研究会報告

ＣＩＡフォーラム研究会報告

個人情報保護法に基づく安全管理措置に関する企業の責任と内部監査の手法及び留意点

研究会No. a 13（グローバル・リーガル・リスクマネジメント研究会）

ＣＩＡフォーラムは、ＣＩＡ資格保持者の研鑽及び相互交流を目的に活動する、一般社団法人日本内部監査協会（ＩＩＡ－ＪＡＰＡＮ）の特別研究会である。各研究会は、担当の座長が責任をもって自主的に運営し、研究期間、目的成果を設定し、研究成果を発信している。

当研究報告書は、ＣＩＡフォーラム研究会No. a 13が、その活動成果としてとりまとめたものである。報告書に記載された意見やコメントは、研究会の「見解」であり協会の見解を代表するものではなく、協会がこれを保証・賛成・推奨等するものでもない。

第１　はじめに

当研究会は、国内外の事業を問わず、企業の存続に重大な影響を与える法的リスク事項、及び、当該リスク対応について研究を行うために設置された研究会である。当研究会では、企業の内部監査人及び監査役や監査法人で勤務する公認会計士のみならず、公認内部監査人（ＣＩＡ）資格を持つ弁護士が複数メンバーとなっている。

本研究は、個人情報の保護に関する法律（以下「個人情報保護法」という。）に基づき個人情報取扱事業者が負う法的義務である個人データの安全管理のための措置（以下「安全管理措置」という。）を講じる義務に関し、これに関する企業の責任、並びに、安全管理措置に関する内部監査の手法及び留意点について、研究会メンバーが各々の経験も交えて議論をした内容を報告書として取りまとめたものである。

以下では、個人情報保護法上の個人情報取扱事業者に該当する株式会社を想定して論じ、当該株式会社を単に「企業」と呼称する。

第２　安全管理措置に関する企業の責任

１　安全管理措置を講じる義務

個人情報保護法23条は「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。」と定め、企業が安全管理措置を講じる義務を定めている。

安全管理措置の内容については、個人情報保護委員会が制定する「個人情報の保護に関する法律についてのガイドライン（通則編）」（以下「ガイドライン」という。）において個人情報取扱事業者が講じるべき措置や当該措置を実践するための手法の例が示されている。ガイドラインが定める安全管理措置の項目については以下第３において述べる。

なお、個人データの取り扱いに関連して企業が潜在的に負うリスクは、企業の業種、規模、個人データの種類等に応じ様々であるし、各企業が講じるべき安全管理措置も決して一律ではない。ガイドラインも「安全管理措置を講ずるための具体的な手法については、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、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。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものであるため、必ずしも次に掲げる例示の内容の全てを講じなければならないわけではなく、また、適切な手法はこれらの例示の内容に限られない。」旨を述べている点に留意が必要である。

２　安全管理措置に不備があった場合に企業が負うリスク

企業の安全管理措置に不備があった場合、企業は以下のようなリスクを負う。

⑴　個人情報保護法上の措置

企業が安全管理措置を講じることなく、個人情報保護法23条に違反した場合、当該企業は個人情報保護法148条が定める個人情報保護委員会による勧告・命令及び公表の対象となり得る。個人情報保護委員会による命令に違反した場合、違反者には１年以下の懲役刑又は100万円以下の罰金刑が科される可能性があり（同法178条）、法人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（個人情報保護法は、従業員だけでなく取締役や派遣社員を含めた「従業者」という概念を用いている）が、その法人又は人の業務に関して当該命令違反を行った場合には、当該法人には１億円以下の罰金刑が科される可能性がある（同法184条１項１号）。

⑵　損害賠償責任

企業の安全管理措置に不備があり、個人情報の漏えい等が生じた場合、企業が個人情報の主体である個人に対して損害賠償責任を負いうる。損害賠償の金額は漏えい等がなされた個人情報の性質や、２次被害（第三者が漏えいした個人情報を用いて本人に接触する等）の有無等、個別の事情によって左右されるが、１人あたりの損害賠償金額は数千円から数万円となる可能性が高い[1]。多数の個人情報が漏えいするようなケースでは、合計の損害賠償金額は多額になりうる。

⑶　レピュテーションの毀損

上記⑴の措置や⑵の賠償責任の有無にかかわらず、安全管理措置の不備が報道等によって公になった場合、企業のレピュテーションが毀損される。特にクレジットカード情報等の支払に関する情報や機微な個人情報が漏えいした場合や、企業のサービスを利用するために個人による個人情報の入力が必要なＢ to Ｃ企業において個人情報の漏えいが生じた場合においては、企業の信用や事業価値が大きく毀損されることとなる。

３　安全管理措置の不備が問題になった実際の事例

企業や公共団体の安全管理措置の不備が問題になった実際の事例としては、以下のようなものがある。

- 退職者が退職後も個人データのデータベースにアクセスできる状態が維持され、かつ特定のＰＣ以外からのアクセスを禁止するアクセス制限が設定されていなか

[1] 特定非営利活動法人日本ネットワークセキュリティ協会発表の「インシデント損害額調査レポート　2021年版」によると、2016年から2018年までにおける１人あたり平均想定損害賠償額は２万8308円

った企業において、退職者がインターネットカフェからシステムにアクセスして故意に大量の個人データを取得した
- 外部者が申込みを行うシステムにおいて、複数人に同一の識別用ＩＤが付与されるというシステム設計のミスにより、他人の個人データが閲覧できる仕様になっていた
- 個人データの入った記憶媒体を従業員が紛失し、その後も発見できなかった
- 従業員が操作するＰＣがフィッシングサイトからマルウェアに感染したことにより個人情報が流出した
- メールを誤送信しメールアドレスが流出した
- 受託先が委託時の取り決めに反してクラウドサーバーで個人データを管理していた

第３　安全管理措置に関する内部監査の手法及び留意点

１　自社の状況に即したリスク評価の重要性

監査資源が有限であることから、安全管理措置に関する内部監査を検討・実施する前に、その前提として、自社における安全管理措置に関連するリスク評価を実施することが必要不可欠である。自社の業態及び規模、取り扱っている個人データの種類・量、個人データをどのように取り扱っているかだけでなく、外国の個人データを取り扱っているか、外部委託をしているか等、自社の具体的な状況に基づき、自社の安全管理措置に不備があった場合にリスク事象が生じうる頻度と自社への影響の大きさを検討しなければならない。

２　安全管理措置の項目ごとの検討

下記表は、ガイドラインが定める安全管理措置の項目（「基本方針の策定」を除く）ごとに、①ガイドラインで例示されている主な手法を記載した上で、②当研究会で議論を行い取りまとめた、当該項目の不備によって想定される個人情報に関連するリスク事象、及び、③同じく当研究会で取りまとめた、当該項目に関し内部監査を実施する際の手法及び留意点を整理したものである。

個人データの取扱いに係る規律の整備			
安全管理措置の項目	**①ガイドラインで例示されている主な手法**	**②不備によって想定されるリスク事象**	**③内部監査の手法及び留意点**
個人データの取扱いに係る規律の整備	・個人データの取扱いの段階ごとに取扱方法、責任者・担当者及びその任務等について定める個人データの取扱規程を策定する ・具体的に定める事項については、以下に記述する各安全管理措置の内容を織り込む	・責任者や担当者が不明になる ・以下の各安全管理措置が防ごうとしているリスクが、ルールの不存在によって生じてしまう ・グループ内の企業間でルールが統一されない	・規程の存在の確認（マイナンバーを含め、取り扱っている個人データの種類に応じた規程があるか確認する） ・規程が法令、ガイドラインと整合しているかの確認 ・事業団体が制定している指針も参考にする ・グループ内の企業で規程を統一するか、整合性は保ちつつ各企業の実態に合わせた調整をするかも検討する

組織的安全管理措置			
安全管理措置の項目	**①ガイドラインで例示されている主な手法**	**②不備によって想定されるリスク事象**	**③内部監査の手法及び留意点**
組織体制の整備	・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 ・個人データを取り扱う従業者及びその役割の明確化、当該従業者が取り扱う個人データの範囲の明確化 ・問題事象を把握した場合の責任者への報告連絡体制 ・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	・役職員が個人データに対する不適当なアクセス権限を持つ ・個人データの機密区分指定を誤って設定してしまう	・関連する規程の有無の確認 ・規程の内容がガイドラインに沿っているか、自社の過去事例や同業他社の事例に照らして不合理でないかの検証 ・規程に従った体制が取られているかの確認
個人データの取扱いに係る規律に従った運用	・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ため、システムログその他の個人データの取扱いに係る記録の整備や業務日誌の作成等を通じて、個人データの取扱いの検証を可能とすること	・個人データに関するインシデントが発生した際にその経緯や記録を確認できない ・個人情報の本人からの開示請求等に対応できない	・台帳の実査 ・自社の事業内容からみて当然あるべきデータが保管されているかの確認 ・廃棄の証票の確認（ミスだけではなく、ルール通りの時期・範囲の廃棄を現場判断で意図的に行っていない事象に注意する）
個人データの取扱状況を確認する手段の整備	・個人情報データベースの種類、データの項目、責任者、利用目的、アクセス権の範囲を明確にすることで個人データの取扱状況を把握する	・役職員が個人情報についてそもそも個人情報であるという旨を認識しない ・個人情報の目的外利用 ・個人情報を直接取得する際に目的を明示しない ・意図せず個人情報の第三者提供を行ってしまう	・ガイドラインで列挙されている、個人情報データベースの種類、データの項目責任者、利用目的、アクセス権の範囲の明確化がされているかの確認 ・台帳及びデータベースの項目設定が本社主導で統一的に行われているか ・項目が適切に入力・記入されているか
漏えい等事案に対応する体制の整備	・漏えい発生時に事実関係の調査、本人への通知、個人情報保護委員会等への報告、再発防止策の検討及び決定、公表等を行うための体制の整備	・インシデント発生時の社内における情報把握の遅れ ・インシデント発生時の報告の不備、不適切な公表・公表遅れ及び対応の遅れ	・規程の有無 ・規程が法令及びガイドラインに沿っているか ・自社の過去事例において、規程に従った処理ができていたか ・ストレステストやシミュレーションの実施有無及び結果の確認。実際の漏えい等事案では通報に時間がかかることが多いので、通報まで含めて訓練をすることが望ましい

取扱状況の把握及び安全管理措置の見直し	・個人データの取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施する ・外部の主体による監査活動と合わせて、監査を実施する ※ガイドラインにおける「監査」は内部監査の趣旨ではない点に注意する	・問題改善の機会を持てない、法令アップデート対応の機会を持てない、技術アップデート対応の機会を持てない	・自社チェック（ガイドラインでいうところの「監査」）のルールが作成されているかの確認 ・自社チェックの実施状況の確認

人的安全管理措置			
安全管理措置の項目	**①ガイドラインで例示されている主な手法**	**②不備によって想定されるリスク事象**	**③内部監査の手法及び留意点**
従業者の教育	・定期的な研修等の実施 ・個人データについての秘密保持に関する事項を就業規則等に盛り込む	・従業者のコンプライアンス意識不足・法令知識の欠如 ・従業者の社内規程及びマニュアルの違反 ・従業者による不適切なソフト等の利用や不審なメール添付ファイルを開いてしまう事象の発生	・教育実施のルールの確認 ・教育の実施記録、参加記録の確認 ・社内規程における、個人情報に関する従業者の義務の存否の確認

物理的安全管理措置			
安全管理措置の項目	**①ガイドラインで例示されている主な手法**	**②不備によって想定されるリスク事象**	**③内部監査の手法及び留意点**
個人データを取り扱う区域の管理	・ＩＣカードやナンバーキー等による入退室管理、持ち込み機器の制限、物理的な配置（覗き込み防止を含む）	・権限を持たない者の侵入・持ち出し・改ざん、覗き込みによる情報取得 ※個人情報を紙の台帳で管理しているかや個人情報が含まれる紙媒体の多寡、社外の人物のマイナンバーを集めるか否かによってリスク程度は変わる	・入退室管理及び持ち込み機器に関するルールの有無 ・入退室管理実態の確認（ＩＣカードやキーの管理状態実査） ・入退室記録の確認 ※どの個人情報が、どの部門のどの場所に集まっているのかを把握する点が重要
機器及び電子媒体等の盗難等の防止	・機器や書類等を施錠できるキャビネット・書庫等に保管したり、機器をセキュリティワイヤー等で固定する	・個人情報が保存された機器や媒体の盗難、紛失	・どの個人情報が、どの部門のどの場所に集まっているのかの把握に注意 ・ルールの有無の確認。情報セキュリティ規程のような上位規程で一元的に定められている場合もある ・管理方法の実査

電子媒体等を持ち運ぶ場合の漏えい等の防止	・暗号化、パスワードによる保護等を行った上で電子媒体に保存する ・封緘、目隠しシールの貼付けを行う ・施錠できる搬送容器を利用する	・盗難、紛失、暗号化が不十分な場合に漏えい等が発生しやすい	・ルールの有無の確認 ・管理方法の実査 ※利便性のためにルール通りの管理がなされていない場合がままある（極端な例では、モバイルＰＣにそのＰＣのログインパスワードが付箋で貼られていることすらある）
個人データの削除及び機器、電子媒体等の廃棄	・書類等の廃棄では復元不可能な手段で廃棄をする ・個人データを削除する場合、容易に復元できない手段を採用する ・個人データが記録された機器、電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等の手段を採用する	・破棄が不十分、不適切な場合は廃棄対象の個人情報が利用や復元されるおそれがある	・ガイドラインを満たすルールの確認 ・委託先の基準の有無の確認 ・実査 ※保有期間を過ぎてもルール通り廃棄せずに個人情報を保持している例がままある

技術的安全管理措置			
安全管理措置の項目	**①ガイドラインで例示されている主な手法**	**②不備によって想定されるリスク事象**	**③内部監査の手法及び留意点**
アクセス制御	・個人情報を取り扱うシステムの限定 ・個人情報を取り扱うシステムを使用できる従業者の限定	・不適切（不必要）な内部者によるアクセスや退職者・契約終了後の契約先（法人・個人）によるアクセス及び当該アクセスによる個人情報の漏えい、盗難、改ざん等	・ルールの確認（従業者・委託先のリストとアクセス制限のリストがリアルタイムで連動するようになっているのかに注意する） ・アクセス制御がルール通りになっているかの実査 ・従業員の入れ替わりに伴うアクセス制御のアップデートができているかの確認。アクセス権限を持っている者のリストをＩＴ部門から入手し、当該リストと従業者・委託先のリストを照合するという手法も考えられる
アクセス者の識別と認証	・ＩＤ、パスワード、ＩＤカード等の使用	・なりすましによる個人情報の漏えい、盗難、改ざん等	・ルールの確認（なりすましが困難な識別手法が取られているか、当該手法は自社の状況に鑑みて十分といえるかを検討） ・ルール通りの識別がなされているかの実査 ・ルールが定期的に見直しされているかの確認

外部からの不正アクセス等の防止	・外部からのアクセスの制限、ウイルスソフト、ログ分析、ソフトウェアのアップデート	・不正アクセスを受ける ・自社への不正アクセスを検知できない	・ルールの確認 ・制限の実査 ・ログの実査（内部監査部門が直接異常を発見するというよりも、事業部門や管理部門が適切にログの確認を行っているかどうかをチェックする）
情報システムの使用に伴う漏えい等の防止	・システム設計時の安全性確保と見直し（攻撃対策を含む）、通信の暗号化、移送する個人データのパスワード等による保護	・不正アクセスを受ける ・役職員の故意や過失があった際に、個人情報の漏えい、盗難、改ざん等が容易に発生してしまう	・暗号化や移送する個人データの保護に関するルールの確認 ・暗号化や移送する個人データの保護に関する実査 ・システムのアップデートや見直しの有無の確認

第４　おわりに

前述の通り、個人データに関連するリスク事象やリスクの大きさ、そして実施すべき安全管理措置（人的・物的リソースをどれだけ割くか、という点も含め）は企業によって様々であり、一定の正解があるものではない。他方、本問題点はその性質上、企業間における意見交換、特に自社の経験や問題意識を交えた議論を行うことが容易ではない分野でもある。本研究は、様々なバックグラウンドを持つ当研究会の各メンバーが、議論を重ねた末にたどり着いた最大公約数的な認識を示すものである。本研究が、安全管理措置に関する企業の責任と内部監査の手法及び留意点に関する、読者の皆様に対する一定の指針となれば幸いである。

＜ＣＩＡフォーラム研究会No.a13（グローバル・リーガル・リスクマネジメント研究会）メンバー＞

（氏名五十音順・敬称略）

阿部　寛、犬塚　重夫、井上　智哉、加藤　雅之、川添　博司、川端　真一、酒井　太郎、
堂山　政行、林田　正人、森居　達郎、安田　健一、吉田　武史、渡邉　宙志、渡辺　忠則

（メンバーの氏名は、2023年７月現在）