

特定個人情報保護評価書(基礎項目評価書)

[記載要領]

この記載要領は平成30年5月21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(以下「委員会」という。)により改訂される可能性があることにご留意ください。

評価書番号	評価書名

・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。
 ・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【〇年〇月〇日終了】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しておく必要があります。

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	

評価の結果、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。

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。

評価実施機関名

・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:〇〇大臣、〇〇庁長官、〇〇県知事、〇〇市長、〇〇市教育委員会、独立行政法人〇〇等)。
 ・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、「I 6. 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。

公表日

・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(「II 1. 対象人数」及び「II 2. 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。

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	[]
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	[]
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	[]

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。

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。

・過去1年以内に、評価実施機関において(事務においてではないことにご注意ください。)、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。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、発生したことになります。
・ここでいう重大事故とは、評価実施機関が法令に基づく安全管理措置義務を負う特定個人情報を漏えい、滅失又は毀損した場合であって、故意による又は特定個人情報の本人(評価実施機関の従業者を除く。)の数が101人以上のものをいいます。ただし、配送事故等のうち評価実施機関の責めに帰さない事由によるものは除きます。

III しきい値判断結果

しきい値判断結果

・上記 II 1. 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		
[]	[]	<p><選択肢></p> <p>1) 基礎項目評価書</p> <p>2) 基礎項目評価書及び重点項目評価書</p> <p>3) 基礎項目評価書及び全項目評価書</p> <p>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。</p>
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	[]	<p><選択肢></p> <p>1) 特に力を入れている</p> <p>2) 十分である</p> <p>3) 課題が残されている</p>
3. 特定個人情報の使用		
目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスクへの対策は十分か	[]	<p><選択肢></p> <p>1) 特に力を入れている</p> <p>2) 十分である</p> <p>3) 課題が残されている</p>
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	[]	<p><選択肢></p> <p>1) 特に力を入れている</p> <p>2) 十分である</p> <p>3) 課題が残されている</p>
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	[]	<p><選択肢></p> <p>1) 特に力を入れている</p> <p>2) 十分である</p> <p>3) 課題が残されている</p>
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	[]	<p><選択肢></p> <p>1) 特に力を入れている</p> <p>2) 十分である</p> <p>3) 課題が残されている</p>
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	[]	<p><選択肢></p> <p>1) 特に力を入れている</p> <p>2) 十分である</p> <p>3) 課題が残されている</p>
不正な提供が行われるリスクへの対策は十分か	[]	<p><選択肢></p> <p>1) 特に力を入れている</p> <p>2) 十分である</p> <p>3) 課題が残されている</p>

・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。

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。

特定個人情報の使用目的を超えた取扱いや事務に必要な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な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。

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。

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。

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する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。

特定個人情報の提供・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。

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。

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。

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。

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。

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. 監査		
実施の有無	[] 自己点検 [] 内部監査 [] 外部監査	
9. 従業員に対する教育・啓発		
従業員に対する教育・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

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。

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。

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員への教育・啓発の実施状況について選択してください。

