2013.07

「個人情報保護マネジメントシステム実施ハンドブック」簡易版　第６章

個人情報保護監査研究会

第6章　リスクなどの認識、分析及び対策

目的外利用や、漏洩、き損により、本人にどんな影響があるか、例えば本人が被る被害や、その賠償、信用失墜、顧客との取引停止となることなどを「リスク」として認識します。

6.1　リスクなどの認識

特定した個人情報に対し、各局面において想定されるリスクを洗い出します。

（各局面：個人情報の取得・入力、利用・加工、移送・送信、保管・バックアップ、消去・廃棄の状況）

法	「目的外利用」リスクの事例	参考：対策の事例
16条	利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。	「個人情報管理台帳」を整備して、従業者に個人情報の利用目的を認識させる。
17条	偽りその他不正の手段により個人情報を取得してはならない。	受託する場合でも、委託元が適切に取得した個人情報であることを確認し「個人情報取扱申請書」などにより、管理者の承認を得る。
18条	利用目的を、本人に通知し、又は公表しなければならない。	書面で取得する場合は書面で本人に通知する。 本人に書面で通知できない場合や、受託する場合はホームページに公表する。

法律第20条では、“漏えい、滅失又はき損の防止”　を定めているのでその観点からも見てみましょう。

	第20条「漏えい」リスクの事例	参考：対策の事例
1	領収証を他の人に発送してしまった。	・窓あき封筒を使用する。 ・発送前に複数の人でダブルチェックする。
2	メールの誤送信 BCCで発信すべきところを、CCで発信してしまった。	・一時保留機能で再チェックする。 ・添付ファイルにパスワードを設定する。
3	ノートＰＣを電車の網棚に忘れた。 携帯を紛失した。	・端末ロック、遠隔ロックを設定する。 ・ファイルを暗号化設定する。

	第20条「滅失」リスクの事例	参考：対策の事例
1	ハードディスクがクラッシュした。	・外付けハードディスク等にバックアップを取る。 ・外部データセンターにバックアップを取る。
2	停電で作成中のデータが消失した。	・UPS（無停電電源装置）を設置する。 ・ノートＰＣに変更する。
3	顧客データを別のデータで上書きしてしまった。	・バックアップしてから作業を始める。 ・別名で保存してから訂正するなど、文書管理ルールの見直しを行う。

	第20条「き損」リスクの事例	参考：対策の事例
1	原本をFAXし、ジャムって破損した。	フラットベッド型FAXを導入する。
2	コーヒーを書類の上にこぼした。	休憩コーナー、休憩時間など職場環境を整備する。
3	ハッカーが侵入し、データが書き変わってしまった	・ファイヤーウォールを設定する。 ・ログの記録と点検を行う。

6.2　リスク分析表の作成

ライフサイクルごとに、想定されるリスク（利用目的の通知漏れ、同意の取得忘れ、漏えい、滅失又はき損、目的外利用など）のリスクを洗い出し、対策を検討します。

以下は、従業者情報のリスク分析の事例です。（縮小版）

業務フロー／リスク分析表(兼　運用監査チェックリスト)

保護管理者
承認

部門	管理部	業務名　「従業員管理」	
業務フロー	採用から従業員管理および退職に至る従業員情報管理業務		2012/4/1

ライフサイクルおよび業務名		台帳	個人情報管理台帳に記載の個人情報名	取得手段入力	媒体	コピー	想定されるリスク	リスク対策	規程・様式	残存リスク
取得	採用業務	1 2 3	履歴書 職務経歴書 成績証明書	本人・直接手渡し	紙	禁止	利用目的の通知漏れ	1．面接キット「同意書(応募者用」	「個人情報取扱規程」3.4.2.4	－
							書面による同意の取得漏れ			
							漏洩(紛失)	1．保管管理者の限定	「安全管理規程」4	－
								2．施錠管理	「安全管理規程」4	－
		4	応募者からの同意書		紙	禁止	漏洩(紛失)	1．保管管理者の限定	「安全管理規程」4	－
								2．施錠管理	「安全管理規程」4	－
移送		－	(応募書類の返却)	－	紙	－	漏洩(誤送付)	1．簡易書留で送付	「安全管理規程」9	
								2．送付表の保管	「安全管理規程」9	－
利用		5	応募者リスト 採用結果票	面接者が記入	紙	禁止	目的外利用(期限を超える保管)	「廃棄記録」による確認	「安全管理規程」4	－
取得	入社手続	1～10	入社時取得書類 従業者現況表 住民票 同意書	本人・直接手渡し	紙	禁止	利用目的の通知漏れ	1．入社手続キット「同意書(従業者用」	「個人情報取扱規程」3.4.2.4	
							書面による同意の取得漏れ	2．授受記録(明細)	「安全管理規程」2	－
保管	従業員管理						目的外利用(期限を超える保管)	台帳見直し時の点検	「安全管理規程」4	
							漏洩(紛失)	保管管理者の限定	「安全管理規程」4	
								施錠管理	「安全管理規程」4	
利用		11	人事管理データ	入力	人事部サーバー	バックアップ	漏えい(不正アクセス)	アクセス権限を1名のみに設定	「安全管理規程」8	ログの不取得のため、不正アクセス検知不可
		12	イントラ登録データ	入力	サイボウズ	バックアップ	漏えい(不正アクセス)	アクセス権限設定	「安全管理規程」8	－
								アクセスログ取得と点検	「安全管理規程」8	－
		13	人事異動稟議書 辞令 人事通達等	入力	人事部サーバー	バックアップ	毀損(誤入力)	担当者と部門長による二重チェック	「安全管理規程」6	－
							漏えい(不正アクセス)	アクセス権限を1名のみに設定	「安全管理規程」8	11と同じ
				印刷	紙	回付	漏えい(不正持ち出し)	通達番号管理、回付先管理	「安全管理規程」6	－
		16 17	年金手帳 雇用保険被保険者証	本人・直接手渡し	紙	禁止	漏洩(紛失)	常時施錠管理	「安全管理規程」3	
								授受記録	「安全管理規程」2	－

「リスク分析表」で明らかにした対策は、「個人情報取扱規程」や「安全管理規程」な

どに、規定されているかどうか確認し、その規程名称と条項番号を記入します。
※　規定が無い場合は「要規定」「規程なし」などと記入し、6.3リスク対策を規定する手順に進みます。

6.2.2　残存リスクの確認

検討した対策が、予算その他の事情で講じられない場合は、残存リスクとして記載します。
残存リスクと認識する前に、「3801是正・予防措置報告書」によって対策を立案する場合もあります。

6.2.3　「リスク分析表」の提出と承認

各部門長は、「3313 リスク分析表」について、個人情報保護管理者の確認・承認を得ます。個人情報保護管理者は、部門で認識されたリスクが、全社で共通して発生すると判断した場合は、組織全体で講じるべき対策を検討します。

6.3　リスク対策を規定する

講じるとしたリスク対策が規定されていない場合は、以下の手順で規定します。

a) 部門長は「3801 是正・予防措置報告書」によって、対策の立案とともに規定するよう立案する。
b) 個人情報保護管理者は、具体的な規程の条文を立案し、「3801 是正・予防措置報告書」に添付して代表者もしくは役員会の承認を得る。
c) 個人情報保護管理者は、改定した規程について従業者に通知し、常時閲覧可能とする。

6.4　リスク分析の見直し

個人情報保護管理者は、毎年 PMS 運用年度のはじめに策定した「3303PMS 年間計画書」に従い、「3313 リスク分析表」見直しを実施するよう、部門長に通達します。また、少なくとも以下の事象が発生した場合には、都度見直しを実施します。

1	「3311 業務フロー」および「3312 個人情報管理台帳」を変更したとき
2	業務に関連する法令・規範等の改定があったとき
3	組織変更等により、業務の流れが変わったとき
4	事業所の移転・模様替え等で、安全管理上の変更が発生したとき
5	情報システムの導入・変更など、セキュリティ環境が変わったとき
6	緊急事態発生後、是正・予防処置を講じるとき

※「3313 リスク分析表」の提出は、メール添付ファイルによる提出、共有ファイルサーバー上の「提出用フォルダー」への保存など、電子ファイルで提出することが一般的です。
　個人情報保護管理者は、保管フォルダーを年度ごとに分けて、「3313 リスク分析表」の履歴を残します。プライバシーマークの更新審査は２年ごとで、定期的な見直しが、計画に従って２回以上行われていることについて審査されます。

■

次回は、「第７章　緊急事態への準備」をご紹介します。＞目次へ

個人情報保護監査研究会　http://www.saaj.or.jp/shibu/kojin.html