日印産連・プライバシーマーク審査センター

# 「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」改正の概要について

## 1. 改正の背景と概要

経済産業省は、この数年相次いで発生した内部不正やサイバー攻撃による個人情報の漏えい事案を受け、同様事案の発生を防ぐための組織における対策として、「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」を改正し、平成 26 年 12 月 12 日付けで告示・施行した。

ガイドラインの主な改正点は、個人情報保護法における以下の規程に関し、それぞれ取組の充実･強化が図られ、また、消費者等に対する分かりやすい説明のための参考事項の追記がされた。

**法第17条　：第三者からの適正な情報取得の徹底**
（適正取得）第17条

**法第20条　：社内の安全管理措置の強化**
（安全管理措置）第20条

**法第22条　：委託先等の監督の強化**
（委託先の監督）第22条

**法第23条　：共同利用制度の明確な説明**
（第三者への提供）第23条第1項
（共同利用）第23条第4項第3号

## 2. 改正点の詳細

今回それぞれ取組の充実・強化が図られた改正の起因となった個人情報の漏えい事案の「問題点」と、対策としての「ガイドラインの主な改正事項」を示す。

### （1）第三者からの適正な情報取得の徹底

**問題点**

●個人情報を取得した者は、提供元がそれを適法に入手したことを十分に確認しないまま（提供元から「誓約書」を取得するという形式的な対応）、当該情報を入手していた。

**ガイドラインの主な改正事項**

●第三者から個人情報を取得する場合 ( ※ ) には、
・提供元の選定に当たり、その個人情報保護法の遵守状況を確認すること。
・個人データの取得方法等について、例えば、取得の経緯を示す契約書等の書面を点検する等により、適法に入手されていることを確認すること。
( ※ ) 不特定かつ多数の者が購入することがでるものから取得する場合、法令に基づき提供される場合、承継、共同利用委託等の場合を除く。

●第三者から個人情報を取得する場合において、当該個人情報が適法に入手されたことが確認できない場合には、偽りその他不正の手段により取得されたものである可能性もあることから、その取得を自粛することを含め、慎重に対応すること。

### （2）社内の安全管理措置の強化

**【内部不正対策】**

**問題点**

大量の個人情報が漏えいする事案が発生した。
その原因は・・・

●個人情報のダウンロードを監視するシステムが、設定されていなかった。

●個人情報を取り扱う部屋へ、私物であるスマートフォンを持ち込むことができた。また、個人情報のデータベースに、そのスマートフォンが接続できる状態になっていた。

●個人情報のダウンロードのログ（記録）について、定期的な確認が行われておらず、長期間にわたり、漏えいの事実を把握できていなかった。

●「性善説」に立った、不十分な社内管理体制になっていた。

**ガイドラインの主な改正事項**

**① 組織的安全管理**

●個人情報保護管理者 (CPO) への役員の任命など、社内体制を整備すること。

●情報セキュリティ等に十分な知見を有する者による社内の監視体制を構築すること。

●スマートフォン等の記録機能を有する機器の接続制限を行う社内規程を整備すること。

**②物理的安全管理**

●業務上許可を得ていない記録機能を有する媒体・機器の持ち込み・持ち出しの禁止と検査を実施すること。
●カメラによる撮影や立ち会い等による記録又はモニタリングを実施すること。
●個人情報を取り扱う部屋への入退室記録の保存をすること。

**③ 技術的安全管理**

●個人情報の監視システムについて、その動作を定期確認すること。
●個人情報へのアクセスやダウンロードのログ ( 記録 ) について、不正が疑われる異常な記録の存否を定期確認すること。

**【サイバー攻撃対策】**

**問題点**

●近年、外部からのサイバー攻撃により、大量の情報が漏えいする事案が発生している。
●従前のガイドラインでは、外部からの脅威について十分な対応が記載されていなかった。

**ガイドラインの主な改正事項**

**① 管理手法の追記**

●有効であると考えられる管理手法を望まれる手法として追記した。
・データベースへのアクセス制御
・ワンタイムパスワード等
・不要アカウントの無効化
・管理者権限の分割
・アクセス記録
・ウイルス対策ソフトウェアの有効性確認
・データ移送時の秘匿化

**②既存の管理手法の修正**

●既に掲載されている管理手法であり、有効かつ一般的な手法であると考えられるが、実施していない事業者も相当程度存在する手法を、より周知を図る観点から、順番を入れ替えて冒頭に記載した。
・ファイアウォールの設置
・ウイルス対策ソフトウェアの導入

## (3) 委託先等の監督の強化

**問題点**

大量の個人情報が漏えいする事案が発生した。
その原因は・・・
●システム開発・管理の委託先 ( 子会社 ) における安全管理措置が十分でなく、そこから個人情報が不正に持ち出された。

**ガイドラインの主な改正事項**

**① 委託先の監督**

●委託先の選定に当たり、委託先の安全管理措置を確認し、CPO 等が評価すること。
●定期的に、委託業務の監査を実施し、その結果について、CPO 等が評価すること。
●委託契約等において、委託先で個人データを取り扱う者の役職又は氏名、損害賠償責任を盛り込むこと。

**②再委託先の監督**

●委託元は、委託先が再委託を行う場合には、委託先から事前報告又は承認の申請を求めること。
●委託元は、委託先を通じて、又は必要に応じて自らが、再委託先に対し、定期的な監査を実施すること。
●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こと。

## (4) 共同利用制度の明確な説明

**問題点**

●「企業ポイント等を通じた連携サービス」で共同利用を行う場合、共同利用者の範囲が明確でなくても共同利用が可能であると誤解を与えている可能性がある。
●最新の共同利用者リストを本人が容易に知り得る状態に置いているだけで、共同利用者の範囲が明確でなくても共同利用が可能と誤解を与えている可能性がある。

**ガイドラインの主な改正事項**

**① 共同利用の趣旨の明確化**

●あらかじめ本人の同意が必要な第三者提供の例外の1つである共同利用について、制度の趣旨が明確に記載された。
●事業者が共同利用を円滑に実施するために共同利用者における責任等を明確にする観点から、あらかじめ取り決め

ておくことが望ましい事項について趣旨が伝わりやすいよう明記された。

**②共同利用者の範囲の明確化**

●共同利用者の範囲について、本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性がある範囲で共同利用ができるのであり、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必要がある旨追記された。

●共同利用者の範囲が明確である具体例が追記された。

## (5) 消費者等本人に対する分りやすい説明の取組について

**趣旨**

●個人情報取扱事業者は、消費者等本人との信頼関係を構築する観点から、消費者等本人に対して、個人情報取扱事業者の個人情報保護を推進する上での考え方や方針等について、冗長で分りにくい説明を避け、消費者等本人に誤解を与えることなく分りやすい表現で説明することが望ましい。

●このことから、個人情報を利活用してサービスを行う事業者が、消費者からパーソナルデータを取得し利用する際に、消費者に対して行う情報提供や個人情報保護を推進する上での考え方や方針等を分りやすく説明した文書等の内容の適切性を第三者が事前に評価する際のツールとして経済産業者が策定した「評価基準」を基に作成した、「分りやすい説明の実施に際して参考 とすべき基準」が追記された。

**「分りやすい説明の実施に際して参考とすべき基準」**

### 1. 記載事項

#### (1) 必要十分な記載事項

1 個人情報の取扱いに関する情報として、以下の 7 項目が記載されていること。

1) 提供するサービスの概要
2) 取得する個人情報と取得の方法
3) 個人情報の利用目的
4) 個人情報や個人情報を加工したデータの第三者への提供の有無及び提供先
5) 消費者等本人による個人情報の提供の停止の可否、訂正及びその方法
6) 問合せ先
7) 保存期間、廃棄

### 2. 記載方法

#### (1) 取得する個人情報とその取得方法に係る記載方法

2 取得する個人情報の項目とその取得方法について、可能な限り細分化し、具体的に記載していること。

3 取得する個人情報の項目やその取得方法のうち、消費者等本人にとって分かりにくいものを明確に記載していること。

#### (2) 個人情報の利用目的に係る記載方法

4 取得する個人情報の利用目的を特定し、具体的に記載していること。

5 個人情報の利用目的が、取得する個人情報の項目と対応して記載されていること。

6 取得する個人情報の利用目的のうち、消費者等本人にとって分かりにくいものを明確に記載していること。

#### (3) 第三者への提供の有無及び個人情報や個人情報を加工したデータの提供先に係る記載方法

7 個人情報取扱事業者が取得する個人情報や個人情報を加工したデータを第三者に提供する場合、その提供先（事後的に提供先を変更する場合は提供先の選定条件を含む）及び提供目的が記載されていること。

8 個人情報取扱事業者が取得した個人情報を加工したデータを第三者に提供する場合、その加工方法が記載されていること。

#### (4) 消費者等本人による個人情報の提供の停止の可否及びその方法に係る記載方法

9 消費者等本人が個人情報取扱事業者による個人情報の取得の中止又は利用の停止が可能であるかが記載され、可能である場合には取得の中止方法又は利用の停止方法を明示して記載していること。

－ 参照資料 －
経済産業分野における個人情報保護ガイドライン説明会配付資料
・「経済産業分野を対象とする個人情報保護ガイドライン等について」（平成 26 年 12 月）
・「平成 26 年 12 月改正版パンフレット」
http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/2612pamphlet.pdf