PCネットワークの管理・活用を考える会2004 in 大阪

ＥＣ時代の法とセキュリティ

― 電子商取引と個人情報保護を中心に ―

平成16年7月16日

大阪市立大学大学院創造都市研究科

松田　貴典

（創造都市研究科「情報法共同研究」グループ指導教官）

EC時代のセキュリティの動向への影響

ーグローバルネットワークの進化よる新たな脆弱性への対応ー

- パーソナル／ユビキタスに伴う『脆弱性』の進化と拡大
- コンピュータ事故・ハイテク犯罪の複雑化・知能化・緻密化
- 知的財産権関連の法的問題事件・事故の増加
- 情報化による『コンプライアンス問題』が重要課題
- コーポレート・ガバナンスへの対応

ＩＣＴの進展による情報システムの脆弱性の増大化

セキュリティ対策の高度化と変化

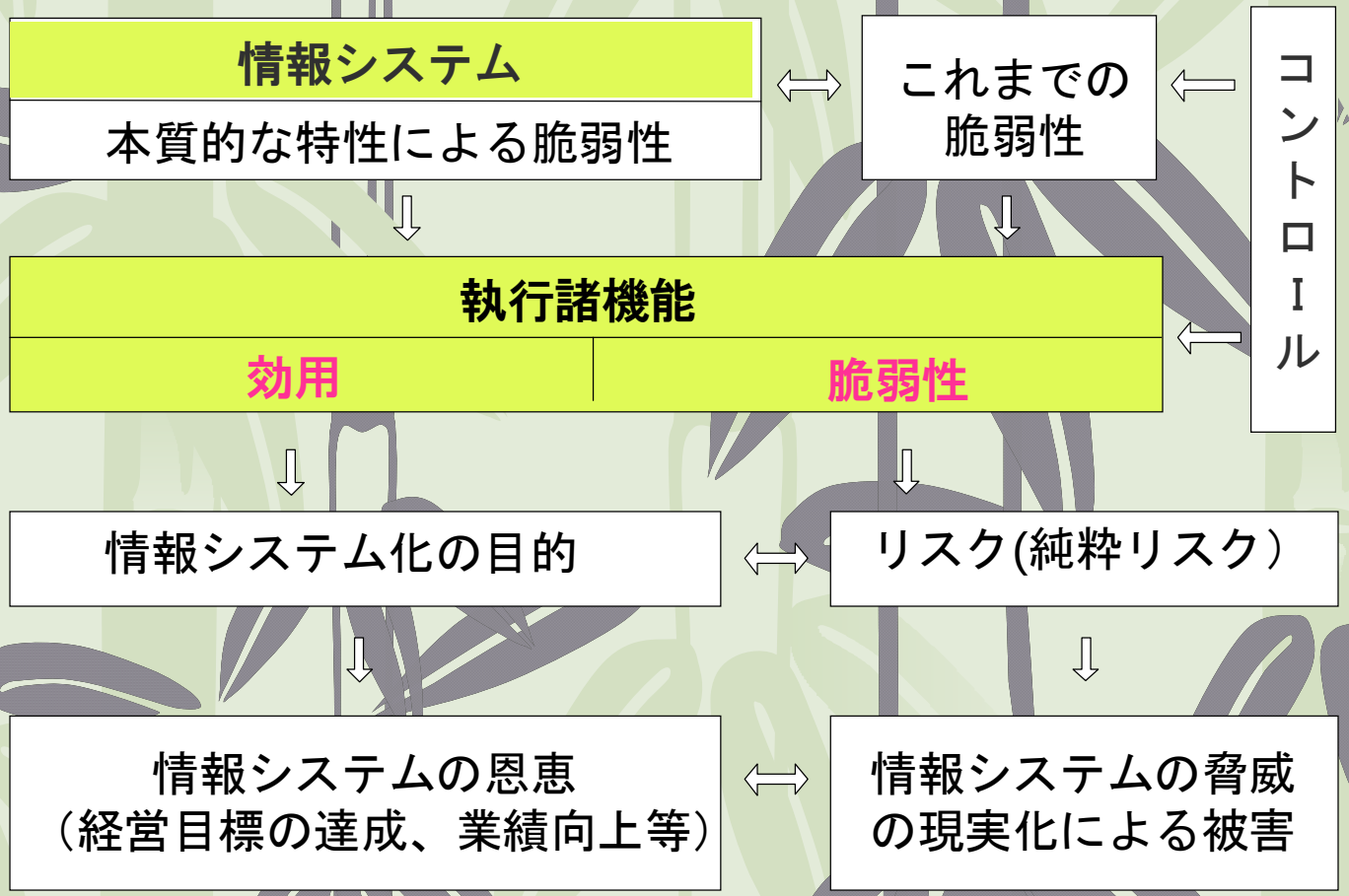
- 社会公共システムの普及
- セキュリティ確保を目的に監査
- 『法的セキュリティ』対策
- コンピュータ事故・ハイテク犯罪に対する『社会的責任（ＣＳＲ）』

監査の視点の高度化と変化

- 安全性・信頼性・効率性に有効性・有用性・遵法性の視点
- 『個人情報の保護』の視点
- 『情報資産の保護』の視点
- 『危機管理』からの視点

情報システムの効用と脆弱性とリスク

（松田貴典著　「情報システムの脆弱性」白桃書房より）



図は青山監査法人システム監査部編　システム監査の方法の「問題の所在と対策概念図」を参考に改訂して作成

情報システムの脆弱性と定義

情報システムの**脆弱性**とは、

「情報資産や人員の管理方法に由来する弱点」(ISMS)

ISMS:Information Security Management System (JIPDEC)

「情報資産の中や周辺環境，管理体制，制度のなどに内在し，損失を発生しやすくさせたり，拡大化させる要因」

上原孝之著「ネットワーク危機管理入門」 翔泳社

「情報システムの構築に伴い不可避的に発生する欠陥」

脆弱性とコントロール（統制）

■企業や組織とは，その目的達成のために，様々な執行諸機能を合理的にまた有機的に結合されたものである

■情報システムに組み込まれた執行諸機能は、効果的に業務を執行する「効用」がある。反面，ITの本質的な特性に起因して，無知，無法，無規制，無対策等のコントロール（統制）欠如とマネジメント（管理）の失敗で「脆弱性」が発生する

■脆弱性は，脅威の現実化（顕在化）の誘因となり，被害の大きさに関連する

■脆弱性には，①情報技術（IT）的側面，②経営管理・組織的側面，③国際・社会的側面，④法・倫理的側面に関連して潜在化する

脆弱性と脅威とリスク

■脆弱性は，通常にコントロールされているが，このコントロールの強弱で脅威の現実化（顕在化）する「リスク」が発生し，高くも低くもなる

■脆弱性のコントロールが弱い間隙（例えば，ネットワークの弱い個所）をついて脅威が現実化し，「被害」が発生する

■「脅威」とは，コンピュータや情報通信システム等の目的達成を阻害したり，情報資産，個人，企業等に不利益や被害をもたらすあらゆる「事象」である

■客観的には，すべての事象は脅威となるが，ある特定の情報システムや情報資産にとって脅威とならないものがある

■リスクは脅威の現実化の可能性（確率概念）である

本日のお話

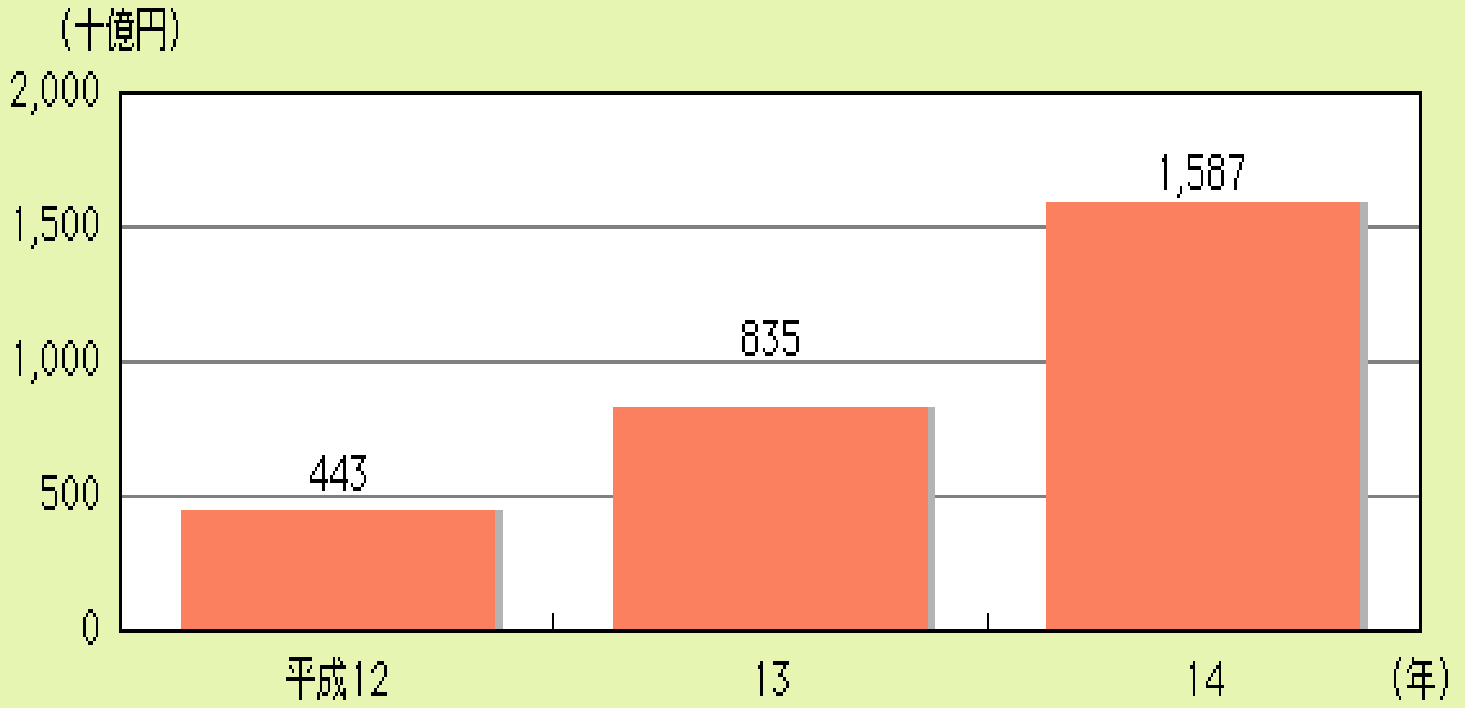
- ECビジネスの環境の推移
- 電子商取引での法的な問題
- 個人情報漏洩事件とその責任
- 個人情報保護法と保護ガイドライン
- 情報セキュリティ対策
- まとめ

ＥＣビジネス環境の推移

ECビジネス環境の推移(1)

■ 平成12−14年における電子商取引(BtoC)の市場

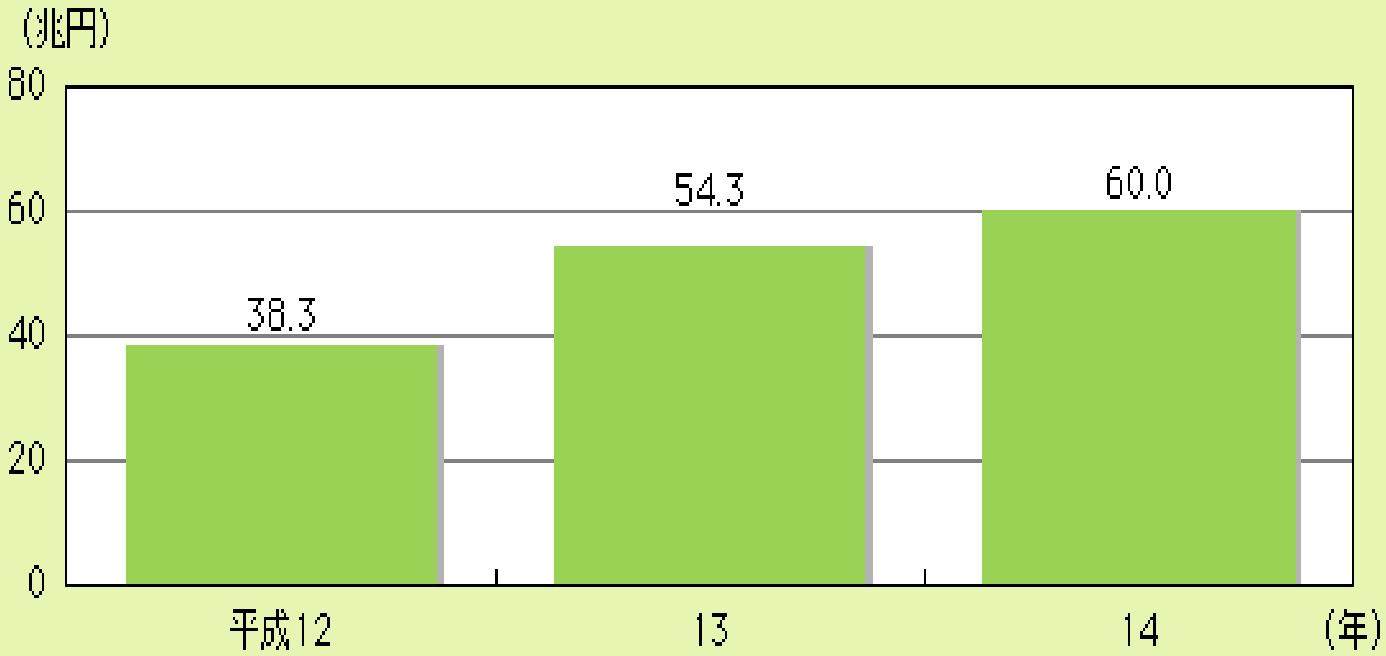
出典:平成15年度版　総務省編　「情報通信白書」 インターネットビジネスの動向



ECビジネス環境の推移(2)

■平成12－14年における電子商取引(BtoB)の市場

出典:平成15年度版　総務省編　「情報通信白書」 インターネットビジネスの動向

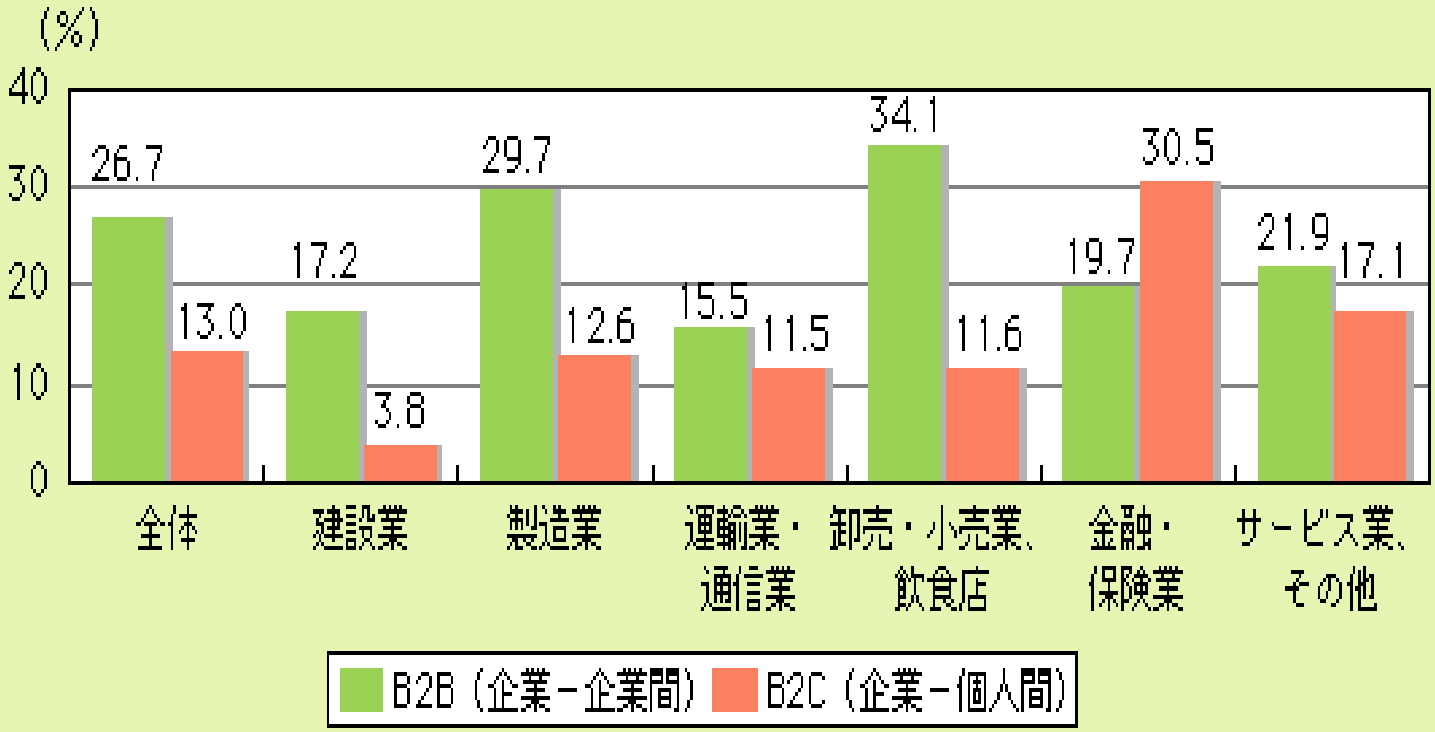


図表①、② (出典)「ITの経済分析に関する調査」

ECビジネス環境の推移(3)

■ 平成12－14年における産業別電子商取引の市場の推移

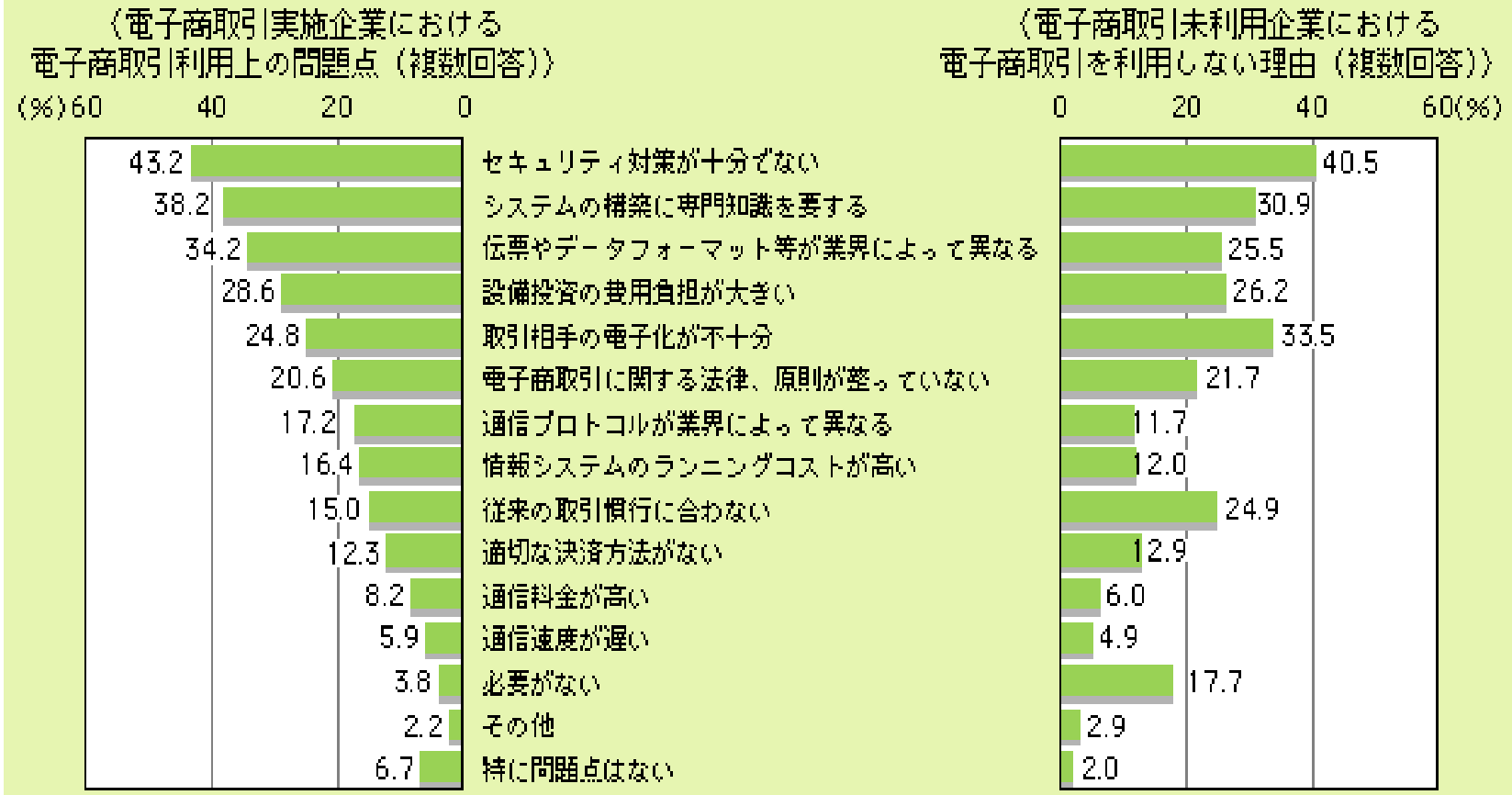
出典:平成15年度版　総務省編　「情報通信白書」 インターネットビジネスの動向



ECビジネス環境の推移(4)

■ 企業における実施上の問題点／実施しない理由

出典：平成15年度版　総務省編　「情報通信白書」 インターネットビジネスの動向



図表③、④　(出典)総務省「平成14年通信利用動向調査」

電子商取引での法的な問題

ー　サイバーショッピングでの事業者が遵守すべきの法律　ー

インターネットビジネスと法との問題

1. インターネットビジネスの法的セキュリティの確保
   ➡ 事業者にとってコンプライアン問題への対応
2. 業種別に法との関連を整理
3. 事例研究：流通業サイバーショッピング
   サイバーショッピング（BoC）でのサービス機能と法
   ① 有店舗と同じく安心して買い物ができること
   ② 注文の商品がすぐに入手できること
   ③ 色・サイズ・形・性能など思った商品が入ること
   また，間違いによる返品・交換等が可能であること
   ④ 取引の決済が正しくなされるシステムであること
4. 法的脆弱性と関連で評価することが必要

1. ビジネスレイヤー（層）とサービス機能との関連で法体系整理が必要
2. ビジネスプロセスに対応した法律（視点：事業者）

サイバーショッピングの機能からの主要な法律事例

機　能	内　　容	法律・制度等
①広告宣伝	適法ホームページの作成 商品の掲載（申込の誘因） 著作物の再利用 認証事業者へ鍵登録 取扱い商品選別等	特定商取引法／金融商品販売法 景品表示法／著作権法 電子署名・認証法 富くじ法，刑法（信用毀損，業務妨害）、食品衛生法，古物営業法等
②通信による契約	契約の成立 消費者の保護など	民法特例法／消費者契約法 電子署名・認証法他
③商品発送	コンテンツのダウンロード 音楽の配信等	著作権法 電気通信事業法他
④決済	電子決済，振込み， クレジット，代引き他	不正アクセス禁止法／刑法等 エスクロー制度他
⑤その他（情報管理等）	クレーム受付，個人情報とプイラバシー保護等	プロバイダー責任法等 個人情報保護法，刑法（名誉毀損）

ビジネスシーン	サイバーショッピングでの一般的問題例
Webでの広告宣伝	■雑誌などから綺麗な写真や図画を無断掲載する ■無作為に広告宣伝メールを送信する等
	■少し品質を誇張して宣伝する（誇大広告） ■販売できない商品の取り扱い（ポルノ，宝くじなど） ■中国産を偽って日本産として表示する等
消費者と電子契約（消費者のシーン）	■レスポンスが悪いので何度も送信ボタンを押した ■商品を購入するには，「はい」を押すこととした （インターネットので契約の成立問題） ■１個の注文したのに１０個が送られきた等
商品発送（消費者のシーン）	■発注した商品と内容が違う ■送金したのに商品が送られてこない
商品到着（事業者のシーン）	■商品を発送したのに入金されない ■１０個発送したのに，１個しかついていないと言われた
その他	■購入者の個人情報を複製し，たのビジネス事業者に販売した（個人情報の漏洩とプライバシーの侵害問題など）

サイバーショッピングの法律例（1）

①広告・宣伝（事業者から消費者）

■　特定商取引（旧訪問販売法）による規制

（平成13年6月1日に施行　改正法平成14年7月1日施行）

☞事業者の行為を規制する行政上のルール

☞インターネットビジネスは通信販売（法2条2項）

☞ソフトウェア，音楽，データ等のダウンロードは同法の適用外

☞ホームページ作成には同法の「未承認広告」の表示義務

☞遅滞無く書面で交付する旨記載の時一部表示の省力

☞連鎖販売取引に係る規制

誇大広告の禁止，規制逃れの防止等

☞業務提供誘販売取引（いわゆるモニター・内職商法の規制）

☞平成14年7月施行　改正特定商取引法

個人は300万円以下の罰金か2年以下の懲役，法人は3億円以下の罰金

特定商取引法による表示義務

特定商取引法第8条，施行規則第7条による表示義務の内容

① 商品の販売価格等（販売価格に商品の送料が含まれない場合には，販売価格及び商品の送料）

② 商品の代金等の支払時期及び支払方法

③ 商品引渡し時期等

④ 商品の引き渡し又は権利の移転後におけるその引取り又は返還（返品）についての特約に関する事項（その特約がない場合についてはその旨）

⑤ 販売業者等の氏名又は名称，住所及び電話番号

⑥ 販売業者が法人である場合，その代表者又は責任者の氏名

⑦ 申込の有効期限があるときには，その期限

⑧ 販売価格等以外に購入者等の負担すべき金銭があるときは，その内容及びその額

⑨ 商品に隠された瑕疵がある場合の販売業者の責任について定めがあるときは，その内容

⑩ 商品の販売数量の制限その他の特別の商品の販売条件等があるときは，その内容

サイバーショッピングの法律例(2)

①広告・宣伝(事業者から消費者)

■　景品表示法による規制

☞ホームページ作成に過大な景品つき販売や虚偽・過大表示の禁止

☞事業者の行為を規制する行政上のルール

☞優良誤認:中国製を秋田伝統工芸と表示

☞有利誤認:優待旅行でないのに優待旅行と表示

☞誤認されるおそれのある表示:無果汁清涼飲料水,原産国表示など)

■　食品衛生法による規制等

サイバービジネスと法律（3）

❒電子消費者契約民法特例法 （平成13年12月25日施行）

電子消費者契約及び電子承諾通知に関する民法特例に関する法律

■　電子商取引における消費者の操作ミスの救済

☞BtoCの電子契約では消費者の申込み確認措置が必要

☞民法95条「要素の錯誤」に該当。但書の「重大な過失があるときは無効の主張ができない」が原則適用されない

■電子商取引等における契約の成立時期の転換

☞承諾通知が申込者に到着した時点で成立（到達主義）

■留意事項

☞ CtoC（オークション），電子メール申込み等は適用外

サイバービジネスと法律（4）

□消費者契約法（事業者と消費者）

（平成13年4月1日施行）

☞消費者の取引（BtoC）の適正を図る民事上のルール

☞消費者と事業者（個人事業者含む）の情報量や交渉力格差の不利益をカバーする目的

☞民法の考え方：契約は対等な当事者間で締結される

☞契約の取消しや無効の主張：

詐欺，脅迫，公序良俗違反など消費者が立証を容易に

☞ホームページの広告は「勧誘」にあたらない？

根拠：不特定多数を相手にしているため

取消し権が行使できる5つのケース

① 不実の告知

例えば「いつでも解約できます」といいながら，契約書には1年間解約が出来ないなど

② 断定的判断の提供

例えば「1年後には必ず値上がりします」といって購入させるなど

③ 非利益事実の不告知

例えばビルが建つことをしりながら，「素晴らしい見晴らしの土地になります」といって購入させるなど

④ 不退去

例えば「お帰りください」といっても帰らないで執拗に売ろうとするような行為

⑤ 退去妨害

例えば「帰りたい」と意思表示しているにも関わらず監禁するなど

サイバービジネスと法律（5）

❒取引の正当性と電子署名・認証制度の法律（事業者と消費者）

❒商業登記法等の一部を改正する法律

- 平成12年4月19公布
- 平成12年10月10日より「商業登記に基礎を置く電子認証制度」の運用開始
- 印鑑証明書/資格証明書に代わる電子証明書の発行

❒電子署名及び認証業務に関する法律

- 平成12年5月31日に公布
- 平成13年4月1日より「電子署名認証法」施行
- 電磁的記録の真正な証明（民訴228条4項）
- 特定認証業務に関する認定制度

  主務大臣より認証機関としての認定を受ける

【参考】求められる消費者としての責任（消費者）

□安全なショッピングをするための自己責任

■誇大広告・宣伝にまどわされない
「すぐに登録を」「今がチャンス」

■派手なサイトのアクセスは避ける

■運営母体が良く知っている企業が安全

■保証や返品の説明が書かれているかチェックする
「何日まで返品可能」「送料の負担」など

■***JADMA***やプライバシーマークを確認

■後払い，代引き，銀行振込などの事後決済システム

■その他：法に定められて表示義務
販売価格,送料，支払方法，住所，氏名，電話など

□求められる消費者責任

インターネットビジネスと法律（6）

□プロバイダー責任法

■インターネットビジネス事業と法律

■　特定電気通信役務提供者の損害賠償責任の制限及び発信者情報開示に関する法律

公布日：平成13年11月30日

施行日：公布日から6ヶ月以内の政令で定める日

■背景

☞電子会議室，チャット等で名誉毀損，プライバシー侵害，著作権侵害等権利侵害（不法行為）の判断が困難

☞プラバイダ等の自主的対応を促すための環境整備が必要

損害賠償責任の制限と発信者情報開示等

■　プロバイダーの損害賠償責任の制限

☞被害者（とする者）に対する責任：削除をしなかった場合

①他人の権利侵害を知っていた時

②違法情報を知っており，知ることができた時

☞発信者に対する責任：削除した場合

①他人の権利侵害している時

②削除の申出があったことを伝え7日以内に反論がない時

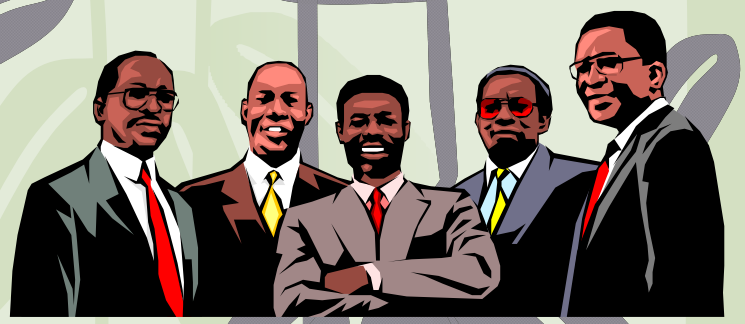
■　プロバイダーの発信者情報開示

☞開示の要件

①　請求者の権利侵害が明白

②　損害賠償請求権の行使のために必要である（裁判等）

個人情報の漏洩事件とその責任



企業等での個人情報の漏洩事件とその責任(1)

■平成１５年６月：ローソンからカード会員情報５６万人分が流出。全会員１１５万人に対して５００円の商品券と社長会からの謝罪文を配布

■平成１５年８月：信販会社アプラスからクレジット顧客情報７万９１１０人分がダイレクトメール会社に流出。対象者に１０００円の商品券とお詫び状を配布

■平成１５年１１月：ファミリーマートのメールマガジン購読者約１８万人の個人情報が流出，委託先企業からの漏洩か。一部がアダルトサイトの架空請求に使われた。

■平成１６年２月：ヤフーＢＢの加入者者情報約４７０万人分がＤＶＤに記録され流出，ソフトバンク関連企業に対して数十億円の恐喝。これまでの最大規模の個人情報流出事件。５００円の金券とお詫び状の配布

■平成１６年３月：通販会社ジャパネットたかたの顧客データ約１４９万人分が流出，内容に住所，氏名，生年月日，電話番号がはいっていた。再発防止対策を最優先のためビジネス業務の中断

■平成１６年３月：ＡＤＳＬ事業者のアッカ・ネットワークスの顧客名簿の２０１人分が流出

自治体での個人情報の漏洩とその責任(2)

❒ 1999.5　U市　住民基本台帳　**約22万件のデータ流出**、売買事件

① 行政　：　一時ストップ・停滞、回復費・損害賠償費用等々

② 市民　：　不安・不快感

③ **3市民が市と業者に損害賠償請求**

■　市→ 4万5千円(3人×1万5千円)の支払を命ずる判決

・1人当たり1万円5千円の内訳:

(慰謝料1万円、弁護士費用5千円)

■　業者(システム開発会社) → 市と同じ判決。

・1人当たり1万円5千円の内訳:

(慰謝料1万円、弁護士費用5千円)

④ **集団訴訟のリスク(最悪のシナリオ)**

■　市→33億円(22万人×1万5千円)

■　事件を起こした業者→市に同じく:33億円(22万人×1万5千円)

■　元請業者→市に同じく:33億円(22万人×1万5千円)

以上を合計すると**総額99億円の訴訟**

個人情報保護対策の実際

出典：日経新聞平成16年6月16日ほか他紙を参考に作成

サントリー	グループ横断の個人情報保護委員会の設置。情報処理委託先社員との守秘義務契約を毎年更新	業務他委託先との管理の強化
NTT	グループ430社に「個人情報管理をトップ自ら取り組むべきである」通達	指示管理の徹底通達
ソフトバンクBB	顧客データベースのアクセス権限を170人から3人に限定。第3者（弁護士等）の助言を受けるべく「個人情報管理諮問委員会」の設置	アクセス権限の限定，外部からの助言
じゃぱネットたかた	高田社長自ら情報セキュリティ最高責任者になり，情報漏洩の問題を認知，対策を実施	トップ責任体制の確立
アッカ・ネットコマース	データベースのアクセス履歴を半永久保存。外部機関に委託し「情報セキュリティ監査」の実施	情報セキュリティ監査
日本信販／日立	不正アクセス防止ソフトの導入，電磁記録媒体の暗号化，社員やグループ各社従業員の教育	暗号化 社員教育徹底

ハイテク犯罪・事故による経済的・社会的損失と責任

- インターネット犯罪で被る企業等の**経済的損失**
  - ■2005年5月4日に発見されたラブレターウイルス
    - ・世界20か国　約4500万台のコンピュータ
    - ・約47億ドル（約5000億円）
  - ■2000年2月のヤフー，アマゾンドットのサイト攻撃
    - ・サイト損失総額　約10億ドル
  - ■米国での感染ウイルス被害額（日経新聞平成16年7月7日付）
    - ・企業：1件200万ドル（約2億2千万円），個人：1件500ドル（5万5千円）
- **集団訴訟のリスク**（最悪のシナリオ）
- コンピュータ犯罪・事故で被る企業等の**社会的責任**
  - ■ プライバシーや**機密情報漏洩が社会的責任と対外的な信用の失墜**
  - ■ 社会システムのトラブルが不安をつのらせる
  - ■ このことが致命的な**「危機事態」**になる。
  - ■ 特に，公共団体，自治体及び個人情報を保有するネットビジネス企業等は，**「個人情報保護」**が最重点課題

個人情報漏洩に対する次への懸念

❒企業内・組織内従業員情報の漏洩
- ■ 紙情報による管理の不行届き
- ■ 内部不満からの持ち出し

❒企業内・組織内従業員情報の管理の強化
- ■ 従業員の基本情報，家族情報
- ■ 従業員の給与・賞与，預金，生命保険等の支払い情報
- ■ 評価・考課情報
- ■ 健康管理，健康診断情報
- ■ 退職者情報
- ■ その他

個人情報保護法と保護ガイドライン

ー個人情報の保護と法的セキュリティー

Ⅰ　個人報保護関連の法制度

●個人情報の保護に関する法律（基本法制）

出典：総務省　HP

民間部門

個人情報取扱事業者の義務等

≪基本法部分≫
・基本理念
・国・地方の責務
・基本方針の策定 等

公的部門

●行政機関の保有する個人情報の保護に関する法律

●独立行政法人等の保有する個人情報の保護に関する法律

●情報公開・個人情報保護審査会設置法

●行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律

地方公共団体（条例）

個人情報保護関連の法制度

◆個人情報保護関連5法

①個人情報の保護に関する法律（平成十五年法律第五十七号）
→基本法

② 行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号）→行政機関個人情報保護法

③独立行政法人等の保有する個人情報の保護に関する法律（平成15年法律第59号）→独立行政法人等個人情報保護法

④情報公開・個人情報保護審査会設置法（平成15年法律第60号）
→情報公開・個人情報保護審査会設置法

⑤ 行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律（平成15年法律第61号）
→行政機関個人情報保護法等関係法律整備等

Ⅱ．個人情報保護法の概要

１．個人情報保護法の対象範囲

- これまで企業の社員が紙や媒体の形で個人情報を持ち出して利益を得た場合、業務上横領罪などが適用されていたが、この法律施行後は、個人情報取扱事業者側に、漏洩防止を図る義務などが課せられる。
- 個人情報とは、顧客個人の情報（住所、氏名、電話、クレジットカードNo.など）が強くイメージされるが、「氏名、生年月日その他の記述等により個人を識別できるもの」のことであり、当然従業員の個人情報も対象である。
- 個人情報取扱事業者とは、5,000件以上の個人情報で構成される情報データベースを事業の用に供しているもの、を指す。（国会での答弁）
- 尚、5,000件という数字は、すべての顧客名簿と従業員名簿を合算して計算される。個人情報データベースとは、個人データの集合物であって、検索可能な状態になっているものを指し、必ずしもコンピュータ管理されているものに限定されているわけではない。

- この法律での個人情報取扱事業者の義務として、7原則が挙げられる。これらは、1980年に国際的な個人情報保護のためにOECDがまとめたガイドラインの8原則にほぼ対応している。

個人情報・個人データ・個人データ・ベース

個人情報

生存する個人のじょうほうであって，当該情報含まれる氏名，生年月日，その他記述により特定の個人を識別できるもの。（第2条第1項）
【例】 データベース化されていない書面，写真，音声等に記録されているもの

個人データ

個人データベース等を構成する個人情報を含む情報の集合物である。（第2条第4項）
【例】 委託を受けて，入力，編集，加工のみをおこなっているもの
存否が明らかになることで公益その他の利益が害されるもの
短期間（政令で定められる）で消去されることになるもの

保有個人データ

個人情報取扱い事業者が開示，訂正，削除等の権限を有する個人データ。（第2条第5項）
【例】 自社の事業活動に用いている顧客情報
事業として題三者に提供している個人情報
従業員等の人事管理情報

Ⅲ. 労働者の個人情報保護について

1.「労働者の個人情報保護に関する行動指針」

- ILO勧告を直接のきっかけとしてまとめられたもので、2000年末に公表。したがって、個人情報保護法制定過程の議論もある程度反映。
- この指針は、「民間企業等が、業務の実態を踏まえつつ、労働者の個人情報の保護に関する規定を整備することを支援、促進」することを目的（指針第1.1）
- 労働者の個人情報保護一般の問題を対象としている点、現代的な問題にも触れている点が特長。

2.「雇用管理に関する個人情報の適性な取扱いを確保するための事業者が講ずべき措置に関する指針」

（厚生労働省：平成16年6月）

3. 個人情報保護に関する法律についての経済産業分野を対象とするガイドライン

（経済産業省：平成16年6月）

労働者の個人情報保護について(1)

No.	個人情報の種類
1	基本情報(住所、電話番号、年齢、性別、出身地、人種、国籍など)
2	賃金関係情報(年間給与額、月間給与額、賞与、賃金形態、諸手当など)
3	資産・債務情報(家計、債権、債務、不動産評価額、賃金外収入など)
4	家族・親族情報(家族構成、同・別居、扶養関係、家族の職業・学歴、家族の収入、家族の健康状態、結婚の有無、親族の状況など)
5	思想・信条情報(支持政党、政治的見解、宗教、各種イデオロギー、思想的傾向など)
6	身体・健康情報(健康状態、病歴、心身の障害、運動能力、身体測定記録、医療記録、メンタルヘルスなど)
7	人事情報(人事考課、学歴、資格・免許、処分歴など)
8	私生活情報(趣味・嗜好・特技、交際・交友関係、就業外活動、住宅事情など)
9	労働組合関係情報(所属労働組合、労働組合活動歴など)

出所:「労働者の個人情報保護に関する研究会報告書」(平成10 年6月)用語の解説(抜粋)

企業としての対応（2）

個人情報保護に関するコンプライアンス・プログラムの必要性

- 義務違反是正命令に違反した場合には、罰金などの罰則が課される。さらに、個人情報の漏洩などの事故が起これば、損害賠償要求などの民事訴訟の対象になることも予想され、敗訴した場合、その賠償額は膨大となる。
- 金額的な損失だけでなく、コンプライアンス・プログラムやリスク管理の是非について問われることになり、企業の社会的責任が追求される。
- 企業では個人情報の保護と活用を全社的な経営課題として位置付け、ビジネスとITの両面から体制を整える必要がある。
- プライバシーマーク制度（JIS Q 15001準拠　BtoC事業者中心）やISMS制度（ISO/IEC　17799(JISX5080)準拠　BtoB事業者中心）への対応
- 次ページ以降に一般的な対策を例示するが、同じ個人情報取扱事業者でも業務内容や、取扱う個人情報の種類が異なるため、各社で最適な対策を検討しなければならない。

情報セキュリティ対策

ー情報セキュリティめぐる対策・制度・基準ー

情報セキュリティ監査制度について

情報セキュリティ監査制度の概要(1) – 経緯・目的 -

●情報セキュリティ監査 → 企業や政府などの情報セキュリティ対策について、独立かつ専門的知識を有する専門家が、客観的に評価を行う手法

●情報セキュリティ監査についての課題

ユーザ企業;どのような効果があるか分からない
誰に頼めばよいか分からない
監査企業側;監査を行っても「正当性」を信じてもらえない
電子政府;どのような情報セキュリティ監査を行うべきかを具体的に示した指針がない

●2002．9から「情報セキュリティ監査研究会」による検討を開始

●2003．4　運用開始

●制度の目的

・電子政府が本格化することに伴う情報セキュリティ確保の重要性の高まりに対する対応

・国際的に整合性のとれた情報セキュリティ監査制度の構築

出展:NPO 日本システム監査人協会法人部会著 「情報セキュリティを取り巻く動向ー自治体個人情報保護を中心にー」 2004

情報セキュリティ監査制度の概要(2) – 枠組み -

●2つの基準　＊経済産業省の告示

・情報セキュリティ管理基準：監査を行う際の判断尺度
JIS X 5080:2002ベース -> コントロール/サブコントロール

・情報セキュリティ監査基準：監査人の行動規範、一般基準/実施基準/報告基準

●3つのガイドライン

・個別管理基準(監査項目)策定ガイドライン：情報セキュリティ管理基準を基に、個別組織の情報セキュリティ管理基準(監査項目)を作るためのガイドライン

・実施基準ガイドライン：情報セキュリティ監査基準を基に、個別組織の情報セキュリティ監査基準を作成するための、監査における管理基準の位置づけなどを示したガイドライン

・報告基準ガイドライン：情報セキュリティ監査基準を基に、個別組織の情報セキュリティ監査基準を作成するための、保証・助言のひな形などを示したガイドライン

●2つのモデル

・電子政府情報セキュリティ管理基準モデル(庁内ネットワークシステム)

・電子政府情報セキュリティ監査基準モデル

＊これらの資料は、下記サイトから入手可能　http://www.meti.go.jp/policy/netsecurity/audit.htm

出展：NPO 日本システム監査人協会法人部会著「情報セキュリティを取り巻く動向ー自治体個人情報保護を中心にー」 2004

情報セキュリティ監査制度の概要（4） – 6つの視点 –

1.「情報資産」のセキュリティ確保

2.「情報資産」に対するマネジメントの効果的実施の確認

3.「保証型監査」と「助言型監査」

4. 保証・助言における「全部」と「一部」の組合せ

5.「助言型監査」とコンサルティング

6.「外部目的監査」と「内部目的監査」

出展：NPO 日本システム監査人協会法人部会著 「情報セキュリティを取り巻く動向ー自治体個人情報保護を中心にー」 2004

情報セキュリティ対策

ー　物理的・システム的・人的管理的　ー

物理的セキュリティ対策

■　秘密管理情報であることの表示

①秘密情報と他の情報との区分表示

②秘密レベルの表示：「極秘」，「厳秘」，「秘」など

■　物理的アクセス制限

①アクセス権者の限定：

・「極秘」：役員のみ，情報閲覧室等の鍵設置

・個人認証，暗証番号等の設定による物理的入室の管理

②アクセス権者の使用・範囲の限定

・情報資料室等の持ち出し禁止

・情報表示の限定，部屋の分離

・監視カメラによる入出者の管理など

■　物理的な機能の制限

・　補助記憶装置の機能制限・不能対応（FD，CD等の書込み不能など）

・　電磁的記録媒体の持込禁止など

システム・技術的セキュリティ対策

■システム・技術的アクセス制限

①アクセス権者の限定

・端末からのアクセス制限：パスワード設定

・アクセスできる端末，回線の制限

・特権ユーザの設定，遠隔ログインの禁止

・アクセス履歴の記録，ログの採取

②アクセス権者の使用・範囲の限定

・OSに補助記憶装置の使用制限機能の設定

③データの暗号化，暗号通信など

■　マネジメントによる管理

①　アクセスログの管理：検証，ログの分析

②　管理者による牽制・教育・指導など

■　システム監査，情報セキュリティ監査の実施

①　外部監査人による定期，不定期の監査の実施，フォローアップなど

管理的・法的管理セキュリティ対策

■　自己（自社，自組織）情報の管理

- 就業規則や誓約書等による契約
- 社内（組織）内の営業秘密管理規則による管理

（入社時のみならず，営業秘密を知りうる立場になる都度，新たに誓約書の提出をもとめる）

■　派遣社員等

- 派遣元事業者（派遣会社）と派遣契約の中で，秘密保持を遵守する旨の規定を入れる（派遣法第24条の4）。
- 派遣社員と秘密保持を遵守する誓約書等による契約

（労働基準法第16条及び派遣法に反しない範囲にとどまる）

■　退職者等

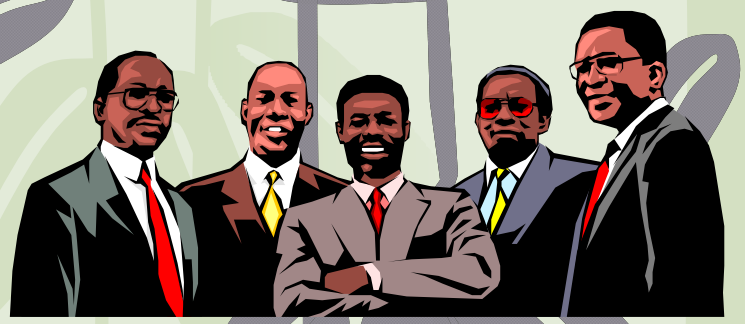
- 退職後の秘密保持契約の締結，個人所有の情報の返還・破棄

■　取引先等

- 取引にあたって，対象範囲を明確にしての秘密保持契約の締結
- 不正競争防止法上の「営業秘密」として，不正使用の禁止

個人情報保護の法的セキュリティ

ー不正競争法防止法・公益通報者保護法ー

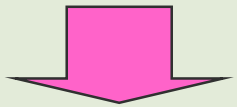


法的セキュリティ

■　法的セキュリティとは，情報資産を法律（条例，規制等を含む）により保護するこであり，以下，二つの側面がある。

①自らが，法律に抵触しないようにする。遵法の側面

②他からの，法律侵害からまもる。法的侵害からの保護の側面



■自らが，情報資産保護のための法律を知る

■法的保護のための専門組織，CSO等の設置

■法的セキュリティのシステム監査の実施が重要

Ⅰ．個人情報の不正競争防止法による保護

■　企業等のソフトウェア開発環境の変化にともない，個人情報の漏洩が多発してきた

■ ライセンス契約，アウトソーシング等の活発化，雇用形態の流動化の伴い，個人情報やソフトウェア，ノウハウの保護を不正競争防止法における営業秘密の保護が効果的である

■　個人情報の不正競争防止法による保護の対象

・個人情報を企業等の「技術上または営業上の秘密情報（営業秘密：トレードシークレット）と位置付ける。

・差止請求権／損害賠償／信用回復措置がとれる

ノウハウ・営業秘密の保護と不正競争防止法(1)

■　技術革新や経済のソフト化に伴う企業等の「技術上または営業上の秘密情報(営業秘密:トレードシークレット)を保護

■ ノウハウ，ライセンス契約，アウトソーシング等の活発化，雇用形態の流動化の伴い，営業秘密の保護が重要

■　GATTやWIPO(世界知的所有権機構)を中心とした知的財産制度の国際的ハーモナイゼーションの高まり

■　平成2年:産業構造審議会財産情報部会の諮問を受け，不正競争防止法の改正，平成5年:全面改訂

・営業秘密の三要件の規程

・差止請求権／損害賠償／信用回復措置など

営業秘密となる三要件と取得環境（２）

■　営業秘密となるための三つの要件

①秘密管理性：秘密に管理されていること

②有　用　性　：生産方法，販売方法その他の事業活動に「有用な技術上または営業上の情報」であること

③非 公 然 性 ：公然としられていないこと

企業相互に取得・保有が発生する

■　情報産業における営業秘密の取得環境と保有者

例：ソフトウェア開発の外部委託

・開発企業の営業秘密：業務機密，製造方法，原価情報，個人情報など

・受託会社の営業秘密：提案内容，開発のノウハウ，技法・手法など

例：その他情報処理サービス，SIサービス，コンサルティング，派遣など

秘密管理が否定された事例（3）

■　無施錠の一般管理庫，秘密表示が無い，アクセスに人的・時間的制約がなかった。

（合同総合コンサルタント事件：大阪地裁　平成11年9月14日判決）

■　パソコンのハードディスク上に，パスワード設定がない，丸秘表示がない，机の引き出しに保管されていた。

（車両変動状況表事件：東京地裁　平成12年12月7日判決）

■　営業時間中に誰でも見れる，機密事項の特段の表示がない。

（人材派遣業者事件：大阪地裁　平成12年7月25日）

■　従業員が顧客から名刺を入手した場合に，保管，持ち出し，返還，枚数の確認等の厳格な管理規程を設けた管理がない。

（消防試験事件：東京地裁：平成13年8月27日判決）

出典：経済産業省「営業秘密管理指針」 報道公表資料より

Ⅱ．ホイッスル・ブローイングによる個人情報保護

■　ホイッスル・ブローイングとは，放置しておけば公益が脅かされるおそれのある怠慢，悪用，危険などを，注意を促すために明るみにだすこと。

■企業内不正あるいは不祥事に対する警告（ホイッスル）を挙げる（ブローイング）こと

■　企業人が自己の知りえた情報をどのように受け止め，行動するかの「倫理的決断」に迫るものである。

■　日本では，1991年に経団連が「企業行動憲章」を制定，その2002年，2004年に改訂

出典：上園忠弘著「企業人の情報倫理－ホイッスルブローイングを軸として－」 大阪大学

ホイッスル・ブローイングのケース

■ 内部的ホイッスル・ブローイング

① 不適切な行動を組織内部の適切な人に報告
② 企業内の従業員が互いに監視し合う
③ その他

■ 外部的ホイッスル・ブローイング

① 不適切な行動を外部的組織の適切な人に報告
② 不適切な行動や不祥事を報道機関等に告発・暴露する
③ その他

■ 政府機関等ホイッスル・ブローイング

① 政府等の監督機関，調査機関に告発・暴露する
② その他

出典：上園忠弘著「企業人の情報倫理－ホイッスルブローイングを軸として－」 大阪大学を参考に作成

ホイッスル・ブローイングの課題

■ 故意・悪意をもった告発

① 人を落とし入れるための告発
② 誹謗・中傷の告発
③ ハラスメントとしての告発
④ 機密情報漏洩のための告発暴露
⑤ その他

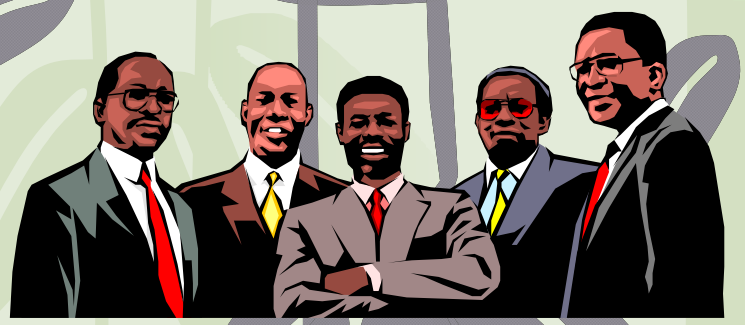
■ 正しい情報として確認できる組織体制

■ 組織内の改善，公益のためである企業内風土つくり

■ 告発者の保護，不利益からの保護

まとめ

ー　ＥＣ時代の情報セキュリティ　ー



情報セキュリティの確立のために

■　危険なトップトップマネジメントの考え方

- 無形の「情報」の財産的価値が理解できない
- セキュリティ投資は利益を生まない
- セキュリティ問題は情報システム部門の問題

■　セキュリティへの新たな考え方

- 対策は情報技術の進化とともに脆弱性は変化し，セキュリティレベルは低下する
- トップマネジメント自らの取組み姿勢が最強の環境と教育
- セキュリティには投資がかかるが、脅威の現実化で投資以上に企業等の資産を失うことになる
- セキュリティへの不考慮が情報資産の消失とともに社会的責任を問われ，危機事態を招くことになる。

企業等が法的な問題を起こさないために

- 情報システムの**法的脆弱性**を知ること
  - トップマネジメント及び管理者が持つべき**情報法知識**
- 情報資産の法的保護とセキュリティ対策の見直し
  - 情報資産の価値評価と対策の見直し
- 個人情報の漏洩，ハイテク犯罪・事故の**社会的責任**
  - 組織的管理（トップミスからの管理責任）
  - 自己管理と自己責任
- 内部管理と新たな牽制機能の強化
  - **システム監査／情報セキュリティ監査**の実施
  - **ホイッスルブローイング（内部告発）の制度化**
    （公益通報者保護法の確立による）

参考／参照文献

1. NPO 日本システム監査人協会法人部会著 「情報セキュリティを取り巻く動向ー自治体個人情報保護を中心にー」 2004　2

2. 藤田護人著 「e-Japan時代の情報セキュリティと個人情報保護」 IMSブックレット　2004

3. 飛田　治則著　個人情報保護法「急がれる企業の取組み（基礎編）」

　　大阪市立大学大学院創造都市研究科　情報法共同研究グループ　2004

4. 孝橋　宏二著 「個人情報保護法に対する当社の対応について」

　　大阪市立大学大学院創造都市研究科　情報法共同研究グループ　2004

5. 喜入　博（KPMGビジネスアシュアランス）著
　　「情報セキュリティリ監査基準制度」（FISC）2003

6. 総務省ホームページ：http://www.soumu.go.jp/s-news/2004/040220_1.html

7. 上園忠弘著「企業人の情報倫理ーホイッスル・ブローイングを軸としてー」 大阪大学

8. 日本ユニシス関西支社のホームページ
　「ホットライン関西」「ちょっと知りたい情報ニュース」
　http://www.unisys.co.jp/KANSAI/chot/chot_info.htm

9. 松田貴典著 「情報システムの脆弱性」 白桃著房　1999

10. 松田貴典著 「ビジネス情報の法とセキュリティ」 白桃著房　2004（7月発刊予定）