法務研究科・講義用レジュメ　　2005年6月15日

法 情 報 学（第９回）

弁護士　川　添　　圭
kawazoe@kondolaw.jp

Ⅰ　情報セキュリティの概念

１　情報セキュリティ確保の必要性

（１）なぜ「情報セキュリティ」が必要なのか

① アナログ技術からデジタル技術中心の社会へ

↓

・コンピュータの普及と低価格化

・インターネットの普及と低価格化

↓

情報・コンテンツのデジタル化

② デジタル化によるメリット

・大量の情報を一括で保存可能（省スペース性）

・再利用，検索が容易（可用性）

・持ち運びが容易（可搬性）

・コピーしても質が劣化しない（高品位）

③ デジタル化によって生じる問題（課題）

・消失の危険の増大（火災等の災害，誤消去，PCのトラブルによる消失）

・著作権侵害の増大（海賊版，カジュアルコピー）

・インターネットを経由した脅威の増大（ウイルス・セキュリティホール）

・オリジナルとコピーとの区別＝オリジナルが持つアイデンティティーの喪失

（２）近年の情報流出の実情

→『2004年度　個人情報漏洩インシデント調査結果＜速報＞）』

（NPO日本ネットワークセキュリティ協会編）

http://www.jnsa.org/active2005_1_1.html

① 漏洩数

調査対象事業者数	366件
合計被害者数	10,435,061人

② 情報種別毎の流出件数

流出した情報	件 数	割 合
氏名	321	89.20%
住所	245	68.10%
生年月日	78	21.70%
性別	47	13.10%
電話番号	141	39.20%
職業	32	8.90%
Emailアドレス	42	11.70%

③ 情報流出の原因

要 因		内 容	割合
技術的要因	人為ミス	設定ミス	2%
		誤操作	11%
		管理ミス	10%
	対策不足	ワーム・ウイルス	1%
		バグ・セキュリティホール	1%
		不正アクセス	2%
非技術的要因	人為ミス	紛失・置き忘れ	21%
		目的外使用	3%
	犯罪	内部犯罪・内部不正行為	10%
		不正な情報持ち出し	3%
		盗難	35%
その他・不明			3%

④ 情報流出の経路

経 路	割 合
Email経由	7%
Web経由	7%
FTP経由	0%
紙媒体経由	46%
FD等可搬記録媒体経由	9%
PC本体	20%
その他	7%
不明	4%

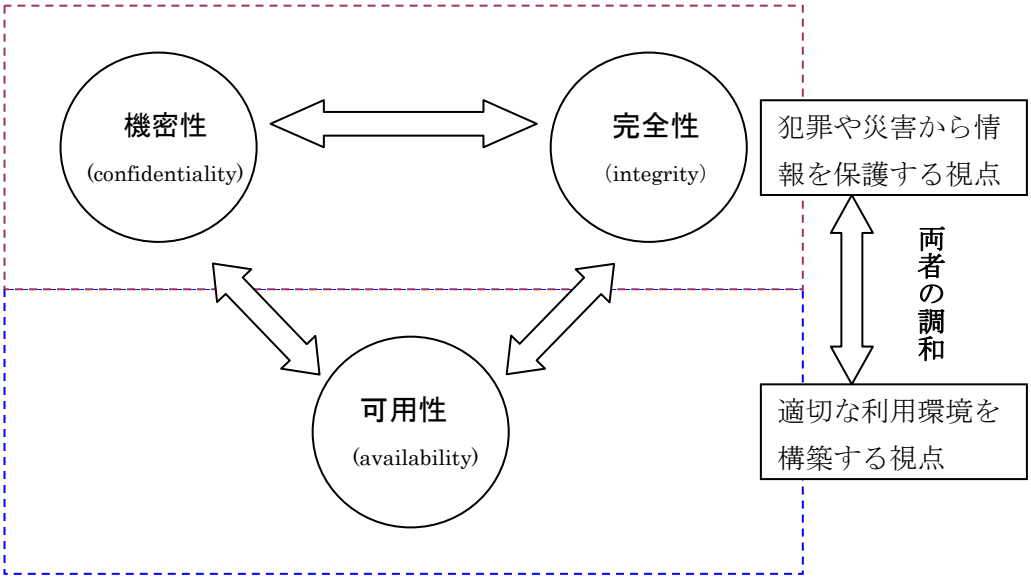
２　「情報セキュリティ」の本質

（１）情報セキュリティとは＝情報の機密性・完全性・可用性を確保し，維持すること

① 機密性：アクセス権限のある者以外からのアクセスを阻止すること

② 完全性：許可されていない者からの改竄・破壊を阻止すること

③ 可用性：許可されている者が情報に対しアクセス可能な状態に置くこと



（２）OECDセキュリティガイドライン（2002年）

① 認識原則（Awareness）

利用者が情報セキュリティの必要性と重要性を認識すべきである。

② 責任原則（Responsibility）

すべての参加者が情報システム及びネットワークのセキュリティに責任を負う。

③ 応答原則（Response）

セキュリティ事故の予防・検出・対応のため時宜を得た協力的方法で行動すべき。

④ 倫理原則（Ethics）

他者の正当な利益を尊重すべきである。

⑤ 民主主義原則（Democracy）

セキュリティの確保は民主主義社会の本質的価値に適合すべきである

⑥ リスクアセスメント原則（Risk assessment）

参加者は情報に対するリスク評価を行うべきである。

⑦ セキュリティ設計及び実施原則（Security design and implementation）

情報セキュリティを情報システムの本質的要素として組み込むべきである。

⑧ セキュリティマネジメント原則（Security management）

セキュリティ確保のために情報セキュリティマネジメントを実施すべきである。

⑨ 再評価原則（Reassessment）

継続的にセキュリティの再評価を行い，適切な修正を行うべきである。

（３）OECD・プライバシー保護と個人データ流通に関する８原則（1980年）

① 収集制限の原則　：個人データは適法・公正な手段によりかつ情報主体に通知または同意を得て収集されるべきである。

② データ内容の原則：収集するデータは利用目的に沿ったものでかつ正確・完全・最新であるべきである。

③ 目的明確化の原則：収集目的を明確にし，データ利用は収集目的に合致するべきである。

④ 利用制限の原則　：データ主体の同意がある場合や法律の規定による場合を除き，収集したデータを目的以外に利用してはならない。

⑤ 安全保護の原則　：合理的安全保護措置により，紛失・破壊・使用・修正・開示等から保護すべきである。

⑥ 公開の原則　　：データ収集の実施方針等を公開し，データの存在・利用目的・管理者等を明示するべきである。

⑦ 個人参加の原則　：データ主体に対して自己に関するデータの所在及び内容を確認させ，または異議申立を保証するべきである。

⑧ 責任の原則　　：データの管理者は諸原則実施の責任を有する。

（４）情報セキュリティを確保するための重要な視点

① マネジメント志向の重要性

② 情報の内容に応じた適切な予防策

③ 漏洩防止と漏洩発覚後の対応

３　国際基準としての情報セキュリティマネジメントシステム（ISMS）

（１）世界の３大マネジメントシステム規格

① ISO 9000シリーズ（品質マネジメントシステム：QMS）

② ISO 14000シリーズ（環境マネジメントシステム：EMS）

③ **ISO/IEC 17799（情報セキュリティマネジメントシステム：ISMS）**

（２）ISO/IEC 17799：2000

・英国規格協会（BSI）の規格（BS 7799）を基本

・1998年改訂（BS 7799：1998）以後2部構成

Part1(BS7799-1)：情報セキュリティマネジメント実践のための規範

Part2(BS7799-2)：情報セキュリティマネジメントの仕様

（３）JIS X5080：2002

・2002年策定，ISO/IEC 17799の和訳

・ISMS評価認証制度の導入＝現在の評価基準(Ver.2)はBS7799-2：2002を踏襲

Ⅱ　情報セキュリティ確保のための法制度

1　営業秘密の保護

① 不正競争防止法２Ⅳ

「秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの」

② 知的財産基本法２Ⅰ

「この法律で「知的財産」とは、発明、考案、植物の新品種、意匠、著作物その他の人間の創造的活動により生み出されるもの（発見又は解明がされた自然の法則又は現象であって、産業上の利用可能性があるものを含む。）、商標、商号その他事業活動に用いられる商品又は役務を表示するもの及び営業秘密その他の事業活動に有用な技術上又は営業上の情報をいう。」

2　個人情報の保護

＜個人情報保護法制＞

① 個人情報保護法（平15法57）

・平成15年5月施行，平成17年4月全面施行

・第1章～第3章（1条～14条）までは規範的・努力規定として個人・団体に適用

・第4章（15条～49条）は個人情報取扱事業者に適用

② 行政機関個人情報保護法（平15法58）

・平成17年4月施行

・適用団体は「行政機関」（２Ⅰ）

③ 独立行政法人等個人情報保護法（平15法59）

・平成17年4月施行

・適用団体は「独立行政法人」

④ 個人情報保護条例

・各地方公共団体が条例で定めるもの

・条例制定状況（http://www.soumu.go.jp/s-news/2005/050422_1.html）

→全2418団体中2368団体が制定済み（97.9%）

情報セキュリティポリシー策定済みの団体は2236団体

3　その他