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７章

個人情報保護監査研究会

第７章　緊急事態への準備

緊急事態は、“起きるもの” として準備する必要があります。
そのため、緊急事態の認識の発生を監視し、検知し、緊急対応し、復旧するための手順を確立しなければなりません。個人情報の漏えい、滅失、き損もしくは法令違反に気付いた者が、速やかに責任ある者まで連絡できるよう手順を定め、いつでも参照できるようにしておきます。

7.1　緊急事態の定義

緊急事態が発生したときは、経済的な不利益、社会的な信用の失墜、本人への影響などを考慮し、その影響を最小限とするため、緊急事態を以下の３つのレベルに区分けて定義します。
また、委託先で発生した事故・事件についても、自社に責任がありますので同様に取り扱います。

レベル	影響度　(事例)	影響	責任者
A (高)	１個人情報が社外へ流出（紙、電子データ） ２個人情報をき損・滅失しサービス不能状態が継続 ３影響範囲が特定できず被害が拡大する恐れ	多数の顧客	代表者
B (中)	１個人情報が社外へ流出（回収可能） ２個人情報をき損滅失してサービス不能状態（短時間） ３影響範囲が特定でき被害が拡大の恐れがない	特定の顧客	代表者
C (低)	上記に相当する事態が発生したが、事前に検知した。 その結果、外部顧客、取引先に影響ないと判明した。	被害なし	個人情報保護管理者

7.2　緊急事態の体制

代表者は、緊急事態発生時に指揮をとり早期解決を図ります。各部門長、連絡先（内線番号、携帯電話番号）、連絡ルートなどを「3371 緊急時連絡網」に定めておきます。

7.3　緊急事態発生時の措置

緊急事態発生の連絡を受けた代表者は、「緊急対策会議」を招集し、以下の措置を決定します。

1	本人への連絡（必須）	当該漏えい、滅失又はき損が発生した個人情報の内容を本人に速やかに通知し、又は本人が容易に知り得る状態におく
2	関係機関（必須）	関係省庁、個人情報保護団体、JIPDEC など
3	警察	サイバーテロ等の恐れがある場合
4	社内通知（必須） 公表（自社ＨＰ公表、 マスコミ発表）	二次被害の防止、類似事案の発生回避などの観点から、可能な限り事実関係、発生原因及び対応策を遅滞なく公表する。

7.4　再発防止措置

緊急事態が収まりまたは最悪の状態から脱した時期に、類似案件が再発しないよう、「是正・予防処置報告書」によって再発防止策を策定し、実施します。再発防止策は、緊急事態発生部門だけでなく、同様の事態が発生する可能性のある部門に対しても教育し、実施します。

7.5　関係機関への事故報告

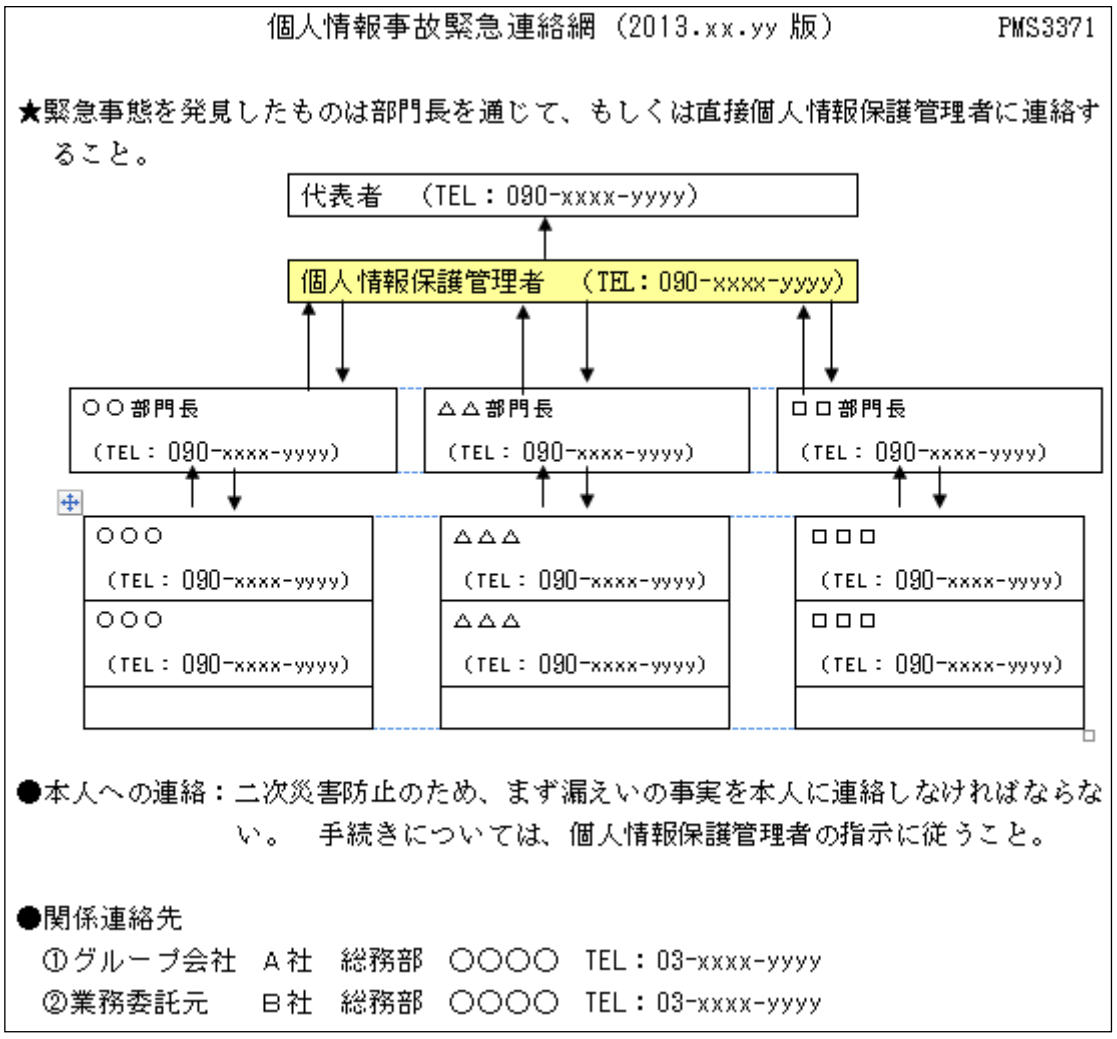
個人情報保護管理者はレベルA、B、Cを問わず、すべての緊急事態発生について、「3373 事故報告書」を作成し、社長の承認を得て審査機関（一般財団法人 日本情報経済社会推進協会（JIPDEC）プライバシーマーク事務局など）に報告します。

※　プライバシーマークを取得していない事業者は、監督官庁に報告します。

7.6　緊急事態への準備・対応に関するマネジメントレビュー

個人情報保護管理者は、１年間に発生した緊急事態の発生の内容と対応結果、サイバーテロなどの外部環境の変化、技術の進歩などを踏まえ、緊急事態への準備・対応に関する手順について有効性を評価し、マネジメントレビューのインプットとして報告します。

ご参考：「緊急時連絡網」の事例



■

次回は、「第８章　個人情報の取得、利用および提供に関する原則」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　　以上