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、穴が全くないように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

Go to the next page ▶

Ⅱ　安全管理措置の実務

Chapter1

Chapter2

Chapter3

Chapter8
委託先の監督　148

Chapter9
クラウドと安全管理措置　168

Ⅲ　個人データの漏えい等の実務

Chapter1

Chapter2

Chapter3

Chapter5
個情委への報告　217

Chapter6
本人通知　244

Chapter7
個情委とのやり取り　254

Chapter11

臨時報告書・適時開示・インサイダー　275

Go to the next page ▶

Ⅳ　個情委の対応（権限行使）

Chapter1
概要　288

Chapter2
報告徴収　291

Chapter3
立入検査　297

Chapter4
指導・助言　300

Chapter5
勧告　305

Chapter6

命令　311

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