

# 個人情報の適正な取得等について(解説)

平成 27 年 2 月 23 日

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

「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(以下、「METI ガイドライン」という。)が、平成 26 年 12 月 12 日に改正されました。

本解説は、この改正の背景を踏まえ、「JIS Q 15001:2006(個人情報保護マネジメントシステム—要求事項)」(以下、「要求事項」という。)及びプライバシーマーク付与適格性審査基準である「JIS Q 15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン 第 2 版 第二部」(以下、「JIPDEC ガイドライン」という。)に基づき個人情報を取り扱うにあたり、個人情報の適正取得や再委託先の監督等、事業者が注意すべき事項について情報提供するものです。

なお、現行の要求事項及び JIPDEC ガイドラインは今回の METI ガイドラインの改正点を包含するため、今回の改正による JIPDEC ガイドラインの変更はありません。

以下では、今回の METI ガイドラインの主な 5 つの改正点(経済産業省公表時点でのリリース(<http://www.meti.go.jp/press/2014/12/20141212002/20141212002.html>))に関連する JIPDEC ガイドラインにおける要求事項の記載について解説します。

プライバシーマーク付与事業者や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。)におかれましては、本解説の内容を再確認され、引き続き、要求事項及び JIPDEC ガイドラインに基づく個人情報の取扱いを行なってください。

なお、METI ガイドラインの改正点の詳細は、本解説の末尾に示す経済産業省公表資料を参照してください。

<u>主な改正点 (METI ガイドライン)</u>		<u>要求事項</u>
1. 第三者からの適正な取得の徹底	⇒	適正な取得 (要求事項 3.4.2.2)
2. 社内の安全管理措置の強化	⇒	安全管理措置 (要求事項 3.4.3.2 等)
3. 委託先等の監督の強化	⇒	委託先の監督 (要求事項 3.4.3.4)
4. 共同利用制度の趣旨の明確化	⇒	共同利用 (要求事項 3.4.2.7 ただし書き 等)
5. 消費者等本人に対する分かりやすい説明のための参考事項の追記	⇒	本人から直接書面によって取得する場合の措置 (要求事項 3.4.2.4)

## 1. 適正な取得 (要求事項 3.4.2.2)について

JIPDEC ガイドラインは、本人以外から個人情報を取得する場合（受託による取得を含む）、提供元又は委託元が個人情報を適正に取り扱っていることを確認するよう規定していること、並びに、定めた手順に従い、提供元又は委託元の個人情報の取扱いについて確認していることを求めている。（JIPDEC ガイドライン第二部 3.4.2.2）また、JIPDEC ガイドラインは、個人情報を取得する場合、定めた手順に従い、事業者内部において個人情報保護管理者の承認を得ることも求めている。<sup>1</sup> そこで、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、これらの求めを踏まえ、個人情報を適正に取得することが求められる。

取得時の具体的な手順としては、METI ガイドラインを参考に、取得前に、取得する個人情報の件数や取得項目のほか、取得する個人情報の利用目的からみた取得項目の適切性、提供元又は委託元の個人情報保護の状況（例えば、個人情報保護方針や個人情報の取扱い、個人情報保護体制（個人情報保護管理者を含む）の公表状況、提供元の法の遵守状況（オプトアウト、利用目的、開示手続、問い合わせ・苦情の受付窓口を公表していることなど））等について確認し、承認を得ることが考えられる。

特に、データベース事業者等の提供者から、広告、DM 送付の目的で個人情報を取得する場合は、JIPDEC ガイドラインが従前より求めているとおり、取得前に承認手続きを通じた確認を行なうよう注意することが必要である。

委託元から個人情報を取得する場合には、通常、取得する個人情報は受託業務の範囲内であることが明らかであると考えられるが、この場合も、事業者は、取得の経緯を示す書面（事業者と委託元との間の契約書や覚書、委託元のウェブサイト等）を確認することが求められる。

なお、事業者は、提供元又は委託元との取引の可否について、万一問題が発生した場合に自社が経営上被るリスクの観点から判断することが求められる点に留意することが必要である。

## 2. 安全管理措置（要求事項 3.4.3.2 等）について

JIPDEC ガイドラインは、取り扱う個人情報のリスク対策として、事業の規模及び実態、取り扱う個人情報の性質及び量等を踏まえた合理的な安全管理措置を講じることを求めている。リスクに応じた安全管理措置とは、具体的には、要求事項 3.3.3 において行ったリスク分析に基づき、METI ガイドラインを参考に必要かつ適切な対策を講じることである。（JIPDEC ガイドライン第二部 3.4.3.2）この対策には、サイバー攻撃対策に対する管理手法のほか、物理的安全管理措置、技術的安全管理措置が含まれる。

---

<sup>1</sup> JIPDEC ガイドラインでは、個人情報を取得する場合、承認手順を定め、手順に従い個人情報保護管理者の承認を得ることが求められている。これは、第三者からの取得であるかによらない。（JIPDEC ガイドライン第二部 3.4.2.4、3.4.2.5）

よって、一律の対策が求められるものではないが、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、リスクに応じた安全管理措置を実施し、適宜リスク及び対策の見直しを行なうことが求められる。

また、安全管理措置のうち社内体制の整備等の組織的安全管理措置は、要求事項 3.3.4(資源、役割、責任及び権限)に定められている。要求事項とその解説及び JIPDEC ガイドラインでは、個人情報保護マネジメントシステムを実施するための体制を整備す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、組織の実態に合わせて、個人情報保護管理者等の個人情報保護マネジメントシステムに係る役割、責任及び権限を明確に定め文書化することが求められる。

### 3. 委託先の監督（要求事項 3.4.3.4）について

JIPDEC ガイドラインは、(1)委託先の評価選定、(2)要求事項で定める事項を盛り込んだ契約の締結、(3)契約内容の遵守状況の確認 等を求めている。(JIPDEC ガイドライン第二部 3.4.3.4) 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、必要かつ適切な委託先の監督を行なうとともに、委託先の監督には再委託先の監督が含まれることに注意することが必要である。

#### (1) 委託先の評価選定

JIPDEC ガイドラインは、委託先の選定にあたり、個人情報の取扱いにおけるリスク及びリスクに応じた安全管理措置を踏まえ、委託する業務については少なくとも自社と同等以上の個人情報の保護水準にあることを確認することを求めている。ここでいう自社とは、要求事項 3.4.3.4 に基づき十分な個人情報の保護水準を満たしている者を指す。委託先に求める個人情報保護の水準は委託する業務内容により異なるため、選定基準も委託する業務毎に異なると考えられる。具体的な選定基準の作成においては、METI ガイドラインが参考となる。

なお、委託先の認識に漏れがないようにするため、個人情報の取扱いの委託先を漏れなく把握することが求められる。このための具体的な対応としては、委託先のリストを作成すること等が考えられる。

#### (2) 要求事項で定める事項を盛り込んだ契約の締結

JIPDEC ガイドラインは、委託先との契約締結にあたり、要求事項に示す事項(要求事項 3.4.3.4 a)～g) )を契約に盛り込むことを求めている。この中には、個人情報の安全管理に関する事項（要求事項 3.4.3.4 b)）、再委託に関する事項（要求事項 3.4.3.4 c)）が含まれる。

このうち、再委託に関する事項（要求事項 3.4.3.4 c)）について、JIPDEC ガイドラインでは、再委託を行なうにあたっての委託者への文書による報告を求めている点に注意することが必要である。再委託の評価選定にあたり、委託する業務について少なくとも

自社と同等以上の個人情報の保護水準にあることが求められることを踏まえると、再委託に関する事項（要求事項 3.4.3.4 c)）の中には、再委託先からの報告が含まれることになる。同様に、契約内容が遵守されていることを委託者が確認できる事項（要求事項 3.4.3.4 e)）には、再委託の契約内容が遵守されていることを委託者が確認できる事項が含まれることになる。

なお、METI ガイドラインにおいては、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とするとしている。JIPDEC ガイドラインを踏まえれば、委託者が再々委託以降の委託を認める場合、再委託先からの報告に再々委託先以降の状況についての報告が含まれることに留意が必要である。

### (3) 契約内容の遵守状況の確認

JIPDEC ガイドラインは、契約締結後、委託先が契約に定めた条項を実施していることを確認することを求めている。委託先に再委託を認めた場合は、委託先に対し、再委託について、契約書に定めた文書による報告を求め、確認することが求められる。

事業者が委託者から受託した業務の再委託を行なおうとする場合は、委託者との契約上、再委託が認められていることを確認することが必要である。再委託が認められている場合は、再委託にあたり委託者に文書で報告を行うとともに、自らも再委託先が再委託契約に定めた条項を実施していることを確認することが求められる。

## 4. 共同利用（要求事項 3.4.2.7 ただし書き 等）について

要求事項とその解説及び JIPDEC ガイドラインは、共同して利用する者の範囲を含め、共同利用者との間で取り決めるべき事項を示している。

そこで、プライバシーマーク付与を受けようとする事業者は、共同利用を実施するにあたっては、引き続き、要求事項とその解説及び JIPDEC ガイドラインを踏まえた取り決めを行なうことが求められる。その際、共同して利用する者の範囲については、METI ガイドラインを踏まえ、本人がどの事業者まで将来利用されるか判断できる程度に明確にすることが求められる。

## 5. 本人から直接書面によって取得する場合の措置（要求事項 3.4.2.4）について

要求事項及び JIPDEC ガイドラインは、少なくとも要求事項 3.4.2.4 a)～h)に示す事項又はそれと同等以上の内容の事項を、あらかじめ、書面によって本人に明示し、本人の同意を得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、この要求事項及び JIPDEC ガイドラインを踏まえた対応を行なうことが求められる。その際、明示事項は、各種ガイドラインを参考に、分かりやすい説明となるよう工夫が求められることにも留意が必要である。

《参考資料》

「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(平成26年12月12日厚生労働省・経済産業省告示第4号)

<http://www.meti.go.jp/press/2014/12/20141212002/20141212002.pdf>

「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」改正案の新旧対照表

[http://www.meti.go.jp/policy/it\\_policy/privacy/downloadfiles/1212sinkyu.pdf](http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212sinkyu.pdf)

「JIS Q 15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン—第2版—」(JIPDEC)

<http://privacymark.jp/reference/index.html#section2>

以上