

特定個人情報保護評価書(全項目評価書)

[記載要領]

評価書番号	評価書名

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ことが必要です。

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)。【☆行政機関にとっては事前通知事項です(行政機関個人情報保護法第10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、「I 8. 他評価実施機関」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。

個人情報保護委員会 承認日【行政機関等のみ】
公表日

・評価書を委員会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。

・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。

[平成30年5月 様式4]

(別添1) 事務の内容

・直接入力せず、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図を、オブジェクト・図として貼り付けてください。

・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)。

(備考)

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。

5. 特定個人情報の提供・移転(委託に伴うものを除く。)	
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
提供先1	
①法令上の根拠	
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	[] <small><選択肢></small> 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	

・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。

・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(行政機関個人情報保護法第10条第1項第6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7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10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、番号法別表第二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、提供の根拠となる別表第二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、別表第二の8の項と16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。)

評価実施時に条例が制定されていない場合には、「〇〇に関する条例案」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。

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。

・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年間に約〇回」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。)

・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21以上の場合は、この評価書には提供先20までで記載し、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。

(別添2) 特定個人情報ファイル記録項目

・「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(行政機関個人情報保護法第10条第1項第4号)。】

・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(行政機関個人情報保護法第10条第1項第5号の2)。】

・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。

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(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、誤字脱字の修正、形式的な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。

・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、「13. 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。

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。

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。

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。

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は評価する場合には「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。

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。

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。

入手した個人番号が本人の個人番号で間違いの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。

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しているか記載してください。

特定個人情報を入手に際して、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。

・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。

3. 特定個人情報の使用	
リスク1: 目的を超えた紐付け、事務に必要な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	

・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な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な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な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。

・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かった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。

・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。

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。

・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、記録事項について点検は行うか(点検を行う場合は、点検の時期、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、残していない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。

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。

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。

・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。

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	
情報保護管理体制の確認	
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 2) 十分に行っている 3) 十分に行っていない 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 2) 十分である 3) 課題が残されている
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	

特定個人情報ファイルの取扱いの委託をしていない場合は「委託しない」を選択し、4. の以下の記載は不要です。

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。

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を選択してください。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。

・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、どの従業員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。

・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。

・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。

・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。
・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。

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。

・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			

評価対象の事務において特定個人情報の提供・移転をしていない場合は「提供・移転しない」を選択し、5. の以下の記載は不要です。

・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。

・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。

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	

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用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。

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	

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・移転前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。

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

--	--	--	--

・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
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
リスク5: 不正な提供が行われるリスク	
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6: 不適切な方法で提供されるリスク	
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
リスク7: 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
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
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	

・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記載するための項目です。
 ・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記載に必要な情報を踏まえて、記載してください。
 ・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)」を選択し、リスク1～4の記載は不要です。また、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、リスク5～7の記載は不要です。

情報提供ネットワークシステムを通じて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。

情報提供ネットワークシステムを通じて特定個人情報を入手する際に、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。

情報提供ネットワークシステムを通じて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。

情報提供ネットワークシステムを通じて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。

情報提供ネットワークシステムを通じて提供する際に、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。

情報提供ネットワークシステムを通じて提供する際に、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。

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。

・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。

7. 特定個人情報の保管・消去		
リスク1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[]	<選択肢> 1) 特に力を入れて遵守している 2) 十分に遵守している 3) 十分に遵守していない 4) 政府機関ではない
②安全管理体制	[]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
③安全管理規程	[]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
④安全管理体制・規程の職員への周知	[]	<選択肢> 1) 特に力を入れて周知している 2) 十分に周知している 3) 十分に周知していない
⑤物理的対策	[]	<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
具体的な対策の内容		
⑥技術的対策	[]	<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
具体的な対策の内容		
⑦バックアップ	[]	<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
⑧事故発生時手順の策定・周知	[]	<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
⑨過去3年以内に、評価実施機関において、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
その内容		
再発防止策の内容		
⑩死者の個人番号	[]	<選択肢> 1) 保管している 2) 保管していない
具体的な保管方法		
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 2) 十分である 3) 課題が残されている

評価実施機関が政府機関の場合は、内閣官房情報セキュリティセンター（NISC）による政府機関における情報セキュリティ対策のための統一的な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。

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。

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。

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。

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です。

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、ウイルス対策ソフトを導入することや、不正アクセス対策を実施することです。

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。

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。

・過去3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。）、個人情報（特定個人情報ではないことにご注意ください。）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個人情報漏えい、滅失又は毀損した場合であって、故意による又は個人情報の本人（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、配送事故等のうち当該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。
【この項目の変更は、重要な変更には該当しません。】

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。】

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。】

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。

リスク2: 特定個人情報が古い情報のまま保管され続けるリスク	
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: 特定個人情報が消去されずいつまでも存在するリスク	
消去手順	[] <選択肢> 1) 定めている 2) 定めていない
手順の内容	
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
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置	

← 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。

← ・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。

IV その他のリスク対策 ※

1. 監査	
①自己点検	[] <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
具体的なチェック方法	
②監査	[] <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
具体的な内容	
2. 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
具体的な方法	
3. その他のリスク対策	

IVに記載する内容への変更は、重要な変更該当するため、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、誤字脱字の修正、形式的な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。

・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。

特定個人情報を取り扱う従業員等に対して、特定個人情報の安全管理が図られるような教育・啓発を行うか、違反行為を行った従業員等に対して、どのような措置を講ずるかについて記載してください。

・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。

VI 評価実施手続

1. 基礎項目評価	
①実施日	
②しきい値判断結果	[<選択肢> 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 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(任意に全項目評価を実施) 3) 基礎項目評価の実施が義務付けられる(任意に全項目評価を実施) 4) 特定個人情報保護評価の実施が義務付けられない(任意に全項目評価を実施)]
2. 国民・住民等からの意見の聴取	
①方法	
②実施日・期間	
③期間を短縮する特段の理由	
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	
②方法	
③結果	
4. 個人情報保護委員会の承認【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

・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。

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。

・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。

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。

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。

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。

・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。

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りますが、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。

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下さい。

・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。

・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。

