

はじめに

本書は、NBL（商事法務）の2024年4月から2025年9月までの17回にわたる連載に、最新情報等を加筆し、内容に応じて編集したものであり、個人情報保護委員会の監視・監督活動における事案対応を基にして、個人情報等の適正な取扱いを確保するための方法等を解説している（なお、本書の執筆は、当委員会事務局に籍を置き、監視・監督の実務に携わった者が担っているが、本書で示された意見は執筆者に属し、当委員会の公式の見解を示すものではない）。

当委員会は、これまで、多数の漏えい等事案や個人情報保護法に関する総合的な案内所（個人情報保護法相談ダイヤル）等に寄せられる情報等を活用した不断の監視等により発覚した個人情報等の不適切な取扱事案等について、事業者等に対して、指導・助言、勧告等の法執行を行ってきた。また、これらの事案を基に、発生原因、再発防止策等の調査・分析や注意喚起等の情報提供も行っている。

本書は、こうした監視・監督活動の視点から、法令およびガイドラインの読み方を整理して、できるだけわかりやすく、漏えい等や不適切な取扱いが発生しないよう、事業者等の皆様にとって実務的に役立つと思われる運用面の留意事項を解説することを目的としている。

個人情報等の取扱いについて、平時から法令を遵守し、安全管理措置を適切に講ずることが肝要であるが、実際の漏えい等事案の原因や不適切な取扱事案の問題点の分析結果は、こうした事案発生を防止するための対策を講じていく上で有効である。また、万一、こうした事案が発生した場合に的確な対応をとることができない場合には、個人の権利利益の侵害がより深刻化するおそれがあるほか、組織に対する信用を毀損することにもなりかねない。したがって、事案発覚後の実践的な運用面の留意事項を理解しておくことも大切である。

本書が、個人情報等の適正な取扱いのために日々心を碎いておられる事業者等の皆様にとって、一助となれば幸いである。

令和7年12月

片岡秀実 小和田敦子

目 次

第1編 個人情報保護委員会の監視・監督活動等

第1章 個人情報保護委員会の監視・監督活動の概要	2
I 委員会の監視・監督活動の範囲	2
II 委員会の監視・監督活動の概要	2
III 最近の指導等の状況	15
第2章 個人情報保護委員会が発信する注意喚起	20
I 委員会の注意喚起とは	20
II 最近発信した注意喚起について	20
III 注意喚起の種類	23
IV おわりに	33
第3章 総合的な案内所等に寄せられる相談内容	34
I 総合的な案内所等における対応	34
II 民間規律に関する総合的な案内所の相談受付状況	37
III 公的規律に関する総合的な案内所の相談受付状況	45
IV マイナンバー苦情あっせん相談窓口	47
V おわりに	49

第2編 漏えい等報告の対応

第1章 漏えい等報告の義務と報告の種類	52
I 漏えい等事態の報告義務	52
II 報告義務がある漏えい等事態（規則7条各号）	53
III 漏えい等報告の種類	61
IV おわりに	66

第2章 漏えい等報告書提出後の対応	67
I 報告書が提出された後に委員会で確認するポイント	67
II 漏えい等報告書受領後の委員会の対応	79
第3章 漏えい等報告の要否に関する考察	81
I 漏えい等報告義務の要否の判断	81
II 漏えい等が「発生したおそれ」がある事態	89
コラム1 事業者と個人情報保護委員会とのコミュニケーションについて	94
コラム2 域外適用と漏えい等報告	97
第3編 具体的な漏えい等事案と安全管理措置	
第1章 組織的安全管理措置	102
I 組織的安全管理措置の概要	102
II 事例考察	108
第2章 個人データの取扱いの委託	116
I はじめに	116
II 個人データの取扱いの委託	117
III 委託先の監督（法25条関係）	121
IV 事例考察	126
V 行政機関等からの委託	131
第3章 内部不正による漏えい等事案への対応	133
I 過去の漏えい等事案	133
II 内部不正による漏えい等の防止のための安全管理措置等	141

目 次

第4章 漏えい等防止に向けた改善のための着眼点	147
I 漏えい等事案に応じた安全管理措置	147
II 個別検討	148

第4編 不正アクセス事案への対応

第1章 最近の不正アクセス事案	162
I 指導等の権限行使と不正アクセス事案	162
II 不正アクセスによる漏えい等の原因	164
III 不正アクセスによる漏えい等の防止策	177

第2章 ランサムウェア事案への対応	181
I はじめに	181
II ランサムウェア攻撃の概要等	181
III ランサムウェア攻撃に関し、報告書が提出された後に委員会で確認するポイント	183
IV ランサムウェア攻撃と安全管理措置	190

第3章 技術的の安全管理措置と再発防止策	192
I 技術的の安全管理措置の概要	192
II 事例考察	197
コラム3 ECサイト事案（ウェブスキミング）に関する問題点	203

第5編 個人情報の適正な取扱い

第1章 不適正利用と違法な第三者提供の事案への対応	208
I 不適正利用の禁止	208
II 破産者マップ等への対応	210
III おわりに	223

第2章	個人情報の適正な取得に関する事例の考察	225
I	個人情報の適正な取得	225
II	委員会が個人情報保護法20条1項に関して公表した事案	227
III	考察	229
第3章	オプトアウト届出事業者である名簿屋への対応	235
I	オプトアウト規定による第三者提供	235
II	名簿屋に対する調査方法	239
III	名簿屋に対する権限行使	244
IV	おわりに	248
第4章	行政機関等の保有個人情報の取扱いにかかる留意点	249
I	はじめに	249
II	公的部門に適用される規律の適用対象	249
III	行政機関等における漏えい等事案	251
IV	行政機関等における安全管理措置等	254
V	行政機関等に対する直近（令和6年度）の指導等の状況	258
VI	保有個人情報の取扱いの委託を受ける個人情報取扱事業者における留意点	260
VII	おわりに	263
コラム4	レセプトデータ等の保有個人情報の利活用に関する注意喚起について	265