「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（法第56条、第58条）」を適用される。

４．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。

５．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

⑴個人情報保護のためのマネジメント体制の確立

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マネジメントシステムを確立し、実施し、維持し及び改善を行うことが望ましい。

なお、その体制の整備に当たっては、日本工業規格JIS Q 15001「個人情報保護マネジメントシステム―要求事項」を、個人データの安全管理措置の実施に当たっては、日本工業規格JIS X 5070「セキュリティ技術―情報技術セキュリティの評価基準」、日本工業規格JIS Q 27001「情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項」、日本工業規格JIS Q 27002「情報技術―セキュリティ技術―情報セキュリティ管理策の実践のための規範」、独立行政法人情報処理推進機構（ＩＰＡ）の「組織における内部不正防止ガイドライン」、総務省・経済産業省の「電子政府における調達のために参照すべき暗号のリスト（ＣＲＹＰＴＲＥＣ暗号リスト）」、ISO／IEC 18033（暗号アルゴリズム国際規格）等を、個人データの安全管理措置の実施状況の確認に当たっては、経済産業省の「情報セキュリティ監査制度」を、それぞれ参考にすることができる。

⑵個人情報保護を推進する上での考え方や方針の策定等

個人情報取扱事業者は、「個人情報保護を推進する上での考え方や方針（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、それをウェブ画面への掲載又は店舗の見やすい場所への掲示等により公表し、あらかじめ、対外的に分かりやすく説明することが、消費者等本人との信頼関係を構築し事業活動に対する社会の信頼を確保するために重要である。

個人情報取扱事業者は、一定の事項に関して公表しなければならないが（２－１－８参照）、事業者の個人情報保護を推進する上での考え方や方針には、消費者等、本人の権利利益の保護の観点から、以下に掲げる点を考慮した事項を盛り込み、本人からの求めに一層対応していくことも重要である。

●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。

㋐取得する個人情報の利用目的（法第18条関係）

すべての利用目的を列記するのではなく、事業内容を勘案して顧客の種類ごとに利用目的を限定して示すなど、事業内容の特性、規模及び実態に応じ、本人にとって利用目的がより明確になるようにすることが望ましい。

㋑＜個人データの取扱いの委託を行う場合＞（法第22条関係）

事業内容の特性、規模及び実態に応じ委託処理の透明化を進めることを盛り込むことが望ましい。

・個人データの委託を行うこと。
・委託する事務の内容

㋒＜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。

㋓＜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

㋔以下の保有個人データに関すること（法第24条、第25条及び第27条関係）。

個人情報の取得元又は取得方法（取得源の種類等）を可能な限り具体的に明記したり、本人から求めがあった場合には、ダイレクトメールの発送停止等自主的に利用停止に応じたりするなど、事業活動の特性、規模、実態を考慮して、本人からの求めに対応していくことを盛り込むことが望ましい。

・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（定めた場合に限る。）
・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を含む。）

㋕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役立つ情報の提供

㋖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）。

●個人情報の保護に関する法律を遵守すること。
●個人情報の安全管理措置に関すること。
●マネジメントシステ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

⑶消費者等本人に対する分かりやすい説明の実施

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、以下に掲げる基準を参考にして、冗長で分かりにくい表現を避け、消費者等本人に誤解を与えることなく分かりやすい表現で表示することが望ましい。