸条件や「特定個人情報の適正な取扱いに関するガイドライン」等に定められた各種条件を満たしていること等を記載することが考えられます。 ○　特定個人情報の漏えい・滅失・毀損を防ぐために、どのような物理的な対策を行っているかを記載してください。物理的な対策とは、例えば、特定個人情報が保有されているサーバの設置場所に監視カメラを設置するなどの方法により入退出者を管理することや、サーバ設置場所、端末設置場所、記録媒体・紙媒体の保管場所について施錠管理がなされていること、サーバ室等への電子記録媒体等の機器類の不要な持込みを制限していること等です。

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

（別添Ⅰ）特定個人情報に関する安全管理措置
2 講ずべき安全管理措置の内容
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。管理区域において、入退室管理及び管理区域へ持ち込む機器等の制限等の措置を講ずる。
○ 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。
○ 基幹的なサーバ等の機器を設置する室等（以下「情報システム室等」という。）を区分して管理する場合は、情報システム室等について、次の①及び②に掲げる措置を講ずる。
① 入退室管理
情報システム室等に入室する権限を有する者を定めるとともに、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員の立会い等の措置を講ずる。
② 情報システム室等の管理
外部からの不正な侵入に備え、施錠装置、警報装置、監視設備の設置等の措置を講ずる。
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。また、電子媒体及び書類等の庁舎内の移動等において、紛失・盗難等に留意する。
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の必要な措置を講ずる。また、記録機能を有する機器の情報システム端末等への接続の制限等の必要な措置を講ずる。
○ 取扱規程等の手続に基づき、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。
○ 「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、庁舎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。
d 個人番号の削除、機器及び電子媒体等の廃棄
○ 特定個人情報等が記録された電子媒体及び書類等について、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。
○ 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。



C 組織的安全管理措置
d 漏えい等事案に対応する体制等の整備
○ 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及び手順等を整備する。
○ 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。

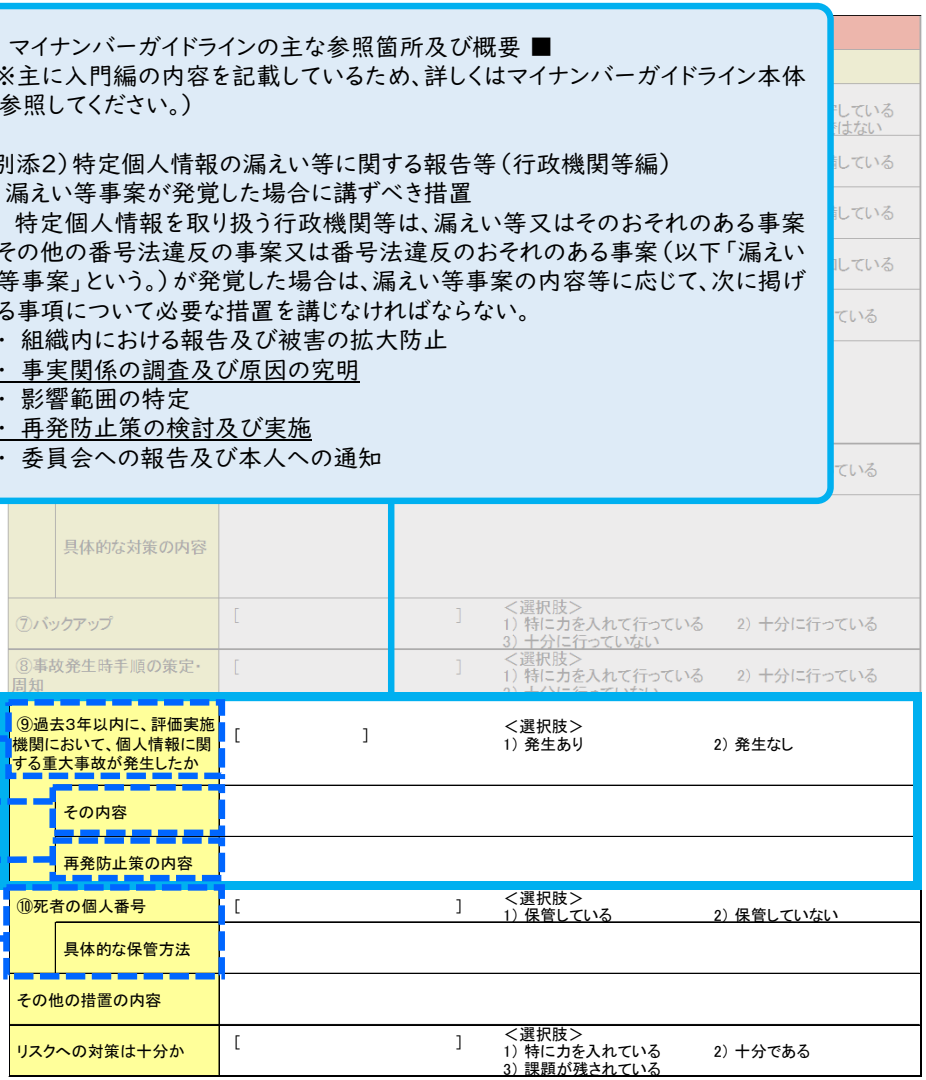
■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

（別添Ⅰ）特定個人情報に関する安全管理措置
2 講ずべき安全管理措置の内容
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して個人番号利用事務等を行う場合、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。
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。
c 不正アクセス等による被害の防止等
○ 情報システムを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等を導入し、適切に運用する。また、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。
○ 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。
d 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、通信経路における漏えい等を防止するための措置を講ずる。
○ 特定個人情報ファイルを機器又は電子媒体等に保存する必要がある場合、原則として、暗号化又はパスワードにより秘匿する。

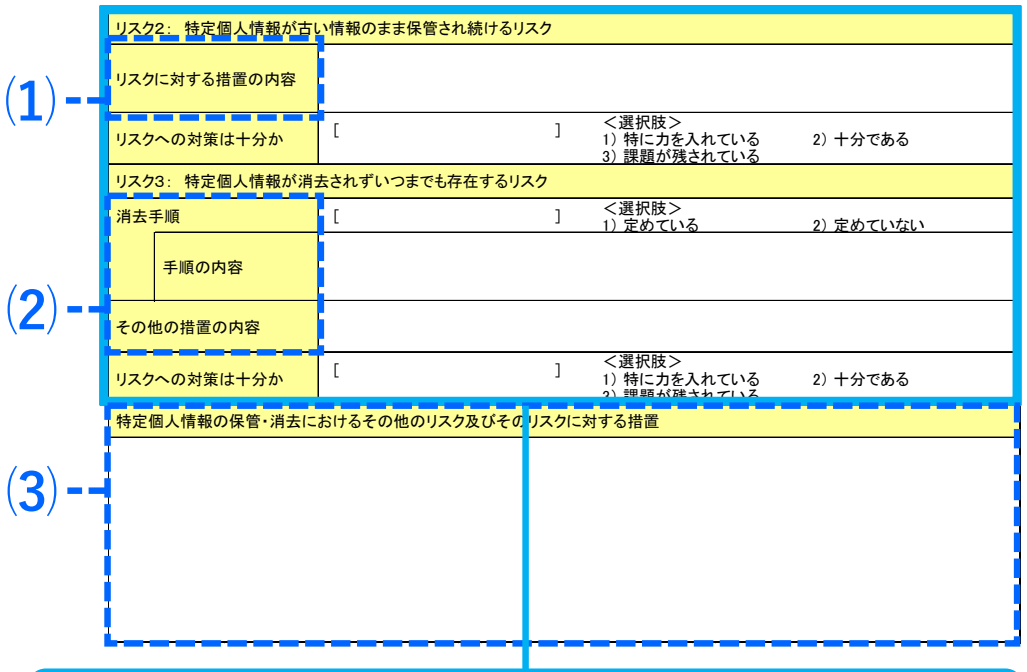
(1)	○ 特定個人情報の漏えい・滅失・毀損を防ぐために、どのような技術的な対策を行っているかを記載してください。技術的な対策とは、例えば、ウィルス対策ソフトを導入することや、暗号化された通信経路を使用すること、不正アクセス対策を実施すること等です。 ○ クラウドサービスを利用する場合は、クラウド環境へ接続する際の通信・アクセス制御等の記載に留意が必要です。
(2)	○ 特定個人情報ファイルの滅失・毀損が発生した場合に復旧できるよう、バックアップを保管しているかどうかを選択してください。
(3)	○ 特定個人情報に関する事故発生時の対応手順を策定して職員に周知しているかどうかを選択してください。

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

（別添2）特定個人情報の漏えい等に関する報告等（行政機関等編）
2 漏えい等事案が発覚した場合に講ずべき措置
○ 特定個人情報を取り扱う行政機関等は、漏えい等又はそのおそれのある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（以下「漏えい等事案」という。）が発覚した場合は、漏えい等事案の内容等に応じて、次に掲げる事項について必要な措置を講じなければならない。
・ 組織内における報告及び被害の拡大防止
・ 事実関係の調査及び原因の究明
・ 影響範囲の特定
・ 再発防止策の検討及び実施
・ 委員会への報告及び本人への通知



(1)	○ 過去３年以内に、評価実施機関において（評価対象の事務に限らないことに御注意ください。）、個人情報（特定個人情報に限らないことに御注意ください。）に関する重大事故が発生したかどうかを選択してください。３年以上前に発生した重大事故であっても、過去３年以内に評価実施機関がその発生を知った場合は、発生したことになります。 ○ ここでいう「個人情報に関する重大事故」については、指針第２の６及び７を参照してください。 【この項目の変更は、重要な変更には該当しません。】
(2)	○ 過去３年以内に発生した全ての重大事故の内容、原因、影響（影響を受けた人数等）、重大事故発生時の対応などを記載してください。 【この項目の変更は、重要な変更には該当しません。】
(3)	○ 重大事故を受けて策定・実施した再発防止策の内容について具体的に記載してください。【この項目の変更は、重要な変更には該当しません。】
(4)	○ 番号法では死者の個人番号についても生存者のそれと同様、安全管理措置義務が課されています。死者の個人番号を保管しているか否かを選択してください。保管している場合は生存者の個人番号と同様の保管方法か否か、生存者の個人番号と異なる方法の場合は保管方法を具体的に記載してください。

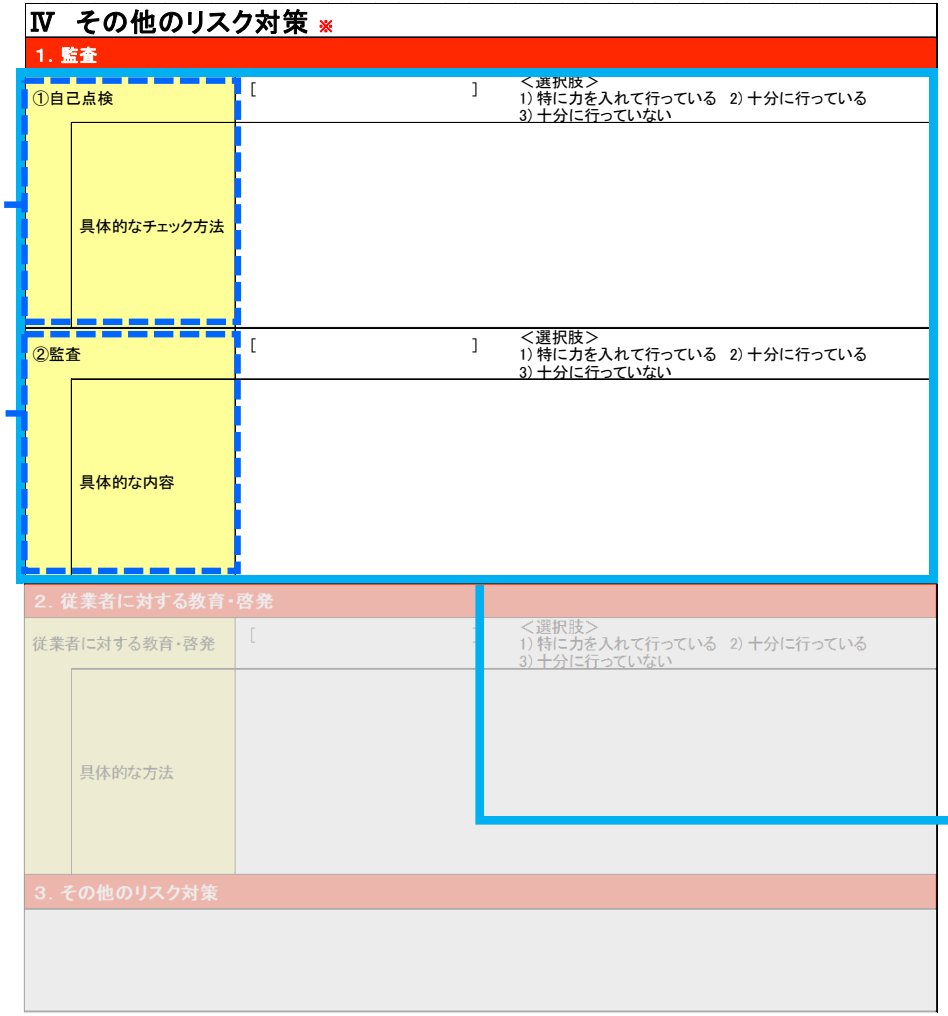


■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

第4−3−(4) 収集・保管制限（抄）
○ 番号法で限定的に明記された事務を処理する必要がなくなった場合で、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廃棄又は削除しなければならない。

（別添Ⅰ）特定個人情報に関する安全管理措置
E 物理的安全管理措置
d 個人番号の削除、機器及び電子媒体等の廃棄
○ 特定個人情報等が記録された電子媒体及び書類等について、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。
○ 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。

(1)	○ 特定個人情報が古い情報のまま保管され続けると、本人に不利益を与えるなどのリスクがあります。特定個人情報を最新の状態で保管するためにどのようなことを行っているか記載してください。
(2)	○ 保管期間を経過した特定個人情報を消去する手順が定められているかどうかを選択してください。 ○ 定められている場合は、特定個人情報を適切な時に安全かつ確実に消去できる手続・体制・手法になっているか、誤って消去すべきでない情報まで消去しないか、消去しなければならない情報の全部又は一部が消去されないままとなることはないかについて記載してください。 ○ 特定個人情報の消去を適切に行うために、実施することを記載してください。例えば、特定個人情報が記録された機器及び電子記録媒体等の消去・廃棄の方法や消去・廃棄の記録をとること等について、記載することが考えられます。また、これらの消去・廃棄を委託する場合には、委託先が消去・廃棄をしたことを確認する方法等について、記載することが考えられます。 ○ クラウドサービスを利用する場合は、特定個人情報の適切な消去について、評価実施機関が詳細を把握することが困難だと思われますので、第三者の監査機関による監査報告書等のレポートを利用し、廃棄・消去に係るプロセスを確認し、その内容を把握すること等を記載することが考えられます。 ○ 既存システムからクラウドサービスへ移行する際は、既存のシステム環境に保管されていた特定個人情報の消去や機器の廃棄、クラウドサービス事業者における特定個人情報の消去等についての記載に留意が必要です。
(3)	○ 特定個人情報の保管・消去において、上記のリスク１～３以外に認識しているリスク及びそれらのリスクへの対策を記載してください。 ○ リスク１～３についての「リスクへの対策は十分か」の質問において「課題が残されている」を選択した場合は、今後の取組の概要、予定等、補足する事項があれば記載してください。



(1)	○　評価書に記載したとおりに運用がなされていることその他特定個人情報ファイルの取扱いの適正性について、評価の実施を担当する部署自らが、どのように自己点検するか記載してください。
(2)	○　評価書に記載したとおりに運用がなされていることその他特定個人情報ファイルの取扱いの適正性について、どのように監査するか記載してください。 ・　監査を行うか否か ・　評価実施機関内の内部監査／外部の第三者による監査の別 ・　監査事項 ・　監査の頻度、方法 ・　監査責任者、監査実施体制 ・　監査の結果をどのように活用するか ○　評価対象の事務において使用するシステムに関する監査を併せて実施している場合は、当該監査についても記載してください。

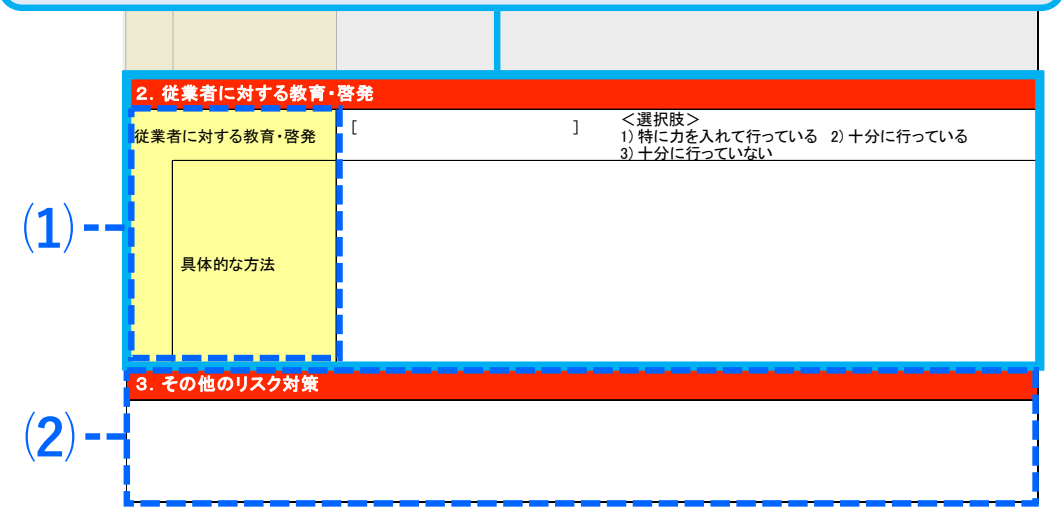
■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

第4−2−(2) 安全管理措置（抄）
○ 個人のプライバシー等の権利利益に影響を与え得る特定個人情報の漏えいその他の事態を発生させるリスクを軽減するための措置として、特定個人情報保護評価書に記載した全ての措置を講ずるものとする。

（別添1）特定個人情報に関する安全管理措置
2 講ずべき安全管理措置の内容
C 組織的安全管理措置
e 取扱状況の把握及び安全管理措置の見直し
○ 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。
○ 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。

■ マイナンバーガイドラインの主な参照箇所及び概要 ■
（※主に入門編の内容を記載しているため、詳しくはマイナンバーガイドライン本体を参照してください。）

（別添Ⅰ）特定個人情報に関する安全管理措置
2 講ずべき安全管理措置の内容
D 人的安全管理措置
b 事務取扱担当者等の教育
○ 保護責任者は、部署内の事務取扱担当者等に特定個人情報の保護に関する必要な教育研修を行う。
・ 事務取扱担当者への教育研修
・ 情報システムの管理に関する事務に従事する職員への教育研修
・ 保護責任者に対する研修
・ 情報システムの管理に関する事務に従事する職員への教育研修
・ 特定個人情報ファイルを取り扱う事務に従事する者への研修
・ サイバーセキュリティに関する研修（具体的内容については、マイナンバーガイドラインを参照すること。）
※ 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。
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職員に対し、法令又は内部規程等に基づき厳正に対処する。



(1)	○ 特定個人情報を取り扱う従業者等に対して、特定個人情報の安全管理が図られるようどのような教育・啓発を行うか、違反行為を行った従業者等に対して、どのような措置を講ずるかについて記載してください。例えば、研修の内容・方法・頻度、未受講者への対応方法等を記載することが考えられます。
(2)	○ 上記の他、リスク対策として取り組んでいることがあれば記載してください。 ○ また、Ⅲ１．から７．までては特定個人情報ファイルの取扱いプロセスにおいて想定されるリスクを列記していましたが、これら以外のリスクを特定し、それらのリスクへの対策を実施している場合も、ここに記載してください。 ○ 組織的及び人的安全管理措置等の観点から、評価実施機関の組織体制や評価対象事務の特性を考慮し、取り組んでいることがあれば記載してください。 ○ 例えば、次のような内容を記載することが考えられます。 ・ 特定個人情報の適切な取扱いについて、継続的な改善を実施するための仕組み ・ 評価対象の事務における事務責任者等の関与の仕組み ・ 特定個人情報保護評価を適切に実施するために整備している体制 ・ 特定個人情報の漏えい事案等が発生した場合の対応

(1)	○　特定個人情報に関する開示・訂正・利用停止請求を受理する部署の名称、住所、電話番号等を記載してください。【☆行政機関にとっては組織の名称及び所在地は事前通知事項です（個人情報保護法第74条第１項第９号）。】
(2)	○　特定個人情報で請求方法が異なる場合は、分かりやすく分けて記載してください。
(3)	○　開示・訂正・利用停止請求について、本人が利用しやすいような措置を講じており、特記して一般に向けて積極的に情報提供したいものがある場合は、記載してください（請求方法の容易化、手数料の減免など）。
(4)	○　開示・訂正・利用停止請求を行うための手数料の金額及びその納付方法について記載してください。
(5)	○　特定個人情報ファイルに含まれる特定個人情報について、個人情報保護法第75条等に基づき、個人情報ファイル簿等で公表を行っているかどうか記載する項目です。公表を行っている場合は、公表している個人情報ファイル名と公表場所（ホームページのリンク先等）を記載してください。評価書での特定個人情報ファイル名と個人情報ファイル簿での個人情報ファイル名は異なっていても構いません。
(6)	○　行政機関、独立行政法人等及び地方公共団体等については、訂正・利用停止請求について、番号法、個人情報保護法以外の法令により、特別の手続がある場合はその旨を個人情報ファイル簿に記載するものとされています（個人情報保護法第75条第１項、同法第74条第１項第10号）。このような場合は、行政機関は、法令名及び条項とともに、当該特別の手続の概要を記載してください。【☆行政機関にとっては法令名及び条項は事前通知事項です（個人情報保護法第74条第１項第10号・第11号・施行令第20条第２号）。】
(7)	○　行政機関については、個人情報保護法第74条第１項第８号に該当する事項（すなわち個人情報保護法第75条第３項の規定に基づき記録項目の一部若しくは第74条第１項第５号若しくは第７号に掲げる事項を個人情報ファイル簿に記載しないこととするとき、又は個人情報ファイルを個人情報ファイル簿に掲載しないこととするとき）があれば、記載してください。【☆行政機関にとっては事前通知事項です（個人情報保護法第74条第１項第８号）。】
(8)	○　特定個人情報ファイルの取扱いに関して問合せをする際の連絡先の部署の名称、住所、電話番号等を記載してください。

(1)	○　この全項目評価書の評価対象の事務について、基礎項目評価を実施した日を記載してください。 ○　基礎項目評価の実施日とは、基礎項目評価を実施・再実施（評価書の修正は含みません。）し、基礎項目評価書の委員会への提出のために評価実施機関内の決裁を了した日です。
(2)	○　基礎項目評価書に含まれるしきい値判断の結果を選択してください。
(3)	○　全項目評価書案を作成した評価実施機関は、これを公示し、広く国民・住民等の意見を求めなければなりません。 ○　採用した意見聴取の方法を記載してください。
(4)	○　意見聴取を実施した日及び期間について記載してください。意見聴取の期間は原則として30日以上ですが、特段の理由がある場合には短縮することができます。
(5)	○　意見聴取の期間を30日より短縮する特段の理由を具体的に記載してください。地方公共団体等が条例等の規定に基づく意見聴取の方法を採用し、30日より短い期間とする場合は、根拠となる条例の名称及び条項を記載してください。
(6)	○　評価実施機関は、国民・住民等からの意見聴取により得られた意見を十分考慮して評価書に必要な見直しを行わなければなりません。得られた主な意見の概要とともに、それらの意見を踏まえて評価書のどの箇所をどのように修正したかを具体的に記載してください。

(1)	○　地方公共団体・地方独立行政法人は、公示し、住民等の意見を求め、必要な見直しを行った全項目評価書について、第三者点検を受けなければなりません。第三者点検を実施した日を記載してください。複数回に分けて実施した場合は実施した期間等の形で記載することができます。 ○　地方公共団体・地方独立行政法人以外の評価実施機関も、任意で第三者点検を受けた場合は、記載することができます。
(2)	○　第三者点検の方法は、原則として、地方公共団体の個人情報保護審議会又は個人情報保護審査会による点検となっていますが、その他の方法によることもできます。採用した方法について記載してください。
(3)	○　第三者点検により指摘された事項、それらを踏まえた評価書の修正等の対応について記載してください。
(4)	○　４．は、しきい値判断の結果、基礎項目評価とともに全項目評価の実施が義務付けられ、全項目評価書について委員会による審査・承認を受けることが必要な行政機関等のみ記載することになります。 ○　評価書について評価実施機関内の決裁を了し、審査・承認を受けるために委員会へ提出する日を記載してください。
(5)	○　承認に向けた審査のプロセス等の対応について記載してください。記載すべき内容は委員会から通知されます。 ○　委員会による審査・承認のために評価書を提出する時点では空欄のままで提出し、委員会の承認を受けた後、公表する前に記載してください。

（別添3）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
(1)	(2)	(3)	(4)	(5)	(6)

○　このページは、評価の再実施又は評価書の修正に伴い、評価書の記載を変更し、提出・公表する際に記載してください（特定個人情報ファイルの新規保有時に提出・公表する評価書では記載しません。）。
○　変更箇所が多数あり、全て記載をすると変更内容が分かりにくくなる場合等は、どのような変更か分かる範囲でまとめて記載することも考えられます。
○　評価の再実施又は評価書の修正の際の変更箇所は、履歴として今までのものを全て記載することが望ましいですが、変更箇所が多数あり、全て記載をすると変更内容等が分かりにくくなる場合等は、例えば、下記の対応も考えられます。
①　今までの評価書の変更箇所は評価実施機関で管理し、直近の変更箇所のみを記載する。
②　変更箇所を行数を超えて入力する必要がある場合は、「別添●●を参照。」などと記載の上、変更箇所の履歴がわかる資料を作成し、評価書の添付資料として併せて提出・公表する。

(1)	○　原則として、記載を変更した評価書の公表日を記載してください。 ○　委員会への提出・公表が、変更前である場合は、変更の予定年月日を記載してください。【☆行政機関にとって、事前通知事項に関する変更の予定年月日は事前通知事項です（個人情報保護法第74条第１項第11号・施行令第20条第１項第２号）。】
(2)	○　記載を変更した又は変更する予定の項目の名称を記載してください。
(3)	○　変更前の記載内容を記載してください。
(4)	○　変更後の記載内容を記載してください。
(5)	○　委員会に提出・公表する時期が、変更前である場合は「事前」と、変更後である場合は「事後」と記載してください。
(6)	○　提出時期が事前の場合は、①重要な変更、②事前通知事項（行政機関のみ）又は③事後で足りるものの任意に事前に提出のうち、いずれの理由により事前に提出・公表するかを記載してください。 ○　事後の場合は、①重要な変更に当たらない旨とその理由（誤字脱字の修正、リスクを明らかに軽減させる変更である等）、②事前通知事項に当たらない旨（行政機関のみ）又は③その他の項目の変更であり事前の提出・公表が義務付けられない旨のいずれかを記載してください。