インターネット協会
第11回セキュリティ・フォーラム
情報セキュリティと法律

弁護士
岡村 久道

情報セキュリティ（Information Security）とは何か？

「情報の機密性、完全性、可用性を確保し維持すること」

OECD「情報システムのセキュリティのためのガイドライン」（1992年）およびISM認定基準

Confidentiality（**機密性**）
Integrity（**完全性**）
Availability（**可用性**）

頭文字をとって「CIA」と呼ばれる

GMITS (ISO / TR 13335)で3項目追加
Accountability（**説明責任**）
Authenticity（**信憑性・真正性**）
Reliability（**信頼性**）

情報セキュリティと法律

- 情報セキュリティ概念は技術に由来しているので、法律との整合性に関する議論なし
- 国際標準の　ISO/IEC 17799 なども、法律領域を前提にしていない。
- これまで法律領域独自で、情報セキュリティ侵害行為を規制してきた。
- 最近では、法律で、システム運営者に情報セキュリティを守るべき責任を負わせる傾向にある。
- しかし、法律でシステム運営者に課せられた情報セキュリティを遵守するために、何をどうすればいいのか分からず、これから混乱が広がる可能性がある。
- 他方、技術領域でも、これから法律を念頭に置いて進めることが必須であるが、この点に関する啓蒙が進んでいないこともあり、法律違反のセキュリティポリシーすら見受けられる状況にある。

機密性 (Confidentiality) 1/3

- アクセスを認可 (authorized) された者だけが、情報にアクセスできることを確実にすること
- わが国の判例中の主要な関連事案
- 日経マグロウヒル事件の東京地判昭和48年2月19日
  - コンピュータ用磁気テープに入った雑誌購読者名簿データを保管中に漏えいさせた外部委託業者に対し、委託元の雑誌社への損害賠償責任を認めた
- 新潟鉄工事件の東京地判昭和60年2月13日 (第一審) 及び東京高判昭和60年12月4日
  - コンピュータシステムに関する会社の機密資料を複写目的で持ち出した従業員に業務上横領罪の成立を認めた
- 前橋信金事件の前橋地判昭和61年5月20日 (第一審) 及び東京高判昭和62年8月31日 (控訴審)
  - 信用金庫 (被告) の事実上分裂した組合の代表者たる職員 (原告) が、他の職員をして被告のオンライン端末機を正規の手続を経由せず無断で操作させて、同信金従業員組合会計名義の預金残高を確認したことが就業規則違反に該当するとして行った懲戒処分の効力が争われた

機密性 (Confidentiality) 2/3

- わが国の判例中の主要な関連事案 (続き)
- 京王百貨店事件の東京地判昭和62年9月30日
  - 百貨店の顧客名簿データが入った磁気テープを、同百貨店に勤務するコンピュータ技術者が複写目的で持ち出した行為が窃盗罪に該当するとした
- さくら銀行顧客信用情報大量漏えい事件の東京地判平成10年7月7日
  - さくら銀行のプログラム開発業務に従事する派遣社員が、持参のフロッピーディスクにメイン顧客データを無断コピーした上、預かっていた項目説明書等の資料 (書類) 4枚を無断コピーして名簿図書館に売却した事案で、資料に関する業務上横領罪の成立を認めた
- 宇治市住民基本台帳データ大量漏えい事件の京都地判平成13年2月23日 (第一審)・大阪高判平成13年12月25日 (控訴審)・最決平成14年7月11日 (上告審)
  - 宇治市の住民基本台帳データ21万数千人分を外部委託業者が事務所内で保管中、持参の光磁気ディスクにアルバイト大学院生が無断でコピーして持ち出し、データを名簿業者がウェブで販売していた事案で、プライバシー権侵害に基づき住民に対する損害賠償責任を市に認めた

機密性（侵害と法的責任）3/3

- 漏えい者の民事責任
  - 損害賠償請求の対象となりうるほか、当該情報が不正競争防止法第2条第4項所定の「営業秘密」に該当する場合には、窃盗・詐欺・強迫など不正な手段による営業秘密の取得行為や開示行為などに対し、差止請求権及び必要な措置（設備の廃棄など）請求権（同法第3条）、並びに損害賠償請求権（同法第4条、民法第709条）を行使することができる。
- 漏えい者の刑事責任
  - 情報が載った他人の有体物（紙や媒体）を持ち出した場合には、刑法の窃盗罪又は（業務上）横領罪が成立しうる。事前に共謀して持ち出させた者には共犯が成立し、事後に事情を知りながら当該財物を譲り受けた者には盗品譲受け罪（第256条）が成立しうる。
  - 自ら持参した媒体にデータを無断でコピーして持ち出した者には、これらの罪が成立しない点で限界がある。データ自体はこれらの罪の客体たる「財物」に該当しないからである。

完全性 (Integrity) 1/2

- 情報および処理方法が完全かつ確実であることを保護すること
- 紛争の典型例は、情報の不正な改ざん行為
  - わが国の判例上では、金融機関におけるオンライン詐欺の事案が多い
  - 三和銀行事件の大阪地判昭和57年7月27日
  - 第一勧銀事件の大阪地判昭和63年10月７日
  - その他
  - 電子計算機使用詐欺罪によって処罰
- 金融機関以外における故意によって完全性が侵害された事例
  - 朝日放送クラッキング事件の大阪地判平成9年10月3日
  - 霞ヶ関中央省庁連続クラッキング事件 (2000年1月発生)
  - ニフティ電子掲示板詐欺事件の京都地判平成9年5月9日
  - パチンコ遊技台裏ロム事件の福岡高判平成12年9月21日

完全性 (Integrity) 2/2

- 過失による完全性の侵害事例の典型例はコンピュータの誤操作事案
  - 日本相互銀行コンピュータ誤操作事件の福岡地判昭和53年4月
  - 三和銀行コンピュータ誤操作事件の札幌高判昭和55年6月
  - 預金者名コンピュータ誤入力事件の東京地判平成10年7月14日
  - 選挙管理委員会誤入力事件の東京地判平成16年5月
- 企業や自治体にとって、内部者の故意行為のみならず、過失行為に対しても適正な対策を講じることの必要性を示している。
- 以上のとおり、完全性が確保されなければ、やはり企業はさまざまな損失を被り、裁判紛争に巻き込まれるおそれもある。仮に加害者に対する民事損害賠償が理論上可能である場合であっても、資力不足が原因で事実上賠償を受けることができないことが多いという事実は、情報漏えい事件の場合と同様である。したがって、やはりここでも「転ばぬ先の杖」として、事前に予防策を講じることが必要となる。

可用性 (Availability) 1/3

- 許可された利用者が、必要な際に情報および関連資産にアクセスできることを確実にすること
- みずほフィナンシャルグループ大規模システム障害発生事件
  - 本件は、3つの銀行の営業統合に伴って統合したオンラインシステムが2002年4月に稼働を開始した際、システムの不具合等からＡＴＭ障害、口座振替の引落遅延等が大量発生したというケースであり、二重引落も大量発生したので完全性の点とも関連している。本件で金融庁は、システム統合にかかるリスクに対する旧経営陣の認識の不十分さを背景に、システムのテストなど最低限必要な準備の未了等が原因であるとして、改善･対応策及び責任の明確化のための措置を確実に実行すること等を内容とする業務改善命令を、銀行法第26条等に基づき同年6月19日に発動した。なお本件では役員の経営責任や顧客に対する損害賠償責任の問題にも発展している。
- 世田谷ケーブル火災事件の東京高判平成2年7月12日
  - 地下の通信用ケーブル専用溝内の火災で電話ケーブルが焼損し加入電話回線等が不通になった事故に基づいた日本電信電話公社 (現ＮＴＴ) に対する損害賠償請求が問題となった。

可用性 (Availability) 2/3

- **ハードディスク・データ消失事件の広島地判平成11年2年24日**
  - 原告がパソコン内蔵ハードディスク容量を増大させるために新たなハードディスクを購入し、販売店（被告）に旧ディスクから新ディスクへの交換を依頼したところ、被告の従業員が誤って旧ディスクを初期化したので、旧ディスク内に記録されていた原告の業務上不可欠な多量のデータがすべて消去された事案で、被告に損害賠償責任が認められた。
- **レンタルサーバ・データ消滅事件の東京地判平成13年9月28日**
  - 納入した製品が可用性を欠くとして取引先から訴えられた事案であり、インターネット接続プロバイダ（被告）のレンタルサーバ内に保管されていた原告の電子商取引サイト用コンテンツデータを、システム変更の際に被告が誤って消滅させたことを理由とする損害賠償請求を一部認容した。
- **東京電送センター事件の東京地判平成8年7月11日**
  - コンピュータ機器の売買契約で、買主が機器に瑕疵を発見したときは直ちに売主に内容を通知すべき約定がある場合、通知を受ける都度、売主が機器を調査して代替品との交換又は修理等の必要な措置を行い、瑕疵ある状態を解消すれば、売主は債務不履行責任を負わないとした。

可用性3/3 (システム障害への法的防御)

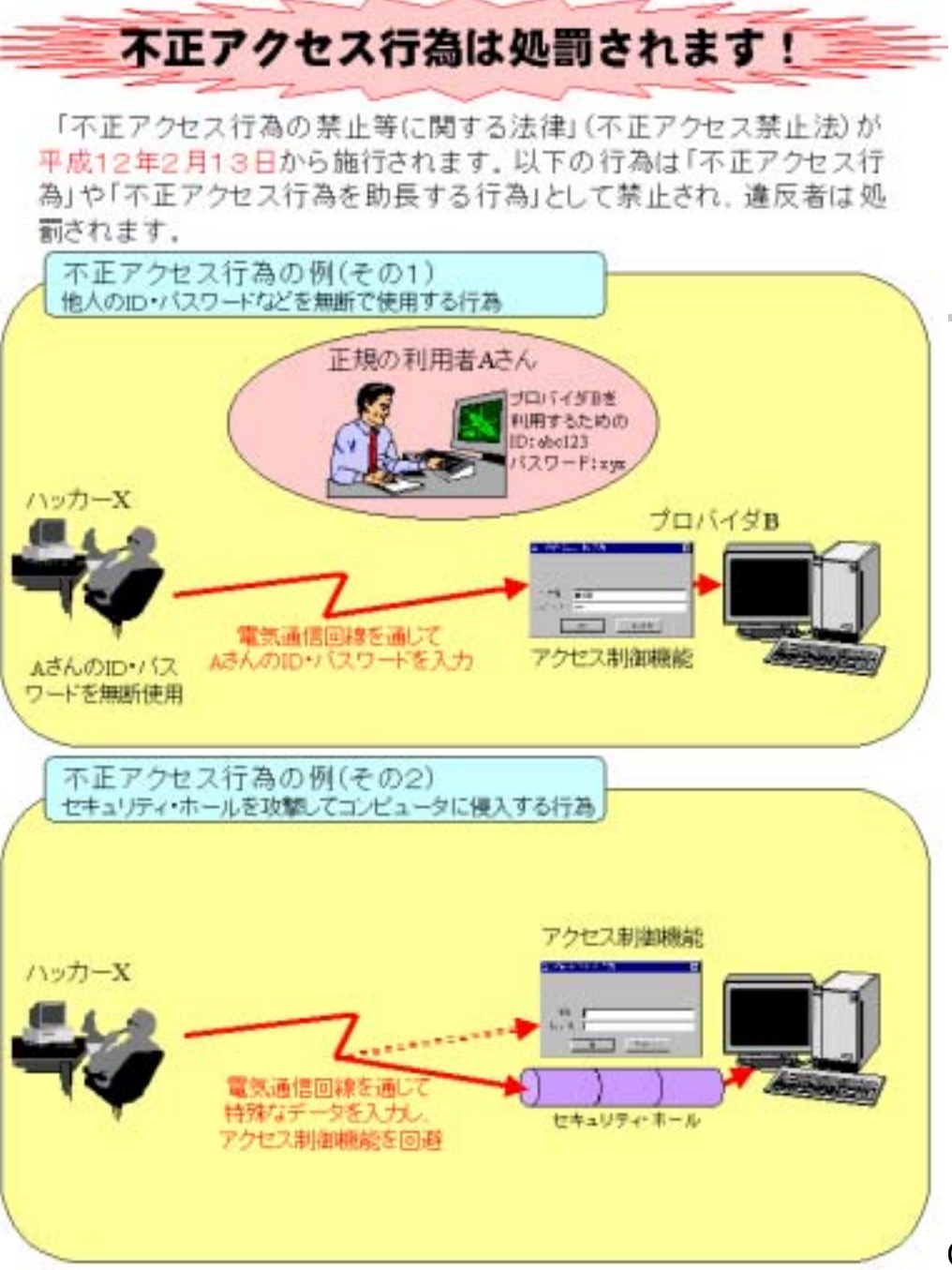
- ニフティ・スパムメール送信差止仮処分事件の浦和地決平成11年3月9日
- ドコモ迷惑メール送信差止仮処分事件の横浜地決平成13年10月29日
- 特定電子メール送信適正化法
  - 迷惑メールのランダム送信による大量の架空メール送信が、第1種電気通信事業者の設備に対し通信障害をもたらすおそれがあることから、これを避けるために、自己又は他人の営業につき広告又は宣伝を行うための手段として送信者がプログラムを用いて作成した架空電子メールアドレスに宛てた電子メールの送信をすることを禁止し、電子メールサービスを行う電気通信事業者について、特定電子メールによる電子メールの送受信上の支障の防止に資するそのサービスに関する利用者への情報提供及び新技術の開発又は導入の努力義務を設け、第1種電気通信事業者は、一時に多数の架空電子メールアドレスに宛てた電子メールの送信がされた場合には、その送信をした者が送信した電子メールにつき、電気通信役務の提供を拒むことができることを規定している。
- 完全性を損なう行為については、刑法上の業務妨害罪を適用しうる場合がある。これには威力業務妨害罪、偽計業務妨害罪、及び電子計算機損壊等業務妨害罪という3つの種類があるが、すべて故意犯に限られている。

情報セキュリティの法的保護

- 不正競争防止法による営業秘密の保護
- 1987年の刑法改正
  - コンピュータ犯罪への対応が行われた結果、電磁的記録不正作出及び供用罪（第161条の2）、電子計算機損壊等業務妨害罪（第234条の2）、電子計算機使用詐欺罪（第246条の2）、が新設され、公正証書原本等不正作出罪（第157条）、公用文書等毀棄（第258条）及び私用文書等毀棄（第259条）の客体に、電磁的記録が追加された。
  - 情報セキュリティ概念との対応関係を検討すると、このうち電子計算機損壊等業務妨害罪は主として可用性、その余の規定は主として完全性を保護する機能を有している。したがって、この刑法改正では、機密性にかかわる規定は新設されなかったことになり、機密性については主として前述の不正競争防止法による民事的保護に委ねられた。

情報ネットワーク関連立法

- 不正アクセス禁止法
- 電子署名法
  - これに関連して法務局による商業登記の電子認証制度を創設したものが平成12年改正商業登記法であり、法人代表者の電子署名の認証を受けることになった。こうした電子署名法制によって、電子メッセージの名義人の同一性（本人確認＝成りすましの防止）及び内容の同一性（非改ざん性＝改ざんの防止）の確認手段が、法的な裏付けを取得したことになる。また、改正公証人法で「私署証書の認証」に当たる電子公証制度が創設され、改正民法施行法で「確定日付の付与」に当たる電子公証制度が創設されている。これらの法整備も電子化された情報の完全性を担保するものということができる。
- IT基本法
  - 第22条において、「高度情報通信ネットワーク社会の形成に関する施策の策定に当たっては、高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護その他国民が高度情報通信ネットワークを安心して利用することができるようにするために必要な措置が講じられなければならない。」と規定しており、ここに「安全性及び信頼性」には情報セキュリティの意味が含まれている。



警察庁「不正アクセス行為の禁止等に関する法律の概要」

http://www.npa.go.jp/hightech/fusei_ac1/main.htm

Okamura 2002

警察庁「不正アクセス行為の禁止等に関する法律の概要」

- 不正アクセス行為とは、識別符号(※1)を入力することで利用(※2)できるようになっているコンピュータ(※3)にネットワークを通じて(※4)アクセスし、このような利用ができる状態にしてしまう行為(※5)です。コンピュータ以外の端末から行うもの(※6)も禁止・処罰されます。
- 他人の識別符号を無断で第三者に提供する行為は、不正アクセス行為を助長する行為として禁止・処罰されます。提供手段に限定はなく、オンラインで行っても、オフラインであっても禁止・処罰されます。提供行為によって金銭的な利益を得たかどうかは関係ありません。

※1 ID・パスワードのほか、指紋、虹彩、音声、署名などを用いるものも含まれます。
※2 ホームページの書き換え、インターネット・ショッピングの注文、データ閲覧、ファイル転送など利用内容に限定はありません。
※3 企業のものも個人のものも広く含まれます。
※4 インターネットなどのオープンネットワークのほか、企業内LANで外部と接続していないものなども含まれます。
※5 利用してしまう行為も含まれます。
※6 例えば、電話機から口座番号と暗証番号をプッシュボタンで入力する行為などです。

http://www.npa.go.jp/hightech/fusei_ac1/main.ht

amura 2002

法律での情報セキュリティ遵守義務付け

- 不正アクセス禁止法
  - 第5条は、「アクセス管理者による防御措置」という表題で、ネットワーク・サーバなどのコンピュータ管理者に対し、いわゆるハッカーなどの不正アクセス被害を受けないようにセキュリティを保つべき義務を課している。但し、法文の「努めるものとする」という文言からも明らかなように、この義務は単なる努力義務にすぎず、これを遵守しなくとも法的なペナルティは課せられない。
- 個人情報保護法案
  - 第25条において「個人情報取扱事業者は、その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。」として、安全管理措置義務を定め、さらに、第26条では従業者に対する監督義務を、第27条では委託先に対する監督義務を、それぞれ個人情報取扱事業者に負わせている。これらの義務を怠った場合、第39条で、主務大臣から勧告及び命令を受け、さらに命令違反には第61条で罰則が規定されており、この罰則には第63条で両罰規定が用意されている。ここにいう個人データとは主としてコンピュータ処理情報を対象としている。
- 労働者派遣法
  - 「派遣元事業主は、労働者の個人情報を適正に管理するために必要な措置を講じなければならない」と規定しており（第24条の3第2項）、違反行為には、厚生労働大臣の指導、助言及び勧告（第48条）、改善命令（第49条）などが用意され、第49条による処分に違反した者は罰則の対象となる（第60条）。

情報セキュリティマネジメントとコーポレートガバナンス

- 企業において情報セキュリティマネジメントを講じることは、コーポレートガバナンス（企業統治）の問題として認識されている。すなわち、コーポレートガバナンスは株主価値の最大化を求めており、企業として情報価値を極大化しつつ情報化投資額の極小化について調和を図るために適切なコントロールを導入する必要がある。さらに企業は顧客や取引先に対し自らのセキュリティ水準を証明する責任がある。

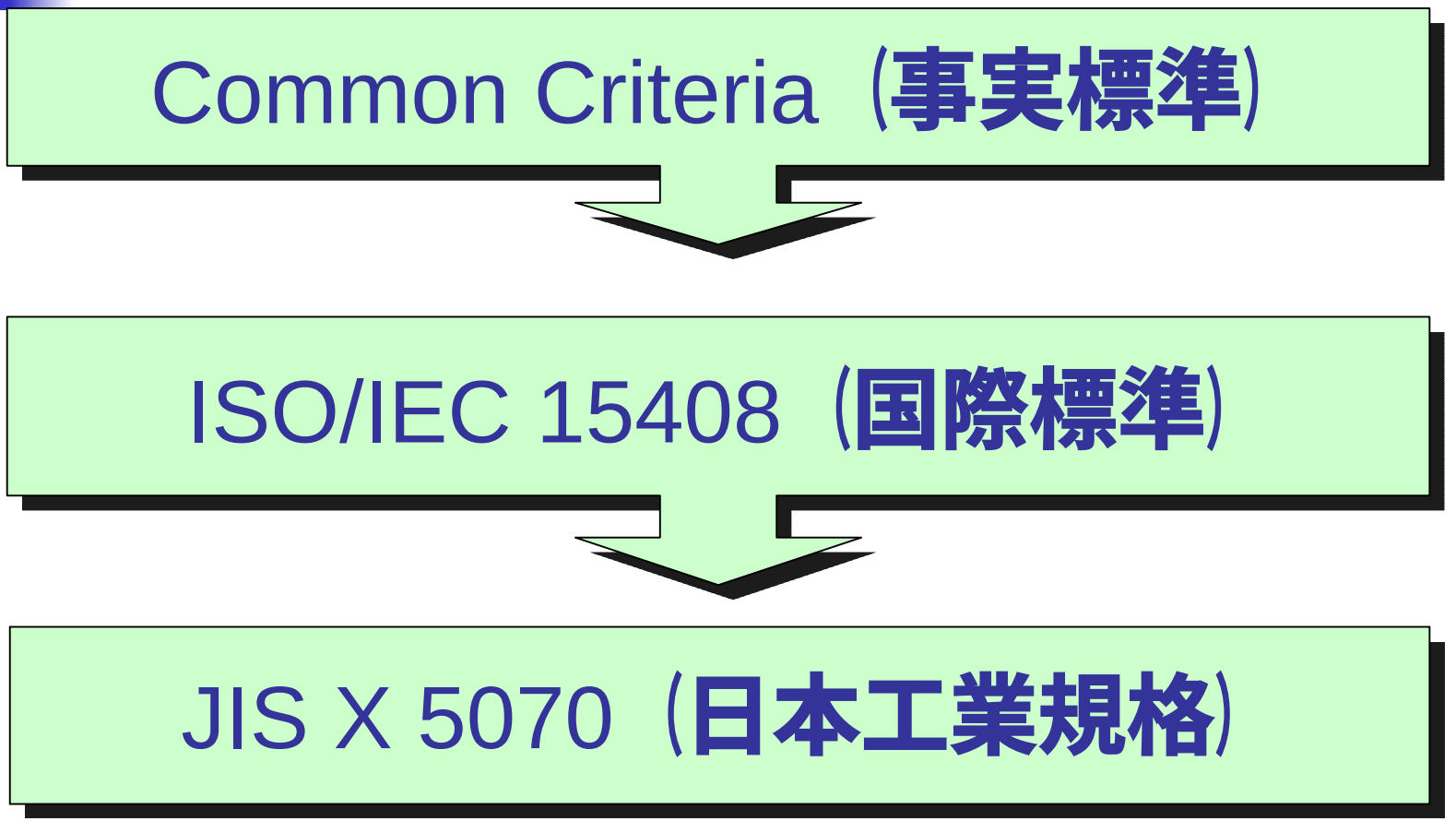
大阪地判平成12年9月20日

- さまざまなリスクに対する企業の対応について、「健全な会社経営を行うためには、目的とする事業の種類、性質等に応じて生じる各種のリスク‥‥の状況を正確に把握し、適切に制御すること、すなわちリスク管理が欠かせず、会社が営む事業の規模、特性等に応じたリスク管理体制（いわゆる内部統制システム）を整備することを要する。そして重要な業務執行については、取締役会が決定することを要するから（商法260条2項）、会社経営の根幹に係わるリスク管理体制の大綱については、取締役会で決定することを要し、業務執行を担当する代表取締役及び業務担当取締役は、大綱を踏まえ、担当する部門におけるリスク管理体制を具体的に決定するべき職務を負う。」と判示して、これを怠った当時の経営陣に対し、当時の為替レートで約計830億円もの支払いを命じた。
- 本判決は情報セキュリティが直接対象となった事案ではない。しかし本判決は、さまざまな種類のリスクと並んで「システムリスク」を摘示しているので、その対象は情報セキュリティ分野にも及んでいる。すなわち、金融庁の「金融検査マニュアル」では、システムリスクとは、コンピュータシステムのダウン又は誤作動等、システムの不備等に伴い金融機関が損失を被るリスク、さらにコンピュータが不正に使用されることにより金融機関が損失を被るリスクとして定義されている。この定義は情報セキュリティに関する前述の定義とはやや異なっているが、大筋において実質的に一致する部分が多い。こうした分野において、本判決がいう「リスク管理体制（いわゆる内部統制システム）」の整備は、本稿のテーマである情報セキュリティマネジメントを意味している。また、本判決が経営陣に求める「会社経営の根幹に係わるリスク管理体制の大綱」こそが、セキュリティポリシーなのである。

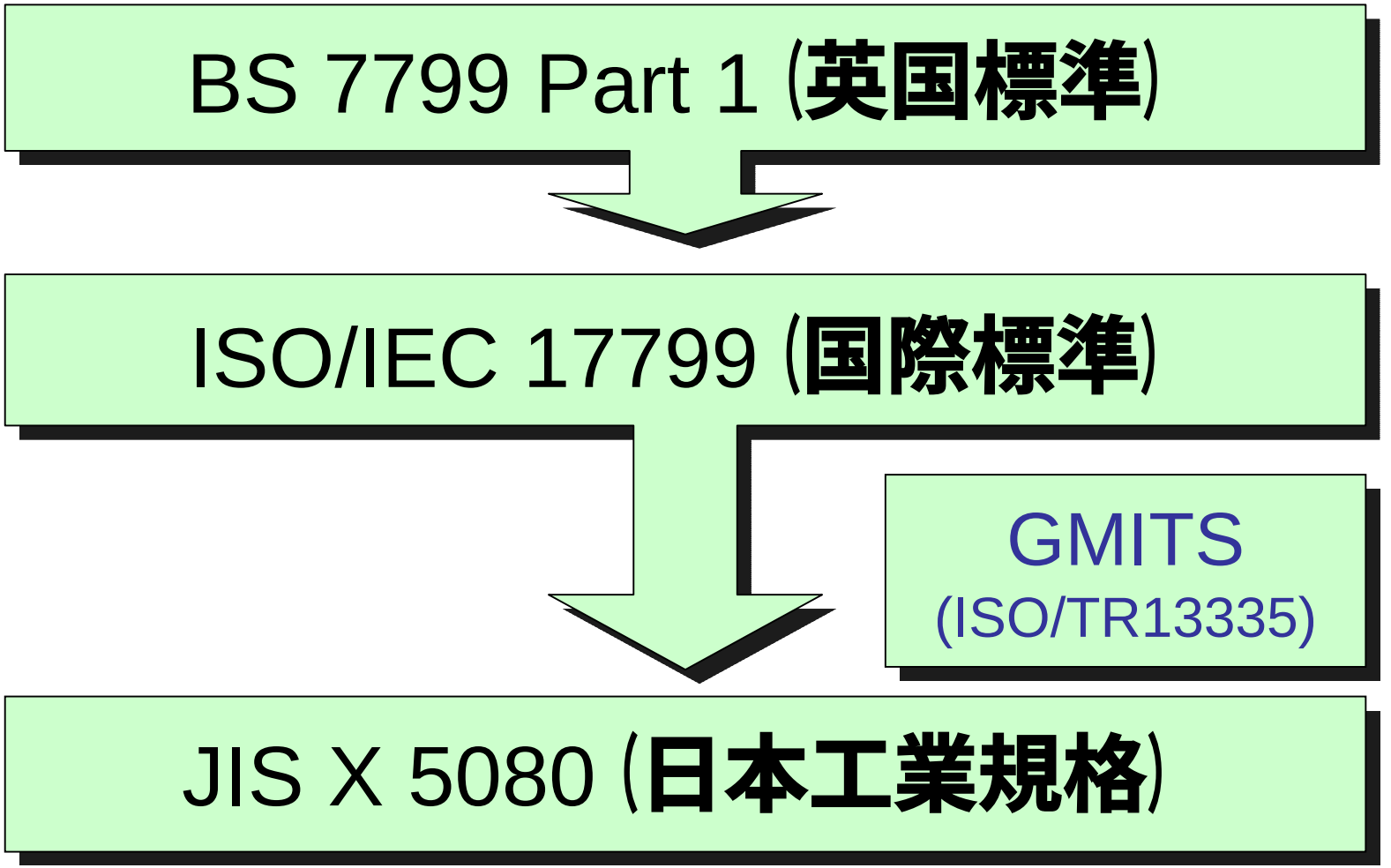
情報セキュリティマネジメント導入に至る実際的な動機

- コンプライアンス（法令遵守）経営
- 情報関連の事故が実際に発生したことに対する再発防止策
- 情報セキュリティマネジメントの導入が、法令によって事業への参入等に要する認定を受けるための条件となっている場合
- 顧客・取引先等からの要請に基づき情報セキュリティマネジメントの導入やISMSの認証取得を迫られる場合

情報技術セキュリティの評価基準の動向



情報セキュリティ・マネジメントの動向



わが国の情報セキュリティの基準と認証基準の動向

1977年告示の「電子計算機システム安全対策基準」
他に総務省「情報通信ネットワーク安全・信頼性基準」
国家公安委員会「情報システム安全対策指針」等

数度の改訂を経て1995年告示の「情報システム安全対策基準」

「情報処理ｻｰﾋﾞｽ業情報システム安全対策実施事業所認定制度(安対制度)」

移行

JIS X 5080（日本工業規格）

「情報セキュリティマネジメントシステム(ISMS)適合性評価制度」

ISO/IEC 17799（JIS X 5080）の目次構成

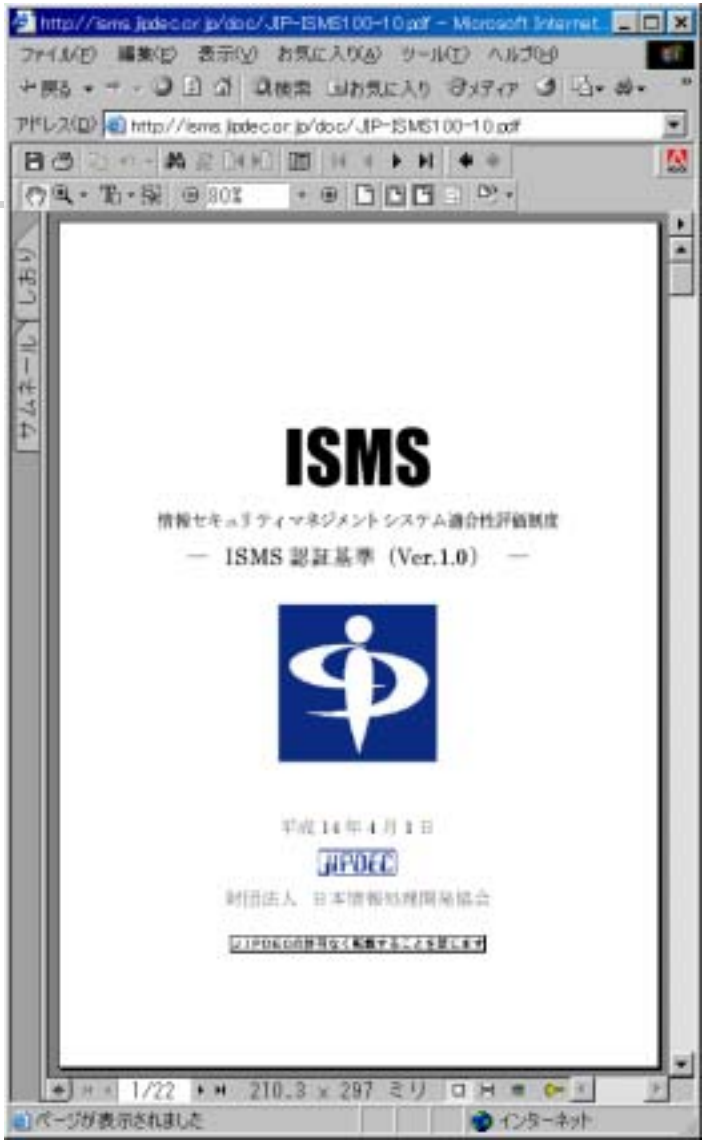
1. 適用範囲
2. 用語と定義
3. セキュリティポリシー
4. セキュリティ組織
5. 財産の分類及び管理
6. 人的セキュリティ
7. 物理的及び環境的セキュリティ
8. 通信及び運用管理
9. アクセス制御
10. システムの開発及びメンテナンス
11. 事業継続管理
12. 準拠

○10のセキュリティドメイン（領域）
○127のコントロール（対策）項目

技術的事項が中心だが、契約処理等の法的事項に関連したものも含まれ、社内規程化にも法務部門の関与必要

ISMS認証基準 (Ver.1.0)

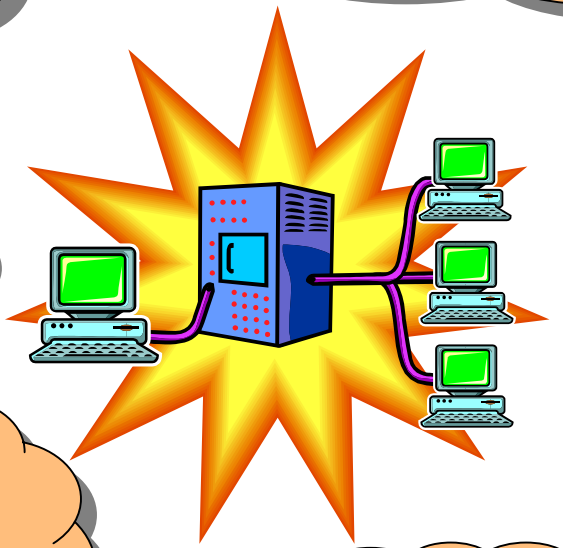
- ISO/IEC 17799:2000をベースとした情報システムのセキュリティ管理に関する適合性評価
- (財) 日本情報処理開発協会が実施
- 位置付けは民間ベースによる第三者認証制度
- 当面は情報処理サービス業を対象
- 2003年度以降は対象範囲を拡大する方向で検討中
- 前述のとおり、技術的事項が中心だが、契約処理等の法的事項に関連したものも含まれており、社内規程化にも法務部門の関与必要



関連する社内諸規定の調整･更新

セキュリティポリシー･
ネットワーク利用規程

システム監
査規程



ドメイン名
管理規程

調整･統合
の必要性

個人情報保護
方針･個人情
報保護規程

懲戒規程

商標等管理
規程

具体例ー6. 人的セキュリティ 1/2

- 6.1において、要員の採用段階からセキュリティの責任に言及し、それを雇用契約に盛り込むこと、雇用中はその監視を行うこと、採用候補者を十分に審査し、すべての従業員及び情報処理設備の外部利用者が、機密保持契約に署名することが望ましいとして、その詳細について触れている。
- 採用候補者を十分に審査することとの関連で、わが国では試用期間の間に不適格であると認めて採用拒否を行うという慣行が存在している。こうした採用拒否いうる場合について、わが国では判例理論の蓄積があるので、これに反しないような取り扱いが必要となる。
- また、労働者の派遣を受け入れる場合は、労働者派遣法の個人情報保護に関する規定が適用されることに注意。
  - 第26条第7項では、労働者派遣の役務の提供を受けようとする者（派遣先企業）は、労働者派遣契約の締結に際し、当該労働者派遣契約に基づく労働者派遣にかかる派遣労働者を特定することを目的とする行為をしないように努めなければならない旨規定している。ここにいう派遣労働者を特定することを目的とする行為には、派遣先がその受け入れる派遣労働者を選別するために行う事前面接や履歴書の送付要請、若年者への限定等が該当するというのが公権的解釈であるから、この規定との関係上で、派遣労働者に対する審査は限定されざるをえない。

具体例ー6. 人的セキュリティ 2/2

- 情報を漏えいさせた場合、損害額の算定が困難である場合が多いので、それに備えて機密保持契約に損害賠償額の予定条項を入れておくことが得策であるように思われる。しかし、わが国の労働基準法第16条は賠償予定を禁止しているので、こうした条項を入れることは同条に違反し無効となる。これに対し、同条は「現実に生じた損害について賠償を請求することを禁止する趣旨ではない」（昭22・9・12発基17号）ので、実損害額を賠償する旨を定めておくことは許される。退職後についても機密保持義務を課すことと同時に、又はこれに代えて、一定期間の競業避止義務を定め、違反した場合は退職金を一定割合支払わない旨の定めが置かれることがあるので、その有効性が問題となる。
- 三晃社事件の最二小判昭和52年8月9日は、労働者が退職後同業他社へ就職する場合は退職金の半額が不支給となる旨の退職金規則について、「被上告会社が営業担当社員に対し退職後の同業他社への就職をある程度の期間制限することをもって直ちに社員の職業の自由等を不当に拘束するものとは認められず、したがって、被上告会社がその退職金規則において、右制限に反して同業他社に就職した退職社員に支給すべき退職金につき、その点を考慮して、支給額を一般の自己都合による退職の場合の半額と定めることも、本件退職金が功労報償的な性格を併せ有することにかんがみれば、合理性のない措置であるとすることはできない」とした。

具体例ー装置のセキュリティ (7.2)

- 装置はセキュリティに対する脅威及び環境上の危険から物理的に保護することが望ましいとするものである。具体的な管理策の内容として、装置の設置及び保護、電源、ケーブル配線のセキュリティ、装置の保守、事業敷地外における装置のセキュリティ、装置の安全な処分又は再使用について規定されている。
- 最後の装置の安全な処分又は再使用については、装置の不注意な処分又は再使用によって危険にさらされるので、取扱いに注意を要する情報を保持する記憶装置は、標準の削除機能ではなく、物理的な破壊又は確実な上書きが望ましいとしている。わが国でも近時は資源有効利用促進法 (リサイクル法) の施行に伴って、企業が廃棄するパソコンから重要情報が漏えいするという事故が報道されており、廃棄時にハードディスクを金槌で叩いて壊すか、専用ソフトによるデータの完全抹消が要請される。(社) 電子情報技術産業協会 (JEITA) が、「パソコンの廃棄・譲渡時におけるハードディスク上のデータ消去に関するガイドライン」を発表している。なお、企業がパソコンを廃棄する場合、廃棄物処理法による規制がある一方、資源有効利用促進法 (改正リサイクル法) によって、廃棄パソコンの回収をメーカーに義務づけ、再資源化に向けた措置を求めている。

具体例ー8.4 システムの維持管理

- 「8.4 システムの維持管理」では、バックアップの必要性などが説かれている。
- レンタルサーバ･データ消滅事件判決は、ログハウス業者が、レンタルサーバを使ってウェブで受注活動を行っていたところ、プロバイダの過失でデータが消滅したというケースであるが、プロバイダ側だけでなく、ログハウス業者側も、バックアップを取っていなかったので、3ヶ月間にわたりウェブでの受注活動が不能になった旨が認定。
- また、ハードディスク･データ消滅事件判決でも、バックアップを取っていなかったことを理由に、5割もの過失相殺減額が認められている。
- 以上のとおり、データが消失した場合、バックアップを取っていなかったという事実は、法的にも極めて重視。

具体例ー8.5 ネットワークの管理

- 「8.5 ネットワークの管理」、「8.6 媒体の取扱い及びセキュリティ」、「8.7 情報及びソフトウェアの交換」に関する管理策も規定されている。電子メールのセキュリティも規定されており、法的な考慮事項を含めたセキュリティリスクが指摘されている一方 (8.7.4.1)、中傷メールの送信など会社の信用を傷つけるおそれのある行為に対する従業員の責任、訴訟で証拠として使いうるメッセージの保存その他の点を含めて、電子メールの使用に関する個別方針の作成が望ましいとされている (8.7.4.2)。
- この点との関連で、労働者たる従業員の電子メールを、使用者たる企業が社内モニタリングすることが適法か否かが問題となる。
- 労働省 (現厚生労働省)「労働者の個人情報保護に関する行動指針」(平成12年12月20日)
  - 使用者は、職場において、労働者に関しビデオカメラ、コンピュータ等によりモニタリングを行う場合には、原則として労働者に対し実施理由、実施時間帯、収集される情報内容等を事前に通知するとともに、個人情報保護に関する権利を侵害しないよう配慮すること、常時のモニタリングは労働者の健康及び安全の確保又は業務上の財産の保全に必要な場合に限り認められること、使用者は原則としてモニタリングの結果のみに基づいて労働者に対する評価又は雇用上の決定を行ってはならないことを求めている。

電子メール社内モニタリングとプライバシー権

- 電子メール無断モニタリング事件（東京地判平成13年12月3日）
  - 会社の上司に電子メールを無断モニタリングされ、プライバシー権を侵害されたことを理由とする損害賠償請求訴訟の事案
  - 会社における職務遂行の妨げとならず、会社の経済的負担も極めて軽微な場合には会社のネットワークシステムを用いた私的電子メールの送受信は社会通念上許され、従業員にプライバシー権が一切ないとはいえないとしつつ、通常の電話装置による場合よりもプライバシー保護は狭く、事業部の最高責任者による監視は相当であり、原告の私的使用の程度は限度を超えていたと判示して、原告の請求を棄却。
- 日経クイック情報電子メール事件（東京地判平成14年2月26日）
  - 従業員に対する誹謗中傷メールの調査過程でメールサーバから偶然発見された別の従業員（原告）による多量の私的メールを理由として、被告会社が原告に対して行った懲戒処分が、プライバシー侵害に該当するか否かが争われた事案で、私用メールは職務専念義務違反で企業秩序違反行為として懲戒処分の対象となり、サーバ上のデータ調査は業務関連情報が保存されていると判断されるから社会的に許容しうる限界を超えていないとして、請求を棄却した。

準　拠

- **法的要求事項への適合**
  - 個別の情報システム毎に関連するすべての法規及び契約上の要求事項を明確にして文書化
  - 知的財産権に関わる法的制限事項を遵守した手順を整備
  - 組織の重要な記録を紛失、消失、破壊、改竄等から保護
  - 個人情報保護に関する法規に従い、個人情報を保護
  - その他
- **セキュリティ方針及び技術適合のレビュー**
  - すべての手続きが情報セキュリティポリシーに準拠して実行されていることを定期的に見直す
  - その他
- **システム監査の考慮事項準拠**
  - 稼働中のシステムに対する監査実施時に業務中断のリスクを最小限に抑える
  - その他

「準拠」について

- 国際標準規格というISOの性格上、「法的要求事項」の具体的内容は示されていない
  - 日本法を分析して、継続的に具体化する作業が必要
- BS7799以降の、B to Cの飛躍的発展に関する視点が不十分
  - 消費者保護の視点から法的に義務づけられている各種の事項を遵守する必要
- 近時は各種の法律が制定されており、それを継続的にレビューして、取り込んでいく必要

個人情報保護法への対応

「個人情報データベース等を事業の用に供している者」（第2条第3項）

個人情報（第2条第1項）

個人データ
（第2条第4項）

保有個人データ
（第2条第5項）

基本原則

個人情報取扱事業者の義務

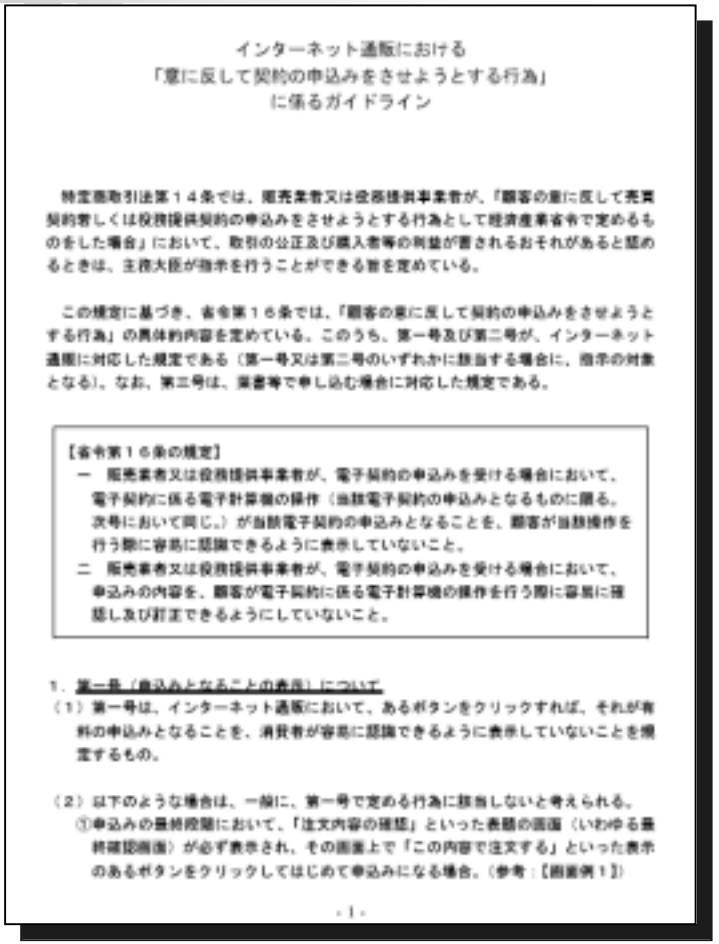
第20条（利用目的の特定）
第21条（利用目的による制限）
第22条（適正な取得）
第23条（取得に際しての利用目的の通知等）

第24条（データ内容の正確性の確保）
第25条（安全管理措置）
第26条（従業者の監督）
第27条（委託先の監督）
第28条（第三者提供の制限）

第29条
（保有個人データに関する事項の公表等）
第30条（開示）
第31条（訂正等）
第32条（利用停止等）

特定商取引法への対応

- パソコンの画面上で申込みができるようなインターネット通販に関して、特定商取引法に基づき、事業者に対し、分かりやすい申込画面の設定を行うことが義務づけられている（特定商取引法第１４条）。
- 具体的には、(1)顧客がパソコンの操作を行う際に、申込みとなることを容易に認識できるように表示していなかったり、(2)申込みを受ける場合において、顧客が申込みの内容を容易に確認及び訂正できるようにしていない場合には、「顧客の意に反して契約の申込み行わせようとうする行為」として、行政処分の対象となる（特定商取引法施行規則第１６条）。
- 経済産業省が「インターネット通販における『意に反して契約の申込みをさせようとする行為』に係るガイドライン」<http://www.meti.go.jp/kohosys/press/0002003/index.html>を公表。



インターネット通販における
「意に反して契約の申込みをさせようとする行為」
に係るガイドライン

特定商取引法第１４条では、販売業者又は役務提供事業者が、「顧客の意に反して売買契約若しくは役務提供契約の申込みをさせようとする行為として経済産業省令で定めるものをした場合」において、取引の公正及び購入者等の利益が害されるおそれがあると認めるときは、主務大臣が指示を行うことができる旨を定めている。

この規定に基づき、省令第１６条では、「顧客の意に反して契約の申込みをさせようとする行為」の具体的内容を定めている。このうち、第一号及び第二号が、インターネット通販に対応した規定である（第一号又は第二号のいずれかに該当する場合に、指示の対象となる）。なお、第二号は、葉書等で申し込む場合に対応した規定である。

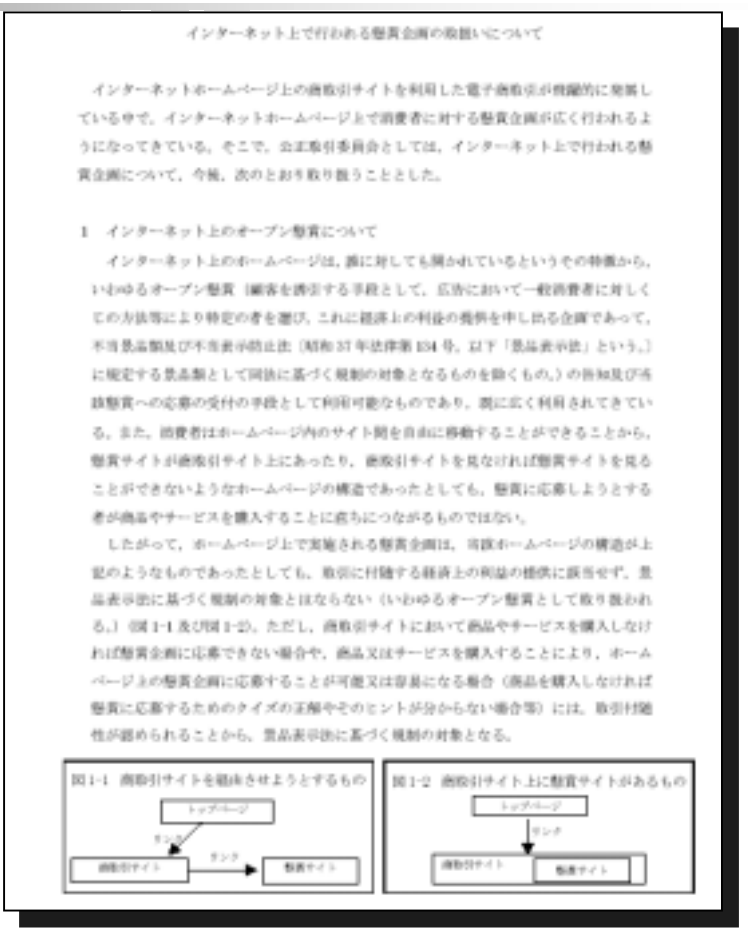
【省令第１６条の規定】
一　販売業者又は役務提供事業者が、電子契約の申込みを受ける場合において、電子契約に係る電子計算機の操作（当該電子契約の申込みとなるものに限る。次号において同じ。）が当該電子契約の申込みとなることを、顧客が当該操作を行う際に容易に認識できるように表示していないこと。
二　販売業者又は役務提供事業者が、電子契約の申込みを受ける場合において、申込みの内容を、顧客が電子契約に係る電子計算機の操作を行う際に容易に確認及び訂正できるようにしていないこと。

１．第一号（申込みとなることの表示）について
（１）第一号は、インターネット通販において、あるボタンをクリックすれば、それが有料の申込みとなることを、消費者が容易に認識できるように表示していないことを規定するもの。

（２）以下のような場合は、一般に、第一号で定める行為に該当しないと考えられる。
①申込みの最終段階において、「注文内容の確認」といった表題の画面（いわゆる最終確認画面）が必ず表示され、その画面上で「この内容で注文する」といった表示のあるボタンをクリックしてはじめて申込みになる場合。（参考：【画面例１】）

公正取引委員会「インターネット上で行われる懸賞企画の取扱いについて」への対応

公正取引委員会は，インターネット上の商取引サイトを利用した電子商取引が飛躍的に発展している中で，インターネットホームページ上で消費者に対する懸賞企画が広く行われるようになってきている状況にかんがみ，インターネットホームページ上で行われる景品提供企画について，取引に付随して提供される景品類を規制している景品表示法の規制の対象となるかどうかを明確化し，各都道府県及び関係団体へ周知を図ることとした。



インターネット上で行われる懸賞企画の取扱いについて

インターネットホームページ上の商取引サイトを利用した電子商取引が飛躍的に発展しているなかで，インターネットホームページ上で消費者に対する懸賞企画が広く行われるようになってきている。そこで，公正取引委員会としては，インターネット上で行われる懸賞企画について，今般，次のとおり取り扱うこととした。

1　インターネット上のオープン懸賞について

インターネット上のホームページは，誰に対しても開かれているというその特質から，いわゆるオープン懸賞（顧客を誘引する手段として，広告において一般消費者に対しくじの方法等により特定の者を選び，これに経済上の利益の提供を申し出る企画であって，不当景品類及び不当表示防止法（昭和37年法律第134号，以下「景品表示法」という。）に規定する景品類として同法に基づく規制の対象となるものを除くもの。）の告知及び当該懸賞への応募の受付の手段として利用可能なものであり，既に広く利用されてきている。また，消費者はホームページ内のサイト間を自由に移動することができることから，懸賞サイトが商取引サイト上にあったり，商取引サイトを見なければ懸賞サイトを見ることができないようなホームページの構造であったとしても，懸賞に応募しようとする者が商品やサービスを購入することに直ちにつながるものではない。

したがって，ホームページ上で実施される懸賞企画は，当該ホームページの構造が上記のようなものであったとしても，取引に付随する経済上の利益の提供に該当せず，景品表示法に基づく規制の対象とはならない（いわゆるオープン懸賞として取り扱われる。）（図1-1及び図1-2）。ただし，商取引サイトにおいて商品やサービスを購入しなければ懸賞企画に応募できない場合や，商品又はサービスを購入することにより，ホームページ上の懸賞企画に応募することが可能又は容易になる場合（商品を購入しなければ懸賞に応募するためのクイズの正解やそのヒントが分からない場合等）には，取引付随性が認められることから，景品表示法に基づく規制の対象となる。

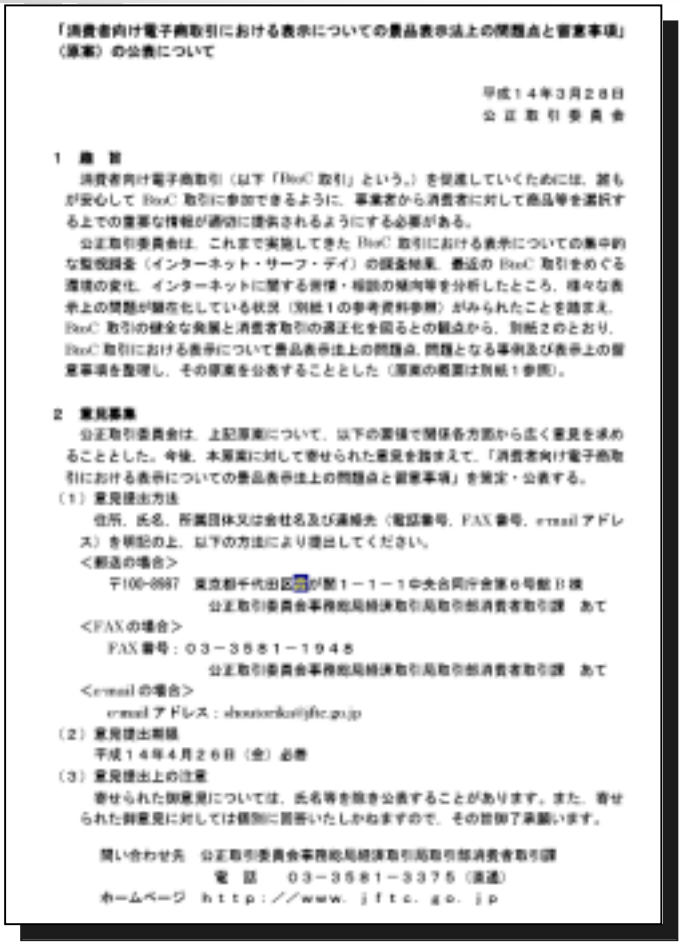
図1-1　商取引サイトを誘引させようとするもの

図1-2　商取引サイト上に懸賞サイトがあるもの

<http://www.jftc.go.jp/pressrelease/02.march/020328.pdf>

公正取引委員会「消費者向け電子商取引における表示についての景品表示法上の問題点と留意事項」への対応

「消費者向け電子商取引（以下「BtoC 取引」という。）を促進していくためには，誰もが安心して BtoC 取引に参加できるように，事業者から消費者に対して商品等を選択する上での重要な情報が適切に提供されるようにする必要がある。公正取引委員会は，これまで実施してきたBtoC 取引における表示についての集中的な監視調査（インターネット・サーフ・デイ）の調査結果，最近の BtoC 取引をめぐる環境の変化，インターネットに関する苦情・相談の傾向等を分析したところ，様々な表示上の問題が顕在化している状況（別紙1の参考資料参照）がみられたことを踏まえ，BtoC 取引の健全な発展と消費者取引の適正化を図るとの観点から，別紙2のとおり，BtoC 取引における表示について景品表示法上の問題点，問題となる事例及び表示上の留意事項を整理し，その原案を公表することとした。」
<http://www.jftc.go.jp/pressrelease/02.march/020328.pdf>



「消費者向け電子商取引における表示についての景品表示法上の問題点と留意事項」（原案）の公表について

平成１４年３月２８日
公 正 取 引 委 員 会

１ 趣 旨

消費者向け電子商取引（以下「BtoC 取引」という。）を促進していくためには，誰もが安心して BtoC 取引に参加できるように，事業者から消費者に対して商品等を選択する上での重要な情報が適切に提供されるようにする必要がある。

公正取引委員会は，これまで実施してきた BtoC 取引における表示についての集中的な監視調査（インターネット・サーフ・デイ）の調査結果，最近の BtoC 取引をめぐる環境の変化，インターネットに関する苦情・相談の傾向等を分析したところ，様々な表示上の問題が顕在化している状況（別紙１の参考資料参照）がみられたことを踏まえ，BtoC 取引の健全な発展と消費者取引の適正化を図るとの観点から，別紙のとおり，BtoC 取引における表示について景品表示法上の問題点，問題となる事例及び表示上の留意事項を整理し，その原案を公表することとした（原案の概要は別紙１参照）。

２ 意見募集

公正取引委員会は，上記原案について，以下の要領で関係各方面から広く意見を求めることとした。今後，本原案に対して寄せられた意見を踏まえて，「消費者向け電子商取引における表示についての景品表示法上の問題点と留意事項」を策定・公表する。

（１）意見提出方法

住所，氏名，所属団体又は会社名及び連絡先（電話番号，FAX 番号，e-mail アドレス）を明記の上，以下の方法により提出してください。

＜郵送の場合＞

〒100-8987 東京都千代田区霞が関１－１－１中央合同庁舎第６号館Ｂ棟
公正取引委員会事務総局経済取引局取引部消費者取引課 あて

＜FAX の場合＞

FAX 番号：０３－３５８１－１９４８
公正取引委員会事務総局経済取引局取引部消費者取引課 あて

＜e-mail の場合＞

e-mail アドレス：shouriseki@jftc.go.jp

（２）意見提出期限

平成１４年４月２６日（金）必着

（３）意見提出上の注意

寄せられた御意見については，氏名等を除き公表することがあります。また，寄せられた御意見に対しては個別に回答いたしかねますので，その旨御了承願います。

問い合わせ先 公正取引委員会事務総局経済取引局取引部消費者取引課
電 話 ０３－３５８１－３３７５（直通）
ホームページ http://www.jftc.go.jp

ご質問

- okamura@mail.law.co.jp
  まで
- http://www.law.co.jp/