法務研究科・講義用レジュメ　　2005年7月13日

法 情 報 学（第１３回）

弁護士　川　添　　圭
kawazoe@kondolaw.jp

Ⅰ　個人情報保護法を前提とした個人情報の管理

１　企業における個人情報管理の必須事項

① 情報管理責任者の設置と台帳による管理〔組織的情報管理措置〕
② 個人情報管理ポリシーの策定と管理規程の整備〔組織的情報管理措置〕
③ 従業員に対する教育・研修の実施〔人的安全管理措置〕
④ 重要な個人情報の集中化・物理的隔離〔物理的管理措置〕
⑤ アクセス権限の設定とアクセスログの保存〔技術的管理措置〕
⑥ 漏洩事件発生時の対応策の整備〔組織的安全管理措置〕
⑦ 利用目的の表示と開示等の請求に対する手続の定め

２　個人情報保護法と企業活動

（１）個人情報保護法と企業活動への影響

① 個人情報の収集・管理・提供に関する各種義務の実践
- 利用目的に応じた個人情報データベースの区分
- 個人情報データベースのチェック
- 外部への委託契約等のチェック
- 漏洩防止の規則制定と懲罰の明確化

② 開示手続とそれに対する対応
- 開示請求の定型化の必要性
- 本人の情報が発見された場合
  →開示等に応じるか，消去するかの選択

（２）個人情報保護法の活用

① 個人情報保護法の再評価
＝企業に対する規制と捉えるのではなく，リスクマネジメントの実践規範として積極的に活用するべき

② 個人情報保護法の実践が企業にもたらすプラス効果

・リスクマネジメントの骨格に関する理解

・対外的なアピール効果

・ISMS評価認証，プライバシーマークの取得＝企業イメージの向上

・情報漏洩事案発生時の対応が企業に対する評価を左右する場面

・ISMS認証やプライバシーマークの取得が民間，公共機関からの受注の必須条件となる事例が増えている

Ⅱ　情報管理に関する国内標準規格

1　ISMS（JIS X 5080）と個人情報コンプライアンス・プログラム（JIS Q 15001）

（1）JIS規格

法的根拠＝工業標準化法（昭24法185，ＪＩＳ法）

第2条　この法律において「工業標準化」とは，左に掲げる事項を全国的に統一し，又は単純化することをいい，「工業標準」とは，工業標準化のための基準をいう。

一　鉱工業品（医薬品，農薬，化学肥料，蚕糸及び農林物資の規格化及び品質表示の適正化に関する法律（昭和二十五年法律第175号）による農林物資を除く。以下同じ。）の種類，型式，形状，寸法，構造，装備，品質，等級，成分，性能，耐久度又は安全度

二　鉱工業品の生産方法，設計方法，製図方法，使用方法若しくは原単位又は鉱工業品の生産に関する作業方法若しくは安全条件

三　鉱工業品の包装の種類，型式，形状，寸法，構造，性能若しくは等級又は包装方法

四　鉱工業品に関する試験，分析，鑑定，検査，検定又は測定の方法

五　鉱工業の技術に関する用語，略語，記号，符号，標準数又は単位

六　建築物その他の構築物の設計，施行方法又は安全条件

（2）JIS X 5080（情報セキュリティマネジメントの実践のための規範）

＜構成＞

10. 1. 1　セキュリティ要求事項の分析及び明示
10. 2　業務用システムのセキュリティ
10. 2. 1　入力データの妥当性確認
10. 2. 2　内部処理の管理
10. 2. 2. 1　リスクにかかわる範囲
10. 2. 2. 2　検査及び管理策
10. 2. 3　メッセージ認証
10. 2. 4　出力データの妥当性確認
10. 3　暗号による管理策
10. 3. 1　暗号による管理策の使用に関する個別方針
10. 3. 2　暗号化
10. 3. 3　ディジタル署名
10. 3. 4　否認防止サービス
10. 3. 5　かぎ管理
10. 3. 5. 1　暗号かぎの保護
10. 3. 5. 2　標準類，手順及び方法
10. 4　システムファイルのセキュリティ
10. 4. 1　運用ソフトウェアの管理
10. 4. 2　システム試験データの保護
10. 4. 3　プログラムソースライブラリへのアクセス制御
10. 5　開発及び支援過程におけるセキュリティ
10. 5. 1　変更管理手順
10. 5. 2　オペレーティングシステムの変更の技術的レビュー
10. 5. 3　パッケージソフトウェアの変更に対する制限
10. 5. 4　隠れチャネル及びトロイの木馬
10. 5. 5　外部委託によるソフトウェア開発
11. 事業継続管理
11. 1　事業継続管理の種々の面
11. 1. 1　事業継続管理手続
11. 1. 2　事業継続及び影響分析
11. 1. 3　継続計画の作成及び実施
11. 1. 4　事業継続計画作成のための枠組み
11. 1. 5　事業継続計画の試験，維持及び再評価
11. 1. 5. 1　計画の試験
11. 1. 5. 2　計画の維持及び再評価
12. 適合性
12. 1　法的要求事項への適合
12. 1. 1　適用法令の識別
12. 1. 2　知的所有権（IPR）
12. 1. 2. 1　著作権
12. 1. 2. 2　ソフトウェアの著作権
12. 1. 3　組織の記録の保護
12. 1. 4　データの保護及び個人情報の保護
12. 1. 5　情報処理施設の誤用の防止
12. 1. 6　暗号による管理策の規制
12. 1. 7　証拠の収集
12. 1. 7. 1　証拠に関する規則
12. 1. 7. 2　証拠の容認性
12. 1. 7. 3　証拠の質及び完全性
12. 2　セキュリティ基本方針及び技術適合のレビュー
12. 2. 1　セキュリティ基本方針との適合
12. 2. 2　技術適合の検査
12. 3　システム監査の考慮事項
12. 3. 1　システム監査管理策
12. 3. 2　システム監査ツールの保護

（3）JIS Q 15001(個人情報保護に関するコンプライアンス・プログラムの要求事項)

＜構成＞

0. 序文
1. 適用範囲
2. 引用規格
3. 定義
4. コンプライアンス．プログラム要求事項
4．1　一般要求事項
4．2　個人情報保護方針
4．3　計画
4．3．1　個人情報の特定
4．3．2　法令及びその他の規範
4．3．3　内部規程
4．4　実施及び運用
4．4．1　体制及び責任
4．4．2　個人情報の収集に関する措置
4．4．2．1　収集の原則
4．4．2．2　収集方法の制限
4．4．2．3　特定の機微な個人情報の収集の禁止
4．4．2．4　情報主体から直接収集する場合の措置
4．4．2．5　情報主体以外から間接的に収集する場合の措置
4．4．3　個人情報の利用及び提供に関する措置
4．4．3．1　利用及び提供の原則
4．4．3．2　収集目的の範囲外の利用及び提供の場合の措置
4．4．4　個人情報の適正管理義務
4．4．4．1　個人情報の正確性の確保
4．4．4．2　個人情報の利用の安全性の確保
4．4．4．3　個人情報の委託処理に関する措置
4．4．5　個人情報に関する情報主体の権利
4．4．5．1　個人情報に関する権利
4．4．5．2　個人情報の利用又は提供の拒否権
4．4．6　教育
4．4．7　苦情及び相談
4．4．8　コンプライアンス．プログラム文書
4．4．9　文書管理
4．5　監査
4．6　事業者の代表者による見直し

（4）ISMS適合性評価制度とプライバシーマーク制度

① 両者の比較

	ISMS適合性評価制度	プライバシーマーク制度
根拠となる規格	JIS X 5080 ISO/IEC 17799(BS7799-1) BS7799-2	JIS Q 15001
位置づけ	企業存続のための適正な資産管理 （リスクマネジメント）	個人の権利利益の保護 （コンプライアンス）
適合性	B2B主体の企業向け(企業間での委託,請負等)	B2C主体の企業向け(小売業等)
対象	全ての情報が対象	個人情報のみを対象
取得単位	事業所(工場)単位，支店単位での取得も可能	１社（全事業所）単位のみ （例外的に部門単位）
取得後の審査	定期審査：１年ごと 更新審査：３年ごと	２年ごとに更新

② 基本的な考え方＝PDCAアプローチ