ことから、地方公共団体の長等が第三者点検を行う場合も、点検者に法令や契約で守秘義務を課すなどした上で、非公表部分も含め全項目評価書を全て提示した上で点検を受けるものとする。非公表については、後記（６）を参照されたい。

ウ　全項目評価の効果

○　全項目評価の効果は、重点項目評価と同様であるが、それに加え、特に全項目評価では、プライバシー等法的に保護される権利利益に対しより侵害性の低い方法を採用できないか否かを具体的に検討するため、プライバシー等保護のためのきめ細かい分析・評価を行うことができる。

○　専門性・中立性を有する委員会が全件審査（地方公共団体等については、全件第三者点検）することで、各機関以外の第三者の視点から、専門的・中立的・客観的な評価を加えることができ、各機関の行った全項目評価の妥当性を確認することができる。

○　個人のプライバシー等に対する影響は、各機関において予測・検討・評価するものであるが、それ以外にも様々な視点からの評価が必要である。例えば一般的にはプライバシー等に対する影響が低いと考えられるものの、特定のカテゴリーの個人、特に社会的少数者の個人にとってはプライバシー等に対する影響が相当程度あると考えられる場合も十分ありうる。

全項目評価では、国民は、意見聴取プロセスを通し、プライバシー等に対する影響やそれを軽減するための措置について様々な立場・視点から意見を述べることができ、各機関の全項目評価書に対し見直しを促すことができる。

また、全項目評価書が公表されることで、国民は、意見聴取プロセスで示された全項目評価書に対し具体的にどのような見直しがなされたかについて確認することができる。

○　公表された全項目評価書を通じて、国民は、各機関が、どのような事務においてどのような法令上の根拠により、具体的にどのように特定個人情報ファイルを取り扱っているか、どのようなリスク対策を行っているかを詳細に確認することができる。

（６）情報保護評価書の公表

○　作成した評価書及びその添付資料は、**原則として全て公表**するものとする。

○　ただし、評価書及びその添付資料を全て公表することで情報セキュリティ上のリスクとなりうる場合[26]や違法行為を助長する恐れも考えられ、かかる懸念を有する各機関が委員会に対しても不十分な情報しか提供しないことも考えられることから、**一定の場合（※）**には、**委員会へは**評価書及びその添付資料の**全てを提出した上で、国民に対しては非公表**とする。

○　（※１）例えば、重点項目評価書、全項目評価書における「Ⅰ２③他との接続」「Ⅱ６①保管場所」などを非公表とすることが考えられる。詳細は、追って委員会より示されることが考えられる。

○　（※２）犯罪の捜査、租税に関する法律の規定に基づく犯則事件の調査、公訴の提起又は維持のために保有する特定個人情報ファイルに関する評価書については、評価書及びその添付資料全体を非公表とする。

４　情報保護評価実施後に行うべき措置

（１）情報保護評価書記載事項の履行

○　情報保護評価は、プライバシー等に対する影響を事前評価した上でそれを軽減・緩和するための合理的措置を講ずることにより、プライバシー等に対し特段の影響を及ぼさないと認められる特定個人情報の取扱いを確立するためのものである。

しかし、情報保護評価書に記載された措置が実際に講じられない場合は、プライバシー等に対し特段の影響を及ぼさないとは言えないこととなる。

また情報保護評価は、各機関が国民のプライバシー等保護にどのように取り組んでいるかについて、各機関自身が宣言し、国民の信頼を獲得することを目的とする。

26　例えば、ネットワーク構成、サーバ構成、アプリケーションのバージョン情報、サーバの物理的位置などを公表すると、セキュリティ上のリスクとなりうることが考えられる。

したがって、言うまでもないことであるが、各機関は、情報保護評価書に記載された事項を、責任をもって履行しなければならないものである。

（２）評価書の事後チェック及び情報保護評価の再実施

○　各機関は、委員会に**情報保護評価書を提出した後**、**少なくとも１年以内に**、情報保護評価書の記載内容が実態と異なっていないかどうかを確認しなければならない。また、その後も１年ごとに事後チェックを実施しなければならない。

事後チェックの結果、情報保護評価書を修正する必要があった場合は、速やかに情報保護評価書を修正するものとし、特段修正の必要がない場合については、事後チェックの結果を公表等する必要はない。

○　各機関には、国民のプライバシー等の権利利益の保護を継続的に行う責務があり、いったん情報保護評価書を作成及び公表しさえすれば、かかる責務が全て履行済みとなるものではない。

各機関は、情報保護評価書にて国民に対して宣言した措置を講じ続ける必要があり、また一度情報保護評価書を作成した後も、個人情報保護に関する技術の進歩や社会におけるプライバシー概念の変容等を踏まえ、適切な見直しを行い、プライバシー等保護のための継続的な取り組みを行うものとする。情報保護評価は、かかる継続的な取り組みを確認するためのものである。

したがって各機関は、プライバシーリスクに対する対策は、時代の変化・技術の進歩・国際動向などによって変化しうるものであり、**情報保護評価を実施してから５年経過するものについては**、リスク対策などを見直す必要がある可能性が高いため、**情報保護評価を再度実施する**ものとする。新規保有時に評価を実施した後、再評価をしたものであっても、当該再評価から５年を経過する前に、再々評価を実施するものとする（再々評価以降についても、同様である）。

○　情報保護評価書の記載に**反する取扱い**がなされたか又はなされている場合は、後記５（２）の通り、**委員会の助言・勧告等**の対象となる。

５　情報保護評価に係る違反に対する措置

（１）情報保護評価の未完了に対する措置

○　情報保護評価は、特定個人情報ファイルの適正な取扱いを確保し、個人のプライバシー等に対する影響を事前に抑止・軽減するために行うものであり、情報保護評価を実施していない特定個人情報ファイルを取り扱う業務・システムは、特定個人情報ファイルの適正な取扱いの確保のための措置や、個人のプライバシー等に対する影響の抑止・軽減措置が十分講じられていないものと考えられる。

かかる業務・システムで取り扱う特定個人情報ファイルについて、情報連携を行わせると、不適正な取扱いがなされていたり、又は個人のプライバシー等に影響を与えうる特定個人情報ファイルがネットワークを通じてやりとりされることとなり、適正な取扱いがなされている他の業務・システム（他の情報提供者又は情報照会者のシステムや情報提供ネットワークシステム等）に対し、悪影響を及ぼすおそれがある。

そこで、**情報保護評価を実施しなければならないにもかかわらず情報保護評価を完了していないもの**について、**情報連携を行うことが禁止されている（番号法第２７条第６項・第２１条第２項第２号）**。

○　情報連携を行わないこととされている機関については、委員会の**助言・指導・勧告・命令権限等に基づき、是正を促す**ものとする。

（２）情報保護評価書の記載に反する取扱いに対する措置

○　**特定個人情報ファイルの取扱い実態が情報保護評価書の記載に反していたとき**は、委員会の**助言・指導・勧告・命令・立入検査権限等に基づき、是正を促す**ものとする。

第７　関連制度との関係性

１　関連制度

○　情報保護評価はプライバシー等への影響を評価するものであり、その評価対象には、個人情報保護対策と情報セキュリティ対策が含まれうるため、両対策に関連する既存制度と情報保護評価との関係を以下に整理する。

○　まず、個人情報保護対策の関連既存制度としては、以下が挙げられる。

①個人情報ファイル簿等（行政機関の長・独立行政法人等のみ）

②プライバシーマーク制度

次に、情報セキュリティ対策の関連既存制度としては、以下が挙げられる。

③政府統一基準群

④ISMS適合性評価制度

⑤ITセキュリティ評価及び認証制度（JISEC）

２　個人情報ファイル簿等

○　行政機関個人情報保護法及び独立行政法人等個人情報保護法上の個人情報ファイル簿により、本人は自己に関する情報の利用実態をより的確に認識することができ、また個人情報ファイル簿は、開示請求等の本人関与の端緒となるものである。

これに対し情報保護評価は、本人関与の端緒のみの目的ではなく、特定個人情報ファイルの適切な取扱いを確保するために、各機関における特定個人情報ファイルの取扱いの流れ及び全体像を明示し、分析・評価することで、各機関が国民のプライバシー等の法的に保護される権利利益保護にどのように取り組んでいるかについて各機関自身が宣言し、国民に対する説明責任を果たし、もって特定個人情報ファイルの取扱いについての国民の信頼を獲得することを目指すものである。

また個人情報ファイルの事前通知並びに個人情報ファイル簿の作成及び公表は、一定の事項について「通知・公表」するものであるが、情報保護評価は「通知・公表」にとどまらず、プライバシー等への影響とその対策を事前に「分析・評価」することにより、プライバシー等への悪影響を未然に防止し、また事後の大規模な仕様変更を防ぎ、不必要な財政支出の防止を目的とするものでもある。

○　このように両制度は目的が一部重複はするものの異なるため、記載項目や記載の深度が異なるものである。

　しかし、記載事項について一定の重複がある個人情報ファイルと情報保護評価双方を義務付けるのは効率的でないため、重点項目評価書及び全項目評価書の記載事項を個人情報ファイルの保有等に関する事前通知事項及び個人情報ファイル（簿）の記載事項を包含するように設計した上で、重点項目評価又は全項目評価を完了した際は個人情報ファイルの保有等に関する事前通知（番号法第２９条第１項並びに第３０条第１項及び第２項により読み替えられて適用される行政機関個人情報保護法第１０条）が行われたものとみなすこととされる（番号法第２７条第５項参照）。

　なお、独立行政法人等については個人情報ファイル簿の作成及び公表義務は規定されているものの（独立行政法人等個人情報保護法第１１条）、個人情報ファイルの事前通知規定は設けられていない。

○　ただし、個人情報ファイル簿の作成及び公表（行政機関個人情報保護法第１１条及び独立行政法人等個人情報保護法第１１条）についても上記のようなみなし規定を置くこととすると、重点項目評価又は全項目評価を完了済の特定個人情報ファイルについては個人情報ファイル簿が存在しない一方で、重点項目評価又は全項目評価を完了していない特定個人情報ファイルについては個人情報ファイル簿のみが存在することとなるため、一覧性を欠くこととなる。

　このため、個人情報ファイル簿が国民による開示請求等の端緒となることに鑑み、重点項目評価又は全項目評価を完了した場合であっても、個人情報ファイル簿の作成及び公表は、引き続き行うものとされており、この点留意する必要がある。

３　プライバシーマーク

○　プライバシーマーク制度は、個人情報保護法を基にして、さらにそれに上乗せした確認を行っているものである。

　これに対し、情報保護評価は個人情報保護法令遵守にとどまらず、プライバシー等保護を目的としたものであり、また個人情報保護法令についても、行政機関、地方公共団体及び独立行政法人については、プライバシーマーク制度と基準となる法令自体が異なるものである。

○　プライバシーマーク制度は個人情報保護法を遵守するための組織**体制**が

とられているか、PDCAサイクルが有効に機能しているか確認するためのものである。

これに対し情報保護評価は、個々の特定個人情報ファイルの取扱いをプライバシー等への影響度の観点から確認するものであり、対象が異なるといえる。

○　したがって、プライバシーマークを取得している各機関であっても、個々の特定個人情報ファイルのプライバシー等への影響を分析・評価したものではないので、情報保護評価を実施する必要がある。

ただし、既にプライバシーマークを取得している各機関については、情報保護評価書にその旨も合わせて記述することで、個人情報保護に関し適切な体制をとっていることを宣言することができるものと考えられる。

４　政府統一基準群、ISMS 適合性評価制度及び IT セキュリティ評価及び認証制度（JISEC）

○　情報セキュリティ対策は、情報資産のCIA（Confidentiality機密性、Integrity完全性、Availability可用性）の維持を図ることを目的とする。

これに対し、情報保護評価の目的はプライバシー等保護であり、プライバシー等保護にとって、セキュリティ対策は一つの手段にすぎないと考えられる。

○　したがって、上記制度の認定等を受けている各機関であっても、情報保護評価を実施する必要がある。

ただし、既に上記制度の認定等を受けている各機関については、情報保護評価書においてその旨も合わせて記述することで、適切なセキュリティ対策を講じていることを宣言することができるものと考えられる。

以上