平成 27 年 5 月 19 日
平成 28 年 2 月 12 日一部改正
平成 30 年 9 月 12 日改正

一般財団法人　日本情報経済社会推進協会（JIPDEC）
プライバシーマーク推進センター

特定個人情報の取扱いの対応について

「行政手続における特定の個人を識別するための番号の利用等に関する法律」（以下、「番号法」という。）（平成 25 年 5 月 31 日公布）に基づく社会保障・税番号制度により、事業者は、個人番号をその内容に含む個人情報（以下、「特定個人情報」という。）の取扱いに際しては、番号法及び個人情報保護委員会より特定個人情報の適正な取扱いを確保するための具体的な指針として公表されている「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」（以下、「特定個人情報ガイドライン」という。）の遵守が必要です。

プライバシーマーク付与事業者、新規に付与を受けようとする事業者（以下、合わせて「プライバシーマーク付与を受けようとする事業者」という。）においては、番号法の遵守はもちろん、「JIS Q 15001:2017（個人情報保護マネジメントシステム―要求事項）」（以下、「規格」という。）への適合も求められることから、番号法及び規格に基づき対応を必要とする事項を以下に示します。

なお、以下に示す事項は、今後国が示す法令等に応じて、見直す可能性があります。

1.規格に基づき対応を必要とする事項

規格に基づき、プライバシーマーク付与を受けようとする事業者が対応すべき事項を以下に示す。

（1）個人情報の特定、リスクアセスメント及びリスク対策（規格 A.3.3.1、A.3.3.3）

《対応を必要とする事項》

- **特定個人情報（個人番号を含む）を、個人情報を管理するための台帳に特定し、個人情報保護リスクを特定し、分析していること。**

《留意事項》

プライバシーマーク付与を受けようとする事業者は、既に定めた手順に従い、個人情報の特定及び個人情報保護リスクの特定し、分析し、対策を実行しているが、特定個人情報もその対象となる。

特定個人情報は、特定個人情報ガイドラインに示す通り、番号法に定めた事務を行う場合を除き、保管することができない。このため、規格 A.3.3.1（個人情報の特定）で個人情報を管理するための台帳の記載項目である保管期限を記載するときは、

この点に留意する必要がある。

また、個人情報保護リスクには、規格の定義（3.43）が示す通り、関連する法令、国が定める指針その他の規範に対する違反も含まれる。よって、プライバシーマーク付与を受けようとする事業者は、番号法に反する取扱いを個人情報保護リスクと認識し、リスク分析を踏まえて対策を講じ、PMS に反映する必要がある。

さらに、規格 A.3.4.3.2（安全管理措置）は、取り扱う個人情報の個人情報保護リスクに応じた安全管理措置を講じることを求めている。プライバシーマーク付与を受けようとする事業者は、引き続き、個人情報保護リスクに応じた措置を実施し、個人情報保護リスク及び対策の見直しを適宜行うことが必要である。なお、安全管理措置については本資料 2.（2）項をあわせて参照のこと。

（2）法令、国が定める指針その他の規範（規格 A.3.3.2）

《対応を必要とする事項》

- **法令等を特定し参照していること。**

《留意事項》

規格 A.3.3.2（法令、国が定める指針その他の規範）を踏まえ、プライバシーマーク付与を受けようとする事業者は、規格 B.3.3.2 を参考に、自社で特定し参照する対象となる法令等を確認すること。

なお、本審査項目は、「プライバシーマーク付与適格性審査基準」A.3.3.2 の審査項目 2.と同等に確認を行う。

（3）資源、役割、責任及び権限（規格 A.3.3.4）

《対応を必要とする事項》

- **事務取扱担当者の役割・権限が内部規程として文書化されていること。**

《留意事項》

規格 A.3.3.4（資源、役割、責任及び権限）では、個人情報の管理のための役割、責任及び権限を明確に定め、文書化することを求めている。

特定個人情報ガイドライン（「(別添) 特定個人情報に関する安全管理措置（事業者編)」を含む）では、特定個人情報等を取り扱う事務に従事する従業者（以下、「事務取扱担当者」という。）の明確化を求めている。

よって、プライバシーマーク付与を受けようとする事業者は、事務取扱担当者の役割、責任及び権限を明確に定め、文書化する必要がある。

（4） 緊急事態への準備（規格 A.3.3.7）

《対応を必要とする事項》

- **重大事態に該当する事案又はそのおそれのある事案が発覚した場合に、個人情報保護委員会に直ちに報告する手順が内部規程として文書化されていること。**
- **重大事態に該当する事案又はそのおそれのある事案が発覚した場合、定めた手順に従って緊急事態への対応を実施していること。**

《留意事項》

規格 A.3.3.7（緊急事態への準備）では、個人情報の漏えい、滅失又はき損が発生した場合に備え関係機関に直ちに報告する手順を定め、緊急事態発生時には手順に従い報告することを求めている。

「特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則」（平成 27 年特定個人情報保護委員会規則第 5 号）では、特定個人情報の安全の確保に係る重大な事態が生じたときは、個人情報保護委員会に報告することを求めている。この報告は、重大事態に該当する事案又はそのおそれのある事案が発覚した時点で直ちに行うことが求められている（「事業者における特定個人情報の漏えい事案等が発生した場合の対応について」（平成 27 年特定個人情報保護委員会告示第 2 号））。

よって、プライバシーマーク付与を受けようとする事業者は、特定個人情報の安全の確保に係る重大な事態が生じた場合に備え、個人情報保護委員会に直ちに報告する手順を定め、当該事態の発生時には手順に従い報告する必要がある。

2. 番号法に基づき対応を必要とする事項

特定個人情報の取扱いにあたり、規格 A.3.3.2（法令、国が定める指針その他の規範）を踏まえ、番号法及び特定個人情報ガイドラインに基づき対応を必要とする事項を示す。これらの事項は、必ずしも規格には含まれていないが、法令遵守は、規格の前提である点に留意が必要である。規格は個人情報の取扱いに関する個々の法令等への違反について規定しているわけではないが、これらの法令等に違反した場合は、規格 A.3.3.2 で求める特定・参照が行われていない、あるいは特定・参照していても適切に管理されていなかったということになり、規格に対しても不適合であるといえる。この場合、プライバシーマーク付与を受けようとする事業者は、法令等を特定し参照する手順を見直す必要がある。

以下は、規格項番毎に、番号法に基づき対応を必要とする事項を示し、対応する上で留意が求められる点の概要を記す。対応にあたっての具体的な方法等は、国が示す資料を適宜確認すること。なお、以下に示す事項のうち規格が求める事項については、「プライバシーマーク付与適格性審査基準」に基づき、付与適格性審査時に確認を行う。

（1） 取得、利用及び提供に関する原則（規格 A.3.4.2）

規格 A.3.4.2 では、事業者に、A.3.4.2.5(本人から直接書面によって取得する場合の

措置)、A.3.4.2.6(利用に関する措置)、A.3.4.2.8(個人データの提供に関する措置)等で本人の同意を得ることを、求めているが、他方で、事業者は、本人の同意の有無にかかわらず、法令等に基づく他人の個人番号を利用した事務を行うために、他人の個人番号を取得、利用、提供する義務を負っており、また、番号法に基づき個人番号を取得、利用、提供する場合には、規格 A.3.4.2 に基づき本人の同意を得ることまでは求めない。

取得、利用及び提供の場面において、番号法に基づく留意点を以下に概略する。

- 個人番号の利用範囲は、番号法第 9 条（利用範囲）に示す範囲（個人番号利用事務、個人番号関係事務）に限定される。規格 A.3.4.2.6（利用に関する措置）と異なり、本人の同意があったとしても、利用範囲を超えた利用は認められない。
- 特定個人情報ファイルの作成は、個人番号利用事務、個人番号関係事務を処理するために必要な範囲に限られている（番号法第 29 条 特定個人情報ファイルの作成の制限)。例えば、個人番号を含むデータベースを作成した場合や、既存のデータベースに個人番号を追加した場合は、当該データベースの利用の範囲に留意する。
- 特定個人情報の提供は、番号法第 19 条（特定個人情報の提供の制限）に規定された場合を除き、禁止である（番号法第 19 条)。また、番号法では特定個人情報に関しては個人情報保護法の第 23 条（第三者提供の制限）の規定は適用除外とされている点に留意する。つまり、番号法では、個人情報保護法第 23 条第 5 項第 3 号の規定も適用されず、個人番号の共同利用は認められない。
- 個人番号の提供を受ける場合は、番号法第 16 条（本人確認の措置）により本人確認が義務付けられ、確認方法が規定されている。

(2)　安全管理措置（規格 A.3.4.3.2）

規格 A.3.4.3.2（安全管理措置）は、取扱う個人情報のリスクに応じて、個人情報のライフサイクル（個人情報の取得から廃棄までの一連の流れ）の各局面の安全対策を策定することを求めている。これに加え、特定個人情報を取扱う場合の安全管理措置では、特定個人情報ガイドライン（「(別添）特定個人情報に関する安全管理措置（事業者編)」を含む）において、個人番号の削除や特定個人情報等を取扱う機器及び電子媒体等の廃棄は所管法令等における保存期間の経過時には速やかに削除・廃棄を行うこと等、規格では求められていない措置を講じなければならないとする事項もあることに留意する。なお、講じなければならないとする事項の確認にあたり、「(別添）特定個人情報に関する安全管理措置（事業者編)」に示す中小規模事業者の範囲を確認するよう留意する。

特定個人情報の保管は、番号法第 19 条（特定個人情報の提供の制限）各号のいずれかに該当する場合を除き、禁止である（番号法第 20 条 収集等の制限）ことにも留意する。

（3） 委託先の監督（規格 A.3.4.3.4）

規格 A.3.4.3.4（委託先の監督）では、委託先に対する、必要、かつ、適切な監督を求めている。個人番号関係事務または個人番号利用事務の全部または一部を委託する場合も、規格に基づき委託先の監督を行う必要がある。これに加えて、特定個人情報ガイドラインでは、委託契約の締結にあたって盛り込むべき規定等が具体的に示されている（第 4-2-（1） 1 B）ことに留意する。よって、規格 A.3.4.3.4（委託先の監督）で定める事項のほかに、特定個人情報ガイドラインが示す事項を契約書等に盛り込む必要がある。

また、委託先に再委託を認める場合も、規格に基づき再委託先の監督を行う必要があるが、これに加えて、番号法第 10 条（再委託）では、個人番号利用事務等の委託、再委託を認めているが、最初の委託元の許諾を得ることが求められることに留意する。また、再委託先が再々委託を行う場合以降も、再委託を行う場合と同様であることにも留意が必要である。

以上

《参考情報》

「行政手続における特定の個人を識別するための番号の利用等に関する法律」（平成 25 年法律第 27 号）
：http://law.e-gov.go.jp/htmldata/H25/H25HO027.html

「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」（平成 26 年 12 月制定、平成 29 年 5 月 30 日最終改正、個人情報保護委員会）
：https://www.ppc.go.jp/files/pdf/my_number_guideline_jigyosha.pdf
（「（別添）特定個人情報に関する安全管理措置（事業者編）」を含む。）

「特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則」（平成 27 年特定個人情報保護委員会規則第 5 号）
：https://www.ppc.go.jp/files/pdf/rouei_kisoku.pdf

「事業者における特定個人情報の漏えい事案等が発生した場合の対応について」（平成 27 年特定個人情報保護委員会告示第 2 号）
：https://www.ppc.go.jp/files/pdf/roueitaiou_jigyosha.pdf

以上

改廃

改正日	改正箇所・理由
2016 年 2 月 12 日	・個人情報保護委員会規則施行に伴う 1.(4)の追加。 ・《参考情報 2》の更新。
2018 年 9 月 12 日	JIS Q 15001 改正に伴う更新