

は し が き

個人情報は漏れないことが当然の時代から、漏れることを前提とする時代になっている。サイバー攻撃の技術は日々進化するし、穴が全くないようシステムを構築して、運用することは、人間がやることである以上は不可能である。また、一昔前のように、個人情報は鍵をかけてしまっておく時代ではなく、活用する時代になったことで、個人情報を用いて業務を行う人が格段に増えている。人が増えれば、ミスが増えるのも当然である。

だからといって、個人情報が安全に取り扱われるための不断の努力をしなくて良い、とは言わないが、企業は様々なリスクに直面しているのであり、個人情報についても、最低限の対策を講じた上で、リスクが高い業務に集中的に対策を講じる「リスクベースアプローチ」を採用する必要性が高まっている。その「リスクベースアプローチ」を採用したときに、最低限の対策とは何か、どのような対策を講じるべきなのか、について、本書では、個人情報保護法及び個人情報保護委員会が公表しているガイドラインを中心に説明をしている。

また、近年では、1つの企業がサイバー攻撃の被害を受けると、サプライチェーン全体、はたまたその企業の競合他社まで影響を受ける事態が発生している。そのような状態になれば、企業は売上げをあげることができなくなるほか、連日のようにニュースに取り上げられて、レピュテーションは地に落ちる事態にもなりかねない。そのため、企業にとっては、個人情報が漏れた場合の対応を迅速に行うことは、その後の事業の再開や、レピュテーションの維持にとって重要である。本書では、迅速な対応を可能とするために、個人情報が漏れた場合の対応についても説明している。

本書が企業における平時の「リスクベースアプローチ」の採用の一助に、また、緊急時の企業活動の迅速な回復の一助になれば幸いである。

2025年10月

木村一輝

目 次

はしがき・i

凡例・xxiv

I 個人情報保護法の基本

Chapter1

個情法の基本的な考え方

2

第1 個人情報保護法における民間部門と公的部門の区別	2
第2 個人情報保護法の基本的な構造	4
① 全事業者に向けたルール	4
② 特定の事業を行っている事業者に向けられたルール	5
第3 個情法の仕組み	6
第4 個情法に違反した場合の個情委の対応	7
第5 個情法に違反した場合の損害賠償責任	8

Chapter2

個人情報の定義

9

第1 「個人情報」	9
① 個人情報の概要	9
② 生存性（要件①）	9
③ 個人関連性（要件②）	10

④ 特定の個人識別又は個人識別符号（要件③）	10
(1) 特定の個人識別性・10	
(2) 個人識別符号・12	
Column：個人識別符号・13	
⑤ 特定の個人識別性の判断基準	14
⑥ 個人情報の範囲	15
⑦ 氏名を削除・マスキングすることと個人情報	18
⑧ 位置情報の個人情報該当性	19
第2 「個人情報」以外の情報	19

Chapter3

個人データの定義 21

第1 電子データの「個人データ」	21
------------------	----

第2 紙媒体の「個人データ」	23
----------------	----

第3 メールと「個人データ」	24
----------------	----

Column：個人情報取扱事業者・24

Chapter4

個人情報・個人データに関する基本的なルール 26

Go to the next page ►

II 安全管理措置の実務

Chapter1

個情法、業法、会社法にもとづく安全管理措置 30

第1 個情法による安全管理措置 30

第2 業法による安全管理措置 31

第3 会社法による安全管理措置 32

① 善管注意義務 32

② 内部統制システム構築義務 33

(1) 法令遵守体制・34

(2) 損失の危機管理体制・34

Column：個人情報の漏えいによる損害・34

(3) グループ会社がある場合・35

Chapter2

個情法における安全管理措置が防止する事態 37

第1 安全管理措置が目指すべきもの 37

第2 漏えい、滅失、毀損 38

第3 その他の個人データの安全管理に支障が生じる事態 39

Chapter3

個情法における安全管理措置の条文 41

Chapter4

安全管理措置の対象となる「個人データ」 43

Chapter5

リスクベースでの安全管理措置の決定 47

第1 リスクベースでの安全管理措置の決定	47
----------------------	----

Column：中小企業の安全管理措置・48

第2 リスクの評価方法	49
-------------	----

- (1) 「事業の規模及び性質」におけるリスク・50
- (2) 「個人データの取扱状況（取り扱う個人データの性質及び量を含む。）」におけるリスク・51
- (3) 「個人データを記録した媒体の性質」におけるリスク・52

第3 リスクベースによる安全管理措置決定の手順	53
-------------------------	----

Chapter6

具体的な安全管理措置 56

第1 基本方針の策定（GL（通則編）10-1）	56
-------------------------	----

- ① 基本方針の名称.....57
- ② 基本方針に定める項目（項目例）.....57
- ③ 苦情の申出先と電話番号.....58
- ④ 基本方針の具体例.....59

第2 個人データの取扱いに係る規律の整備（GL（通則編）10-2）	61
-----------------------------------	----

- ① 個人データのライフサイクルに応じた規律の整備.....61
- ② 「規律」の形式.....62
- ③ 「個人データの取扱いに係る規律」に従った運用を確保する重要性.....63

第3 組織的安全管理措置 (GL (通則編) 10-3)	63
------------------------------	----

① 組織体制の整備 (GL (通則編) 10-3(1))	65
(1) 責任者の設置等・66	
Column : 「望ましい」「しなければならない」・67	
(2) 個人データの取扱いに関する責任者の設置及び責任の明確化・68	
(3) 個人データを取り扱う従業者及びその役割の明確化・70	
(4) 従業者が取り扱う個人データの範囲の明確化・72	
(5) ルール違反の場合の報告連絡体制の整備・72	
(6) 漏えい等の場合の報告連絡体制の整備・73	
(7) 個人データを複数の部署で取り扱う場合の各部署の役割分担及び責任の明確化・75	
② 個人データの取扱いに係る規律に従った運用 (GL (通則編) 10-3(2))	75
③ 個人データの取扱状況を確認する手段の整備 (GL (通則編) 10-3(3))	77
Column : データマッピング・79	
④ 漏えい等に対応するための体制 (GL (通則編) 10-3(4))	79
⑤ 取扱状況の把握及び安全管理措置の見直し (GL (通則編) 10-3(5))	82
(1) 監査の主体・82	
(2) 監査の内容・83	

第4 人的安全管理措置 (GL (通則編) 10-4)	86
-----------------------------	----

① 周知徹底	87
② 適切な教育	88
(1) 教育すべき事項・89	
(2) 教育の頻度・形式・92	
③ 就業規則等における秘密保持に関する事項の規定	92
(1) 入社時における秘密保持の誓約・93	
(2) 在職時 (就業規則)・94	
(3) 在職時 (プロジェクトの参加時など)・95	
(4) 退職時・95	
Column : 密密管理の範囲・97	

第5 物理的安全管理措置 (GL (通則編) 10-5)	98
------------------------------	----

① 個人データを取り扱う区域の管理 (GL (通則編) 10-5(1))	99
(1) 管理区域と取扱区域・100	

(2) 管理区域における管理手法（入退室管理及び持ち込む機器等の制限等）・100	
(3) 取扱区域における管理手法・102	
② 機器及び電子媒体等の盗難等の防止（GL（通則編）10-5(2)）	103
(1) 施錠できるキャビネット・書庫等での保管・104	
(2) セキュリティワイヤー等での固定・104	
③ 電子媒体等を持ち運ぶ場合の漏えい等の防止（GL（通則編）10-5(3)）	104
(1) 個人データの暗号化、パスワードによる保護等・105	
(2) 封緘、目隠しシールの貼付け・105	
(3) 施錠できる搬送容器の使用・106	
④ 個人データの削除及び機器、電子媒体等の廃棄（GL（通則編）10-5(4)）	106
(1) 個人データが記載された書類等の破棄・107	
(2) 電子データの消去・107	
Column：適切なタイミングでの破棄・108	
(3) 他の業者への委託・109	
Column：個人情報の適切な廃棄・消去がなされていない事例・109	

第6 技術的の安全管理措置（GL（通則編）10-6）	110
-----------------------------------	-----

① アクセス制御（GL（通則編）10-6(1)）	112
(1) 情報システムの限定・113	
(2) 情報システムによってアクセスすることができるデータの限定及び情報システムを使用できる従業者の限定・114	
② アクセス者の識別と認証（GL（通則編）10-6(2)）	115
(1) 識別と認証・115	
(2) パスワードの設定と管理・116	
Column：パスワードの設定・118	
(3) 多要素認証・120	
Column：アカウントに対する攻撃・122	
(4) 不要なアカウントの管理・123	
Column：パスワード管理ツール（パスワードマネージャー）・123	
③ 外部からの不正アクセス等の防止（GL（通則編）10-6(3)）	124
(1) 不正アクセスの遮断・125	
(2) 不正ソフトウェアの有無の確認・126	

(3) ソフトウェア等の最新化・127
(4) ログ等の定期的な分析による不正アクセス等の検知・128
④ 情報システムの使用に伴う漏えい等の防止 (GL (通則編) 10-6(4))130
(1) 情報システムの設計時の安全性の確保・継続的な見直し・130
(2) 個人データを含む通信の経路又は内容の暗号化・130
Column : 暗号化・131
(3) パスワード等による保護・131
(4) 内部不正の防止・132

第 7 外的環境の把握 (GL (通則編) 10-7)	134
------------------------------------	-----

① 外的環境の把握をしなければならない場合134
② 外的環境の把握の内容135
(1) ガバメントアクセス・136
(2) データローカライゼーション・137

Chapter7

従業者の監督

140

第 1 従業者の監督の概要	140
----------------------	-----

第 2 「従業者」の範囲	140
---------------------	-----

第 3 「必要かつ適切な監督」の内容	141
---------------------------	-----

① 従業者監督の概要141
② 従業者のプライバシー143
(1) 従業者のプライバシー保護の重要性・143
(2) 限定的な運用・144
(3) 従業者への通知・協議（就業規則での明示を含む）・144
(4) 厳格な安全管理措置の実施・145
③ 従業者の監視と個情法145
Column : 従業者の監督のポイント・146
④ 退職予定者に対する監督147

Chapter8

委託先の監督

148

第1 委託と安全管理措置

148

- ① 委託を行った場合の安全管理措置 148
- ② 委託を行った場合に講じるべき安全管理措置 150
 - (1) 委託先に対して個人データの管理を委ねている場合・150
 - (2) 委託元が個人データを管理している場合・153

第2 委託先の監督の概要

153

第3 適切な委託先の選定

155

第4 委託契約の締結

155

- ① 委託についての基本的な条項 159
- ② 授受についての条項 159
- ③ 安全管理措置の内容に関する条項（保管についての条項） 160
- ④ 取扱状況の把握に関する条項 161
- ⑤ 漏えい等の場合の対応に関する条項 162
- ⑥ 委託が終了した場合の対応に関する条項（廃棄についての条項） 163
- ⑦ その他の条項 163

第5 委託先における個人データの取扱状況の把握

164

第6 再委託先の監督

165

- ① 再委託先の監督義務者 166
- ② 再委託の場合の委託元の実施事項 167

Chapter9

クラウドと安全管理措置

168

第1 クラウドサービスの利用と法的な整理

168

第2 安全管理措置の具体的な内容	169
① クラウド事業者に提供していない場合	169
② クラウド事業者に提供している場合	170
(1) クラウド事業者に委託している場合・170	
(2) クラウド事業者に第三者提供する場合・170	
第3 クラウドを利用する場合の外的環境の把握	171

Chapter10

苦情処理 172

第1 事業者に対して直接寄せられる苦情	173
第2 個情法相談ダイヤル	174
第3 認定個人情報保護団体	175
① 認定個人情報保護団体の概要	175
② 認定個人情報保護団体の業務	176
③ 認定個人情報保護団体が行う業務としての苦情処理	177
第4 地方公共団体の窓口	178
第5 消費者団体	178
① 適格消費者団体	178
② 適格消費者団体からの申入れ	179

Chapter11

安全管理措置の公表等 181

III 個人データの漏えい等の実務

Chapter1

個人データの漏えい等が発生した場合の対応の概要 184

Chapter2

「個人データ」の「漏えい等」の定義 186

第1 「漏えい等」の定義 186

- | | |
|---------------------------|-----|
| ① 漏えい | 187 |
| ② 意図にもとづく「提供」と「漏えい」の関係 | 189 |
| ③ 第三者に閲覧されないうちにすべてを回収した場合 | 191 |
| ④ 滅失 | 191 |
| ⑤ 毀損 | 192 |
| ⑥ 個人データの漏えい、滅失、毀損の判断方法 | 192 |

第2 「個人データ」の漏えい等の判断方法 193

- | | |
|-------------------------|-----|
| ① 個人データの一部の漏えい等 | 193 |
| ② 個人データを印刷した紙媒体が漏えいした場合 | 194 |

Chapter3

個人データの漏えい等事案への対応（安全管理措置） 196

第1 事業者内部の報告・被害拡大防止措置 197

第2 影響範囲の確定 198

第3 影響範囲の特定 198

第4 再発防止策の検討及び実施	198
-----------------	-----

第5 個人情報保護委員会への報告及び本人への通知	199
--------------------------	-----

Chapter4

個人情報保護委員会への報告及び本人通知の概要(対象事態) 200

第1 要配慮個人情報が含まれる個人データの漏えい等	203
---------------------------	-----

Column : 要配慮個人情報・205

第2 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等	206
---	-----

- ① 「財産的被害が生じるおそれ」 207
- ② 実際に財産的被害が生じる可能性と「財産的被害が生じるおそれ」 208
- ③ 財産的被害が生じた後に被害回復を行った場合 208

Column : クレジットカード番号の漏えい等・209

第3 不正の目的をもって行われたおそれがある行為による個人データの漏えい等	211
---------------------------------------	-----

- ① 「当該個人情報取扱事業者に対する行為」 211
- ② 「不正の目的」 211
- ③ 不正目的での「個人データ」の漏えい等 212
- ④ 不正目的での個人データの漏えい等の判断時期 214

第4 個人データに係る本人の数が千人を超える漏えい等	214
----------------------------	-----

第5 事業者に帰責性がない場合	215
-----------------	-----

第6 漏えい等の「おそれ」	215
---------------	-----

第7 高度な暗号化	216
-----------	-----

Chapter5

個情委への報告

217

第1 個情委への漏えい等報告の意義	217
第2 個情委への報告の概要	217
第3 速報	218
① 速報の報告時期	218
② 速報において報告すべき事項	221
(1) 概要・221	
(2) 個人データの項目・222	
(3) 個人データに係る本人の数・222	
(4) 原因・222	
(5) 二次被害又はそのおそれの有無及びその内容・222	
(6) 本人への対応の実施状況・223	
(7) 公表の実施状況・223	
(8) 再発防止のための措置・223	
(9) その他参考となる事項・223	
③ 報告方法	235
④ 漏えい等報告の主体	236
⑤ 速報の提出が遅延した場合	238
第4 確報	238
① 確報の報告時期	238
② 速報において報告すべき事項	240
③ 報告方法	241
④ 速報後に報告対象事態（4類型）でないことが判明した場合	241
第5 権限委任分野における漏えい等報告	242

Chapter6

本人通知

244

第1 本人通知の意義	244
------------	-----

第2 本人通知の時期	244
------------	-----

第3 本人通知の内容	246
------------	-----

① 通知すべき事項	246
-----------	-----

② 本人通知の例	247
----------	-----

(1) 宛先・248

(2) 送主の名義・249

(3) 表題・249

(4) 記載項目・249

第4 本人通知の方法	251
------------	-----

第5 本人通知が不要な場合	251
---------------	-----

① 本人通知が不要である場合	251
----------------	-----

② 本人の権利利益を保護するため必要なこれに代わるべき措置の内容	253
----------------------------------	-----

Chapter7

個情委とのやり取り

254

第1 漏えい等報告の重要性	254
---------------	-----

第2 個情委の担当者との連絡	255
----------------	-----

第3 個情委への説明	255
------------	-----

① データの法的な位置づけ	255
---------------	-----

② 安全管理措置	256
----------	-----

第4 本人通知のタイミング	258
---------------	-----

Chapter8

マイナンバーが漏えい等したおそれがある場合	259
-----------------------	-----

第1 マイナンバー法と個情法	259
----------------	-----

第2 マイナンバー法の基本的な仕組み	260
--------------------	-----

第3 マイナンバーが漏えい等した場合の個情委への報告	261
----------------------------	-----

① マイナンバー法が定める報告対象事態	261
---------------------	-----

② 報告対象事態の詳細	262
-------------	-----

③ 個情委への報告事項	262
-------------	-----

第4 本人への通知	265
-----------	-----

Chapter9

お詫びの品	267
-------	-----

Chapter10

損害賠償	269
------	-----

第1 個人情報の漏えいと損害賠償請求	269
--------------------	-----

第2 個人情報の漏えいにおいて損害賠償を認めた事案	270
---------------------------	-----

第3 慰謝料の金額	271
-----------	-----

第4 「集団訴訟」	272
-----------	-----

① 消費者裁判手続特例法	272
--------------	-----

② 個人情報の漏えいと消費者裁判手続特例法	273
-----------------------	-----

Chapter11

臨時報告書・適時開示・インサイダー 275

第1 有価証券報告書又は半期報告書の提出期限の延長	275
① 有価証券報告書	275
② 半期報告書	276
第2 決算短信の公表の延期	276
第3 臨時報告書	277
第4 適時開示	280
① 有価証券上場規程による適時開示事由	280
② 有価証券報告書・半期報告書に関する適時開示	281
③ 生じた損害に関する適時開示	282
④ 重要な事項の決定	283
⑤ 重要な事項の発生	285
⑥ その他	286

Go to the next page ►

IV 個情委の対応（権限行使）

Chapter1

概要

288

Column：指導、助言、勧告の違い・288

Chapter2

報告徴収

291

第1 報告徴収が行われる場合

291

第2 報告徴収の相手方

292

第3 事案解明のための報告徴収

292

第4 再発防止策の実施状況を確認するための報告徴収

293

Column：再発防止策の進捗に関する公表・294

第5 報告徴収の手続

294

第6 報告徴収を受けた事業者の対応

295

Chapter3

立入検査

297

第1 立入検査が行われる場合

297

第2 立入検査の内容

298

第3 立入検査の相手方	298
第4 立入検査の手続	299
第5 立入検査を受けた事業者の対応	299

Chapter4 指導・助言

第1 指導・助言が行われる場合	300
第2 指導・助言の内容	302
第3 指導・助言の相手方	303
第4 指導・助言の手続	303
第5 指導・助言なされた事案の公表	304
① 詳細な事案の公表	304
② 四半期ごとの公表	304

Chapter5 勧告

第1 勧告が行われる場合	305
第2 勧告の内容	307
第3 勧告の相手方	309
第4 勧告の手続	309

第5 勧告がなされた事案の公表	310
-----------------	-----

Chapter6

命令	311
----	-----

第1 命令が行われる場合	311
--------------	-----

第2 命令の内容	312
----------	-----

第3 命令の相手方	312
-----------	-----

第4 命令の手続	312
----------	-----

第5 緊急命令	313
---------	-----

第6 命令がなされた事案の公表	314
-----------------	-----

Chapter7

漏えい等報告した場合の権限行使	315
-----------------	-----

Go to the next page ►

V 漏えい等事案の対応の実務

Chapter1

委託先事業者からの漏えい等 320

第1 漏えい等に対する安全管理措置 321

- ① 平常時の安全管理措置 321
- ② 漏えい等した場合の安全管理措置 321

第2 委託先から委託元への通知 322

- ① 委託先から委託元への通知と委託先の義務免除 322
- ② 通知の内容 323
- ③ 通知の効果 323

第3 個情委への報告 324

- ① 個情委への報告の概要 324
- ② 委託先と委託元の連名報告 325

第4 本人通知 327

第5 委託先に残存していた個人データ 329

第6 委託先と委託元に対する個情委の処分 330

第7 再委託先からの漏えい等 330

Column：再委託先の把握・331

第8 委託元が行政機関等である場合 332

- ① 行政機関等に対して適用される条文 332
 - (1) 安全管理措置・332
 - (2) 漏えい等が生じた場合の対応・333

② 行政機関等から委託を受けた民間の委託先	334
-----------------------	-----

第9 委託先に対する責任追及	335
----------------	-----

Chapter2

共同利用先からの漏えい等	337
--------------	-----

Chapter3

クラウド事業者からの漏えい等	339
----------------	-----

第1 クラウドサービスの利用と法的な整理	339
----------------------	-----

第2 個情委への報告（代行報告）	341
------------------	-----

Chapter4

内部不正	343
------	-----

第1 内部不正調査のポイント	343
----------------	-----

第2 内部不正と「漏えい」	344
---------------	-----

① 内部不正と漏えい	344
------------	-----

② 内部不正と漏えいの「おそれ」	345
------------------	-----

第3 内部不正者等に対する処分	346
-----------------	-----

① 内部不正者に対する懲戒処分	346
-----------------	-----

② 内部不正者や個人データの提供を受けた者に対する刑事告発	346
-------------------------------	-----

(1) 適用される法令・346

(2) 個人情報データベース等不正提供等罪・347

(3) 両罰規定・347

(4) 被害届や告訴状の提出・349

第4 内部不正と安全管理措置義務違反	349
--------------------	-----

Chapter5

不正アクセス・ランサムウェア 351

第1 不正アクセス・ランサムウェアの調査のポイント	351
---------------------------	-----

第2 不正アクセス・ランサムウェアにおける報告対象事態	352
-----------------------------	-----

① 報告対象事態	352
----------	-----

(1) 不正アクセス・ランサムウェアにおける「漏えい等」	352
------------------------------	-----

(2) 報告対象事態	352
------------	-----

② 漏えい等の「おそれ」	353
--------------	-----

第3 個情委への報告	354
------------	-----

第4 不正アクセス・ランサムウェアと安全管理措置	355
--------------------------	-----

Column：ランサムウェア・356

Chapter6

フィッシング詐欺 359

第1 フィッシング詐欺による情報の窃取	360
---------------------	-----

第2 窃取された個人情報の利用と漏えい	361
---------------------	-----

Chapter7

暗号化した個人データの漏えい等 363

第1 暗号化した個人情報の位置づけ	363
-------------------	-----

第2 暗号化と安全管理措置	363
---------------	-----

第3 暗号化した個人データの漏えい等	364
① 暗号化と「漏えい」	364
② 漏えい等報告及び本人通知の義務	364
(1) 暗号化による漏えい等報告及び本人通知が不要な場合	364
(2) 高度な暗号化にあたる暗号	366
(3) 復号鍵の適切な管理	368
(4) 高度な暗号化とパスワード	369

Chapter8

ミスによる個人データの漏えい等 371

第1 メールの誤送信	371
第2 公開設定の誤り	372

事項索引 · 374