Ⅱ．個人情報保護対策の場面ごとの取組事例

１．個人情報保護対策の準備（規程づくり・体制づくり）の場面

本節では、個人情報保護対策そのものを効果的かつ効率的に実施する前提となる、規程づくり、体制づくりの事例を取り上げている。また、特に効果的・効率的と考えられる工夫を事例として示すようにした。

例えば、規程づくりのためのユニークな方法としては、問題となる事例が社内外で起きるたびに「ヒヤリ・ハット集」として紹介しながら、その内容を次年度以降の社内規程に取り込んでいくことで、職員に違和感無く規程を導入するという方法を採用している事例（⑦）を紹介している。また、効率的な取組としては、規程類の作成そのものは自社で行い、最終チェックだけを外部の専門家に委託する方法を取っている事例（⑤）や、規程等があまりに多くなり過ぎ、有名無実化することを懸念して従業者が守るべき規程はごくごく限定している事例（⑧）、勉強会の中で規程を作成する事例（⑨）、品質管理の全社運動と一体として実施している事例（⑫）、規程等作成担当者の当事者意識を喚起し、積極的に関与してもらいながら効率的に行うために、担当者に予め改善点を宿題にして持ち寄ってもらう事例（⑮）なども紹介している。

さらに、規程変更を柔軟に行うために、規程の構成を 3 階層に分けて軽微な変更を容易に行うことができるようにしている事例（⑭）もある。

また、体制構築のための取組としては、役職ごとに責任者と代行者を置き、別な役職ではその関係を逆転させることで、相互監視作用を狙った事例（④）や、より円滑に個人情報保護を実現できるように、個人情報保護とは全く関係の無い既存組織に個人情報保護のための役割を担わせているような事例（②）を紹介している。

本節で紹介している取組事例

1-①：事業領域ごとに管理者と推進実務担当を設置
1-②：既存の委員会に個人情報保護の役割を付託することで違和感無く体制を構築
1-③：本社と支店等との分権
1-④：タスキがけ人事による効率的な管理体制
1-⑤：規程類は社内で整備し、外部の専門業者のチェックを受ける
1-⑥：新ルール適用前に試行実施の期間を確保
1-⑦：ヒヤリ・ハット事例集の作成・掲示
1-⑧：規程を絞って従業者にわかりやすく説明。常時携帯用のカードも作成
1-⑨：勉強会と規程作成を同時進行で実施。優先テーマから先に担当者を決めて規程作成
1-⑩：リスク管理台帳で管理・共有

1-⑪：縦糸と横糸の調和したマネジメントシステム
1-⑫：品質管理の全社運動と一体となって推進
1-⑬：社内の各機能分野から広く人材を集めて全社体制で推進
1-⑭：規則のレイヤーを 3 段階に分けることで、軽微なルール変更を迅速に実施
1-⑮：セキュリティ委員会のメンバーに、セキュリティ改善点を 10 個以上見つけてくることを宿題化
1-⑯：サービス態様ごとにマニュアルを作成して、社員の対応を現実に沿ったものとする

1-①【事業領域ごとに管理者と推進実務担当を設置】（製造業：約 300,000 人（グローバル））

・A 社では、ドメイン（事業領域）ごとに CSO（チーフ・セキュリティ・オフィサー）とプロフェッショナル（現場の情報セキュリティ推進実務担当）を設置しており、全社－ドメイン－事業場の 3 層管理体制を採っている。

1-②【既存の委員会に個人情報保護の役割を付託することで違和感無く体制を構築】
（電気・ガス・水道業：約 60 人）

・C 社では、既存で常設の IT 委員会の活動内容に個人情報保護に関する活動を付加し、個人情報に関するデータのサーバへの移管や、個人パソコンの定期的なチェックを行っている。IT 委員会は各部の情報機器、ネットワークなど IT に詳しい人によって構成されている。

・車輌委員会が車内に情報を置き去りにしていないかをチェックする。この委員会はもともとは交通事故防止のための委員会だが、個人情報保護の視点を取り入れて活動を展開している。

・もともとあった組織に役割分担をして取組を進めることで、従業者にとって抵抗感が少なかったと考えている。

1-③【本社と支店等との分権】（信用業：約 3,700 人）

・I 社では、全社的には個人情報保護に関する専任組織が、規程類の整備や教育指導、管理を行っている。各部・支店単位においては各組織長及び次長が、個人情報保護責任者及び個人情報保護代行者となって管理下の組織における個人情報保護に係る業務を管理している。

1-④【タスキがけ人事による効率的な管理体制】（信用業：100 人未満）

・K 社では、各役職に責任者と代行者を設置することとし、1 人で複数の業務の責任者を兼任することの無いよう、タスキがけ人事としている。例えば、個人情報管理において、A 氏が責任者で、B 氏が代行者である場合、情報セキュリティ管理では、B 氏が責任者で、A 氏を代行者としている。タスキがけ人事をすることで、少ない人数で複数の業務をこなしつつ、牽制できる態勢としている。

1-⑤【規程類は社内で整備し、外部の専門業者のチェックを受ける】（信用業：100 人未満）

・K 社では、経費抑制のため、種々の規程類は自主ルールやガイドライン等を参照しながら社内で作成した後、外部の専門業者による個人情報保護に関する診断を受けている。

1-⑥【新ルール適用前に試行実施の期間を確保】（信用業：100 人未満）

・K 社では、新たに整備又は変更した規程の本格実施前に、1 ヶ月半ほどの試行期間を設け、ルールの抜け漏れや、ルール間の不整合を修正した。

・従業者においては当初新ルールに対する不満は大きかったが、習熟度の高まりと共に定着した。

1-⑦【ヒヤリ・ハット事例集の作成・掲示】（情報サービス業：約 1,600 人）

・O 社では、世間で実際に発生した個人情報事故事例や社内でヒヤリやハットした事象について紹介し、“世間の事故を社内で発生させないために、また、ヒヤリやハットを事故に繋げないためにどのような行動を取ることが求められるか”を記載した「ヒヤリ・ハット集」を随時作成・社内通知している。

・事例集の形式ではあるが、単なる注意喚起の通達ではなく実際には行動基準を示しており、既成事実化した上で次年度は社内ルール集に正式に織り込むことで、従業者の抵抗や戸惑いを極小化しながら円滑なルール策定に役立てている。

1-⑧【規程を絞って従業者にわかりやすく説明。常時携帯用のカードも作成】
（情報システム／製造業：約 500 人）

・R 社では、規程は全部で 38 あるが、分かりやすい 2 つの規程（「利用者向けガイドライン」と「情報資産取扱ガイドライン」）だけを見ればよい、と従業者には通達し、わかりやすく周知している。

・規程の目的、守るべきこと、事故の連絡ルートなどをまとめた「セキュリティカード」を従業者全員に配布し、常に携帯するようにしている。

1-⑨【勉強会と規程作成を同時進行で実施。優先テーマから先に担当者を決めて規程作成】
（その他サービス業(教育・学習支援)：約 180 名）

・ケ社では、単なる勉強会で終わってしまっては、参加者だけが理解して終わってしまうので意義が薄く、その後仕切りなおして規程等を作り始めると対応に時間がかかってしまうと考えた。そこで、毎回勉強会のテーマを決めて開催し、その中で勉強したことについてすぐに規程や関連資料を作成するようにした。そのことで勉強に身が入ったし、時間を効率的に使用できた。

・必ずしも専任の担当者がいなかったこと、個人情報保護にはさまざまな分野やテーマが存在していたことから、テーマや対策内容別に重要・緊急マップを策定して、重要度と緊急度で色分けを行い、特に緊急性と重要性が高い対策について、それぞれに担当を決めて規程作成や準備などを行った。誰がいつまでに策定するのか、ということを明確にすることが効率化と確実な規程類の整備につながった。

1-⑩【リスク管理台帳で管理・共有】(情報サービス業(アウトソーシング等)：約 1,000 名)

・ク社では、所属部署ごとにリスクアセスメントを行って、潜在リスク、残留リスクそれぞれを洗い出し、管理台帳に登録し、所属全従業者が共有している。

・原因究明と未然防止策は、品質向上のための全社運動と連携して対応している。

潜在リスク台帳	個別の個人情報毎に想定シナリオを洗い出し、リスクについて業務フローから見た未然防止策を記載(合理的な判断に基づくレベルで記載)そのうえで、現在の対応状況を再点検し対応状況欄へ記載(「○」対応済み、「△」対応予定、「×」未対応又は対応困難)
残留リスク台帳	「潜在リスク管理台帳」の対応状況欄が「×」または、不十分と認識しているものを「残留リスク管理台帳」へ登録し管理策を策定する。情報管理統括責任者は各部より提出された「残留リスク管理台帳」登録のリスクレベルに応じた管理策を総合的に評価して承認する。そして、4ヶ月単位で実施している自主点検時に継続フォローする

図表　ク社における個人情報の安全管理に関するリスク対策表（一部抜粋）

管理段階	手段	対処すべきリスク	選択した対処方法
入手	手渡し	・覗き見による不正アクセス	・入力場所の限定
		・外部記憶媒体によるウイルス感染	・外部記憶媒体の受領時にはウイルスチェックを実施する
	FAX	・受領時の紛失	・個別の場合→受領確認の電話 ・不特定多数の場合→受領記録を付ける
	郵送	・郵便物の盗難	・郵便受けの施錠管理、定期回収 ・郵便物の直接受渡し
		・誤配送	・収集窓口の明確な公表及び収集代行サービスを活用する ・指定封筒の使用
		・受領時の紛失	・受領記録を付ける
		・外部記憶媒体によるウイルス感染	・外部記憶媒体の受領時にはウイルスチェックを実施する
	メール	・通信経路上の盗聴、改ざん	・原則メールによる収集は行わない。やむを得ず使用する場合は、ファイルへのパスワードを設定、若しくは暗号化を依頼する
		・メール受信によるウイルス感染	・ウイルス対策の全社的な構築
			・不審なメール自身、メッセージ、添付ファイルを無視する
	Web 収集	・通信回線上の盗聴、改ざん	・各拠点間回線の VPN 化、収集データの暗号化
			・情報主体自らのＩＤ，パスワード設定の依頼
	直接入力	・覗き見による不正アクセス	・収集場所の限定

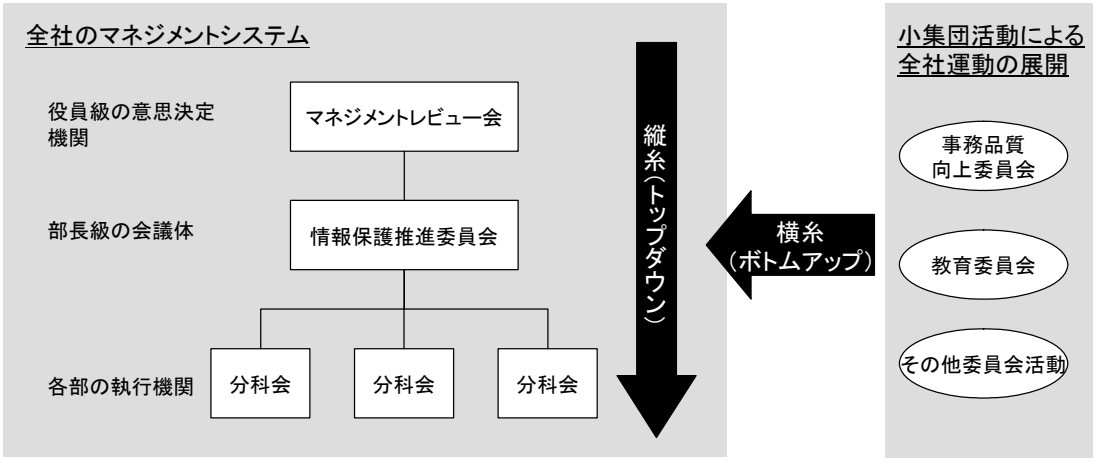
注）本報告書に掲載したク社の「リスク対応表」は実際に同社で使用されているリスク対応表の一部を抜粋・加工したものであり、項目や内容は完全のものではありません。

1-⑪【縦糸と横糸の調和したマネジメントシステム】

（情報サービス業(アウトソーシング等)：約 1,000 名）

・ク社では、役員級のマネジメントレビュー会を頂点とする情報管理に関するマネジメントシステムによる“縦糸”に加え、小集団活動による全社運動という“横糸”が組みあわされ、全社が一丸となった事務サービスの品質向上の一環として、個人情報保護の改善に取り組んでいる。

図表　“縦糸”と“横糸”の調和したマネジメントシステム



1-⑫【品質管理の全社運動と一体となって推進】

（情報サービス業(アウトソーシング等)：約 1,000 名）

・ク社では、全役職員参加の小集団活動による全社運動が創業以来、企業風土として根付いている。個人情報保護についても、この運動の一環として取り込まれ、ボトムアップ的に日々改善活動が実施されている。

・全社運動としては、事務ミスの未然防止活動やクリーンオフィスキャンペーンなどが定期的に実践されている。個人情報保護に関する対応もこれらに取り入れられ、運動の一部として実践されている。

・全社運動がいかに定着しているかを示す事例として、一般的に情報管理部門が作成して配布することの多い「情報管理に関する携行カード」について、従業員が自分たちで必要性を認識し、議論を行い、作成したということがあげられる。

図表　全社運動の活動ニュース

クリーンオフィス　ニュース

2009年8月20日発行
事務品質向上委員会
職場環境改善部会

第1回クリーンオフィスキャンペーン実施結果のご報告

「第1回クリーンオフィスキャンペーンテーマ：個人情報保護について」　※各点検項目 10 点満点　計 100 点満点

確認方法	No.	分類	チェック項目	A部	B部 C部 D部 E部	F部	G部	H部	I部	J部	K部	L部	M部	N部	P部 Q部	O部	合計
フロア訪問	1	PC	ユーザーID・パスワード・個人情報が貼り付けられていないか。	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	130点
	2		離席の際、パソコン画面に個人情報が出ている状態になっていないか。(パソコンのロックがされているか)	10点	10点	10点	10点	10点	10点	10点	8点	10点	10点	10点	10点	10点	128点
	3		帰宅時、パソコンの管理ができているか。 (電源OFFされているか？ノート型はワイヤー等で盗難防止がされているか？)	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	130点
	4	机上・机下	個人情報掲載書類が放置された状態で離席・帰宅されていないか。 離籍時、個人情報掲載の帳票やリストは裏返しにしているか。	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	130点
	5		机下に書類を置いていないか。	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	130点
	6	コピー機 プリンター FAX	コピー機、プリンター、FAX機にプリントされた個人情報掲載書類が放置されていないか。 (原紙、印刷物、コピーしたもの、受信したもの等)	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	9点	9点	128点
	7	施錠管理	個人情報掲載書類は施錠できる場所で保管されているか。 (施錠管理されてない場所で保管・放置されていないか。) 個人の机の施錠確認	10点	10点	10点	10点	0点	10点	10点	10点	10点	10点	10点	10点	10点	120点
	8		帰宅時、個人情報掲載書類の保管場所の施錠はできているか。 ロッカー・ローキャビの施錠確認	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	130点
	9	ゴミ処理	個人情報掲載書類が一般ごみに捨てられていないか。	10点	10点	10点	9点	10点	10点	10点	10点	10点	10点	10点	10点	9点	128点
	10	カード	携行カードの携行確認	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	10点	130点
合計				100点	100点	100点	99点	90点	100点	100点	98点	100点	100点	100点	99点	98点	1284点

点検者からのコメント

・採点対象外で点検項目ではありませんが、「セキュリティボックス」の状態も点検させていただきました。
　△△ビルでは満杯状態が多く、投入口元まで書類が入っている状態が見受けられました。
　手を入れれば容易に抜き取りできてしまう状態でしたので、好ましくないと思いました。
・部にもよりますが、一部の管理職の机が雑然としていました。
・携行カードは、首から提げるなどして、常に身に付けていただけますようお願いいたします。
・年々良い結果となってきております。
　クリーンオフィスへの心がけ、整理整頓が各部に浸透しているようで、
　意識の高さが窺えました。

７月２２日（水）～７月２４日（金）、８月５日（水）にかけて実施いたしました、『第一回クリーンオフィスキャンペーン』につきまして、ご多忙中のところ、多大なご協力をいただきまして誠にありがとうございました。今回は『個人情報保護』をテーマに点検を行ないました。

点検結果につきましては、結果表のとおりです。減点項目のある部署につきましては、改善への取り組みをお願いいたします。また、点検者のコメントも参考にしていただければ幸いです。

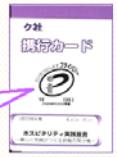
引き続き、個人情報保護を心がけていただきまして、情報漏洩・紛失の防止にお取り組みをお願い申しあげます。

携行カード変更シール配付について
お知らせ

８月の●●ビル移転（フロアー変更および集約移転）に伴い、携行カードの内容が一部変更になります。

つきましては、８月下旬に変更シールを配付いたしますので、各自貼り付けをお願いいたします。

変更シールは
必ず貼り付けて
下さい！



1-⑬【社内の各機能分野から広く人材を集めて全社体制で推進】

（製造業：約 12,000 人）

・シ社では社内の各機能分野（人事、法務、広報、販売、IT など）から広く人材を集めて個人情報統括部を設置し、同室を中心に全社体制で個人情報保護を推進した。

1-⑭【規則の階層を 3 段階に分けることで、軽微なルール変更を迅速に実施】

（情報サービス業(ソフトウェア)：約 5,500 人）

・セ社では、様々な環境の変化や事象の発生に合わせて、規則の見直しを実施している。例えば、JIS 基準の変更に合わせて変更したこともある。

・それ以前にも、同社グループ全体で体系整理を行ったこともあった。具体的には、規則の階層を 3 段階程度に分けることで、簡易な変更にはすぐに対応できるようにした（それまでは会社規則として全てを定めていたので、変更に際して役員会の決議が必要になるなど、手続きが容易ではなかった)。

・今も見直し継続中であるが、方向性としては、ルール相互の間の関係性や整合性を見直そうとしている。現在の規則は文書の規則、システムの規則、個人情報の規則、文書持ち出しの規則などが輻輳してしまっているのが問題だと認識している。

1-⑮【セキュリティ委員会のメンバーに、セキュリティ改善点を 10 個以上見つけてくることを宿題化】

（情報サービス業（アウトソーシング等）：約 30 人）

・タ社では各自がセキュリティ委員会において、10 個以上セキュリティ改善点を考えてくることを宿題にし、委員会を実施した。

・メンバーに改善案まで考えさせると躊躇してしまうと考え、宿題をセキュリティ改善点の洗い出しにとどめた。

・セキュリティ改善点への対応は、委員会メンバーから主担当と、期限を決めて実施し、2 週間後に進捗の報告を実施している。進捗はエクセルシートで管理している。

1-⑯【サービス態様ごとにマニュアルを作成して、社員の対応を現実に沿ったものとする】

（その他サービス業（警備）：約 13,000 人）

・ト社では、同じ警備業務といっても、サービス態様ごとに「警備輸送部門」、「常駐警備」など、部門が分かれているので、それぞれ個人情報保護についてはどのような視点で注意すべきか、ということを分けてマニュアルを作成している。

・マニュアルは基本編（関連法令等)、機械警備編、警備輸送編、常駐警備編、事例編（他の会社で生じた事故情報などを掲載）などで構成されており、基本編以外はサービス態様によって内容を変えている。

・基本編は ISO 内部統制室情報資産グループで作成している。一方で、サービス態様別のマニュアルは、サービス態様別に、それぞれの担当部門に依頼して作成してもらい、ISO 内部統制情報資産グループでは「基本編」と「マニュアルのフレーム」の作成、サービス態様別のマニュアルの内容のチェックを行う。