特定個人情報保護評価書（基礎項目評価書）

(2)

(1)

評価書番号	評価書名

(3)

個人のプライバシー等の権利利益の保護の宣言

特記事項	

評価実施機関名

公表日

［令和7年5月　様式2］

○　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）を単位に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。

特定個人情報保護評価書（基礎項目評価書）

評価書番号	評価書名

個人のプライバシー等の権利利益の保護の宣言

(1)

特記事項	

(2)

評価実施機関名

(3)

公表日

(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）。 ○　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)	○　評価の実施・再実施又は評価書の修正に伴い評価書を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（「Ⅱ１．対象人数」及び「Ⅱ２．取扱者数」を除く。）。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。

［令和7年5月　様式2］

Ⅰ　関連情報

(1)	1. 特定個人情報ファイルを取り扱う事務
	①事務の名称
(2)	②事務の概要
(3)	③システムの名称
(4)	2. 特定個人情報ファイル名
(5)	3. 個人番号の利用
	法令上の根拠
	4. 情報提供ネットワークシステムによる情報連携
	①実施の有無　[　　]　＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
	②法令上の根拠
	5. 評価実施機関における担当部署
	①部署
	②所属長の役職名
	6. 他の評価実施機関
	7. 特定個人情報の開示・訂正・利用停止請求
	請求先
	8. 特定個人情報ファイルの取扱いに関する問合せ
	連絡先
	9. 規則第9条第2項の適用　[　　]適用した
	適用した理由

(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。
(3)	○　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。
(4)	○　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。 ○　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。
(5)	○　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。

Ⅰ　関連情報	
1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	
②事務の概要	
③システムの名称	
2. 特定個人情報ファイル名	
3. 個人番号の利用	
法令上の根拠	
4. 情報提供ネットワークシステムによる情報連携	
(1) ①実施の有無	[　　] ＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
(2) ②法令上の根拠	
5. 評価実施機関における担当部署	
(3) ①部署	
②所属長の役職名	
(4) 6. 他の評価実施機関	
(5) 7. 特定個人情報の開示・訂正・利用停止請求	
請求先	
8. 特定個人情報ファイルの取扱いに関する問合せ	
(6) 連絡先	
9. 規則第9条第2項の適用	[　　]適用した
適用した理由	

(1)	○　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、決定した後に評価書を修正し、再提出するよう努めてください。
(2)	○　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、利用特定個人情報提供省令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。）。条例に基づく独自利用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。
(3)	○　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。
(4)	○　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。
(5)	○　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。
(6)	○　特定個人情報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。

Ⅰ　関連情報

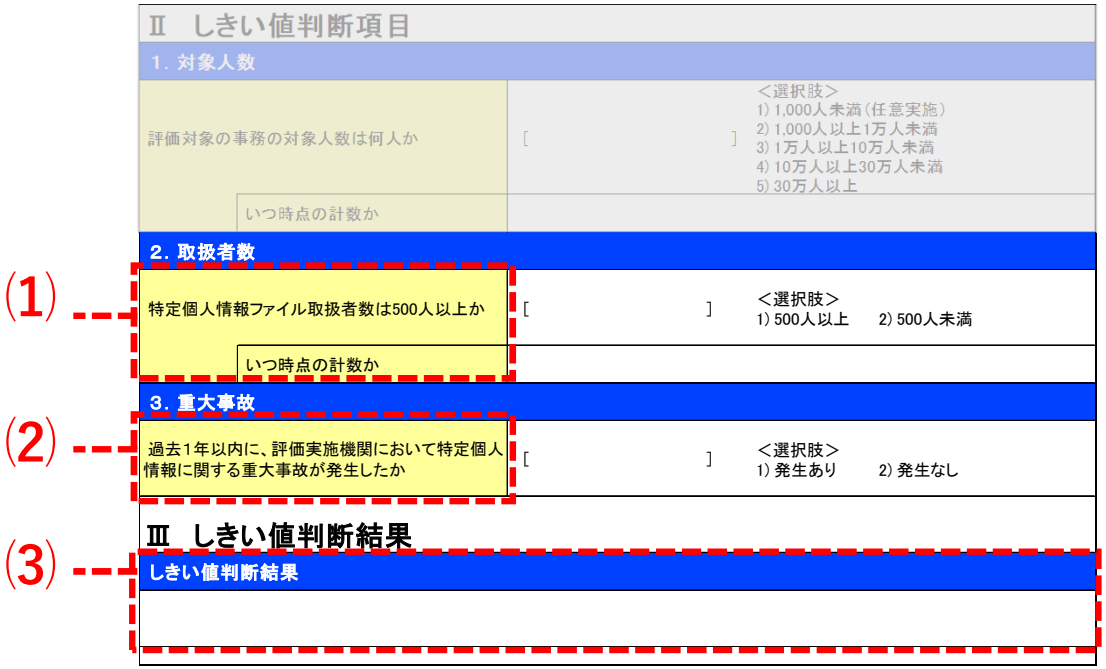
1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	
②事務の概要	
③システムの名称	
2. 特定個人情報ファイル名	
3. 個人番号の利用	
法令上の根拠	
4. 情報提供ネットワークシステムによる情報連携	
①実施の有無	[　　] ＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	
5. 評価実施機関における担当部署	
①部署	
②所属長の役職名	
6. 他の評価実施機関	
7. 特定個人情報の開示・訂正・利用停止請求	
請求先	
8. 特定個人情報ファイルの取扱いに関する問合せ	
連絡先	
(1) **9. 規則第9条第2項の適用**	[　　]適用した
適用した理由	

(1)	○　評価は、特定個人情報ファイルを保有する前（又は重要な変更を加える前）に、実施（又は再実施）することを原則としていますが、災害その他やむを得ない事由により、評価を実施せずに特定個人情報ファイルを保有せざるを得ない場合（又は保有する特定個人情報ファイルに重要な変更を加えざるを得ない場合）は、規則第９条第２項の規定（緊急時の事後評価）に基づき、特定個人情報ファイルの保有後（又は特定個人情報ファイルに重要な変更を加えた後）速やかに評価を実施するものとされています。 ○　同項を適用した場合、「規則第９条第２項の適用」の欄において、「適用した」にチェックを付けた上で、事前評価が困難であった理由を簡潔かつ具体的に説明してください。なお、この適用理由について、保護評価制度の趣旨に照らして疑義等がある場合には、個人情報保護委員会事務局からその記載内容について照会等を行う可能性があります。 ※　なお、既に個人番号利用事務等として定着している事務については、過去に評価を実施した実績があるものであり、同様の事務を実施した実績が全くない個人番号利用事務等と比較して、「評価を事前に実施することが困難である」とはいえないことから、特定個人情報保護評価制度の趣旨又は目的を踏まえ、当該特定個人情報ファイルの保有等に一定の緊急性があるときであっても、原則どおり事前評価を実施するものとされているため、注意してください。 ○　緊急時の事後評価を適用した後、原則どおり特定個人情報ファイルに重要な変更を加える前に再実施（事前評価）した場合は、当該項目のチェックを外し、「適用した理由」を空欄に戻してください。

(1)
(2)

Ⅱ　しきい値判断項目		
1. 対象人数		
評価対象の事務の対象人数は何人か	[　　]	＜選択肢＞ 1) 1,000人未満（任意実施） 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
いつ時点の計数か		
2. 取扱者数		
特定個人情報ファイル取扱者数は500人以上か	[　　]	＜選択肢＞ 1) 500人以上　2) 500人未満
いつ時点の計数か		
3. 重大事故		
過去1年以内に、評価実施機関において特定個人情報に関する重大事故が発生したか	[　　]	＜選択肢＞ 1) 発生あり　2) 発生なし
Ⅲ　しきい値判断結果		
しきい値判断結果		

(1)	○　評価対象の事務の対象人数を選択してください。また、対象人数がいつ時点の計数か記載してください。ただし、評価の実施が義務付けられない事務について、任意で評価を行う場合、対象人数が1,000人以上であっても、「1,000人未満（任意実施）」を選択してください。 ○　なお、対象人数とは、「特定個人情報ファイルを取り扱う事務において保有する全ての特定個人情報ファイルに記録される本人（個人番号によって識別される特定の個人）の数の総数」をいい、その事務において経常的に取り扱う特定個人情報の本人の数をいうと考えられます。そのため、対象人数は当該事務における受給者、被保険者等に限定されません。例えば、医療保険の場合であれば、その被保険者だけではなく、被扶養者等についても個人番号を保有するのであれば、被保険者の数だけではなく、被扶養者の数も対象人数に含まれます。 ○　また、個人番号の利用開始時点において保有する特定個人情報ファイルに記録される本人の数を対象人数とするのではなく、その事務において経常的に取り扱う特定個人情報の本人の数を合理的に推測して、対象人数を記載してください。これまでその事務において経常的に取り扱ってきた個人情報の本人の数のうち個人番号と紐付くと考えられる数、その事務において今後経常的に取り扱うことが予測される個人情報の本人の数のうち個人番号と紐付くと考えられる数、特定個人情報の保存期間の予測等により推測することが考えられます。システム設計上又は予算上想定している人数があれば、それを記載することも考えられます。 ○　給付申請やデータの削除時期が集中することなどにより、対象人数が期間によってばらつきがある場合は、これまでその事務において経常的に取り扱ってきた特定個人情報の本人の数のピークの水準等により、対象人数を合理的に推測することとなります。
(2)	○　計数の時点については、「2024年４月１日」のように詳細な日付を記載することも可能ですが、例えば、「2024年４月時点」といった記載とすることも可能です。 ※ この欄については、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、「2024年４月時点」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)	○　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評価実施機関の従業者及び委託先の従業者の人数の総数を選択してください。また、取扱者数がいつの時点の計数か記載してください。 ○　計数の時点については、「2024年４月１日」のように詳細な日付を記載することも可能ですが、例えば、「2024年４月時点」といった記載とすることも可能です。 ※ この欄については、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、「2024年４月時点」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。
(2)	○　過去１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。）、特定個人情報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。過去１年以上前に発生した重大事故であっても、過去１年以内に評価実施機関がその発生を知った場合は、この項目を選択してください。 ○　ここでいう「特定個人情報に関する重大事故」については、指針第２の６を参照してください。
(3)	○　上記Ⅱ１．から３．までを選択すると、指針第５の２に定めるしきい値判断に当てはめた結果が、自動表示されます。 ○　結果は、以下のいずれかとなりますが、いずれの場合も、しきい値判断で実施が義務付けられていない評価を追加的に任意で実施することができます。 ・基礎項目評価及び全項目評価の実施が義務付けられる。 ・基礎項目評価及び重点項目評価の実施が義務付けられる。 ・基礎項目評価の実施が義務付けられる。 ・特定個人情報保護評価の実施が義務付けられない。

Ⅳ　リスク対策

1. 提出する特定個人情報保護評価書の種類

(1)

[　　]

＜選択肢＞
1) 基礎項目評価書
2) 基礎項目評価書及び重点項目評価書
3) 基礎項目評価書及び全項目評価書

2)又は3)を選択した評価実施機関については、それぞれ重点項目評価書又は全項目評価書において、リスク対策の詳細が記載されている。

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。）

(2)

目的外の入手が行われる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

3. 特定個人情報の使用

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

■ 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
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
α 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)	○　Ⅳ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。例示されている各リスク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。 ○　しきい値判断で評価の実施が義務付けられ、提出した評価書の種類を選択してください。ただし、基礎項目評価書のみを任意で提出する場合は、「１）基礎項目評価書」を、重点項目評価書又は全項目評価書を任意で提出する場合は、任意で提出される評価書名が含まれる選択肢を選択してください。
(2)	○　特定個人情報の目的外の入手が行われるリスクに対する措置について、その内容を確認し、実施状況を選択してください。

【「２）十分である」を選択できる水準】
次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合
＜典型的なリスク対策（例）＞
①　対象者、必要な情報の種類、入手方法等を踏まえ、“対象者以外の情報”や“必要な情報”以外の入手を防止するための措置を、システム面、人手による作業の面から講じている。

「典型的なリスク対策（例）」の位置付け

○ 「典型的なリスク対策（例）」は、あくまでも例示であり、**<u>１つでも実施していない対策があれば、「十分である」を選択できないというものではない</u>**。

○ **<u>「特に力を入れている」を選択できる水準</u>**は、「十分である」を選択できる水準を満たした上で、さらに、**<u>評価実施機関独自の取組を実施</u>**している場合に選択することができると考えられる。

○ 「典型的なリスク対策（例）」には、**<u>組織的安全管理措置、人的安全管理措置</u>**については記載していないが、**<u>マイナンバーGLに則り、必要な措置を講ずる必要</u>**がある。
・組織的安全管理措置：
　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、漏えい等事案に対応する体制等の整備、取扱状況等の把握及び安全管理措置の見直し
・人的安全管理措置：
　事務取扱担当者の監督、事務取扱担当者等の教育、法令・内部規程違反等に対する厳正な対処

Ⅳ リスク対策

1. 提出する特定個人情報保護評価書の種類

[ ]

＜選択肢＞
1) 基礎項目評価書
2) 基礎項目評価書及び重点項目評価書
3) 基礎項目評価書及び全項目評価書

2)又は3)を選択した評価実施機関については、それぞれ重点項目評価書又は全項目評価書において、リスク対策の詳細が記載されている。

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。）

目的外の入手が行われる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

3. 特定個人情報の使用

(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
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

4. 特定個人情報ファイルの取扱いの委託 [ ]委託しない

委託先における不正な使用等の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

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

不正な提供・移転が行われる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

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）

目的外の入手が行われる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
不正な提供が行われる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

(1)	○ 特定個人情報の使用目的を超えた取扱いや事務に必要のない情報との紐付けが行われるリスクに対する措置（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等）について、その内容を確認し、実施状況を選択してください。

【「2）十分である」を選択できる水準】
次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合
＜典型的なリスク対策（例）＞
① 宛名システムやその他の業務システムにおいて、記録されている特定個人情報のうち業務上必要のない特定個人情報に、各業務担当者がアクセスできないようにアクセス制御を行っている。

■ 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
F 技術的安全管理措置
α 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。

Ⅳ リスク対策

1. 提出する特定個人情報保護評価書の種類

[　　]

＜選択肢＞
1) 基礎項目評価書
2) 基礎項目評価書及び重点項目評価書
3) 基礎項目評価書及び全項目評価書

2)又は3)を選択した評価実施機関については、それぞれ重点項目評価書又は全項目評価書において、リスク対策の詳細が記載されている。

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。）

目的外の入手が行われる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

3. 特定個人情報の使用

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
(1) 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

4. 特定個人情報ファイルの取扱いの委託　[　　]委託しない

委託先における不正な使用等の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

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

不正な提供・移転が行われる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

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）

目的外の入手が行われる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
不正な提供が行われる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

(1)	○　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に対する措置（ユーザ認証の管理等）について、その内容を確認し、実施状況を選択してください。

【「2）十分である」を選択できる水準】
次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合
＜典型的なリスク対策（例）＞
①　ユーザ認証の管理を行っている。
②　アクセス権限の発効・失効の管理を行っている。
③　アクセス権限の管理を行っている。
④　特定個人情報の使用の記録、分析（改ざん等の防止に係る対策を含む。）を行っている。

（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
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には、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。

Ⅳ　リスク対策

1. 提出する特定個人情報保護評価書の種類

[　　]

＜選択肢＞
1) 基礎項目評価書
2) 基礎項目評価書及び重点項目評価書
3) 基礎項目評価書及び全項目評価書

2)又は3)を選択した評価実施機関については、それぞれ重点項目評価書又は全項目評価書において、リスク対策の詳細が記載されている。

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。）

目的外の入手が行われる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

3. 特定個人情報の使用

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
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

(1)

4. 特定個人情報ファイルの取扱いの委託　　[　　]委託しない

(2)

委託先における不正な使用等の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

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

不正な提供・移転が行われる		＜選択肢＞ 1) 特に力を入れている

【「2）十分である」を選択できる水準】

次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合

＜典型的なリスク対策（例）＞

① 委託先における情報保護管理体制の確認を行っている。
② 委託先における特定個人情報ファイルの閲覧者・更新者を制限している。
③ 委託先における特定個人情報ファイルの取扱いの記録を行っている。
④ 委託先から他社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。
⑤ 委託先における特定個人情報の消去に関するルールを定めている。
⑥ 委託契約において、特定個人情報ファイルの取扱いに関する規定を設けている。
⑦ 再委託が行われる場合、再委託先による特定個人情報ファイルの適切な取扱いを確保するための措置を講じている。

■ 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4−2−(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委託しない場合は「委託しない」を選択し、４．の評価は不要です。
(2)	○　委託先における不正な使用等のリスクに対する措置（委託契約書中の特定個人情報ファイルの取扱いに関しての規定や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担保等）について、その内容を確認し、実施状況を選択してください。 ※　「４．特定個人情報ファイルの取扱いの委託」において「委託しない」を選択した場合、この項目の評価は不要です。

【「2）十分である」を選択できる水準】
次のような典型的なリスク対策（例）を実施することなどにより、事務・サービスまたはシステムの特性を考慮したリスク対策を講じている場合
＜典型的なリスク対策（例）＞
① 特定個人情報の提供・移転に関するルールが定められている。
② 特定個人情報の提供・移転を記録し、その記録を一定期間保存している。
③ 当該記録を定期に及び随時に分析するための体制を整備している。
④ 当該記録について、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じている。

必要のない情報との紐付けが行われるリスクへの対策は十分か	[ ]	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
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
4. 特定個人情報ファイルの取扱いの委託		[ ]委託しない
委託先における不正な使用等の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
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
不正な提供・移転が行われる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
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）
目的外の入手が行われる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
不正な提供が行われる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

(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。）

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
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)	○ 特定個人情報ファイルの提供・移転をしない場合は「提供・移転しない」を選択し、５．の評価は不要です。
(2)	○ 特定個人情報の不正な提供・移転が行われるリスクに対する措置（提供・移転に関するルールを定める等）について、その内容を確認し、実施状況を選択してください。 ※ 「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。）」において「提供・移転しない」を選択した場合、この項目の評価は不要です。

■ 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。）

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。

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。

（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。
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)

(2)

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）
目的外の入手が行われる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
不正な提供が行われる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

(1)	○ 特定個人情報の入手のために情報提供ネットワークシステムに接続しない場合は「接続しない（入手）」を、特定個人情報の提供のために情報提供ネットワークシステムに接続しない場合は「接続しない（提供）」を選択してください。 ※ 情報提供ネットワークシステム・中間サーバーを通じた特定個人情報の入手又は提供に関するリスク対策を評価するための項目です。
(2)	○ 特定個人情報の目的外の入手が行われるリスクに対する措置について、その内容を確認し、実施状況を選択してください。 ※ 情報提供ネットワークシステム・中間サーバーのアプリケーション仕様等は、関係省庁等から送付されているこの項目の選択に必要な情報を踏まえて、選択してください。 ※ 「６．情報提供ネットワークシステムとの接続」において「接続しない（入手）」を選択した場合、この項目の評価は不要です。

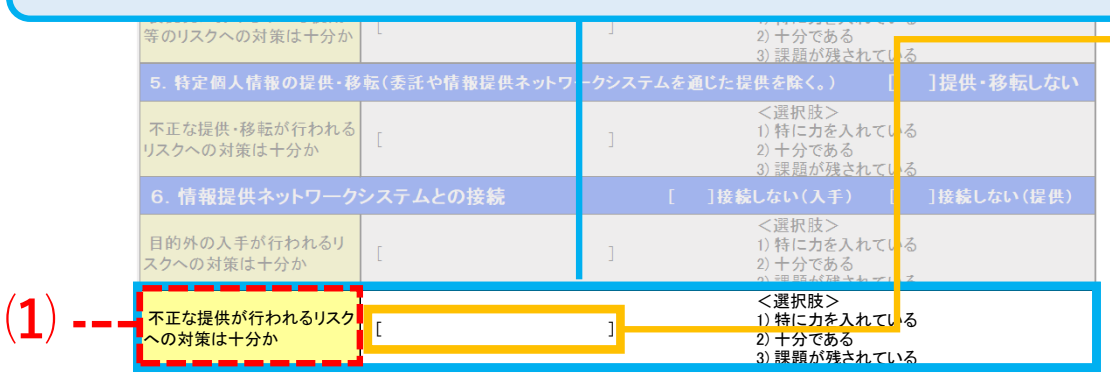
【「２）十分である」を選択できる水準】
次のような典型的なリスク対策（例）を実施することなどにより、事務・サービスまたはシステムの特性を考慮したリスク対策を講じている場合
＜典型的なリスク対策（例）＞
① 自庁システム側において、必要最低限の人数、参照範囲となるよう、職員のアクセス権限を設定している。
② アクセス権限の所持者は、ＩＤ、パスワード等を適切に管理するとともに、離席時のログアウトを徹底する。

■ 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。

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。
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。



【「2）十分である」を選択できる水準】
次のような典型的なリスク対策（例）を実施することなどにより、事務・サービスまたはシステムの特性を考慮したリスク対策を講じている場合
＜典型的なリスク対策（例）＞
① 自庁システムの副本登録画面について、必要最低限の人数、情報の範囲となるよう、職員のアクセス権限を設定する。
② アクセス権限の所有者は、ＩＤ、パスワード等を適切に管理するとともに、離席時のログアウトを徹底する。
③ 副本登録を自動連携により行う場合は、サーバーにアクセス権限等を付与する。
④ 住民基本台帳事務における支援措置対象者等については自動応答不可フラグを設定する等、必要な対応を行う。
⑤ 「マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドライン」の次の留意事項等を遵守している。
（例）
・ 住基ネット照会によりマイナンバーを取得するのではなく、申請者からマイナンバーの提供を受け、その上で記載されたマイナンバーの真正性確認を行うこと。
・ 申請者からマイナンバーが得られない場合にのみ行う住基ネット照会は、４情報又は住所を含む３情報による照会を原則とすること。
・ 複数人での確認や上長による最終確認を行った上でマイナンバーの紐付けを行い、その記録を残すこと。
・ 更新時には、本人からマイナンバーを取得し、登録されているマイナンバーに誤りがないか、確認すること。

(1)	○ 特定個人情報の不正な提供が行われるリスクに対する措置について、その内容を確認し、実施状況を選択してください。 ※ 情報提供ネットワークシステム・中間サーバーのアプリケーション仕様等は、関係省庁等から送付されているこの項目の選択に必要な情報を踏まえて、選択してください。 ※「６．情報提供ネットワークシステムとの接続」において「接続しない（提供）」を選択した場合、この項目の評価は不要です。

(1)

7. 特定個人情報の保管・消去		
特定個人情報の漏えい・滅失・毀損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
8. 人手を介在させる作業		[　　]人手を介在させる作業はない

■ 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
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。

【「2）十分である」を選択できる水準】
次のような典型的なリスク対策（例）を実施することなどにより、事務・サービスまたはシステムの特性を考慮したリスク対策を講じている場合
＜典型的なリスク対策（例）＞
① 内閣サイバーセキュリティセンター（ＮＩＳＣ）による政府機関等のサイバーセキュリティ対策のための統一基準群（「政府機関等のサイバーセキュリティ対策のための統一基準」中「第３部　情報の取扱い」、「第５部　情報システムのライフサイクル」、「第６部　情報システムの構成要素」、「第７部　情報システムのセキュリティ要件」、「第８部　情報システムの利用」等）及びそれに基づく各府省庁ポリシーを遵守している。（評価実施機関が政府機関の場合のみ）
② 地方公共団体においては、地方公共団体における情報セキュリティポリシーに関するガイドライン等を参考に地方公共団体において策定した情報セキュリティポリシー等（第３編第２章中「２．情報資産の分類と管理」、「３．情報システム全体の強靭性の向上」、「４．物理的セキュリティ」、「６．技術的セキュリティ」等）を遵守している。
③ 漏えい・滅失・毀損を防ぐために、物理的安全管理措置や技術的安全管理措置を実施している。
④ 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。
⑤ 過去の漏えい等事案を踏まえた、再発防止策を実施している。

(1)	○ 特定個人情報の漏えい・滅失・毀損リスクに対する措置（事故発生時手順の策定・周知等）について、その内容を確認し、実施状況を選択してください。

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)

(2)

7. 特定個人情報の保管・消去	
特定個人情報の漏えい・滅失・毀損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

8. 人手を介在させる作業	[　]人手を介在させる作業はない
人為的ミスが発生する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
判断の根拠	

9. 監査	
実施の有無	[　] 自己点検　[　] 内部監査　[　] 外部監査

10. 従業者に対する教育・啓発	
従業者に対する教育・啓発	[　　] ＜選択肢＞ 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない

11. 最も優先度が高いと考えられる対策	[　]全項目評価又は重点項目評価を実施する
最も優先度が高いと考えられる対策	[　　] ＜選択肢＞ 1) 目的外の入手が行われるリスクへの対策 2) 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への対策 3) 権限のない者によって不正に使用されるリスクへの対策 4) 委託先における不正な使用等のリスクへの対策 5) 不正な提供・移転が行われるリスクへの対策（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。） 6) 情報提供ネットワークシステムを通じて目的外の入手が行われるリスクへの対策 7) 情報提供ネットワークシステムを通じて不正な提供が行われるリスクへの対策 8) 特定個人情報の漏えい・滅失・毀損リスクへの対策 9) 従業者に対する教育・啓発
当該対策は十分か【再掲】	[　　] ＜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
判断の根拠	

【「2）十分である」を選択できる水準】

次のような典型的なリスク対策（例）を実施することなどにより、事務・サービスまたはシステムの特性を考慮したリスク対策を講じている場合

＜典型的なリスク対策（例）＞

① 「マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドライン」の次の留意事項等を遵守している。

（例）

- 住基ネット照会によりマイナンバーを取得するのではなく、申請者からマイナンバーの提供を受け、その上で記載されたマイナンバーの真正性確認を行うこと。
- 申請者からマイナンバーが得られない場合にのみ行う住基ネット照会は、４情報又は住所を含む３情報による照会を原則とすること。
- 複数人での確認や上長による最終確認を行った上でマイナンバーの紐付けを行い、その記録を残すこと。
- 更新時には、本人からマイナンバーを取得し、登録されているマイナンバーに誤りがないか、確認すること。

② 特定個人情報の入手から保管・廃棄までのプロセスで、人手が介在する局面ごとに人為的ミスが発生するリスクへの対策を講じている。

※ 人為的ミス発生防止の着眼点として、次の資料が参考となる。
いずれも個人情報保護委員会ウェブページ公表資料：
https://www.ppc.go.jp/legal/kensyuushiryou/

- 「特定個人情報を取り扱う際の注意ポイント」
- 「特定個人情報の漏えい等の防止について－地方公共団体における単純な事務ミスを防止するための着眼点－」

(1)	○ 事務において人手を介在させる作業がない場合は「人手を介在させる作業はない」を選択し、８．の評価は不要です。
(2)	○ 人手を介在させる作業におけるリスク対策の措置状況の水準（「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」）を選択した判断の根拠を記載してください。 ※ 特定個人情報保護評価指針の解説第９の２（１）に記載例を掲載しています。

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
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。

【「2）十分である」を選択できる水準】

次のような典型的なリスク対策（例）を実施することなどにより、事務・サービスまたはシステムの特性を考慮したリスク対策を講じている場合

＜典型的なリスク対策（例）＞

① 研修計画を策定している。
② 事務取扱者の適切な監督を行っている。
③ 次の事務取扱者等への教育研修を行っている。
- 事務取扱者への研修
- 特定個人情報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への研修
- 保護責任者への研修
- 事務取扱者へのサイバーセキュリティ研修（おおむね１年ごと）

※ 未受講者には、再受講の機会を付与する等の必要な措置を講ずること。

■ 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。）

（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
- 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)	○ 評価の実施を担当する部署自らによる自己点検、評価実施機関内の内部監査又は外部の第三者による監査を実施している場合には、それぞれ選択してください。
(2)	○ 特定個人情報の安全管理を図るための、特定個人情報を取り扱う従業者への教育・啓発の実施状況について選択してください。

7. 特定個人情報の保管・消去	
特定個人情報の漏えい・滅失・毀損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
8. 人手を介在させる作業	[　]人手を介在させる作業はない
人為的ミスが発生する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
判断の根拠	
9. 監査	
実施の有無	[　] 自己点検　[　] 内部監査　[　] 外部監査
10. 従業者に対する教育・啓発	
従業者に対する教育・啓発	[　　] ＜選択肢＞ 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
11. 最も優先度が高いと考えられる対策	[　]全項目評価又は重点項目評価を実施する
最も優先度が高いと考えられる対策	[　　] ＜選択肢＞ 1) 目的外の入手が行われるリスクへの対策 2) 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への対策 3) 権限のない者によって不正に使用されるリスクへの対策 4) 委託先における不正な使用等のリスクへの対策 5) 不正な提供・移転が行われるリスクへの対策（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。） 6) 情報提供ネットワークシステムを通じて目的外の入手が行われるリスクへの対策 7) 情報提供ネットワークシステムを通じて不正な提供が行われるリスクへの対策 8) 特定個人情報の漏えい・滅失・毀損リスクへの対策 9) 従業者に対する教育・啓発
当該対策は十分か【再掲】	[　　] ＜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
判断の根拠	

(1)	○　評価対象の事務において、重点項目評価又は全項目評価を実施する場合は、「全項目評価又は重点項目評価を実施する」を選択し、11．の評価は不要です。
(2)	○　Ⅳの２．～７．又は10．において、実施状況を評価した各リスク対策のうち、最も優先度が高いと考えられる対策を選択してください。
(3)	○　Ⅳの２．～７．又は10．において、評価したリスク対策の措置状況の水準（「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」）が自動転記されます。
(4)	○　最も優先度が高いと考えられるリスク対策について、その措置状況の水準（「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」）を選択した判断の根拠を記載してください。 ※　特定個人情報保護評価指針の解説第９の２（１）に記載例を掲載しています。

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記載する必要がある場合は、「別添●●を参照。」などと記載の上、別途、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。 ○　個人情報保護委員会への提出・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。
(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)	○　個人情報保護委員会に提出・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)	○　記載の変更、記載を変更した評価書の提出・公表について、特に説明を必要とする場合は、記載してください。