全項目評価書の記載ポイント集（2016．1．16改訂）

特定個人情報保護評価書（全項目評価書）			審査の観点					
	項目名	記載要領　別添4	審査の番号			考慮事項	指摘事項	改善点／事例
Ⅲ特定個人情報	1.特定個人情報ファイル名	・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。	(9) (10) (11)			特定個人情報ファイルを取り扱うプロセスにおいて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、特定個人情報保護評価の対象となる事務の実態に基づき、特定しているか。 特定されたリスクを軽減するために講ずべき措置についての記載は具体的か。 記載されたリスクを軽減させるための措置は、個人のプライバシー等の権利利益の侵害の未然防止、国民・住民の信頼の確保という特定個人情報保護評価の目的に照らし、妥当なものか。	評価書に安全対策用語のみが記載され、具体的内容の記載が求められているが、具体的な記述がされていないものがある。 リスクに対する措置の内容について、リスクを防止するためのコントロールが正しく書けていない場合がある。（努力目標を記載している事例がある）	主語を明確にし、具体的な対応を記述して、市民にもどのような対策が講じられているのか分かるような記述とする。 市町村におけるセキュリティ対策基準やデータ保護管理規程などを盛り込んで、どのような対策を行っているのか、分かり易く記述する。
	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	**リスク1: 目的外の入手が行われるリスク**	(11)	③		特定個人情報の入手について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。		
		対象者以外の情報の入手を防止するための措置の内容	(11)	③	24	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講じている対策を具体的に記載しているか。	直接入手のみを記述し、他市町村からの入手について言及していない場合がある。 「防止に努める」などの事例では、防止対策が十分であると判断することが出来ない。 「対象者以外の入手が出来ない仕組みとなっている」などの記載事例があり、具体的な記述となっていない。	住民からの入手、他部署からの入手、他市町村からの入手（情報提供ネットワークシステムを介しない入手）など入手方法の違いごとに、対象者以外の情報を入手しないように分けて記述する。 「防止する」等の明確な表現で記述する。 「○○ネットワークからの入手では、対象者以外の情報がシステムでフィルタリングされ、対象者のみの情報が受け渡される仕組みとなっている」等、具体的な仕組みの内容を記載する。
		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	(11)	③	25	事務を遂行する上で必要な情報以外の特定個人情報を入手しないよう講じている対策を具体的に記載しているか。	直接入手のみを記述し、他市町村からの入手について言及していない場合がある。 「不必要な情報が入手出来ない仕組みとなっている」などの記載事例があり、具体的な記述となっていない。	入手方法ごとに不必要な情報を入手しないように対策を講じる旨を記述する。 「○○ネットワークからの入手では、目的外の項目が除外されて受け渡される仕組みとなっている」等、具体的な仕組みの内容を記載する。
		その他の措置の内容	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。					
		リスクへの対策は十分か	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。				各項目で「リスク対策は十分であるか」の問いに対して、回答のほとんどが「十分である」と記載されている事例がある	リスク対策を少しでも実施していれば、安全圏であり、「十分である」といった安易な認識を持っていると考えられる。もっと客観的に評価する必要がある。 対策を実施する必要があると認識すれば、「課題が残されている」といった回答をすべきである。課題認識事項があれば、改善対策を検討し、実施計画をたてて、優先的的に改革推進すべきである。また、対策強化を図っているのであれば、「特に力を入れている」という回答もありえる。 【事例】 リスク対策には、対策レイヤー別に物理的対策、システム的対策、管理的対策、法・倫理的対策があり、これらの対策を組み合わせて、必要不可欠な対策を実施することが重要である。具体例として、鍵をかける、データの暗号化、パスワード設定、2人以上によるチェックと牽制など。
		リスク2: 不適切な方法で入手が行われるリスク						

全項目評価書の記載ポイント集（2016．1．16改訂）

特定個人情報保護評価書（全項目評価書）			審査の観点					
	項目名	記載要領　別添4	審査の番号			考慮事項	指摘事項	改善点／事例
の取り扱いプロセスにおけるリスク対策	た入手を除く）	リスクに対する措置の内容	特定個人情報の入手に際して、詐取（さしゅ）・奪取が行われない、入手元が使用目的を認識できる、入手元に不必要な負担を 負わせない等の観点から、適切な方法で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。	（11）	③	26	特定個人情報の入手に際して、適切な方法で入手するために講じている措置を具体的に記載しているか。	この項は記載要領に詐取とあり、特定個人情報を入手する側の問題である。入手元に対して不安や不必要な負担を負わせないような観点からの入手措置が記述されていない。 入手元に対して不必要な負担を負わせない対策のみが記載され、職員の悪意による詐取（さしゅ）・奪取を防止する対策が記載されていない事例がある。	人を騙したり、脅したり、隠れてコピーするなどは違法行為である。本人に対して入手目的を明確にして不安感を無くし、必要最小限の情報の入手に止めるようにする。 搾取や奪取を防止するために、「職員向けに法令遵守の教育を行っている」「罰則等の周知を行っている」「入手方法について別の者が毎回チェックを行っている」等の具体策を記述する。
		リスクへの対策は十分か						
		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	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。	（11）	③	27	特定個人情報を入手する際に、その特定個人情報が本人の情報であることを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	本人が来庁して本人確認を行う場合だけが書かれていて、代理人が来庁する場合の備えが記述されていないものが散見される。	代理人による申請の場合、代理権限の確認および代理人の本人の身元（実存）確認を行うことを記載する。
		個人番号の真正性確認の措置の内容	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。	（11）	③	28	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確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	「真正性」とは、①正当な権限において作成された記録に対し、②虚偽入力、書き換え、消去及び混同が防止されており、かつ、③第三者から見て作成の責任の所在が明確であることとある。評価書ではこの3点を考慮せず、不正確な情報の入手防止策の記述に止まっている。	真正性の確認： 申告者の個人番号カードを確認できる場合は、券面事項とICチップ内の券面事項確認領域内の情報を確認し、申請者の個人番号及び基本4 情報を確認することにより真正性の確認を行う。 申告者の個人番号カードを確認できない場合は、宛名システムに個人番号及び基本4 情報を確認し、真正性を確認する。確認できない場合には、既存住基システム、又は住基ネットに照会をして真正性を確認する。 [出典：地方公共団体における番号制度の導入ガイドライン] P.99 【事例】 受付に際しては公に発行された証明書等（例えば、市役所の窓口で個人番号に係る提出をした場合の証明書等）で真正性を確保する。疑義が生じた場合には、相手先に問合せを行う。
		特定個人情報の正確性確保の措置の内容	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。	（11）	③	29	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講じている措置を具体的に記載しているか。	「定期的に整合性をチェックする」等の記載事例があり、どのような整合性のチェックを行うのか具体的に記述されていない。また定期的とは、どのぐらいの頻度で行われるのか不明確であり、対策が十分であると評価出来ない	「○○に記録された本人確認情報と、○○のファイルの対応する項目とを、全件、年に1回、プログラムで整合性チェックを行う」等、具体的に記述する。
		その他の措置の内容		（11）	③	31	特定個人情報の入手において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。		
		リスクへの対策は十分か						
		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						

全項目評価書の記載ポイント集（2016．1．16改訂）

特定個人情報保護評価書（全項目評価書）		審査の観点					
項目名	記載要領　別添4	審査の番号			考慮事項	指摘事項	改善点／事例
リスクに対する措置の内容	特定個人情報を入手する際に際して、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〈ださい。	（11）	③	30	特定個人情報を入手する際に、情報の安全確保の観点から講じている措置を具体的に記載しているか。	入手方法ごとの対策となっていなかったり、入手後の書類をどのように処理するのかの記述がない事例がある。 届出書等について、使用後の保管対策のみ記載され、入手の際の対策が記載されていない事例がある。	【事例】 受付カウンターには、隣から見えないように衝立を設置する。また、記載したメモ等は、処理手続きを完了したのちに、高性能シュレッダー等にかけて廃棄する。
リスクへの対策は十分か							
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	・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〈 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〈ださい。						
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		（11）	④		特定個人情報の使用について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。		
宛名システム等における措置の内容	・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〈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〈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〈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〈ださい。	（11）	④	32	宛名システム等において、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、講じている対策を具体的に記載しているか。	宛名システムと他のシステムとの措置が明確に分かれて書かれていない。	宛名システムにおいて、特定個人情報ファイル（住民基本台帳ファイル、本人確認情報ファイル、送付先情報ファイル）等を扱うシステムおよび他のシステム間で必要のない紐付けが行われないための措置を記述する。
事務で使用するその他のシステムにおける措置の内容		（11）	④	33	事務で使用するその他のシステムにおいて、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、講じている対策を具体的に記載しているか。		
その他の措置の内容							
リスクへの対策は十分か							
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							
ユーザー認証の管理							
具体的な管理方法	・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〈 ださい。 ・認証の管理を行わない場合、行わな〈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〈ださい。	（11）	④	34	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、なりすましが行われないために講じている対策について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	特定個人情報にアクセスするユーザの認証方法、なりすましを防止するために講じている対策が具体的に記載されていない。	端末機やサーバー等のシステムの操作は許可された者以外には操作はさせないようにID、パスワードを設定する。 パスワードルールについては、パスワード長、複雑性、有効期間等を具体的に記載する。 【事例】 パスワードはワンタイムパスワードを使用している。 端末の利用認証方法、システムの利用認証方法を区別して管理する必要がある。それぞれの利用について次の①と②を組み合わせて認証している。 ①ユーザIDの入力　又は　ICカード認証 ②パスワードの入力　又は　生体認証
アクセス権限の発行・失効の管理							

全項目評価書の記載ポイント集（2016．1．16改訂）

特定個人情報保護評価書（全項目評価書）			審査の観点					
	項目名	記載要領　別添4	審査の番号			考慮事項	指摘事項	改善点／事例
3．特定個人情報の利用	具体的な管理方法	・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。	(11)	④	35	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の発効・失効の管理について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	アクセス権限の発行、失効を管理するための手続き、承認者が具体的に記載されていない。	規程・基準に基づいたコントロール手順を記述する。 ユーザ管理については、新規登録、削除、変更の手続き方法、タイミング等を具体的に記載する。 発行管理では、情報をアクセスできる人数は最低限に絞って認定する。また、発行にあたっては、所属長の責任で持って発行する仕組みにする。 失効管理では、職員等の異動（転勤、出向、退職等）時には、速やかにID，パスワードを無効にし、アクセスできないようにする。 承認者の在任期間を示した管理表と申請書の承認者を照合し、承認が妥当であることを確認できる仕組みにする。
	アクセス権限の管理							
	具体的な管理方法	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。	(11)	④	36	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チェックをしている内容を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	コントロールのレベルが形容詞で表現されている事例が多く管理策として評価できない。	ID、パスワードが放置されていないか、分かり易い場所に記載されていないか、管理部署等（人事部、内部監査部）による、定期的な監査を実施する。 不必要な形容詞を外し事実のみ記述する。「アクセス権限を設定し制限をかけている」「管理者がアクセス権限を削除する」。 具体的且つ定量的に記述する。「送付後1日以内に市町村ＣＳから削除する」「年に1回見直している」等
	特定個人情報の使用の記録							
	具体的な方法	・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。	(11)	④	37	特定個人情報の入手から消去までの各過程において、特定個人情報ファイルの取扱い記録やアクセスの失敗の記録などを残していることを具体的に記載しているか。 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具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	特定個人情報の使用の記録について、操作履歴（アクセスログ・操作ログ）の確認方法や活用方法が具体的に記載されておらず実効性を評価出来ない。 アクセスログ・操作ログは、情報量が膨大になることが想定される。確認方法が明確でないと実効性を評価出来ない。	ログ取得については、ログ取得対象、ログ保存期間、分析頻度等を具体的に記載する。 ログモニタリングについては、モニタリング方法、承認等を具体的に記載する。 アクセスログ・操作ログの確認を何故行うのか、何時行うのか、誰が行うのか、どの様に行うのかを具体的に記述する。 【事例】 「事故発生後の検証を目的とし」「事故発生前の予防を目的とし」「システムアラートの通知時に」 「システム管理者が」「部署長が」「権限外、対象外、時間外、などをキーに抽出分析を行っている」「自動検知システムがある」等 具体的に記述出来ない場合は基準元を記述する。「○○に記載された管理基準に従い行っている。」「○○の手順書に従い行っている」。 具体的且つ定量的に記述する。「半年に1回」「システムアラートの通知時に」等。
	その他の措置の内容							
	リスクへの対策は十分か							

全項目評価書の記載ポイント集（2016．1．16改訂）

特定個人情報保護評価書（全項目評価書）		審査の観点					
項目名	記載要領　別添4	審査の番号			考慮事項	指摘事項	改善点／事例
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	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。	（11）	④	38	従業者が特定個人情報ファイルを事務外で使用しないよう講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	体制、仕組み、教育に分けて記述されていない。	情報セキュリティに関する教育・啓発により、業務外で使用することの指導・研修の徹底などが求められる。 さらに、違反行為を行った職員に対する罰則や処分の規程の設定などが必要である。
リスクへの対策は十分か							
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							
不正に複製されるリスクに対する 措置の内容	番号法第28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。	（11）	④	39	特定個人情報ファイルを取り扱う者が特定個人情報ファイルを不正に複製しないよう講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	ネットワークが分断されているため、システム間連携により特定個人情報ファイルを転送できない仕組みの場合の対策について記載が無い場合がある。	USBメモリ等の媒体によるデータ交換を行っている場合の、媒体管理、複製管理について、具体的に記載する。
リスクへの対策は十分か							
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。	（11）	④	40	特定個人情報の使用において、その他のリスク及びそれらのリスクへの対策についての具体的な記載はあるか。		
特定個人情報ファイルの取扱いの委託の有無 ・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	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。	（11）	⑤		特定個人情報の委託について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	特定個人情報ファイルの取扱を外部に委託している場合は、委託した業務に対する責任は委託元にあることを認識して、委託元でのリスク対策を正しく記載する。 委託先に業務を丸投げする事によりリスク転嫁し、自らの責任を逃れることにならないようにすること。 最終的に責任は、委託元にある。	外部委託先での情報セキュリティ管理策は、○○市の情報セキュリティポリシー、情報セキュリティ管理基準に準拠すること、遵守状況を定期的に報告すること、また、実施状況を監査できることを契約で定める。
情報保護管理体制の確認	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。	（11）	⑤	41	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確認する手続等について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、 妥当なものか。	委託先選定の具体的な条件が記載されていない。 委託先における情報保護管理体制の妥当性が記載されていない。 委託先の選定について「可能な限り○○を条件としている。」等、曖昧な基準となっている事例がある。	委託先選定の具体的な条件を記載する。 委託先における情報保護管理体制の妥当性を記載する。 委託先におけるリスク対策は、委託元で実施されているリスク対策と同等以上の施策を求めること。 委託先での特定個人情報ファイルを取り扱い方法、基準を明確にし、どのように委託先に周知させ、また遵守状況を確認しているかについて記載する。 「○○の認証取得を条件とする」等の明確な基準を記述する。
特定個人情報ファイルの閲覧者・更新者の制限	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。						
具体的な制限方法	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。	（11）	⑤	42	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ことを具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	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するルールとその確認方法が記載されていない。	特定個人情報ファイルの閲覧者・更新者のリストを作成して管理する。

全項目評価書の記載ポイント集（2016．1．16改訂）

特定個人情報保護評価書（全項目評価書）			審査の観点					
	項目名	記載要領　別添4	審査の番号			考慮事項	指摘事項	改善点／事例
4．特定個人情報ファイルの取扱いの委託	特定個人情報ファイルの取扱いの記録	・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。						
	具体的な方法	・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。	（11）	⑤	43	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記録を残している場合は、その方法や保存期間等を具体的に記載しているか。また、記録を残していない場合は権限のない者による不正な使用を防止できる理由を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	特定個人情報ファイルの取扱記録の内容のみの記載の取得のみでは、漏洩リスクの抑止として不十分である。 記録を残していない場合の正当な理由が記載されていない。	特定個人情報ファイルの取扱記録を定期的に確認、モニタリングにより不正な取扱が無いかを確認する。 【事例】 取扱記録は○○年保管している。
	特定個人情報の提供ルール	・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。						
	委託先から他者への提供に関するルール	・ルールを定めている場合、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。	（11）	⑤	44	委託に伴う特定個人情報の提供に関するルールを定めている場合、ルールの内容やルール遵守の確認方法を具体的に記載しているか。また、委託先から他者への提供を認めていない場合、提供されていないことを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報 保護評価の目的に照らし、妥当なものか。	委託先から他者への提供する場合は委託元の管理ルールに準拠しているということが記載されていない。	委託先から他者への提供する場合は、委託元の指示に基づき、委託元の具体的な規程・基準に従っていることを記載する。 指示に基づかない提供がなされていないことを、定期的に監査をして確認する。
	委託元と委託先間の提供に関するルール						委託元と委託先間の提供に関するルールが、記載されていない。	契約書に記載されている事を明記する。
	特定個人情報の消去ルール	・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。						
	ルールの内容と遵守の確認方法	・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。	（11）	⑤	45	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場合は、ルールの内容やルール遵守の確認方法を具体的に記載しているか。また、委託契約終了後に消去されていることを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当 なものか。	委託先における特定個人情報の消去方法が、具体的に記載されていない。	【事例】 ○○市の情報セキュリティ規程に基づき、契約終了後の消去を物理的に行っている事を相互に確認している。
	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	・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。					特定個人情報ファイルの取扱いを委託する場合には、委託先の監査のみならず、自己点検についても、委託先に実施させることが重要である。	委託先の特定個人情報ファイルの取扱について、監査（自己点検を含む）を実施することを規定に盛り込む。
	規定の内容	・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。	（11）	⑤	46	委託先と締結する委託契約における特定個人情報ファイルの取扱いに関する規定について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	セキュリティ事故が発生した場合の対応が記載されていない。 特定個人情報ファイルの取扱いに関する規定について具体的な記載がない。	・事故が発生した時の対応について記載する。 ・委託契約書において下記事項について明記する。 -業務上知り得た情報の秘密の保持 -第三者への委託の禁止又は制限 -目的外使用及び第三者への提供の禁止 -複製の禁止 -事故発生時の報告義務 -検査の実施 -違反した場合の契約の解除及び損害賠償 -委託業務終了時の返還、廃棄 -法令、規程等の遵守 -事故時等の公表 -責任者、委託内容、作業者、作業場所の特定
	再委託による特定個人情報ファイルの適切な取扱いの確保	適切な取扱いの確保がされているかを選択						

全項目評価書の記載ポイント集（2016．1．16改訂）

特定個人情報保護評価書（全項目評価書）			審査の観点					
	項目名	記載要領　別添4	審査の番号			考慮事項	指摘事項	改善点／事例
	具体的な方法	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。	（11）	⑤	47	特定個人情報ファイルの取扱いを再委託している場合、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具体的に記載しているか。記載された対策は、特定個人情報保護評価 の目的に照らし、妥当なものか。	再委託を許可する条件が記載されていない。	【事例】 「再委託は委託元へ申請を行い、委託元が定める委託先選定基準を満たす場合のみ、再委託を許可している。」
	その他の措置の内容		（11）	⑤	48	特定個人情報ファイルの取扱いの委託において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。		
	リスクへの対策は十分か							
	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	**リスク1：不正な提供・移転が行われるリスク**		（11）	⑥		特定個人情報の提供・移転について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。	同一庁内の他部署への移転についても同様に記載する。	
	特定個人情報の提供・移転の記録	・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。						
	具体的な方法	・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。	（11）	⑥	49	特定個人情報の提供又は移転の記録を残している場合は、その記録の内容や記録方法、保存期間等を具体的に記載しているか。また、記録を残していない場合は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具体的に記載しているか。		【事例】 「特定個人情報の提供・移転を行う際に、提供・移転の記録をシステムで管理し、データベースに○年間保存する。記録する内容は、提供・移転日時、操作者、操作端末等とする。」
	特定個人情報の提供・移転に関するルール	・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。						
	ルールの内容	・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。	（11）	⑥	50	特定個人情報の提供・移転に関するルールを定めている場合は、ルールの内容やルール遵守の確認方法を具体的に記載しているか。		【事例】 「特定個人情報の提供・移転にあたっては、番号法等関係法令で定められた事項についてのみ行う。」
	その他の措置の内容							
	リスクへの対策は十分か							
	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	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。	（11）	⑥	51	特定個人情報を提供・移転する際に、情報漏えいや紛失のリスクを軽減するための措置や提供先・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具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。		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。 中間サーバー間における相互認証を行う。 情報漏えいや紛失のリスクを軽減するための措置を記述する。 ファイル操作履歴のログを収集している場合、ログの確認頻度や保存期間等を具体的に記載する。
	リスクへの対策は十分か							
	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							

全項目評価書の記載ポイント集（2016．1．16改訂）

特定個人情報保護評価書（全項目評価書）			審査の観点					
	項目名	記載要領　別添4	審査の番号			考慮事項	指摘事項	改善点／事例
を通じた提供を除く）	リスクに対する措置の内容	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。	（11）	⑥	52	誤った特定個人情報を提供・移転することや誤った相手に提供・移転することを防止する措置を具体的に記載しているか。		システム間の相互認証等により、リスク対策がシステム上担保されている場合は、その旨を具体的に記載する。
	リスクへの対策は十分か							
	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。	（11）	⑥	53	特定個人情報の提供・移転において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。		
6．情報提供ネットワークシステムとの	情報提供ネットワークシステムとの接続の有無	・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、今後、関係省庁等から送付される予定の 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。	（11）	⑦		情報提供ネットワークシステムとの接続について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。		情報提供ネットワークシステムから入手するか又提供するかを明確にする。
	リスク1: 目的外の入手が行われるリスク							中間サーバーを経由して情報提供ネットワークシステムと接続する場合と直接接続する場合と明確にしてどのように対応するか言及する。
	リスクに対する措置の内容	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。	（11）	⑦	54	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具体的に記載しているか。		既存住基システムのソフトウェアにおける措置と中間サーバーの運用、ソフトウェア、プラットフォームにおける措置をそれぞれ記載する。
	リスクへの対策は十分か							
	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	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。	（11）	⑦	55	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講じている対策を具体的に記載しているか。		端末側環境（取扱者、取扱ソフト、運用）、中間サーバー側環境（運用面、ソフトの面）についても言及する。
	リスクへの対策は十分か							
	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	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。	（11）	⑦	56	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講じている措置を具体的に記載しているか。		処理の後先も含めて、内容の整合性チェックも行う。
	リスクへの対策は十分か							
	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	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。	（11）	⑦	57	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講じている措置を具体的に記載しているか。		届出書など紙媒体や電子媒体の処理も言及する。
	リスクへの対策は十分か							

全項目評価書の記載ポイント集（2016．1．16改訂）

特定個人情報保護評価書（全項目評価書）			審査の観点					
	項目名	記載要領　別添4	審査の番号			考慮事項	指摘事項	改善点／事例
接続	**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	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。	（11）	⑦	58	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具体的に記載しているか。		
	リスクへの対策は十分か							
	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	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。	（11）	⑦	59	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講じている措置を具体的に記載しているか。		
	リスクへの対策は十分か							
	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	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。	（11）	⑦	60	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することや、誤った相手に提供することを防止するために講じている措置を具体的に記載しているか。		
	リスクへの対策は十分か							
	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。	（11）	⑦	61	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、その他のリスク及びそれらのリスクへの対策についての記載はあるか。		
	リスク1：特定個人情報の漏えい・滅失・毀損リスク		（11）	⑧		特定個人情報の保管・消去について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。		
	①NISC政府機関統一基準群	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。							
	②安全管理体制	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安全管理規程	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安全管理体制・規程の職員への周知	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。						

全項目評価書の記載ポイント集（2016．1．16改訂）

特定個人情報保護評価書（全項目評価書）		審査の観点					
項目名	記載要領　別添4	審査の番号			考慮事項	指摘事項	改善点／事例
⑤物理的対策	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 いることです。					入退出者管理や機器や媒体保管場所の施錠管理及び災害対策（耐震設備、無停電装置など）について一部だけ記載され、項目が網羅されていない事例がある。	[記載を要する事項] ・入退出者管理 ・機器や媒体保管場所の施錠管理 ・災害対策（耐震設備、無停電装置など）
具体的な対策の内容		（11）	⑧	62	特定個人情報の漏えい・滅失・毀損を防ぐために行っている物理的な対策について具体的に記載しているか。		
⑥技術的対策	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、不正アクセス対策を実施することです。						[記載を要する事項] ・ウィルス対策ソフトの導入 ・不正アクセス対策の実施 ・無許可媒体への接続禁止
具体的な対策の内容		（11）	⑧	63	特定個人情報の漏えい・滅失・毀損を防ぐために行っている技術的な対策について具体的に記載しているか。	「ウイルス対策ソフトの定期的パターン更新を随時行う。」といった記述では、最新のものに更新されているとは言えない。 モバイル接続機器に対する対策を記載していない。 不正アクセス検知のための通信ログ確認について「定期的に確認している」等、頻度、方法が具体的に記載されていない。 外部記憶媒体のみの対策となっている場合があり、スマートフォンなど新しい情報通信デバイスに対する対策が漏れている。	【事例】 「ウイルスパターンファイルは常に更新し、可能な限り最新のものを使用する。」 「許可された媒体以外への出力をソフトウェアで禁止している。」 「不正なアクセスがないか、毎月1回通信ログを確認している」 「ログは、不正アクセスの記録のみフィルタリングしたものを抽出印刷し、目視で確認後、ファイルに保管している」等、具体的な確認方法、管理方法も記述する。 「USBポートは、業務で使用する機器に限定され、外部記憶媒体やその他の機器に接続出来ないよう設定されている」
⑦バックアップ	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。					「⑦バックアップは，施錠できる保管庫に保管している。」といった記述が多く、通常の電算センターから遠く離れた場への保管が考慮されていない事例が多い。（当該電算センターが被災した場合に重要な情報が消失するリスクがある。）	バックアップ・データの遠隔地への保管と運用の方法を検討し、その内容を記述する。 【事例】 「バックアップ媒体は、耐震・耐火機能を満たした区画に設置した保管庫に保管するほか、遠隔地での保管も実施している。」
⑧事故発生時手順の策定	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。					主にセキュリティ障害、通常事故についての記載事例が多く、大規模災害による滅失・毀損リスクに対する管理策が不足している。 特に住民情報は、災害時に重要な役割を果たす。	地域防災計画の想定を考慮する。 BCP策定状況とすり合わせて記載する。 【事例】 「火災水害、耐震対策がされている。」 「地域防災計画に基づきBCPが策定されておりIT-BCPも公開されている。」 「全庁BCPは策定されているが、情報システムについては、非常用電源、耐震対策について課題が残されている。」

全項目評価書の記載ポイント集（2016．1．16改訂）

特定個人情報保護評価書（全項目評価書）			審査の観点					
	項目名	記載要領　別添4	審査の番号			考慮事項	指摘事項	改善点／事例
7．特定個人情報の保管・消去	⑨重過去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	・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。】						重大事故とは、個人情報の本人の数が101人以上と示されているが、人数基準を超えていても、姓名を付していない他人のメールアドレスを宛先（TO）に記載した場合などは、個人情報の漏洩とは言えないので記載する必要はない。 重大事故の質的基準は、故意に評価実施機関の従業者が個人情報を漏洩、滅失又は毀損した場合のみが示されているので、そのほかの事例は考えないでよい。
	その内容	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。】	（11）	⑧	64	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、重大事故発生時の対応などについて具体的に記載しているか。		【事例】 「地域包括支援センター運営業務におけるＵＳＢメモリの紛失 ①発生時期 平成26年4月18日から平成26年5 月25 日までの間（平成26年5月26日に所在不明の事実が判明） ②事案の概要 K市から委託を受け、高齢者の医療・福祉・介護の相談に応じる業務等を実施している地域包括支援センターの業務実績報告に用いるＵＳＢメモリの一つの所在が不明となった。 ③原因 業務報告書提出の手順に従った「受取確認簿」によるＵＳＢメモリの授受等に係る管理の不徹底が紛失の原因の一つと考えられる。 ④影響 当該ＵＳＢメモリには1,696人分の個人情報が含まれていた。 そのうち、「実態把握名簿」に記録された個別の相談対応等に関する情報（氏名、住所、生年月日、要介護度、世帯状況、緊急連絡先の氏名等）についてはパスワード設定によるセキュリティを確保していた が、支援対象者の氏名が記載されていた「業務実績報告書」についてはパスワード設定なしに記録されていた。 ⑤事故発生時の対応 ・区役所所管課及び地域包括支援センター双方において確認できる箇所を点検 ・区役所所管課により当該ＵＳＢメモリに記録されていた本人への謝罪文の郵送及び電話、窓口等での状況説明等の対応」
	再発防止策	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。】	（11）	⑧	65	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いるか。		[事例] 「情報の重要度に応じた方法により実態把握名簿等を保管するなど、K市情報セキュリティ基準に定められた取扱いを遵守するとともに、速やかに業務実績報告書の手引きの手順をチェックの上、「受取確認簿」の様式を改め、ＵＳＢメモリの授受に係る区役所所管課及び地域包括支援センター職員双方の確認を徹底し、ＵＳＢメモリの所在を常に把握している。」

全項目評価書の記載ポイント集（2016．1．16改訂）

特定個人情報保護評価書（全項目評価書）		審査の観点					
項目名	記載要領　別添4	審査の番号			考慮事項	指摘事項	改善点／事例
⑩死者の個人番号	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。						保管している場合 ・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具体的な保管方法を記述する。
具体的な保管方法		（11）	⑧	66	死者の個人番号を保管している場合は保管方法を具体的に記載しているか。	保管している場合で、「各種証明発行に必要な期間保管する。」とあって具体的な保管方法が記載されていない事例がある。	保管している場合、「生存者の個人番号と同様な方法で各種証明発行に必要な期間に限り保管する。」
その他の措置の内容							
リスクへの対策は十分か							
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	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。	（11）	⑧	67	特定個人情報を最新の状態で保管するために行っている措置を具体的に記載しているか。		【事例】 「特定個人情報ファイル（送付先情報ファイル）は、送付先情報の連携を行う必要が生じた都度作成・連携することとしており、システム上、連携後速やか（1営業日後）に削除する仕組みとする。 また、媒体を用いて連携する場合、当該媒体は連携後、連携先である機構において適切に管理され、市町村では保管しない。 そのため、送付先情報ファイルにおいて特定個人情報が古い情報のまま保管され続けるリスクは存在しない。」
リスクへの対策は十分か							
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	・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。						保管期間が定められていない情報の保管方法について、データの互換性を将来に渉って確保するための措置を記載する。 保管期間が経過した個人情報の確認手順も記載する。
手順の内容		（11）	⑧	68	保管期間を経過した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等について具体的に記載しているか。	「システム上、保管期間の経過した特定個人情報を一括して削除する仕組みとする。」とあって、保管期間が定められていない。	【事例】 「保管期限が定められていないものは、永続性のあるフォーマット○○を用い、媒体□□により保管する。」
その他の措置の内容							
リスクへの対策は十分か							
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。	（11）	⑧	69	特定個人情報の保管・消去において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。		【事例】 「送付先情報ファイルは、機構への特定個人情報の提供後、速やかに市町村CSから削除される。その後、当該特定個人情報は機構において管理されるため、送付先情報ファイルのバックアップは取得しない予定である。」

全項目評価書の記載ポイント集

特定個人情報保護評価書（全項目評価書）			審査の観点					
項目名			記載要領　別添4	審査の番号			考慮事項	指摘事項	改善点／事例
IVその他のリスク対策	1監査	①自己点検	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。	（11）	⑨		特定個人情報ファイルの取扱いについて自己点検・監査や従業者に対する教育・啓発を行っているか。	自己点検は主体者自らが実施するものであるが、委託先（特定個人情報ファイル取扱い事業者、情報システム運用事業者等）に対しても同様の自己点検を実施させることが必要である。自己点検は自組織に適したチェックリストをブラッシュアップして、管者用と職員用を作成する。それぞれの回答内容を集約し、その差異分析して、課題や脆弱点を洗い出して、管理者・担当者及び職員を交えて、情報セキュリティ対策の見直しを実施することが重要である。	[記載を要する事項] ①どのようなチェックリストを用いているのか ②実施対象は誰なのか ③実施頻度はどうか ④誰に報告するのか
		具体的なチェック方法				70	評価書に記載したとおりに運用がなされていること等について、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具体的に記載しているか。	多くの事例で、各評価実施機関が作成している規程や書類名や役職名を入れて実態を具体的に記述していない。 ただし、法令名等をいたずらに羅列しても、内容が明瞭になるわけではなく、住民にとっては何も分からない。	【事例】 「年1回、評価書の記載内容通りの運用がなされていることを、本市の情報セキュリティガイドラインに基づき，住民基本台帳ファイルセキュリティチェックリストにより、担当部署で自己点検を行っている。その結果は情報セキュリティ責任者に報告し、不備があれば改善策を策定し実施している。」
		②監査	・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。					特定個人情報保護の監査では、内部監査のみならず、外部監査を実施してはじめて「特に力を入れて行っている」と言える。 多くの自治体等では、内部監査のみを記述している事例が多い。内部監査は組織内部の要員によって行われるため、厳密な意味で「公平中立的立場からの監査」を受けたとは言えず、リスクがあると思われる。それ故、内部監査に加えて、少なくとも一年に一度の外部監査を行うべきである。	[記載を要する事項] ①どのような監査基準に基づいて、監査を実施いるのか ②監査人は誰なのか ③実施頻度はどうか ④誰に報告するのか
		具体的な内容	監査事項、頻度、実施体制、活用			71	評価書に記載したとおりに運用がなされていること等について、どのように監査するか具体的に記載しているか。		従来から実施している外部監査に特定個人情報保護関係の監査を追加する旨を記述する。 【事例】 「年1回，評価書の記載内容通りの運用がなされていることを、システム監査基準に基づき，外部の専門家による監査を実施している。その結果は情報セキュリティ責任者に報告し、不備があれば改善策を策定し実施している。」
	2従業者に対す	従業者に対する教育・啓発	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。						SR（企業や公共企業体の社会的責任：CSR，GSR等）が厳しく問われる時代であり、教育は戦略的投資となっている。また、徹底したセキュリティ教育を実施している企業や組織体等は、SRを実行しており、社会から信頼を得て高いレピュテーション評価が得られる。 従業者への教育・啓発は、直ぐに効果が見えるものではない。しかし、個人情報保護、セキュリティに関しては、教育が最も重要であり、組織のなかで、セキュリティ文化を醸成することが、最も重要なのである。

全項目評価書の記載ポイント集

特定個人情報保護評価書（全項目評価書）			審査の観点		
項目名		記載要領　別添4	審査の番号	考慮事項	指摘事項	改善点／事例
る教育・啓発	具体的な内容		72	特定個人情報を取り扱う従業者等に対しての教育・啓発や違反行為をした従業者等に対する措置について具体的に記載しているか。	個人情報保護、情報セキュリティに関する研修を行っていることのみを記載している。	定期的に行われる個人情報保護・情報セキュリティ研修について記述する。 ・組織全体向け研修 ・階層別研修 ・業務所管別研修等 規程・法令の違反者は懲戒処分、罰則があることも明記する。 研修後、理解度チェックテスト等により効果測定を行う。 【事例】 「・従業者に対して、新人研修にて個人情報保護及び情報セキュリティ教育を実施している。また、年に一度、異動に合わせて、定期的に個人情報保護及び情報セキュリティの集合教育を実施している。」 「・従業者毎の教育・研修受講記録により、受講確認できる仕組みがあり、未研修を防止している。」
3その他のリスク対策	その他のリスク対策	・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。				【事例】 「セキュリティ委員会の設置 従業者に対する教育・啓発は最も重要な対策の一つであるが、その結果として一人ひとりのセキュリティ認識を高めることが重要である。そのためには、情報を共有し、トップマネジメントをはじめとする情報セキュリティに対する意識改革が必要である。その実行組織として、「情報セキュリティ委員会」を設置し、定期的な会議をおこなって、情報セキュリティ意識の改革と文化の醸成をはかることに努めている。」