

情報保護評価報告書の記載様式項目（案）

1 事業の概要

→事業及びシステムの概要を記述する

（質問例）

- ・事業の概要、目的、法律上の根拠、担当部署
- ・システムの概要、全体構成図、利用技術
- ・システム改修の場合は、さらに改修点について記載する

コメント [1]: 米要約・概説

コメント [2]: 加 Ig

コメント [3]: 豪①

コメント [4]: 加 Ie

コメント [5]: 法 1 0 I ②組織の名称のほか、部署名も記載する

コメント [6]: 豪②、加 IVc

2 個人情報のフロー

→当該システムにおける個人情報の流れを記述する

（質問例）

- ・当該システムにおける個人情報の流れ
- ・個人情報の取扱いに複数の組織が関与するか
- ・個人情報を取り扱う職員数・端末数

コメント [7]: 英フル（４）

コメント [8]: 米概説

コメント [9]: 法 3 I II

コメント [10]: 米 2. 1、豪② 1. 1、加 IIIab、法 1 0 I ④記載項目

コメント [11]: 法 1 0 I ④個人の範囲に相当

3 プライバシーへ与える影響及びその対策の概要

（詳細は以下の各項目で記載すること）

→当該システムにおける、プライバシーへ与える影響及びその対策の要約を記述する

コメント [12]: 米 1. 1、豪② 1. 1

コメント [13]: 米 3. 1、英 DPA コンプラチェック II 1. 2. 2に類似のものあり

コメント [14]: 法 3 I

4 収集・利用する個人情報

→プライバシーに与える影響を十分考慮し、特定の目的のために必要な種類・範囲の情報のみを収集・利用していることを具体的に記述する

（質問例）

- ・収集・利用する個人情報の項目及び量（個人数及び一個人当たりの情報数）
- ・かかる個人情報を取得する法的権限
- ・かかる個人情報を取得する必要性・目的（特定の項目や種類がなぜ必要なのか）
- ・収集・利用する個人情報の種類・量は、事業の目的と整合しているか
- ・情報は識別されない形又は匿名にて収集できないのか、できる場合なぜ識別される形で収集されるのか

コメント [15]: 豪② 1。法 1 0 I ③の個人情報ファイルの利用目的の転記では、特定の項目や種類がなぜ必要かわからない場合は、法 1 0 I ③の利用目的よりも詳細に記載する。

コメント [16]: 豪② 1、英 DPA コンプラチェック II 3. 1

コメント [17]: 豪② 1

5 個人情報の収集方法

→プライバシーに与える影響を十分考慮し、適切な収集方法を用いていることを具体的に記述する

(質問例)

- ・ 個人情報はどこからどのようにいつ収集されるか

(例) 本人から、情報連携基盤を通じて〇〇省〇〇局〇〇課から、公表情報から

- ・ なぜその情報源から個人情報を収集するのか。他にプライバシー侵害の可能性がより低い情報源はないのか。

- ・ 従前から収集している個人情報を、本事業のために転用するか。利用目的を変更する場合は、従前の利用目的と本事業の利用目的との間にどのような関連性があるか。転用する場合は、転用を可能とする法律上の根拠とそれに該当する事実を具体的に説明する。

- ・ 本人から直接書面に記録された個人情報を取得する場合は、あらかじめ利用目的を本人に明示するに当たり、どのような方法をとっているか。利用目的の明示が不要な除外事由に該当する場合は、除外事由を具体的に示す。

- ・ 収集の時期・頻度

コメント[18]: 米2. 2. 2. 3、豪②1. 1、1. 3、加Iva、法10I⑤

コメント[19]: 米2. 2. 2. 3が類似の考え方をとっている

コメント[20]: 法3Ⅲ

コメント[21]: 法8Ⅱ

コメント[22]: 法4

コメント[23]: 豪②1. 3

6 個人情報の利用方法

→プライバシーに与える影響を十分考慮し、必要な利用方法に限定していることを具体的に記述する

(質問例)

- ・ 個人情報を具体的に誰がどのようにいつから利用するか

- ・ データマッチング、データマイニングを行うか

- ・ かかる利用方法は、事業の目的・収集目的と整合しているか

- ・ 個人情報を元に、個人の権利利益に影響を与えうる決定を行うか

- ・ 個人情報を閲覧できる者、更新できる者をどのように必要最小限に限定しているか

- ・ 個人情報の利用が上記の通りにしか行えないようどのような措置を講じているか

(例) 職員への研修、アクセス制御等のシステム上の措置

- ・ 目的外利用を特定部局・機関のみに限定しているなどの措置を講じているか

コメント[24]: 米3. 3

コメント[25]: 豪②2. 3、英フル(8)ショート(8)、米3. 2に類似のものあり

コメント[26]: 豪②2. 1

コメント[27]: 米3. 2、ISO6

コメント[28]: 米3. 3に類似のものあり

コメント[29]: 米3. 4

コメント[30]: 法8Ⅳ

7 個人情報の管理方法

→ プライバシーに与える影響を十分考慮し、適切な管理方法をとっていることを具体的に記述する

(例) 業務に必要な者のみにアクセス権限を与える、誰がアクセスしたかのログを収集する、外部記憶装置を接続できないようにする、個人情報の記録された書面は施錠された場所に保管するなど

(質問例)

- ・「番号」に係る個人情報をそれ以外の個人情報と区別して厳格な管理方法をとっているか。どのような管理方法をとっているか。区別していない場合は、その理由を記載する。
- ・機微性の高いデータをその他のデータと区別して厳格な管理方法をとっているか。どのような管理方法をとっているか。区別していない場合は、その理由を記載する。
- ・個人情報について、どのような組織的管理体制をとっているか
- ・委託先がある場合、どのように委託先を管理しているか
- ・死者の識別情報を保有している場合、どのように管理しているか。

8 個人情報の第三者提供

→ プライバシーに与える影響を十分考慮し、第三者提供について適切な運用を行っていることを具体的に記述する

(質問例)

- ・個人情報を第三者（委託先を含む）に提供するか。提供する場合、提供先を記載する。
- ・提供する場合、提供が可能となる法律上の根拠とそれに該当する事実を具体的に説明する。またどのような組織に対し何のためにどのようにいつ提供を行うのか。
- ・第三者提供は、事業の目的及び収集目的と整合しているか
- ・本人の同意を取得しているか
- ・提供する個人情報の種類、数、頻度
- ・提供先での利用方法・管理方法はどのようなものか
- ・提供先から、さらに再提供されるか

コメント[31]: 法 6 I

コメント[32]: 「番号」に係る個人情報は、他の個人情報に比べ、番号法等に基づき特に厳格な管理が要請されるため

コメント[33]: 英 DPA コンプラチェック II 8. 1. 5

コメント[34]: 英 DPA コンプラチェック II 1. 1. 2 に類似の項目あり

コメント[35]: 行政機関及び独立行政法人等については、行政機関個人情報保護法の規定等を踏まえた指針（行政機関の保有する個人情報の適切な管理のための措置に関する指針について（平成16年9月14日総管情第84号総務省行政管理局長通知）及び独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針について（平成16年9月14日総管情第85号総務省行政管理局長通知）

コメント[36]: 法 6 II

コメント[37]: 米 6. 1

コメント[38]: 加 IVh、法 10 I ⑥ 経常的提供先（行政機関個人情報保護法上の経常的提供先にも、一定期間ごとに提供する提供先、不定期であっても依頼があれば必ず提供することとしている提供先なども含まれる。）

コメント[39]: 法 8 II IV、豪② 3

コメント[40]: 豪② 3

コメント[41]: 米 6. 5

コメント[42]: 法 9、米 6. 1 に類似のものあり

コメント[43]: 米 6. 3

9 個人情報の保管期間

→ プライバシーに与える影響を十分考慮し、適切な期間としていることを具体的に記述する

(質問例)

- ・ 収集した個人情報はすべて保管されるか
- ・ 収集した個人情報の保管期間
- ・ かかる期間は、事業の目的及び収集目的と整合しているか (不必要に長期間保管していないか、個人の権利実現のために十分な期間保管しているか)
- ・ 保管期間が長期になるほど、情報の正確性・完全性を保障する必要があるが、それに留意した対応をとっているか

コメント [44]: 米 1. 4、5. 2

コメント [45]: 米 5. 1

コメント [46]: 米 5. 1

コメント [47]: 英 DPA コンプラチェック II 5. 2. 2 に類似の項目あり

10 個人情報の抹消方法

→ プライバシーに与える影響を十分考慮し、適切な抹消方法をとっていることを具体的に記述する

(質問例)

- ・ 保管期間が到来したものを適切に抹消できるような手順を設けているか
- ・ 個人情報の廃棄はどのようにして安全に行われるのか

コメント [48]: 英 DPA コンプラチェック II 7. 4. 1

コメント [49]: 豪② 5. 1

11 個人情報の正確性の確保・救済

→ プライバシーに与える影響を十分考慮し、個人情報の正確性確保のために適切な方法を用いていることを具体的に記述する。また個人の被害を救済するために、適切な方法を用いていることを具体的に記述する。

(質問例)

- ・ 個人情報が不正確な場合に、本人及び行政機関が被る損害について評価がなされているか
- ・ どのように、またどの程度の頻度で情報の正確性をチェックしているか (例) 個人情報入力時の照合・確認、誤りを発見した場合の訂正手続
- ・ 本人による誤り訂正の実質的な機会があるか
- ・ 個人情報が誤って削除されたり改変されたりしないよう、どのような措置を講じているか
- ・ 開示請求、利用停止請求、訂正請求について、本人が利用しやすいような措置を講じているか (例) マイ・ポータル上で×情報について自動表示を行っている
- ・ 個人情報に関する個人からの苦情をどのように処理しているか。個人からの苦情を保管等管理しているか。
- ・ 「番号」の盗用、個人情報の漏えい等、問題が発生した際の対応手順を定め

コメント [50]: 豪② 6、英 DPA コンプラチェック II 4. 1. 1

コメント [51]: 法 5、米 2. 4、英 DPA コンプラチェック II 4. 1. 2

コメント [52]: 米 2. 4

コメント [53]: 法 4 7 I、米だと 7 に個人が救済を求める手続についての項目がある。なお法 1 0 I ⑧の請求を受理する組織の名称及び所在地についても記載する。

コメント [54]: 法 4 8

コメント [55]: ISO AnnexD の 6 にクレームを収集したかとの項目あり。第三者機関側のみならず情報保有機関側でも行うかは要検討

ているか。定めている場合、それはどのような手順か。

- ・災害発生時等の対応手順を定めているか。特に救済や個人情報の正確性確保のためにどのような対応をとることが予定されているか。

1.2 監査等

→プライバシーに与える影響を十分考慮し、適切な監査等を行っていることを具体的に記述する

(質問例)

- ・個人情報にアクセスする職員に関する手続や認証があるか
- ・個人情報の収集から廃棄までの各過程において、どの職員がどの個人情報を取り扱ったか記録しているか。
- ・上記を記録している場合、記録のスキームはどのようなになっているのか
(例) 何の情報をどこに記録後、媒体に移しているか。行政機関の委託先による取扱いについても記録されているのか。
- ・上記を記録している場合、かかる記録はどの程度の頻度で誰が確認しており、どの程度の期間保管されているのか
- ・監査は実施しているか。実施している場合どのような事項について監査しているか。監査の結果をどのように活用しているか。
- ・個人情報の不正利用を防止するための措置の有無
(例) 特定の記録にアクセスがなされた際、記録が適正に利用されたか確認するため、上席者へ通知がなされる
- ・システムへの新しいアクセスや情報の新しい利用は、どのように確認・レビューされ、承認されるのか

※行政機関個人情報保護法、諸外国質問票、ISO22307などを参考にして作成

コメント [56]: 行政機関及び独立行政法人等の場合は、指針に基づき個人情報の適切な管理に関する定めを整備しており、その中で安全確保上の問題への対応について通常規定している。独立行政法人等に該当しない関係機関については、この限りでない。

コメント [57]: 豪②5、英 DPA コンプラチェック II 7. 5

コメント [58]: 米 8. 3
紙媒体も対象とする場合は、「電子媒体、紙媒体を問わず」などとすることが考えられる。

コメント [59]: 英 DPA コンプラチェック II 2. 1. 1。米 6. 4 では第三者提供について記録保管

コメント [60]: 英 DPA コンプラチェック II 2. 1. 3

コメント [61]: 英 DPA コンプラチェック II 2. 1. 2、米 6. 5 では第三者提供について記録監査

コメント [62]: 米 8. 1。
なお、行政機関及び関係機関においては、指針第 10 にて、個人情報の適切な管理のために講ずべき最小限の措置として監査及び点検の実施が記載されているが、独立行政法人等に該当しない関係機関については、この限りでない。

コメント [63]: 豪②2. 3、5。米 8. 1 に類似のものあり

コメント [64]: 米 8. 4