

Ⅲ. 「勧告」、「命令」、及び「緊急命令」についての考え方

法第34条第1項

主務大臣は、個人情報取扱事業者が第16条から第18条まで、第20条から第27条まで又は第30条第2項の規定に違反した場合において個人の権利利益を保護するため必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる。

法第34条第2項

主務大臣は、前項の規定による勧告を受けた個人情報取扱事業者が正当な理由がなくその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときは、当該個人情報取扱事業者に対し、その勧告に係る措置をとるべきことを命ずることができる。

法第34条第3項

主務大臣は、前二項の規定にかかわらず、個人情報取扱事業者が第16条、第17条、第20条から第22条まで又は第23条第1項の規定に違反した場合において個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべきことを命ずることができる。

法第56条

第34条第2項又は第3項の規定による命令に違反した者は、6月以下の懲役又は30万円以下の罰金に処する。

法第58条第1項

法人（法人でない団体で代表者又は管理人の定めのあるものを含む。以下この項において同じ。）の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関して、前二条の違反行為をしたときは、行為者を罰するほか、その法人又は人に対しても、各本条の罰金刑を科する。

法第58条第2項

法人でない団体について前項の規定の適用がある場合には、その代表者又は管理人が、その訴訟行為につき法人でない団体を代表するほか、法人を被告人又は被疑者とする場合の刑事訴訟に関する法律の規定を準用する。

法第34条に規定される経済産業大臣の「勧告（第1項）」「命令（第2項）」及び「緊急命令（第3項）」については、個人情報取扱事業者が本ガイドラインに沿って必要な措置等を講じたか否かにつき判断して行うものとする。

すなわち、本ガイドライン中、「しなければならない」と記載されている規定について、それに従わなかった場合は、法第16条から18条まで、第20条から27条まで又は第30条第2項の規定違反と判断され得る。違反と判断された際、実際、「勧告」を行うこととなるのは、個人の権利利益を保護するため必要があると認めるときである。一方、本ガイドライン中、「望ましい」と記載されている規定については、

それに従わなかった場合でも、法第16条から18条まで、第20条から27条まで又は第30条第2項の規定違反と判断されることはないが、個人情報保護の推進の観点から個人情報取扱事業者においては、できるだけ取り組むことが望まれる。

「命令」は、単に「勧告」に従わないことをもって発することはなく、正当な理由がなくてその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときに限られる。なお、「勧告」に従わなかったか否かを明確にするため、経済産業大臣は、「勧告」に係る措置を講ずべき期間を設定して「勧告」を行うこととする。

「緊急命令」は、個人情報取扱事業者が法第16条、第17条、第20条から22条まで又は第23条第1項の規定に違反した場合において、個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときに、「勧告」を前置せずに行う。

なお、「命令」及び「緊急命令」に従わなかったか否かを明確にするため、経済産業大臣は、「命令」及び「緊急命令」に係る措置を講ずべき期間を設定して「命令」及び「緊急命令」を行い、当該期間中に措置が講じられない場合は、「罰則（第56条、第58条）」を適用される。

IV. ガイドラインの見直し

個人情報の保護についての考え方は、社会情勢の変化、国民の認識の変化、技術の進歩等に応じて変わり得るものであり、本ガイドラインは、法の施行後の状況等諸環境の変化を踏まえて毎年見直しを行うよう努めるものとする。

V. 個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格

個人情報取扱事業者は、その事業規模及び活動に応じて、個人情報の保護のためのコンプライアンス・プログラムを策定し、実施し、維持し及び改善を行うことが望ましい。

なお、その体制の整備にあたっては、日本工業規格 JISQ15001「個人情報保護に関するコンプライアンス・プログラムの要求事項」（当ガイドラインに基づいて改訂される予定）等を、個人データの安全管理措置の実施にあたっては、日本工業規格 JISX5070「セキュリティ技術 — 情報技術セキュリティの評価基準」及び日本工業規格 JISX5080「情報セキュリティマネジメントの実践のための規範」等を参考にすることができる。

また、個人情報取扱事業者は、以下の事項を参考として「個人情報保護に関する考え方や方針に関する宣言（いわゆる、プライバシーポリシー、プライバシーステートメント等）」を策定し、ホームページへの掲載等により公表することが望ましい。

- ① 事業の内容及び規模を考慮した適切な個人情報の取扱いに関すること

- i. 取得する個人情報の利用目的（法第18条関係）
 - ii. <本人の同意なく第三者提供する場合>（法第23条第2項及び第3項関係）
 - ・ 利用目的に第三者提供が含まれていること
 - ・ 第三者に提供される個人データの項目
 - ・ 第三者への提供の手段又は方法
 - ・ 本人の求めに応じて第三者への提供を停止すること
 - iii. <共同利用する場合>（法第23条第4項及び第5項）
 - ・ 特定の者との間で共同利用すること
 - ・ 共同して利用される個人データの項目
 - ・ 共同利用者の範囲
 - ・ 共同して利用する者の利用目的
 - ・ 共同して利用する者のうち、個人データの管理について責任を有する者の氏名又は名称
 - iv. 以下の保有個人データに関すること（法第24条関係）
 - ・ 自己の氏名又は名称
 - ・ すべての保有個人データの利用目的
 - ・ 「開示等の求め」に応じる手続
 - ・ 保有個人データの利用目的の通知及び開示に係る手数料の額（定めた場合に限る）
 - ・ 苦情の申出先（認定個人情報保護団体の対象事業者*である場合には当該認定個人情報保護団体の名称及び苦情解決の申出先も含む。）
 - v. 開示等の求めに応じる手続に関すること（法第29条関係）
 - ・ 申請書の様式（定めた場合に限る）
 - ・ 受け付ける方法（定めた場合に限る）
 - ・ 保有個人データの特定に資する情報の提供
 - vi. 問い合わせ及び苦情の受付窓口に関すること（法第23条第5項、第24条第1項、第29条第1項及び第31条関係）
-
- ② 個人情報の保護に関する法律を遵守すること
 - ③ 個人情報の安全管理措置に関すること
 - ④ コンプライアンス・プログラムの継続的改善に関すること

※「認定個人情報保護団体の対象事業者」とは、認定個人情報保護団体の構成員である個人情報取扱事業者（傘下企業）、又は団体が苦情処理等の業務を行うことについて当該団体と契約関係等にある事業者等