2013.04

「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　　序章

個人情報保護監査研究会

個人情報保護監査研究会では、中堅企業がプライバシーマークを取得する際に必要な基本知識をわかりやすく解説するため「個人情報保護マネジメントシステム実施ハンドブック」を策定しています。
2013年５月号の会報から、その内容の一部を抜粋し、連載でご紹介していきます。

序章　はじめに

１．個人情報保護の歴史

1980年９月23日にOECD理事会勧告が採択された後、1989年経済産業省「個人情報保護ガイドライン、1998年4月「プライバシーマーク」制度発足、2003年5月30日「個人情報の保護に関する法律 」の一部施行を経て、2005年4月1日「個人情報の保護に関する法律」が全面施行となりました。

２．個人情報保護マネジメントシステム（PMS)とは

事業者が自社の事業のために利用する個人情報の取扱について、PDCAサイクルを実行する仕組みです。

３．JIS Q15001：2006　個人情報保護にマネジメントシステム－要求事項

JISQ15001:2006規格は、プライバシーマークの認証基準です。　**１適用範囲**　から、**3.9事業者の代表者による見直し**　まで、事業者がしなければならないPMS(＝PDCA）が規定されています。

4．最近の情報漏えい事故

NPO日本ネットワークセキュリティ協会（JNSA）が、2011年1月1日から12月31日の間に、新聞やインターネットニュースなどで報道されたインシデントについて　「2011年 情報セキュリティインシデントに関する調査報告書」（2012/12/7版）を公表しています。

	2010 年度	2011 年度
漏えい数	557 万 9316 人	628 万 4363 人
インシデント件数	1679 件	1551 件
想定損害賠償総額	1215 億 7600 万円	1899 億 7379 万円
一件当たりの平均漏えい人数	3468 人	4238 人
一件当たり平均損害賠償額	7556 万円	1 億 2810 万円
一人当たり平均損害賠償額	4 万 3306 円	4 万 8533 円

情報漏えいインシデントを起こした組織が、積極的にインシデントを公表する姿勢が定着し、緊急事態発生時の社内ルール（対応手順）の明確化および社内周知の重要性が認識されてきています。

5. 用語の定義

個人情報保護法など法令・規範と、プライバシーマーク認証基準（JIS）の比較を説明しています。今回は紙面の都合で、経済産業省ガイドラインとの比較は省略しています。

JIS		引用：JIS Q 15001:2006（骨子）	条	法令・規範等
2.1	個人情報	JIS：“生存する”の定義はなく、死者の情報も含まれる。 また、“保有期間”、” 件数” の定義は無く、一瞬、1 件でも個人情報として取り扱う。 上記の他は、法律と同じ	2条	生存する、個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。 政令：過去６カ月以内のいずれの日においても５０００件を超えないものは除外
2.3	事業者	事業を営む法人その他団体又は個人。 JIS：単に事業者と呼ぶ	2条3	「個人情報取扱事業者」 個人情報データベース等を事業の用に供している者をいう。
2.6	本人の同意	JIS：本人が個人情報の取扱いに関する情報を与えられた上で，承諾する意思表示が必要。 法律では単に同意を得るとし、手段まで言及していない。	16条	あらかじめ本人の同意を得ないで、前条の規定により特定された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。
3.2	個人情報保護方針	事業者の代表者が，個人情報保護の理念を明確にし、規格が要求する６項目を含めて公表する文書。	基本方針	基本方針 6：事業者が行う措置の対外的明確化
3.3.1	特定	法：利用目的の特定 JIS：個人情報の特定 自らの事業の用に供するすべての個人情報を漏れなく特定すること。	15条	利用目的をできる限り特定しなければならない
3.3.3	リスク等の認識	漏えい，滅失又はき損については、法律と同じ概念。 JIS：法令等に対する違反，経済的不利益、社会的信用失墜，本人への影響を考慮する。	20条	漏えい、滅失又はき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。
3.4.2.1	利用目的の特定	法とほぼ同じ概念 取得する個人情報の利用目的をできる限り特定し、利用目的の達成範囲内で取り扱わなければならない。	16条1	あらかじめ本人の同意を得ないで、前条の規定により特定された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。
3.4.2.2	適正な取得	法とほぼ同じ概念 適法、かつ、公正な手段によって個人情報を取得しなければならない。	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。
3.4.2.4	明示	法とほぼ同じ概念 本人から，書面に記載された個人情報を直接に取得する場合には，少なくとも規格が定める事項を，あらかじめ書面によって本人に明示しなければならない。	18条2	契約書その他の書面に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。
3.4.2.5	公表	法とほぼ同じ概念 個人情報を直接書面以外（3.4.2.4 以外）の方法によって取得した場合に，広く一般に自己の意思を知らせること。	18条	個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。
3.4.2.6	目的外利用	取得時に特定した利用目的の達成に必要な範囲を超えて個人情報を利用すること。書面によって本人に通知し、本人の同意を得る必要がある。 JIS：書面で通知し同意を得なければならない。	18条3	利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。
3.4.2.8	提供	法と同じ概念 個人情報を、委託、第三者提供、共同利用、合	23条	あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

		併に伴う提供を行う場合は、本人の同意が必要。		
—	オプトアウト	JIS：法ではオプトアウトでも可。 JIS では不適合となる	23条	あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。
3.4.3.1	正確性の確保	法と同じ概念 利用目的の達成に必要な範囲内において、個人情報を、正確、かつ、最新の状態で管理すること。	19条	利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない。
3.4.3.2	安全管理措置	法と同じ概念 取扱う個人情報のリスクに応じて、漏えい、滅失又はき損の防止その他の安全管理のために必要かつ適切な措置を講じること。	20条	取り扱う個人データの漏えい、滅失又はき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。
3.4.3.3	従業者の監督	法と同じ概念 従業者に個人情報を取扱わせるに当たって、安全管理が図られるよう、監督すること。	21条	従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。
3.4.3.4	委託先の監督	個人情報を委託する場合に，十分な個人情報の保護水準を満たしている者を選定し、監督すること。 JIS：選定しなければならない。 法では監督のみ	22条	個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。
3.4.4	本人の権利	本人から求められる開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止の求めのすべてに応じることができる権限を有するものに関して，本人から利用目的の通知，開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止を求められた場合は，遅滞なくこれに応じなければならない。 JIS：法のような理念までは規定していない。	3条	個人情報は、個人の人格尊重の理念の下に慎重に取り扱わなければならない。
3.4.4.1	開示対象個人情報	法とほぼ同じ概念 事業者が，本人から求められる開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止の求めのすべてに応じることができる権限を有するもの。 JIS：消去までの期間を問わない。	2条5	「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データをいう。 政令：６か月以内に消去するものは除外する。
3.4.4.2	開示等の求め	法とほぼ同じ概念 本人から、当該本人が識別される個人情報について、利用目的の通知，開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止を求めること。	24～27条	第 25 条：開示 第 26 条：訂正等 第 27 条：利用停止等 第 28 条：理由の説明 第 29 条：求めに応じる手続
3.4.4.3	周知	法とほぼ同じ概念 開示等の求める場合に提出する様式、手数料の支払い方法など、手順を公表すること。	24条	保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。
3.6	苦情	苦情は、責任ある者まで報告が上がる仕組みが必要である。 JIS：責任ある者とは代表者もしくはその代理の者をいう。	31条	個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。 ２～前項の目的を達成するために必要な体制の整備に努めなければならない。

■

次回は、「第１章　プライバシーマーク認証取得計画」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